**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**

**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**

**ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ**

**«ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ»**

# Cyber Intelligence: Μια νέα προσέγγιση στο χώρο της Κυβερνοασφάλειας

**Γαλάνης Αθανάσιος-Χαρίσης**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**Υπεύθυνος**

**Σταμούλης Γεώργιος**

**Λαμία, 2016**

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**

**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**

**ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ**
**ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ**

**ΚΑΤΕΥΘΥΝΣΗ:**

**«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»**

# Cyber Intelligence: Μια νέα προσέγγιση στο χώρο της Κυβερνοασφάλειας

**Γαλάνης Αθανάσιος-Χαρίσης**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**Επιβλέπων**

**Σταμούλης Γεώργιος**

**Λαμία, 2016**

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία: 20/10/2016

Υπογραφή

# Cyber Intelligence: Μια νέα προσέγγιση στο χώρο της Κυβερνοασφάλειας

**Γαλάνης Αθανάσιος-Χαρίσης**

**Τριμελής Επιτροπή:**

Σταμούλης Γεώργιος (επιβλέπων)

Αντωνής Κωνσταντίνος

Λουκόπουλος Αθανάσιος

**Επιστημονικός Σύμβουλος:**

Κίκιρας Παναγιώτης

## *Ευχαριστίες και αφιερώσεις…*

Πάνω από όλα είναι ο Θεός, ο οποίος με Οδηγεί σωστά στα Βήματά του και χωρίς τη βοήθειά Του δεν θα μπορούσα να πετύχω τίποτα στη ζωή μου…

Να ευχαριστήσω τους ανθρώπους που ήταν δίπλα μου και με το δικό τους τρόπο βοήθησαν και αυτοί κατά τη διάρκεια της συγγραφής της εργασίας αυτής…

Θα ήθελα να ευχαριστήσω θερμά τους Καθηγητές μου, κ.Σταμούλη Γεώργιο και κ.Κίκιρα Παναγιώτη, των οποίων οι συμβουλές και η καθοδήγηση για την συγγραφή της παρούσας Διπλωματικής ήταν κάτι παραπάνω από πολύτιμες…

Αφιερώνω εξαιρετικά την εργασία αυτή στη σύζυγό μου Κατερίνα και στην μικρούλα μου Ραφαέλα, οι οποίες αποτελούν το πιο γλυκό κομμάτι της ζωής μου…

# ΠΕΡΙΕΧΟΜΕΝΑ

## ΚΕΦΑΛΑΙΟ 3$^{Ο}$: CASE STUDY:ΥΛΟΠΟΙΗΣΗ ΜΕΘΟΔΟΛΟΓΙΩΝ CI ΣΤΟΝ ΤΡΑΠΕΖΙΚΟ ΤΟΜΕΑ



## ΚΕΦΑΛΑΙΟ 4$^{Ο}$: ΕΠΙΛΟΓΟΣ



INDEX εικόνων

## ΠΕΡΙΛΗΨΗ:

Η παρούσα Διπλωματική Εργασία αφορά την έννοια του Cyber Intelligence, η οποία έννοια είναι μία ερευνητική περιοχή του τομέα της Κυβερνοασφάλειας ή Cyber Security. Στην εργασία αυτή αναλύονται οι έννοιες του Cyber Security και Cyber Intelligence και γίνεται ο διαχωρισμός τους, ενώ αναφέρονται τεχνικές και μεθοδολογίες συλλογής, επεξεργασίας και διαμοιρασμού των δεδομένων, μέσω της εφαρμογής του Cyber Intelligence. Επίσης, γίνεται αναφορά στα είδη των επιτιθέμενων, στις κατηγορίες των ευαίσθητων στοιχείων τα οποία κινδυνεύουν να υποκλαπούν, στις απαιτήσεις της εφαρμογής του Cyber Intelligence και στα οφέλη που προσφέρει αυτό. Επιπρόσθετα, γίνεται μία εκτενής αναφορά στα διάφορα εργαλεία που χρησιμοποιούνται αλλά παραθέτουμε και μία μελέτη περίπτωσης εφαρμογής διαδικασιών Cyber Intelligence στον τραπεζικό τομέα.

## ABSTRACT:

This thesis concerns a survey conducted for the purposes of Cyber Intelligence, which concept is an evolution of the cyber or Cyber Security sector. This paper analyzes the concepts of Cyber Security and Cyber Intelligence and becomes their separation, while mentioned techniques and methodologies of collection, processing and sharing of data through the application of Cyber Intelligence. Reference is also made to the types of attackers, the categories of sensitive data which risk being intercepted, the requirements of the application of Cyber Intelligence and the benefits it offers. Furthermore, there is an extensive report on the various tools used, and also we have listed a case study for application of Cyber Intelligence processes in the banking sector.

# ΚΕΦΑΛΑΙΟ 1$^{Ο}$: ΑΝΑΣΚΟΠΗΣΗ ΤΗΣ ΕΡΓΑΣΙΑΣ

## 1.1.Γενικά στοιχεία της εργασίας

Η Πληροφορική, ως επιστήμη, εμπεριέχει πολλούς κλάδους και αποκτά ιδιαίτερο ενδιαφέρον η μελέτη τους. Ένας από τους ταχέως αναπτυσσόμενους κλάδους της, είναι και ο κλάδος της Ασφάλειας των Υπολογιστών ή αλλιώς Cyber Security, σε αγγλική ορολογία. Η Ασφάλεια των Υπολογιστών έχει αναπτυχθεί αρκετά θα λέγαμε έχοντας στο οπλοστάσιο της αρκετές μεθόδους και τεχνικές οι οποίες αποσκοπούν ακριβώς σε αυτό, δηλ. στην προστασία των υπολογιστών, υπολογιστικών συστημάτων και δικτύων από τις λεγόμενες Κυβερνοεπιθέσεις ή επιθέσεις ή τα διάφορα ψηφιακά συμβάντα, τα οποία στοχεύουν στο να προκαλέσουν ζημιά στα συστήματα αυτά όπως δυσλειτουργία και υποκλοπή ευαίσθητων δεδομένων. Δυστυχώς, έχει αποδειχθεί ότι οι μέθοδοι και οι τεχνικές που χρησιμοποιεί το Cyber Security σε ορισμένες περιπτώσεις κρίνονται ανεπαρκής και δεν μπορούν να καλύψουν σε έναν ικανοποιητικό βαθμό την Ασφάλεια των υπολογιστών και των συστημάτων τους. Όμως, υπάρχει και μία μετεξέλιξη του Cyber Security, η οποία μας δίνει πλέον την έννοια του Cyber Intelligence. Το Cyber Intelligence αποτελεί ουσιαστικά μία απάντηση και μία αρκετά ικανοποιητική λύση, στα «κενά» της Κυβερνοάμυνας των υπολογιστικών συστημάτων που εμφανίζονται λόγω της ανεπάρκειας του Cyber Security, συμπληρώνοντας το.

Τα ερωτήματα για τα οποία έγινε προσπάθεια να απαντηθούν είναι γιατί θα πρέπει το Cyber Intelligence να χρησιμοποιείται στα υπολογιστικά συστήματα, συμπληρώνοντας το Cyber Security, τι μπορεί να κερδηθεί από την χρήση του αλλά και με ποιόν τρόπο μπορεί να εφαρμοστεί, μέσω μεθοδολογιών και τεχνικών.

Η ανεύρεση των απαραίτητων πληροφοριών για την συγγραφή της παρούσης Διπλωματικής έγινε με την αναζήτηση πηγών από το Διαδίκτυο, οι οποίες αφορούν είτε κάποια επιστημονικά άρθρα και δημοσιεύσεις για το εν λόγω θέμα, ή κάποιες ιστοσελίδες με συναφές περιεχόμενο.

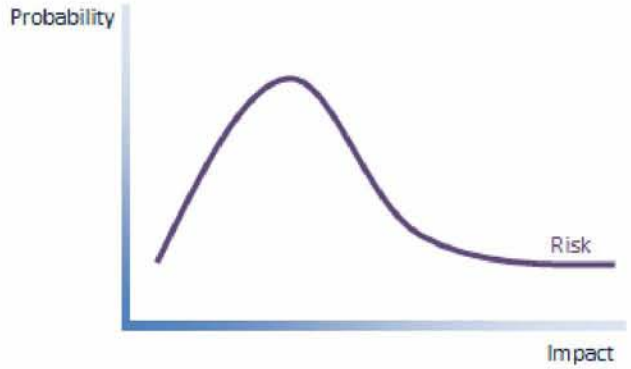
# ΚΕΦΑΛΑΙΟ 2$^{Ο}$: CYBER SECURITY ΚΑΙ CYBER INTELLIGENCE

## 2.1. Η έννοια του Cyber Security

Πρώτα από όλα, ας μιλήσουμε λίγο για το τι είναι η Κυβερνοασφάλεια ή Cyber Security, πριν προχωρήσουμε στις έννοιες του Cyber Intelligence. Η Κυβερνοασφάλεια ή Cyber Security (πολλοί την αποκαλούν και Information Technology Security) είναι ο κλάδος της Πληροφορικής ο οποίος έχει ως αντικείμενο την προστασία των υπολογιστών και των δικτύων τους, των προγραμμάτων και επίσης των διάφορων προσωπικών και ευαίσθητων δεδομένων, από κακόβουλους χρήστες.

Η εφαρμογή του Cyber Security πλέον είναι απαραίτητη στην σημερινή εποχή. Ο λόγος είναι ο εξής: Υπάρχουν πολλοί φορείς και οργανισμοί ανά τον κόσμο, όπως εταιρείες, στρατιωτικά τμήματα, κυβερνητικοί οργανισμοί και χρηματοπιστωτικά ιδρύματα, και σε όλους αυτούς τους οργανισμούς παράγεται σε καθημερινή βάση, ένας τεράστιος όγκος πληροφοριών. Πολλές από τις πληροφορίες αυτές είναι απόρρητες και δεν θα πρέπει να έχουν πρόσβαση εξωτερικοί ή κακόβουλοι χρήστες. Άρα λοιπόν, δημιουργείται η ανάγκη για την προστασία των απόρρητων πληροφοριών αυτών, κάτι που αντιμετωπίζεται, έως ένα βαθμό, από την εφαρμογή του Cyber Security.

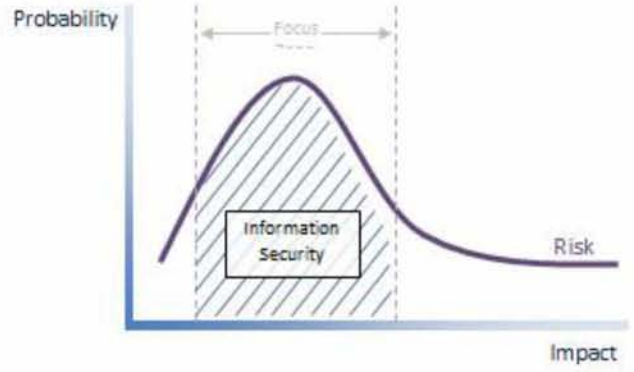
Αφού μιλάμε για την έννοια της Κυβερνοασφάλειας, θεωρώ ότι θα ήταν καλό να αναφερθούμε και στην έννοια, ας μου επιτραπεί ο ορισμός, του Κυβερνο-ρίσκου δηλ του Cyberrisk. Το Cyberrisk είναι ουσιαστικά ο κίνδυνος στον οποίο εκτίθεται ένας οργανισμός και ο κίνδυνος αυτός σχετίζεται φυσικά με Κυβερνοεπιθέσεις που γίνονται έχοντας στόχο τον ίδιο τον οργανισμό. Το Cyberrisk όμως δεν είναι κάτι συγκεκριμένο. Είναι μία ομάδα κινδύνων, όπου ο κάθε κίνδυνος διαφέρει από τους υπόλοιπους πχ στον τρόπο που θα γίνει μία επίθεση, στο τι στοχεύει αυτή η επίθεση, στα κίνητρα του/των επιτιθέμενου/επιτιθέμενων και άλλα πολλά. Παρόλα αυτά, θα μπορούσαμε να κατηγοριοποιήσουμε τους κινδύνους αυτούς σε 2 μεγάλες ομάδες: Στην ομάδα κινδύνων όπου οι επιθέσεις μπορεί να έχουν μεγάλες και αρνητικές επιπτώσεις σε έναν οργανισμό και στην ομάδα κινδύνων όπου η πιθανότητα του να συμβούν οι επιθέσεις είναι απειροελάχιστη. Βλέποντας την εικόνα 2.1, αντιλαμβανόμαστε την σχέση μεταξύ πιθανότητας ενός κινδύνου, δηλ πιθανότητα ενός ψηφιακού συμβάντος (επίθεσης) και την επίπτωση που έχει το συμβάν αυτό, σε έναν οργανισμό.




(εικόνα 2.1: Σχέση πιθανότητας συμβάντος και επίπτωσης του σε οργανισμό)

Ουσιαστικά βλέπουμε ότι, καθώς προχωράμε προς τα δεξιά, αυξάνεται η επίπτωση των επιθέσεων σε έναν οργανισμό, με ταυτόχρονη αύξηση της πιθανότητας να συμβούν. Μετά την κορυφή της καμπύλης, ενώ η επίπτωση συνεχίζει και αυξάνεται, η πιθανότητα του να συμβούν οι επιθέσεις εκείνων των κατηγοριών, αρχίζει και μειώνεται και τελικά, παρατηρώντας την «ουρά» του γραφήματος αυτού, φαίνεται ότι επιθέσεις που μπορούν να προκαλέσουν μεγάλες αρνητικές επιπτώσεις σε έναν οργανισμό, έχουν μικρή πιθανότητα υλοποίησης.

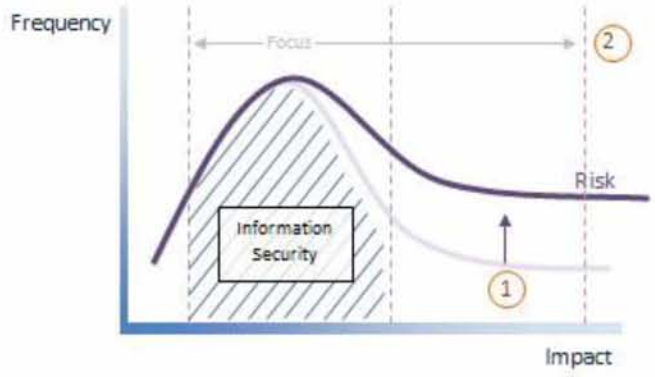
Ας δούμε τώρα την εικόνα 2.2. Παρατηρούμε ότι η εφαρμογή του Information Security εστιάζει στην περιοχή της καμπύλης, όπου οι πιθανότητες του να έχουμε κάποιο ψηφιακό συμβάν, είναι αρκετά αυξημένες.




(εικόνα 2.2: Η «περιοχή» του Information Security)

Το πλάτος της «περιοχής» αυτής εξαρτάται από ορισμένους παράγοντες, όπως διάφορα είδη επιθέσεων με «όπλα» κάποια κλασσικά malwares (ιοί, trojans, spyware, phishind, Ddos κλπ) υπό την έννοια του ότι επενδύεται χρόνος και χρήμα σε διαδικασίες και ενέργειες για να αντιμετωπιστούν οι επιθέσεις αυτές.

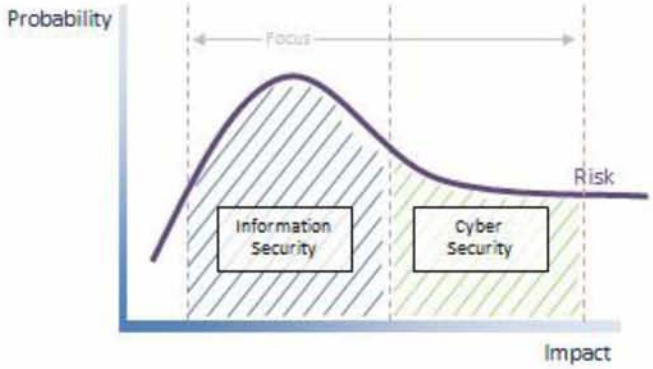
Όμως, συμβαίνει το εξής περίεργο: Ομάδες επιθέσεων οι οποίες είχανε αρχικά μικρή πιθανότητα να συμβούν, τώρα πλέον παρατηρείται μία αύξηση στην **συχνότητα** των επιθέσεων αυτών, σύμφωνα με την εικόνα 2.3)




(εικόνα 2.3: Η αύξηση της πιθανότητας ομάδων επίθεσης)

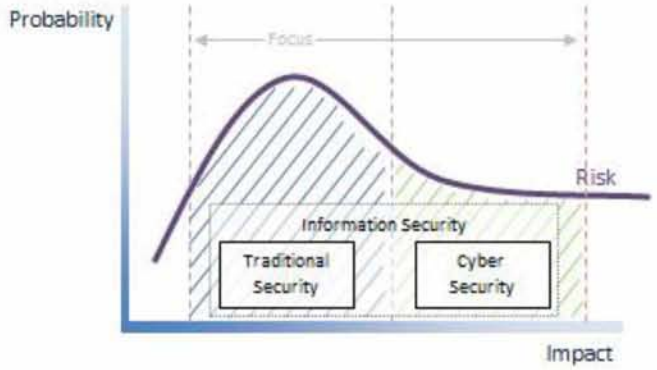
Εκτός της αύξησης της συχνότητας των συγκεκριμένων επιθέσεων, πλέον οι διαδικασίες και ενέργειες του οργανισμού εστιάζουν σε μία μεγαλύτερη περιοχή, για να προλάβουν την εξέλιξη αυτή. Θα λέγαμε ότι η αύξηση της συχνότητας των επιθέσεων σχετίζεται με τη βελτίωση των τρόπων επίθεσης, με την αυξημένη βούληση των επιτιθέμενων για επίθεση η οποία συνδέεται με κάποια κίνητρα αλλά και με την αυξημένη «επιφάνεια» επίθεσης του οργανισμού η οποία έχει συνάφεια με την χρήση περισσοτέρων συστημάτων, δικτύων, προγραμμάτων και εφαρμογών από τον τελευταίο.

Παρατηρώντας την εικόνα 2.4, το Cyberrrisk αφορά την νέα «περιοχή» επιθέσεων, και στην οποία εφαρμόζονται διαδικασίες και τεχνικές του Cyber Security.




(εικόνα 2.4: Οι «περιοχές» Information Security και Cyber Security)

Στην εικόνα 2.4 φαίνεται ότι τα Information Security και Cyber Security αναφέρονται σε διαφορετικές ομάδες επιθέσεων, αλλά το πιο σωστό είναι αυτό που βλέπουμε στην εικόνα 2.5, όπου και το Traditional Security και το Cyber Security βρίσκονται κάτω την ίδια ομπρέλα του Information Security.




(εικόνα 2.5:Η «ομπρέλα» του Information Security)

Άρα τελικά, διαπιστώνουμε ότι το Cyber Security έχει ως στόχο να προστατεύει έναν οργανισμό έναντι επιθέσεων οι οποίες ενώ αρχικά ανήκαν στις ομάδες χαμηλού κινδύνου, τώρα θεωρούνται πλέον επικίνδυνες και χρήζουν αντιμετώπισης. [1]

## 2.2. Κλασσικοί τρόποι άμυνας (Cyber Security)

Θα πρέπει να αναφέρουμε τον κλασσικό τρόπο αντιμετώπισης ψηφιακών συμβάντων, ο οποίος δεν είναι άλλος εκτός από την στρατηγική της ανίχνευσης και της απόκρισης (monitor and response strategy). Η τυπική διαδικασία έχει ως εξής:

- Συλλογή ψηφιακών συμβάντων, υπογραφών και δεικτών απειλών (threat indicators).
- Με βάση τις παραπάνω πληροφορίες, δημιουργούνται συστήματα και λογισμικά σχετικά με την ασφάλεια, όπως firewalls, antimalware και endpoint protection software, συστήματα ανίχνευσης και πρόληψης διείσδυσης (IDS-Intrusion Detection Systems, IPS-Intrusion Prevention Systems).
- Οι πληροφορίες που συλλέχθηκαν στο πρώτο στάδιο, χρησιμοποιούνται επίσης και για την δημιουργία κατάλληλων alerts, τα οποία ανιχνεύονται από τα Κέντρα Ασφάλειας (SOC-Security Operations Centers) σε συνδυασμό με τα SIEM εργαλεία (Security Information and Event Management).
- Ακολουθεί η ανάλυση των alerts από τα άτομα της SOC υπηρεσίας, τα οποία προωθούν τα σημαντικότερα alerts στην ομάδα απόκρισης (IRT-Incident Response Team) για περαιτέρω ανάλυση και εκτίμηση.
- Η ομάδα IRT ουσιαστικά εξετάζει τα alerts αυτά, ελέγχει τα διάφορα log αρχεία και προσπαθεί να ανασυνθέσει τα ζωτικά στοιχεία μίας επίθεσης.
- Από την ανασύνθεση αυτή, εμποδίζεται μία τρέχουσα επίθεση, ενώ στη συνέχεια γίνεται επαναφορά και «καθάρισμα» του «μολυσμένου» συστήματος με ταυτόχρονη απόκτηση εμπειρίας, η οποία προλαμβάνει και προστατεύει τον οργανισμό από άλλες, μελλοντικές επιθέσεις ιδίας φύσεως.
- Περιοδικά συντάσσονται αναφορές, βάσει των οποίων θα μπορεί η Διοίκηση να πεισθεί να χορηγήσει μεγαλύτερα χρηματικά ποσά, για την ασφάλεια των πληροφοριών του οργανισμού.

## 2.3. Η έννοια του Cyber Intelligence

Πριν μιλήσουμε για το τι είναι το Cyber Intelligence, ας αναφερθούμε πρώτα σε κάποια γενικά στοιχεία. Η γενικότερη έννοια του Intelligence θα λέγαμε ότι έχει σχέση με την έννοια της αντικατασκοπείας και γενικότερα με την άντληση χρήσιμων πληροφοριών, οι οποίες μπορούν να υποστούν κάποιου είδους επεξεργασία και από αυτή να προκύψουν δεδομένα τα οποία θα είναι άμεσα εκμεταλλεύσιμα. Ένα βασικό συστατικό του Intelligence είναι τα TTP's, δηλ τα Tactics, Techniques and Procedures (Τακτικές, Τεχνικές και Διαδικασίες), έννοιες οι οποίες προϋπήρχαν πολύ νωρίτερα από την εμφάνιση του Διαδικτύου. Κάποιοι υποστηρίζουν ότι το

[1] **University of Maryland, 2016, About Cyber Security, [Online].Available:http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfmhttp://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296**

Intelligence έχει περισσότερο την μορφή της επίθεσης, αφού σχετίζεται με την άντληση πληροφοριών από τους «αντιπάλους», ενώ κάποιοι άλλοι θεωρούν το Intelligence ως μία μορφή άμυνας, αφού τελικά ο στόχος του είναι ακριβώς αυτός, δηλ. η άμυνα του εκάστοτε οργανισμού. Μπορούμε να αναφέρουμε το εξής παράδειγμα: Σε στρατιωτικό πεδίο εφαρμογών, θα ήταν ιδιαίτερα χρήσιμο για τους αξιωματικούς του στρατού, να γνωρίζουν εκ των προτέρων για το εάν οι αντίπαλοι τους, πρόκειται είτε να επιτεθούν (άρα να μπορούν να κατευθύνουν το στράτευμα το καλύτερο δυνατόν σε θέματα άμυνας), είτε να αμυνθούν (οπότε σε αυτήν την περίπτωση να διοικήσουν πάλι με τον καλύτερο δυνατό τρόπο το στράτευμα, προετοιμάζοντας το για επίθεση). Σε αυτό το σημείο λοιπόν, μπορούμε να δώσουμε τον ορισμό του Intelligence, ο οποίος είναι το 1° σημείο, ενώ και τα 3 σημεία είναι τα στοιχεία που αποκομίζουμε από την εφαρμογή του Cyber Intelligence:

1. Το Intelligence είναι το προϊόν το οποίο παράγεται από τις διαδικασίες της συλλογής, της επεξεργασίας, της αξιολόγησης, της ένταξης, της ανάλυσης και της μετάφρασης των πληροφοριών που έχουν αντληθεί και οι οποίες πληροφορίες σχετίζονται με ξένα κράτη, με εχθρικά ή δυνητικώς εχθρικά στοιχεία ή δυνάμεις.
2. Οι διαδικασίες οι οποίες οδηγούν στην παραγωγή του άνωθι προϊόντος.
3. Οι φορείς οι οποίοι υλοποιούν τις άνωθι διαδικασίες.

Εάν θέλαμε να δώσουμε έναν πιο απλό ορισμό θα λέγαμε ότι το Intelligence είναι ένα προϊόν αλλά συνάμα και μία γενική διαδικασία, οι οποίες σχετίζονται με την συλλογή, επεξεργασία και ανάλυση πληροφοριών έχοντας ως σκοπό, την επίτευξη ενός συγκεκριμένου στόχου.

Η έννοια του Intelligence στηρίζεται σε 3 κύριους πυλώνες: Στο HUMINT (Human Intelligence), στο OSINT (Open Source Intelligence) και στο SIGINT (Signals Intelligence). Υπάρχει και ο MASINT (Measurement And Signature Intelligence). Τους πυλώνες αυτούς τους αναλύουμε παρακάτω. [2]

## 2.4. HUMINT (Human Intelligence)

Σύμφωνα με τον τίτλο, συλλέγονται πληροφορίες από ειδικούς αναλυτές, οι οποίοι μετατρέπουν αυτές τις πληροφορίες σε χρήσιμα δεδομένα. Με τη βοήθεια των χρήσιμων δεδομένων αυτών, μπορεί να οργανωθεί η άμυνα του εκάστοτε οργανισμού. Καταρχήν, λέγοντας Human Intelligence εννοούμε τις πληροφορίες που μπορεί να αποκομίσει κάποιος έχοντας ως πηγή πληροφόρησης τους ίδιους τους ανθρώπους. Η μετεξέλιξη του HUMINT είναι η Cyber-Humint, η οποία επινοήθηκε το 2010 από τον Ed Alcantara. Επίσης, ο Amit Steinhart ισχυριζόταν ότι ο συνδυασμός ειδικών στο HUMINT μαζί με ειδικούς υπολογιστών σε τομείς του social engineering, ήταν ένα από τα πλεονεκτήματα του Cyber-Humint. Σκοπός του τελευταίου είναι να προστατεύει μία επιχείρηση έναντι κάποιας επίθεσης τύπου APT-Advanced Persistent Threat, διότι σε τέτοιες περιπτώσεις επιθέσεων, οι ειδικοί της Κυβερνοασφάλειας των επιχειρήσεων, θα αντιληφθούν μία επίθεση πολύ αργά-όταν ήδη οι επιτιθέμενοι θα έχουν εισχωρήσει στα IT συστήματα των επιχειρήσεων αυτών. Σε αυτήν την περίπτωση, οι επιτιθέμενοι προσπαθούν να αποσπάσουν ευαίσθητες πληροφορίες από τους υπαλλήλους μίας επιχείρησης οι οποίοι υπάλληλοι αποτελούν τον αδύναμο κρίκο της ασφάλειας της επιχείρησης αυτής. Οι ειδικοί που ασχολούνται με την εφαρμογή του Cyber-Humint, παρακολουθούν τους επιτιθέμενους αυτούς

[2] **Robert M.Lee, An Introduction To Cyber Intelligence, (2014, Jan 16), [Online].**
**Available:http://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/**

με ειδικά λογισμικά έχοντας ως στόχο το να προβλέψουν επιθέσεις πριν αυτές ακόμα συμβούν και αναλόγως να εφαρμόσουν αντίμετρα άμυνας. [3]

## 2.5.OSINT (Open Source Intelligence)

Η έννοια του OSINT είναι συνυφασμένη με την αναζήτηση πληροφοριών στο Διαδίκτυο από πηγές οι οποίες είναι διαθέσιμες στο ευρύ κοινό. Η ευρύτερη έννοια του OSINT είναι η αναζήτηση πληροφοριών σε ένα γενικό φάσμα (εφημερίδες, ραδιόφωνο, τηλεόραση, περιοδικά, δημογραφίες, δορυφορικές λήψεις, ακαδημαϊκές δημοσιεύσεις, videos και άλλα πολλά. Οι ειδικοί του cyber security εφαρμόζουν τεχνικές OSINT κυρίως μέσω του Διαδικτύου και προσπαθούν να ανακαλύψουν ή καλύτερα να αντλήσουν πληροφορίες από έγκυρες και σχετικές με το εν λόγω θέμα προς διερεύνηση, πηγές, μέσα από έναν τεράστιο φάσμα διαθέσιμων πηγών. Ο τελικός σκοπός τους βέβαια είναι να βρουν τις κατάλληλες πληροφορίες οι οποίες θα τους καθοδηγήσουν στο να προετοιμάσουν την άμυνα της επιχείρησης για επικείμενες επιθέσεις τρίτων.

## 2.6.SIGINT (Signals Intelligence)

Κατά αντίστοιχο τρόπο, οι μέθοδοι SIGINT αποσκοπούν στην συλλογή πληροφοριών υποκλέπτοντας σήματα-πληροφορίες στο Διαδίκτυο τα οποία χρήζουν συνήθως αποκρυπτογράφησης.

---

[3] **Wikipedia, (2016, February 29), Cyberhumint, [Online]. Available: https://en.wikipedia.org/wiki/Cyber-HUMINT**

**InfoSec Institute, (2016), [Online]. Available: http://resources.infosecinstitute.com/osint-open-source-intelligence/**

**Wikipedia, (2016, September 26), [Online]. Available: https://en.wikipedia.org/wiki/Signals_intelligence**

## 2.7.MASINT (Measurement and Signature Intelligence)

Σε αυτήν την περίπτωση έχουμε να κάνουμε με ανίχνευση και αναγνώριση ή περιγραφή των ψηφιακών υπογραφών κάποιων «στόχων», η οποία αναγνώριση αποτελεί ένα εργαλείο επίθεσης κακόβουλων χρηστών του Διαδικτύου. [4]

## 2.8.Τα βήματα του Intelligence

Το Intelligence έχει κάποια συγκεκριμένα βήματα υλοποίησης. Αυτά τα βήματα είναι τα εξής:

1. **Μία κατεύθυνση και ένας σχεδιασμός:** Εδώ, θα πρέπει να καθοριστεί ένας στόχος και κάποιες απαιτήσεις, βάσει των οποίων θα παραχθούν δεδομένα Intelligence (από τις πληροφορίες που έχουν συλλεχθεί). Για παράδειγμα, έχοντας αναλύσει ένα malware, μπορούμε να δούμε από ποιους servers (τύπου command and control) προέρχεται, να το μπλοκάρουμε για να μην διεισδύσει στα υπολογιστικά μας συστήματα αλλά και να ανιχνεύσουμε τον τύπο των υπολογιστικών συστημάτων που χρησιμοποιεί ο επιτιθέμενος, με σκοπό να είμαστε προετοιμασμένοι για τυχόν μελλοντικές επιθέσεις. Φυσικά το βήμα αυτό ανήκει σε μία δυναμική κατάσταση, δηλ αν εντοπίσουμε για παράδειγμα μία νέα πληροφορία την οποία δεν είχαμε προηγουμένως διαθέσιμη, ορίζουμε ένα νέο στόχο.
2. **Η συλλογή των πληροφοριών:** Υπάρχουν ορισμένες πηγές από τις οποίες μπορούμε να αντλήσουμε πληροφορίες όπως από το Διαδίκτυο, από log αρχεία των FireWalls και των IDS (Intrusion Detection Systems), από τα διάφορα Honeypots και από πολλά άλλα. Από την αρχή του σχεδιασμού εφαρμογής του Intelligence, θα πρέπει να γνωρίζουμε τις διαθέσιμες μας πηγές, βάσει του στόχου που έχουμε θέσει.
3. **Η επεξεργασία των πληροφοριών:** Εδώ, θα πρέπει να μπορούμε να έχουμε αποθηκεύσει τις πληροφορίες που έχουμε συλλέξει και μέσω διαδικασιών parsing, να μπορούμε να τις μετατρέπουμε σε κάτι χρήσιμο, σε μορφή δεδομένων. Για παράδειγμα, η μετατροπή δυαδικής πληροφορίας σε κώδικα ASCII αποτελεί μία τέτοια διαδικασία επεξεργασίας.
4. **Παραγωγή δεδομένων:** Μέσα από μία διαδικασία «μετάφρασης» και ανάλυσης, της οποίας η ποιότητα εξαρτάται άμεσα από τον εμπλεκόμενο/εμπλεκόμενους αναλυτές, παράγεται το προϊόν Intelligence, το οποίο είναι κάτι χρήσιμο, κάτι που μπορεί να «καταναλωθεί» και έχει φυσικά σχέση με τον στόχο που έχει τεθεί.
5. **Η διάδοση των δεδομένων:** Εδώ πλέον έχουμε τα δεδομένα (δηλ το προϊόν Intelligence) τα οποία μπορούν να χρησιμοποιηθούν από τον πελάτη. Η όλη διαδικασία θεωρείται πως έχει αποτύχει εάν ο πελάτης δεν έχει πρόσβαση στα δεδομένα ή έχει μεν πρόσβαση αλλά δεν μπορεί να τα χρησιμοποιήσει (να τα «καταναλώσει»).

---

[4] **Wikipedia (2016, September 16), Measurement and Signature Intelligence, [Online]. Available: https://en.wikipedia.org/wiki/Measurement_and_signature_intelligence**

**Robert M. Lee, (2014, January 16), An introduction to Cyber Intelligence, [Online]. Available: http://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/**

## 2.9.Γενικά στοιχεία

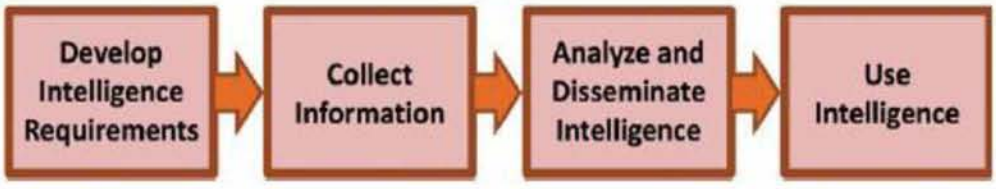
Τώρα θα πρέπει να εξετάσουμε την έννοια του threat intelligence διεξοδικά, για να μπορέσουμε να καταλάβουμε και την λειτουργία της αλλά και την σημασία της στην επιστήμη της Ασφάλειας των υπολογιστών.

Οι επαγγελματίες οι οποίοι ασχολούνται με το τομέα της Κυβερνοασφάλειας, προσπαθούν να κάνουν σωστά τη δουλειά τους και να παίξουν συμβουλευτικό και συνάμα προστατευτικό ρόλο για τις εταιρείες ή τους οργανισμούς στους οποίους παρέχουν τις υπηρεσίες τους αλλά δυστυχώς μειονεκτούν σε ένα σημείο: Δεν μπορούν να γνωρίζουν τον τρόπο με τον οποίο θα επιτεθούν οι hackers στην εν λόγω εταιρεία η στον οργανισμό. Έτσι λοιπόν, για να μπορέσει ο επαγγελματίας ο οποίος παρέχει υπηρεσίες cyber security να κατανοήσει τα ρίσκα και τα τρωτά σημεία της ασφάλειας του οργανισμού, θα πρέπει να αντιληφθεί πρωτίστως τα κίνητρα, τις προθέσεις και τις ικανότητες των επιτιθέμενων. Με αυτόν τον τρόπο λοιπόν, γεννήθηκε η ιδέα του threat intelligence. Με άλλα λόγια, πριν περίπου 8 χρόνια, ιδρύθηκε η εταιρεία iSight, της οποίας το αντικείμενο είναι ακριβώς αυτό, δηλ η παραγωγή και παροχή πληροφοριών από διαδικασίες cyber threat intelligence (CTI). Και για να μιλήσουμε λίγο πιο αναλυτικά, η εταιρεία αυτή προσπαθεί να καλύψει όλες τις πιθανές τρωτότητες ενός οργανισμού, με το να ανακαλύπτει και να ξεσκεπάζει τις μεθόδους, τις τακτικές και τις τεχνικές των επιτιθέμενων. Φυσικά, το πεδίο του cyber intelligence είναι ακόμη φρέσκο και λίγα άτομα γνωρίζουν στοιχεία για αυτό.

## 2.10. Βασικά χαρακτηριστικά του cyber intelligence

Η έννοια του cyber intelligence έχει τα εξής σημεία αναφοράς:

- Βασίζεται σε πληροφορίες οι οποίες πηγάζουν από ειδικές δραστηριότητες κατά τις οποίες διεξάγονται στρατηγικές «αντικατασκοπείας», στοχεύοντας ομάδες κυβερνο-εγκληματιών και άλλων ομάδων ή ατόμων που θεωρούνται υπεύθυνα για οργάνωση και εκτέλεση κυβερνο-επιθέσεων. Υπάρχουν ειδικά προγράμματα τα οποία χρησιμοποιούνται ευρέως από τμήματα στρατών και αστυνομιών ανά τον κόσμο, για τον σκοπό αυτό.
- Εστιάζει στα βασικά στοιχεία ενός οργανισμού τα οποία κρίνονται ζωτικής σημασίας και τα οποία είναι αυτά που θα πρέπει να προστατεύονται. Αναφορικά, τέτοια στοιχεία μπορούν να είναι ιστοσελίδες, βάσεις δεδομένων πελατών, εφαρμογές, απόρρητα/ευαίσθητα δεδομένα, δίκτυα κ.α.
- Είναι προσανατολισμένη σε μία συγκεκριμένη φιλοσοφία διαδικασιών, την οποία παραθέτουμε παρακάτω, στην εικόνα 2.6.




(εικόνα 2.6: Διαδικασία προγραμμάτων cyber intelligence)

Έχουμε λοιπόν την ανάπτυξη των απαιτήσεων, την συλλογή των πληροφοριών, την ανάλυση/διασπορά και την χρήση του intelligence. Αυτή η διαδικασία αποτελεί την ραχοκοκαλιά του cyber intelligence και αυτή θα πρέπει να ακολουθούν ευλαβικά, τηρώντας αρχεία σε κάθε βήμα, οι επαγγελματίες του χώρου της Κυβενοασφάλειας, οι οποίοι δυστυχώς και επί το πλείστον, δεν λειτουργούν με συστηματικό τρόπο και δεν λαμβάνουν υπόψιν διαθέσιμες πηγές που θα τους βοηθούσαν. Ένα άλλο λάθος τους είναι το ότι δεν προσπαθούν να «πακετάρουν» χρήσιμες πληροφορίες οι οποίες θα μπορούσαν να χρησιμοποιηθούν από διάφορους χρήστες, άτομα, ή ακόμη και από συναδέλφους τους (δηλ από επαγγελματίες Κυβερνοασφάλειας) για την εφαρμογή του cyber intelligence. Η διαδικασία που απεικονίζεται παραπάνω, θα πρέπει να γίνει κατανοητή και θα πρέπει να συντάσσονται έγγραφα σε κάθε βήμα τα οποία να αναφέρουν τις διεργασίες που θα πρέπει να ακολουθούνται.

- Προσαρμόζεται σε διαφορετικούς «καταναλωτές» δεδομένων, υπό την έννοια του ότι υπάρχει μία ασταμάτητη ροή δεδομένων η οποία «καταναλώνεται» από:

_Τους αναλυτές SOC, οι οποίοι θα αποφασίσουν αν ένα “alert” αξίζει προσοχής ή όχι.
_Η ομάδα IR μπορεί να χρειάζεται λεπτομερείς πληροφορίες για το αν το “alert” αυτό σχετίζεται και με άλλα συμβάντα στο δίκτυο.
_ Η ομάδα CISO ίσως θελήσει να κάνει εκτίμηση ρίσκου συνδέοντας το “alert” αυτό με παράνομες ανακτήσεις δεδομένων από κακόβουλους χρήστες.

## 2.11. Τα θετικά σημεία του cyber intelligence

Ουσιαστικά μιλάμε πλέον για εφαρμογή συγκεκριμένης στρατηγικής, από την οποία απορρέουν τα εξής πλεονεκτήματα:

Σε επίπεδο τακτικής:

1. Αποφεύγεται το φαινόμενο των “false alerts”, καθώς φιλτράρονται εκείνα τα οποία δεν χρήζουν προσοχής.
2. Υπάρχει προτεραιότητα στο ποιες τρωτότητες θα διορθωθούν πρώτες (patching). Φυσικά μιλάμε για το patching των πιο επικίνδυνων και προχωράμε στις όχι και τόσο επικίνδυνες.
3. Η ύπαρξη αυτοματισμού κατά του οποίου οι κρίσιμες πληροφορίες οδηγούνται στα εργαλεία SIEM και με αυτόν τον τρόπο συσχετίζονται οι επιθέσεις με τις πληροφορίες αυτές γρηγορότερα και με μεγαλύτερη ακρίβεια.
4. Με την ανάλυση των δεικτών (indicators), η ομάδα SOC θέτει προτεραιότητες για το ποια alerts χρήζουν άμεσης αντιμετώπισης άμεσα.

Σε επίπεδο λειτουργίας:

1. Η ομάδα IR τροφοδοτείται με υλικό το οποίο διευρύνει την έρευνα της και έτσι σχηματίζει μία εικόνα των προθέσεων, των μεθόδων αλλά και των στόχων των επιτιθέμενων.

2. Επίσης, η ομάδα IR επαναφέρει γρήγορα τα compromised συστήματα και παρεμποδίζει μελλοντικές επιθέσεις ιδίου τύπου.

Σε επίπεδο στρατηγικής:

1. Η Διοίκηση του οργανισμού οδηγείται από μία νέα φιλοσοφία με την οποία γίνονται αντιληπτές οι κρίσιμες/επικίνδυνες απειλές και η οποία αντίληψη μεταφράζεται σε μία σωστή διαχείριση των χρημάτων και του προσωπικού, έχοντας ως στόχο την προστασία ευαίσθητων στοιχείων και διαδικασιών του οργανισμού.
2. Θεσπίζεται δίαυλος επικοινωνίας μεταξύ της ομάδας CISO και διευθυντικών στελεχών για θέματα ρίσκου των επιχειρήσεων, πιθανών ενεργειών κακόβουλων χρηστών αλλά και επενδύσεων σε θέματα ασφάλειας.

Θα πρέπει να τονιστεί ότι μία από τις βασικότερες χρήσεις του cyber intelligence είναι το να βοηθάει την Διοίκηση να αποφασίζει για την διαχείριση του προϋπολογισμού με στόχο τον επαρκή μετριασμό του κινδύνου.

## 2.12. Επιλέγοντας τα σημεία της άμυνας

Ένα μεγάλο πρόβλημα για αυτούς που ασχολούνται επαγγελματικά με θέματα Κυβερνοασφάλειας είναι η τεράστια «επιφάνεια» συστημάτων και λογισμικού που θα πρέπει να προστατεύσουν από κακόβουλες επιθέσεις. Φανταστείτε ένα Κέντρο Λειτουργιών Ασφάλειας (SOC-Security Operations Center) να παρακολουθεί κάθε εφαρμογή που υπάρχει, κάθε δίκτυο ή μέρος αυτού, κάθε ροή δεδομένων. Ή ακόμα, μία ομάδα IR-Incident Response, να παρακολουθεί κάθε alert και κάθε ψηφιακό συμβάν. Τελικά, από ότι φαίνεται, χρειάζεται να προηγηθεί ένα κατάλληλο «φιλτράρισμα» των πληροφοριών που σχετίζονται με τα άνω και να μπορούν έτσι να δοθούν προτεραιότητες. Ουσιαστικά, η εφαρμογή κανόνων cyber intelligence δημιουργεί κάποιες απαιτήσεις, με την βοήθεια των οποίων επισημαίνονται οι πραγματικοί «κίνδυνοι», συλλέγονται χρήσιμες πληροφορίες σε ότι έχει να κάνει με cyber intelligence, ενώ αυτές οι πληροφορίες στη συνέχεια είναι διαθέσιμες για διάφορους χρήστες. Με αυτόν τον τρόπο αποφεύγεται σπατάλη χρόνου και χρήματος καθώς δεν συλλέγονται «άχρηστα» δεδομένα. Παρακάτω, βλέπουμε τις κατηγορίες των ευαίσθητων δεδομένων. Αυτές αποτελούν το πρώτο μέρος ανάπτυξης του cyber intelligence.

### 2.12.1. Δεδομένα πιστωτικών καρτών και τραπεζικών λογαριασμών

Ας σκεφτούμε τις αρνητικές επιπτώσεις του να κλαπούν ή να χαθούν δεδομένα πιστωτικών καρτών ή τραπεζικών λογαριασμών. Τα δεδομένα αυτά, μόλις ανακτηθούν από μη εξουσιοδοτημένα άτομα, πωλούνται ακριβά σε websites του dark web και το κόστος αυτών των ενεργειών φθάνει σε δυσθεώρητα ύψη. Το τελευταίο αποτελείται από νομικές αποζημιώσεις,

από υπηρεσίες παρακολούθησης λογαριασμών και ειδοποίησης σε περιπτώσεις απώλειας/κλοπής δεδομένων και από την απομάκρυνση των πελατών λόγω δημιουργίας αρνητικού κλίματος και απώλειας αξιοπιστίας του οικονομικού οργανισμού.

## 2.12.2.Προσωπικές πληροφορίες

Εδώ έχουμε τις προσωπικές αναγνωρίσιμες πληροφορίες (PII-Personal Identifiable Information) οι οποίες δεν είναι άλλες από ονοματεπώνυμα, διευθύνσεις, Αριθμοί Κοινωνικής Ασφάλισης (Social Security Numbers), κλπ. Τα PII's λοιπόν, στην περίπτωση που έχουν υποκλαπεί, πωλούνται από μη εξουσιοδοτημένους χρήστες οι οποίοι τα διανέμουν κυρίως στο dark web έναντι υψηλών αμοιβών και τα οποία χρησιμοποιούνται από εγκληματικές οργανώσεις οι οποίες κατασκευάζουν βάσει αυτών (των PII's) ψεύτικους λογαριασμούς τους οποίους είτε χρησιμοποιούν για χρηματοδότηση παράνομων δραστηριοτήτων, είτε ως βάση για επιθέσεις σε διάφορους στόχους (πχ άλλες εταιρείες). Και εδώ φυσικά η απώλεια των PII's μεταφράζεται σε υψηλό κόστος για τον τραπεζικό οργανισμό, το οποίο αποτελείται από το κόστος προστίμων, το κόστος απώλειας εμπιστοσύνης των πελατών προς το πρόσωπο της εταιρείας και φυσικά ο ίδιος ο τραπεζικός οργανισμός αποτελεί πόλο έλξης για καινούργιους επιτιθέμενους, λόγω των τρωτοτήτων οι οποίες ήρθαν στην επιφάνεια, ελκύοντας την δημιουργία, και άλλων, νέων επιθέσεων. Πολλές φορές, οι επιτιθέμενοι εκμαιεύουν πληροφορίες προσωπικού περιεχομένου από διάφορα μέσα κοινωνικής δικτύωσης (social media) όπως Facebook, LinkedIn και άλλα, στοχεύοντας κυρίως υψηλόβαθμα στελέχη επιχειρήσεων και οργανισμών. Με αυτόν τον τρόπο, κατασκευάζουν phising e-mails με τις προσωπικές πληροφορίες αυτές, με σκοπό να διεισδύσουν σε εταιρείες, με την επισύναψη κακόβουλου λογισμικού, στα φαινομενικά «αθώα» e-mails αυτά (phising).

## 2.12.3. Στοιχεία πνευματικής ιδιοκτησίας

Τα στοιχεία πνευματικής ιδιοκτησίας μίας εταιρείας ή οργανισμού αποτελούν ευαίσθητα δεδομένα τα οποία σε περίπτωση κατά την οποία κλαπούν ή πέσουν σε χέρια μη εξουσιοδοτημένων χρηστών, θα αποτελεί μία τροχοπέδη στο προβάδισμα του οργανισμού, το οποίο είχε αποκτήσει έναντι του ανταγωνισμού, στην ελεύθερη αγορά. Τα στοιχεία αυτά είναι τεχνικά εγχειρίδια, εγχειρίδια παραγωγής, βιβλία, προγράμματα software, σχέδια μηχανικών, βίντεο κλπ.

## 2.12.4. Εμπιστευτικές εμπορικές πληροφορίες

Αυτές αποτελούνται από λίστες πελατών, εμπορικά μυστικά, οικονομικές πληροφορίες, συγχωνεύσεις και λοιπές πληροφορίες οι οποίες συνδέονται και επηρεάζουν τιμές μετοχών. Η διαρροή διάφορων e-mails και σχετικών εγγράφων συναφών με τις εμπορικές πληροφορίες

αυτές σημαίνει την δαπάνη μεγάλων ποσών από την πλευρά των μετόχων καθώς και την έναρξη ερευνών ποινικού δικαίου.

### 2.12.5. Διαπιστευτήρια

Τα διαπιστευτήρια (credentials) αποτελούν αρκετές φορές στόχο από κακόβουλους χρήστες και στην περίπτωση που ανακτηθούν από αυτούς, σημαίνει την πρόσβαση σε κάθε ευαίσθητη πληροφορία και στοιχείο της εταιρείας.

### 2.12.6. Λειτουργικά συστήματα

Σε αυτήν την περίπτωση, τα λειτουργικά συστήματα δεν ανήκουν στην κατηγορία των στοιχείων που μπορούν να υποκλαπούν αλλά περισσότερο είναι η έννοια του ότι δύναται μία εταιρεία, δεχόμενη επίθεση (Ddos), να έχει προβλήματα στο website της, να έχει δυσλειτουργίες στις χρηματικές της συναλλαγές και βάσει αυτών να πυροδοτηθούν άλλου είδους προβλήματα, όπως η μείωση ικανότητας παραγωγής της και η δημόσια εικόνα της.

## 2.13. Η πλευρά των επιτιθέμενων

Αναλύσαμε προηγουμένως ότι το πρώτο μέρος ανάπτυξης του cyber intelligence αποτελείται από τις διάφορες υποκατηγορίες ευαίσθητων δεδομένων. Τώρα θα δούμε και το δεύτερο μέρος το οποίο δεν είναι άλλο από τους επιτιθέμενους ή κακόβουλους χρήστες ή hackers. Ας δούμε λίγο πιο αναλυτικά το μέρος αυτό, με την διεξαγωγή μίας ανάλυσης η οποία μας βοηθάει στο να αποφασίσουμε:

- Ποιες κατηγορίες απειλών να παρακολουθούμε
- Από αυτές, ποιες εντάσσονται σε πλαίσιο προτεραιότητας παρακολούθησης και άμεσης αντιμετώπισης
- Ποιες κατηγορίες απειλών δεν απαιτούν ιδιαίτερη σπατάλη σε πόρους. Εδώ, έχουμε την λεγόμενη «συρρίκνωση του προβλήματος» (“shrinking the problem”)

Παρατηρώντας την εικόνα 2.7, βλέπουμε τις διάφορες κατηγορίες των επιτιθέμενων, τους στόχους τους και τα «όπλα» που χρησιμοποιούν.

| | Cybercriminals | Competitors and Cyber Espionage Agents | Hacktivists |
|---|---|---|---|
| Motivation | Obtain financial returns | Obtain commercial, political, or military advantages | Express political beliefs and ideologies<br>Discredit or damage opponents |
| Assets Targeted | Credit card and financial account data<br>Personal information<br>Credentials | Intellectual property<br>Business information<br>Credentials | Operational systems<br>Credentials |
| Attack Types and Tools | Malware<br>Phishing<br>Social engineering<br>Botnets<br>Credential escalation<br>Many others | Malware<br>Phishing<br>Social engineering<br>Botnets<br>Credential escalation<br>Many others | Malware<br>Phishing<br>Social engineering<br>DDoS |

(εικόνα 2.7:Οι διάφορες κατηγορίες των επιτιθέμενων, οι στόχοι τους και τα «όπλα» που χρησιμοποιούν)

Αναλύοντας την εικόνα 2.7, διαπιστώνουμε ότι υπάρχουν διάφορα κίνητρα τα οποία προκαλούν τις επιθέσεις αυτές όπως οικονομικά, πολιτικά, στρατιωτικά ή ιδεολογικά. Οι στόχοι μίας επίθεσης μπορεί να είναι προσωπικά δεδομένα, χρηματοπιστωτικά δεδομένα, πληροφορίες λειτουργίας μιας επιχείρησης ή λειτουργικά συστήματα. Τα διάφορα «εργαλεία» που συνήθως χρησιμοποιούνται είναι κάποια malwares, τεχνικές social engineering, botnets, phising, Ddos. Οι επιτιθέμενοι μπορεί να είναι κυβερνοεγληματίες, ακτιβιστές ή άτομα που ασχολούνται με ενέργειες βιομηχανικής ή στρατιωτικής αντικατασκοπείας.

### 2.13.1.Κυβερνοεγκληματίες

Αυτοί σχετίζονται με το παράνομο κέρδος. Αναφέρουμε ότι στοχεύουν σε τραπεζικούς λογαριασμούς ή πιστωτικές κάρτες με σκοπό είτε την κλοπή χρημάτων (ουσιαστικά με την μεταφορά ποσών χρημάτων από λογαριασμούς ατόμων σε δικούς τους λογαριασμούς) με την

κλασσική έννοια, είτε με την χρησιμοποίηση αυτών των χρημάτων σε παράνομες δραστηριότητες (monetization). Όμως, θα πρέπει να γνωρίζουμε ότι υπάρχουν διάφορες κατηγορίες κυβερνοεγκληματιών. Υπάρχουν λοιπόν κυβερνοεγκληματίες οι οποίοι στοχεύουν για παράδειγμα βιομηχανίες, χρηματοπιστωτικά ιδρύματα, νοσοκομεία, μέσα ενημέρωσης ή τοπικές κυβερνήσεις χωρών. Άλλοι στοχεύουν εφαρμογές σχετικές με ανθρώπινους πόρους (human resources), συστήματα, βάσεις δεδομένων πελατών ή τα POS (Point Of Sales) συστήματα. Θα πρέπει λοιπόν, οι επαγγελματίες οι οποίοι ασχολούνται με τον τομέα του cyber intelligence να παρακολουθούν τις διάφορες υπάρχουσες κατηγορίες των κυβερνοεγκληματιών αλλά και να ανιχνεύουν τυχόν νέες κατηγορίες που αναδύονται στο web. Φυσικά, θα πρέπει να είναι και ενήμεροι με τα «εργαλεία» (“tools”) ή «όπλα» (“weapons”) που αυτοί χρησιμοποιούν.

### 2.13.2. Άτομα ή ομάδες που σχετίζονται με τη βιομηχανική αντικατασκοπεία

Σε αυτήν την περίπτωση έχουμε κάποιους κακόβουλους χρήστες οι οποίοι διεξάγουν επιθέσεις με σκοπό την ανάκτηση δεδομένων εμπορικής φύσεως σχετικής με θέματα ανταγωνισμού. Αρχικά, τέτοιου είδους επιθέσεις είχαν ως στόχο την υποκλοπή δεδομένων στρατιωτικού, αεροδιαστημικού και κυβερνητικού χαρακτήρα. Τώρα πλέον, στην διευρυμένη τους μορφή, στοχεύουν δίκτυα υπολογιστών με σκοπό την ανάκτηση στοιχείων για την απόκτηση πλεονεκτημάτων στην ελεύθερη αγορά, ή σε οικονομικό και πολιτικό επίπεδο. Άρα λοιπόν, οι επαγγελματίες οι οποίοι ασχολούνται με θέματα cyber intelligence, θα πρέπει να λάβουν υπόψιν τους όχι μόνο την ύπαρξη αλλά και τους πιθανούς στόχους τέτοιων επιθέσεων όπως έγγραφα, σχέδια και ειδικά λογισμικά.

### 2.13.3. Άτομα ή ομάδες που εκφράζουν ορισμένες ιδεολογίες

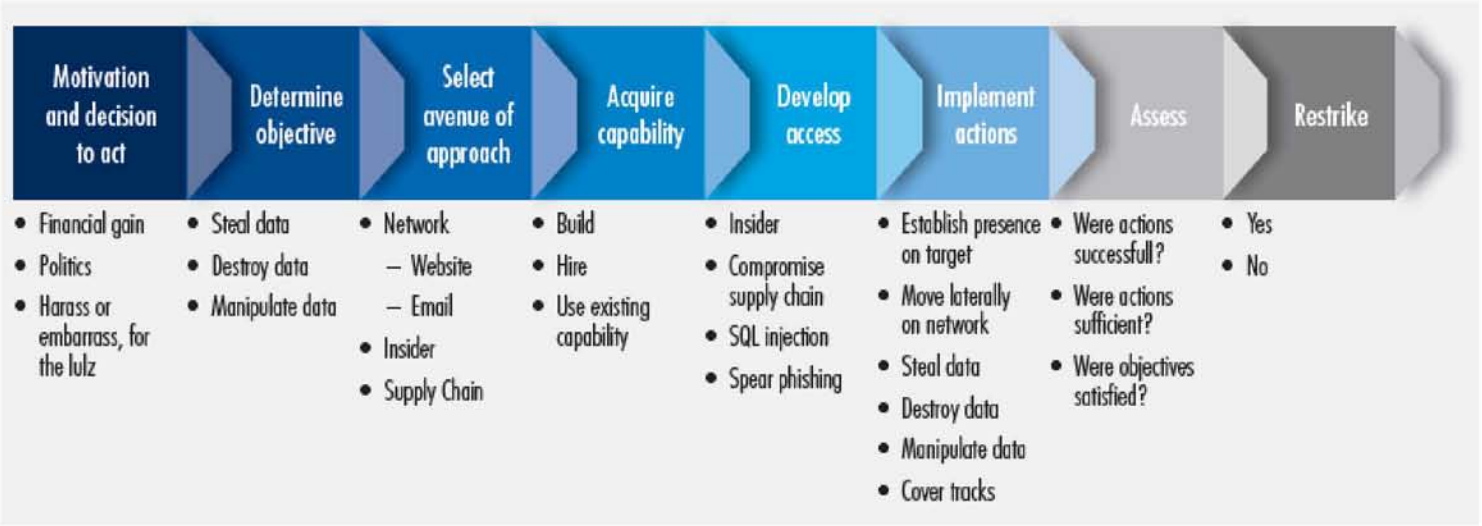
Εδώ έχουμε άτομα ή ομάδες οι οποίες εκφράζουν την δική τους οπτική γωνία σε πολιτικό, ιδεολογικό ή κοινωνικό επίπεδο. Και το πράττουν αυτό, δυσφημίζοντας για παράδειγμα κάποιους φορείς (μέσω κυβερνοεπιθέσεων) οι οποίοι εντάσσονται σε ιδεολογικό πλαίσιο αντίθετο με εκείνο που αντιπροσωπεύουν αυτοί. Εστιατόρια, τράπεζες, εταιρείες, μέσα κοινωνικής δικτύωσης και εμπορικά καταστήματα αποτελούν μερικούς από τους στόχους αυτών των ομάδων και οι οποίοι συμβολίζουν τον καπιταλισμό, ένα συγκεκριμένο τρόπο ζωής ή γενικότερα κάποια φιλοσοφία, αντίθετη με τα πιστεύω τους.

### 2.13.4. Η «αλυσίδα θανάτου» (the kill chain)

Έχοντας μιλήσει προηγουμένως για διάφορες κατηγορίες επιτιθέμενων, υπάρχει ένας γενικός κανόνας, βάσει του οποίου διεξάγονται επιθέσεις στον Κυβερνοχώρο. Ο κανόνας αυτός ονομάζεται kill chain αγγλιστί, και εμείς εδώ τον βαπτίσαμε αυθαίρετα ως «αλυσίδα θανάτου» (ας μας επιτραπεί ο όρος αυτός). Ουσιαστικά το kill chain αποτελεί μία σειρά ενεργειών, από την πλευρά των επιτιθέμενων, η οποίες έχουν ως τελικό στόχο το να προκαλέσουν ζημιά σε έναν οργανισμό, η οποία συνήθως είναι είτε έχει σχέση με υποκλοπή ευαίσθητων δεδομένων, ή με

phising, ή με κάποια μετάδοση ιού. Υπάρχουν δύο γενικοί τρόποι με τους οποίους οι ειδικοί της άμυνα προσπαθούν να αντιδράσουν στο kill chain. Ο ένας τρόπος είναι να μελετούν το πώς λειτουργεί το κακόβουλο λογισμικό εντός των υπολογιστικών συστημάτων του οργανισμού, έχοντας ως βοήθεια τα διάφορα αρχεία log, για την καταγραφή της λειτουργίας αυτής και την ανακάλυψη του μοτίβου της επίθεσης. Αυτός ο τρόπος μπορεί να χρησιμοποιείται κάποιες φορές αλλά δεν είναι πάντα ο καλύτερος, εάν σκεφτούμε ότι το κακόβουλο λογισμικό βρίσκεται ήδη μέσα στα υπολογιστικά συστήματα και το πότε οι ειδικοί θα πρέπει να «τραβήξουν το καλώδιο από την πρίζα» και να κλείσουν όλα τα υπολογιστικά συστήματα, για να μην έχουν μη αναστρέψιμα και καταστροφικά αποτελέσματα, απαιτεί την κατάλληλη εμπειρία.

Ο άλλος τρόπος είναι η πρόληψη από τη θεραπεία, δηλ. να μπορούν οι ειδικοί να χτίζουν την εκάστοτε άμυνα του οργανισμού, πριν την εμφάνιση κάποιου ψηφιακού συμβάντος. Εδώ, θα πρέπει να ξεκαθαρίσουμε ορισμένα πράγματα. Καταρχήν θα μιλήσουμε για το αγγλικό όρο “Speed Of Cyber”. Ο όρος αυτός μας δείχνει ότι μία Κυβερνοεπίθεση μπορεί να λάβει χώρα σε χρόνους της τάξεως msec. Δηλ. το χρονικό διάστημα το οποίο απαιτείται για να «ταξιδέψουν» τα πακέτα κακόβουλου λογισμικού από την πηγή τους στον οργανισμό, είναι απειροελάχιστο. Όμως, εδώ υπάρχει και κάτι άλλο. Ο χρόνος που απαιτείται από την απόφαση μέχρι και την υλοποίηση μίας επίθεσης είναι πολύ μεγάλος, και μπορεί να είναι ημέρες, εβδομάδες, μήνες ή ακόμη και χρόνια. Και αυτό διότι μια επίθεση, για να λάβει σάρκα και οστά, χρειάζεται σχεδιασμό, επιλογή των κατάλληλων διόδων και τρωτοτήτων (μέσα από τις οποίες θα περάσει το κακόβουλο λογισμικό), η συλλογή πληροφοριών σχετικών με το «στόχο» (δηλ. που να γίνει και γιατί η επίθεση, ποια δεδομένα αξίζει τον κόπο να υποκλαπούν κλπ), εκπαίδευση (στο πώς να κατασκευάζονται τα διάφορα «όπλα» της επίθεσης), επινόηση και εφαρμογή της όλης διαδικασίας επίθεσης και τελικά η ίδια η επίθεση. Στην εικόνα 2.8 βλέπουμε την μορφή ενός kill chain.




(εικόνα 2.8: Η μορφή ενός kill chain)

Γίνεται αντιληπτό ότι το παραπάνω χρονικό διάστημα δίνει την ευκαιρία στους ειδικούς της Κυβερνοάμυνας να διεξάγουν τις δικές τους ενέργειες Intelligence, σχετικές με το kill chain. Αυτές μπορεί να είναι οι εξής:

- Ανίχνευση του ποιος/ποιοι μπορεί να στοχεύουν τον οργανισμό.
- Ανίχνευση των ικανοτήτων αλλά και των προθέσεων των επιτιθέμενων
- Το χρονικό πλαίσιο εντός του οποίοι θα διεξαχθεί μία επίθεση
- Το σημείο από το οποίο θα ξεκινήσει η επίθεση
- Ο τρόπος με τον οποίο σκοπεύουν (οι επιτιθέμενοι) να διεισδύσουν εντός των υπολογιστικών συστημάτων του οργανισμού

Είναι γεγονός ότι κάθε βήμα στο kill chain αποτελεί και μία ευκαιρία για απόκρουση της επίθεσης και συνάμα μία ευκαιρία να δράσει αυτή η απόκρουση αρνητικά στην ψυχολογία των επιτιθέμενων, οι οποίοι θα διαπιστώνουν ότι πλέον η άμυνα του οργανισμού προσαρμόζεται αναλόγως των συνθηκών και θα είναι αρκετά δύσκολο για τους επιτιθέμενους να φτάσουν στον τελικό τους στόχο, πράγμα που μπορεί ακόμη και να προκαλέσει την ακύρωση της επίθεσης. Στις εικόνες 2.9 και 2.10, παραθέτουμε πίνακες με τις πιθανές ενέργειες της άμυνας, εντός του δικτύου του οργανισμού ή εκτός αυτού, αντιστοίχως. Ο πίνακας στην εικόνα 2.10 αποτελεί μία προέκταση του πίνακα στην εικόνα 2.9.

| Phase | Detect | Deny | Disrupt | Degrade | Deceive | Destroy |
|---|---|---|---|---|---|---|
| Reconnaissance | Web analytics | Firewall ACL | | | | |
| Weaponization | NIDS | NIPS | | | | |
| Delivery | Vigilant user | Proxy filter | In-line AV | Queuing | | |
| Exploitation | HIDS | Patch | DEP | | | |
| Installation | HIDS | "chroot" jail | AV | | | |
| C2 | NIDS | Firewall ACL | NIPS | Tarpit | DNS redirect | |
| Actions of Objectives | Audit log | | | Quality of Service | Honeypot | |

(εικόνα 2.9: Ενέργειες άμυνας εντός του οργανισμού)

| Phase | Detect | Deny | Disrupt | Degrade | Deceive | Destroy |
|---|---|---|---|---|---|---|
| Motivation | Open Source Intelligence | Public Relations, Reputation for prosecuting | | Public Relations | | |
| Objectives | Web analytics, Open Source Intelligence | | | OPSEC | Public Relations | |
| Avenue of approach | Web / Network analytics | | Dynamic Defense | Dynamic Defense, OPSEC | Direct towards stronger defenses | |
| Capability | Open Source Intelligence | | Insider threat program | Dynamic Defense | Direct towards stronger defenses | |
| Access | Open Source Intelligence, web/network analytics | Insider threat program | | Dynamic Defense, OPSEC | | |
| Actions | Insider threat program, Supply chain awareness, Intel-driven CND | Role based access | | Quality of Service | Honeypot | |
| Assess | Web analytics, Social Media | Public Relations | | | Public Relations, Honeypot | |
| Restrike | Web / Network analytics, Open Source Intelligence, | Dynamic Defense | | | Public Relations, Honeypot | |

(εικόνα 2.10: Ενέργειες άμυνας εκτός των πλαισίων του οργανισμού)

## 2.14. Οι πληροφορίες του cyber intelligence

Οι πληροφορίες του cyber intelligence αποτελούν ένα πολύ χρήσιμο εργαλείο για τους επαγγελματίες του είδους, καθώς με αυτές, μπορούν να χτίσουν μία καλύτερη άμυνα για τις εταιρείες για τις οποίες εργάζονται (παρέχοντας υπηρεσίες) έναντι πολύπλοκων κυβερνοεπιθέσεων. Πρωτίστως όμως, κρίνεται απαραίτητη η γνώση και των συστημάτων αλλά και του ανθρώπινου δυναμικού, προκειμένου να παραχθούν τέτοιου είδους πληροφορίες. Και η γνώση αυτή ουσιαστικά αποτελείται από συγκεκριμένες οδηγίες οι οποίες κατευθύνουν το προσωπικό στο πως θα κάνει την δουλειά του σωστά αλλά και στο πως οι πληροφορίες του cyber intelligence μπορούν να είναι προσβάσιμες και άμεσα χρησιμοποιήσιμες από προσωπικό και συστήματα IT security. Φυσικά, υπάρχουν διαφορές στην παραγωγή τέτοιου είδους πληροφοριών, αναλόγως της κάθε περίπτωσης. Παρακάτω, αναφέρουμε κάποιες κατηγορίες ατόμων, για τις οποίες υπάρχουν και διαφορετικές απαιτήσεις.

### 2.14.1.Τακτικοί χρήστες

Τα NOC (Network Operation Centers), έχουν ως αντικείμενο να διαχωρίζουν τις πραγματικές επιθέσεις από την «κίνηση» στα δίκτυα η οποία παράγεται από τους νόμιμους χρήστες, έχοντας στα χέρια τους «νόμιμες» ψηφιακές υπογραφές και «ακίνδυνα» URL's, με την βοήθεια των οποίων χρησιμοποιούν τα firewalls, τα συστήματα IDS/IPS και άλλα συστήματα ασφάλειας.

Αποφασίζεται σε ποια σημεία του συστήματος θα πρέπει να γίνει πρώτα patching, ενώ οι ομάδες ανάλυσης SOC, παρατηρεί και αναλύει σε βάθος κάποιο/κάποια alerts. Και για να το κάνει αυτό, θα πρέπει να τροφοδοτεί τα SIEM εργαλεία της (Security Information and Event Management) με πληροφορίες που πηγάζουν από τις διαδικασίες του cyber intelligence, και οι οποίες θα πρέπει να είναι ακριβείς, έγκυρες και έγκαιρες. Επίσης, οι ομάδες SOC, θα πρέπει με τη χρήση των πληροφοριών του cyber intelligence, να μπορούν να διαχωρίζουν ποια από τα alerts είναι μεμονωμένα και ποια αποτελούν κομμάτια μίας μεγαλύτερης και πολυπλοκότερης επίθεσης.

### 2.14.2.Λειτουργικοί χρήστες

Σε αυτήν την κατηγορία ανήκουν οι ομάδες IR (Incident Response), οι forensic αναλυτές, και τα τμήματα ανίχνευσης απάτης (fraud detection departments). Όλοι οι προαναφερθέντες, χρειάζονται πληροφορίες του intelligence προκειμένου να:

- Αποφασίζουν εάν ένα alert συνδέεται με μία μεμονωμένη επίθεση ή με μία πολύπλοκη επίθεση.
- Εκμαιεύσουν περαιτέρω πληροφορίες και στοιχεία από μία επίθεση
- Εντοπίσουν τις πηγές των επιθέσεων
- Αποφασίζουν ποια από τα συστήματα έχουν «διαπεραστεί» από κακόβουλους χρήστες και ποια από αυτά χρειάζονται άμεση εξυγίανση

Όλες οι παραπάνω διαδικασίες χρειάζονται αναλύσεις των malwares και των υπό επίθεση συστημάτων καθώς και αναφορές των TTP's (Tactics, Techniques and Procedures- Τακτικών, Τεχνικών και Διαδικασιών) συγκεκριμένου είδους επιτιθέμενων.

### 2.14.3.Στρατηγικοί χρήστες

Οι στρατηγικοί χρήστες, συμπεριλαμβανομένων και των ομάδων CISO και IT managers, χρησιμοποιώντας αναφορές του cyber intelligence, οδηφούνται στο να παίρνουν τις καλύτερες αποφάσεις σχετικά με τις χρηματοδοτήσεις των έργων της Κυβερνοασφάλειας ,της βελτίωσης των διαδικασιών συναφών με αυτή και των νέων τεχνολογίων. Έχει πλέον αποδειχθεί ότι ο μετριασμός του ρίσκου μίας εταιρείας συνδέεται άμεσα με την σωστή εφαρμογή κανόνων threat intelligence.

## 2.14.4.Το στρατηγικό επίπεδο του Cyber Intelligence

Σε αντιστοιχία με τις 3 παραπάνω παραγράφους, υπάρχουν 3 επίπεδα του Cyber Intelligence. Το ένα από αυτά είναι το στρατηγικό επίπεδο, το οποίο και θα αναλύσουμε σε αυτήν την παράγραφο. Ο ορισμός του στρατηγικού επιπέδου, στην γενικότερη μορφή του, έχει ως εξής: ***Το στρατηγικό επίπεδο είναι το επίπεδο στο οποίο ένα έθνος, ως ένα μέλος ή μία οντότητα η οποία ανήκει σε μία ευρύτερη ομάδα αποτελούμενη από άλλα έθνη-μέλη, αποφασίζει για τις καλύτερες δυνατές συμμαχίες με γνώμονα την θέσπιση ορισμένων κανόνων λειτουργίας και την επίτευξη στόχων σχετικών με την ασφάλεια και επίσης, χρησιμοποιεί εθνικούς πόρους για την υλοποίηση των στόχων και των κανόνων αυτών.*** Άρα λοιπόν, έχοντας υπόψιν αυτόν τον ορισμό, θα μπορούσαμε να ισχυριστούμε ότι το στρατηγικό επίπεδο του Cyber Intelligence και η εφαρμογή του είναι ουσιαστικά η περίπτωση στην οποία ένα γκρουπ ή ένας οργανισμός, ο οποίος αποτελεί έναν εκπρόσωπο του γενικού συνόλου, αποφασίζει για τους στόχους που θα πρέπει να επιτευχθούν αλλά και για την καθοδήγηση η οποία θα βοηθήσει στην επίτευξη των στόχων αυτών. Και εδώ θα ήταν καλό να πούμε για την εκτίμηση των κινδύνων που διατρέχει ένας φορέας, η οποία μπορούμε να πούμε ότι πηγάζει από τα σημεία του τι πολύτιμα δεδομένα έχει ο φορέας αυτός τα οποία θέλουν κάποιοι κακόβουλοι χρήστες να υποκλέψουν μέσω ψηφιακών επιθέσεων, πόση αξία έχουν αυτά αλλά και πόσο καλά μπορούν αυτά τα δεδομένα να προστατευτούν. Αυτές λοιπόν τις ερωτήσεις θα πρέπει να απαντήσει η Διοίκηση του φορέα, προκειμένου να μπορεί να υπάρξει η εκτίμηση των κινδύνων. Μετά της εκτίμησης αυτής, θα πρέπει να παραχθεί το λεγόμενο «τοπίο απειλών», δηλ να μπορεί η Διοίκηση να εντοπίζει για το εάν ένας ή κάποιοι κακόβουλοι χρήστες θα αποφασίζουν να επιτεθούν, να γνωρίζει εκ των προτέρων σε ποιο/ποια «σημεία» ζωτικής σημασίας επρόκειτο να λάβει χώρα η επίθεση και να έχει ήδη ανιχνεύσει ύποπτες ενέργειες κατά τις οποίες οι επιτιθέμενοι χρησιμοποιούν διάφορους υπολογιστικούς πόρους (πχ botnets) για την υλοποίηση κάποιας επίθεσης. Άρα λοιπόν, έχοντας ως εργαλείο την Intelligence, οι ομάδες ή τα άτομα που είναι υπεύθυνα για την άμυνα του οργανισμού, μπορούν είτε να αντικρούσουν μία επίθεση, ή να μετριάσουν τις αρνητικές επιπτώσεις της.

Τους σκοπούς ή καλύτερα το αντικείμενο του Intelligence, καθορίζεται από μία ομάδα ατόμων, όπως ο Διευθύνων Σύμβουλος, ο Επικεφαλής των Οικονομικών Υπηρεσιών, ο Διευθυντής των Διαδικασιών και Λειτουργιών, ο Manager των συνεργαζόμενων ομάδων και διάφορα εταιρικά συμβούλια. Όλα λοιπόν αυτά τα άτομα, καθορίζουν την έννοια του Στρατηγικού Cyber Intelligence, το οποίο είναι ένα σύνολο πολιτικών και διαδικασιών. Μέσα στην ομάδα αυτή, δεν βρίσκονται ορισμένα άτομα, όπως οι Επικεφαλής Πληροφοριών και Ασφάλειας Πληροφοριών (Chief Information Officers-CIO's, Chief Information Security Officers-CISO's). Ο λόγος που συμβαίνει αυτό είναι καθαρά οικονομικός: Ενώ κρίνεται απαραίτητο, για τους CIO's και CISO's, να βρίσκονται σε θέσεις σχετικές με την ασφάλεια και την λειτουργία των δικτύων, συνήθως δεν συμβαίνει αυτό.

Θα μπορούσε, σε αυτό το σημείο, να ρωτήσει κάποιος: Σκεπτόμενοι το στρατηγικό intelligence, ποιος τύπος του θα ήταν πλέον σημαντικός για τον οργανισμό, στον οποίο θα υλοποιηθούν διαδικασίες CI; Σε αυτό το ερώτημα, αρμόδια για να απαντήσει, είναι η Διοίκηση του εν λόγω οργανισμού. Θα μπορέσει όμως να απαντήσει, έχοντας πρωτίστως ανιχνεύσει κάποιες πληροφορίες οι οποίες δείχνουν ότι κάτι έχει αλλάξει στην παρούσα κατάσταση και το οποίο έχει

επηρεάσει τους κινδύνους στους οποίους εκτίθεται ο οργανισμός. Και αυτό, σε συνδυασμό με τα παρακάτω σημεία:

- Το γεγονός του ότι στο αντικείμενο και γενικότερα στο επαγγελματικό πεδίο του οργανισμού, μπαίνει και κάποιος άλλος ανταγωνιστής.
- Το γεγονός του ότι υπάρχουν κάποιες ενδείξεις ότι πχ ο συγκεκριμένος ανταγωνιστής, μέσω αθέμιτων μέσων (με μεθόδους exploitation), είχε προσπαθήσει σε παρελθοντικό χρόνο, να υποκλέψει στοιχεία και πληροφορίες πνευματικής ιδιοκτησίας.
- Ενδείξεις ότι ο συγκεκριμένος ανταγωνιστής έχει αναπτύξει σχέσεις συνεργασίας με όλους ή έστω με κάποιους προμηθευτές του οργανισμού και μέσω των σχέσεων αυτών, επηρεάζει αρνητικά τις σχέσεις μεταξύ του τελευταίου και των προμηθευτών του.
- Ενδείξεις ότι στο παρασκήνιο λαμβάνουν χώρα ενέργειες που σχετίζονται με ψηφιακές απειλές και οι οποίες έχουν ως στόχο τον ίδιο τον οργανισμό.

Όλη η πληροφόρηση Intelligence, είναι ζωτικής σημασίας διότι επηρεάζει την όλη φιλοσοφία λειτουργίας ενός οργανισμού στην λήψη κρίσιμων αποφάσεων, με θετικό εννοείται πάντα, ρόλο. Οι αποφάσεις που θα έπαιρνε η εκάστοτε Διοίκηση, χωρίς την εφαρμογή του Intelligence, θα στηρίζονταν κυρίως στην εμπειρία και στο τι θα φαινόταν πιο πρακτικό, χωρίς να δίνεται προτεραιότητα σε διαδικασίες και λειτουργίες, όπως θα έπρεπε. Με την εφαρμογή του Intelligence, συμβαίνει ακριβώς αυτό: Δίνεται προτεραιότητα σε διαδικασίες και λειτουργίες, με στοχευμένο τρόπο πάντα, και με σκοπό την καλύτερη δυνατή άμυνα του οργανισμού.

Το στρατηγικό λοιπόν, Cyber Intelligence, θα λέγαμε ότι επηρεάζει με θετικό τρόπο, την Διοίκηση, στην λήψη αποφάσεων ζωτικής σημασίας, γεγονός το οποίο οδηγεί σε καλύτερη στρατηγική, πολιτική, αρχιτεκτονική και επενδυτικές ενέργειες του εν λόγω οργανισμού. Βέβαια, ο εκάστοτε οργανισμός έχει τις δικές του ανάγκες και ιδιαιτερότητες για την εφαρμογή του CI, αφού σε μέγεθος, σε πολυπλοκότητα και σε αντικείμενο ενασχόλησης παρουσιάζει διαφορετικότητα σε σχέση με τους άλλους και επομένως, θα πρέπει οι εκάστοτε διαδικασίες CI να «χτίζονται» βάσει των αναγκών του. Υπάρχουν 6 κριτήρια, με την βοήθεια των οποίων μπορούν να οριστούν τα επίπεδα του Cyber Inteligence, για τον εν λόγω οργανισμό. Αυτά τα κριτήρια είναι τα εξής:

- Η «ταυτότητα», η φύση και το αντικείμενο του οργανισμού
- Η λήψη των αποφάσεων του οργανισμού
- Το χρονικό πλαίσιο μέσα στο οποίο ο οργανισμός πρόκειται να λειτουργεί
- Η «έκταση» συλλογής πληροφοριών
- Η ανίχνευση και ο χαρακτηρισμός κάποιων υποψήφιων επιτιθέμενων
- Η ικανότητα της συλλογής πληροφοριών Intelligence

Υπάρχουν οργανισμοί και ιδιωτικού αλλά και δημοσίου χαρακτήρα των οποίων οι Διοικήσεις μπορούν να χρησιμοποιούν τα παραγόμενα δεδομένα CI, τα οποία θα οδηγούν τον εκάστοτε οργανισμό στην καλύτερη δυνατή ανάπτυξη εφαρμογών στρατηγικής και πολιτικής, για ένα μεγάλο χρονικό διάστημα, των 3+ ετών.

Η συλλογή των πληροφοριών συνδέεται με διάφορους τομείς όπως για παράδειγμα ο τομέας στον οποίο ανήκει ο οργανισμός (και παρελκόμενοι τομείς όπως τομέας R&D, τομέας αλυσίδας εφοδιασμού) και τομέας ανίχνευσης υποψήφιων επιτιθέμενων (χαρακτηρισμού ικανοτήτων και κινήτρων τους). Να προσθέσουμε ότι το στρατηγικό CI, εστιάζει σε προθέσεις διάφορων

υποψήφιων επιτιθέμενων (είτε έχουν φανερωθεί από αυτούς είτε όχι), σε γεωπολιτικά γεγονότα και σε δείκτες στρατηγικής σημασίας.

Επίσης, η έννοια της διαχείρισης του κινδύνου, συνδέεται με άμεσο τρόπο με την εφαρμογή του στρατηγικού CI. Η διαχείριση του κινδύνου αποτελείται από μία λίστα ενεργειών όπως η ανίχνευση απειλών, τρωτοτήτων του συστήματος, επιπτώσεων μίας επίθεσης στο σύστημα και ανάλογων αντίμετρων. Φυσικά, θα πρέπει να γίνουν κατανοητά από τη Διοίκηση, τα πλαίσια λειτουργίας του οργανισμού στα οποία υπάρχει κίνδυνος διείσδυσης από κακόβουλους χρήστες και θα πρέπει να οριστεί και η κατάλληλη ορολογία, για να διασφαλίζεται μία καλύτερη επικοινωνία μεταξύ των μελών του οργανισμού. Το Ινστιτούτο NIST (National Institute for Standards and Technology's) μας παρέχει την βασική ορολογία, για τους σκοπούς της βέλτιστης επικοινωνίας, οι οποίοι είναι οι εξής:

**Risk (Κίνδυνος/Ρίσκο):** Ένας «βαθμός» βάσει του οποίου μία οντότητα απειλείται από κάποιο γεγονός.

**Threat Agent (Απειλή):** Ο σκοπός και η μέθοδος που χρησιμοποιείται στην προσπάθεια να γίνει εκμετάλλευση μίας τρωτότητας.

**Impact (Επίπτωση):** Το μέγεθος της επίπτωσης των αρνητικών αποτελεσμάτων ενός επιτυχούς Threat Agent.

**Countermeasure (Αντίμετρα):** Ενέργειες, διαδικασίες, συσκευές, τεχνικές και άλλα μέτρα που χρησιμοποιούνται για τον μετριασμό των διάφορων τρωτοτήτων.

### 2.14.4.1.Απαιτήσεις του στρατηγικού επιπέδου του Cyber Intelligence

Όπως είδαμε και προηγουμένως, υπάρχει άμεση σύνδεση μεταξύ του στρατηγικού CI και του Risk Management του οργανισμού, στον οποίο οι «καταναλωτές» δεδομένων CI είναι η ίδια η Διοίκηση. Το Ινστιτούτο NIST (National Institute for Standards and Technology's) τονίζει ότι για να είναι αποτελεσματική η εφαρμογή του στρατηγικού CI, θα πρέπει να υπάρχει μία σοβαρή δέσμευση, άμεση εμπλοκή και συνεχή υποστήριξη από τη Διοίκηση. Οι απαιτήσεις της τελευταίας χωρίζονται στις εξής 3 κατηγορίες:

1. **Commander's Critical Information Requirements (CCIR):** Οι πληροφορίες αυτές βοηθούν τη Διοίκηση να πάρει αποφάσεις στρατηγικής σημασίας.
2. **Priority Intelligence Requirements (PIR):** Οι πληροφορίες αυτές συνδέονται με τους πιθανούς/υποψήφιους «εχθρούς».
3. **Friendly Force Information Requirements (FFIR):** Οι πληροφορίες που μας δείχνουν την εικόνα «ασφάλειας» την οποία παρουσιάζει ο οργανισμός στο κοινό.

Όσον αφορά την εκτίμηση του ρίσκου, αναφέρουμε παρακάτω για το πώς την επηρεάζει ο ανθρώπινος παράγοντας. Εδώ όμως τώρα, θα μιλήσουμε για αυτή, για τη γενικότερη μορφή της και για το τι ακριβώς σημαίνει για τον οργανισμό. Το βασικότερο στοιχείο που συνδέεται με την

εκτίμηση ρίσκου είναι τα περιουσιακά στοιχεία του οργανισμού, εννοώντας στοιχεία πνευματικής ιδιοκτησίας, πληροφορίες χρηματοπιστωτικής φύσεως, επιχειρηματικές λειτουργίες και προσωπικές ιδιωτικές πληροφορίες (PII's-Personally Identifiable Information). Από αυτά τα στοιχεία θα πρέπει να αποφασιστεί ποια είναι τα πλέον ζωτικής σημασίας και περισσότερο ευάλωτα στο να υποκλαπούν. Η ίδια η Διοίκηση θα πάρει τις άνωθι αποφάσεις και εκτός από αυτές θα πρέπει να συμπεριληφθούν και άλλες δραστηριότητες του τύπου αξιολόγησης απειλών και τρωτοτήτων και ανάλυση της επίπτωσης τους (σε επαγγελματικό επίπεδο και σε επίπεδο λειτουργίας) σε περίπτωση διείσδυσης, και όλα αυτά θα οδηγήσουν στο στήσιμο μίας καλύτερης άμυνας έναντι επιθέσεων. Επίσης, στην προσπάθεια βελτίωσης της άμυνας του οργανισμού θέτονται και κάποια ερωτήματα όπως:

- Το ρίσκο της εταιρείας στο οποίο αυτή λειτουργεί, βρίσκεται σε χαμηλά ή υψηλά επίπεδα;
- Σε περίπτωση διείσδυσης και ανάκτησης ευαίσθητων πληροφοριών του οργανισμού από τρίτους, ποια θα είναι η αξία τους;
- Ποιοι είναι οι κίνδυνοι στους οποίους εκτίθενται η εμπιστευτικότητα (confidentiality), η ακεραιότητα (integrity) και η διαθεσιμότητα (availability) των περιουσιακών στοιχείων του οργανισμού;
- Ποιες νομικές υποχρεώσεις συνδέονται με τις αποθηκευμένες πληροφορίες (πχ με τα PII's);

Υπάρχουν διαφόρων μεγεθών οργανισμοί. Οι μεγαλύτερου μεγέθους, μπορούν να αναπτύξουν στο εσωτερικό τους διαδικασίες CI ενώ οι οργανισμοί μικρότερων οικονομικών μεγεθών θα πρέπει να προσλάβουν εξωτερικούς συνεργάτες-επαγγελματίες για της εφαρμογή κανόνων CI.

## 2.14.4.2.Οι μέθοδοι εκτίμησης ρίσκου σύμφωνα με το NIST

Το Ινστιτούτο NIST (National Institute for Standards and Technology's) έχει δώσει 3 διαστάσεις ή μεθόδους στην εκτίμηση του ρίσκου ενός οργανισμού: Την Threat Assessment (Εκτίμηση Απειλής), την Vulnerability Assessment (Εκτίμηση Τρωτοτήτων) και την Impact Assessment (Εκτίμηση Επίπτωσης).

Σχετικά με την 1η Εκτίμηση, την Threat Assessment, ο οργανισμός, για να μην βρεθεί προ εκπλήξεως έχοντας την ψευδαίσθηση ότι δεν αποτελεί στόχο, θα πρέπει να μπορεί να πληροφορείται, για το εάν υπάρχουν απειλές, και αν υπάρχουν, ποια περιουσιακά στοιχεία θα μπορούσαν να βρεθούν στο στόχαστρο των επιτιθέμενων αλλά και τους λόγους για τους οποίους συμβαίνει κάτι τέτοιο. Όταν εντοπιστούν οι εν δυνάμει επιτιθέμενοι και οι οποίοι μπορεί να ανήκουν σε ομάδες τρομοκρατών, ακτιβιστών, εγκληματιών κλπ, ο οργανισμός θα πρέπει να διεξάγει αναλύσεις οι οποίες θα δείξουν τις προθέσεις, τα κίνητρα, τις αναλυτικές και τις τεχνικές τους ικανότητες και η οποία ανάλυση αποτελεί μία αέναη διαδικασία. Προσθέτοντας, ο οργανισμός θα πρέπει να υπολογίσει το κόστος των παράπλευρων ζημιών που θα έχουν προκληθεί από μία επίθεση και τις οποίες δεν είχαν υπολογίσει οι επιτιθέμενοι, ενώ στη συνέχεια θα πρέπει να κάνει μία εκτίμηση επίπτωσης στον οργανισμό στην περίπτωση υποκλοπής στοιχείων πνευματικής ιδιοκτησίας. Η Threat Assessment σε συνδυασμό με την Vulnerability Assessment, την οποία θα αναλύσουμε παρακάτω, μας παρέχει την λεγόμενη επιφάνεια επιθέσεων – attack surface, δηλ. τα σημεία στα οποία ο οργανισμός έχει πιθανότητα να δεχθεί επίθεση. Επίσης, υπάρχουν οι πολύ καλά εκπαιδευμένες και ενημερωμένες οι λεγόμενες Red Teams, οι οποίες μπορούν να «έρθουν» στη θέση των hackers, με την έννοια ότι μπορούν να προσεγγίζουν με μεγάλη ακρίβεια τον τρόπο με τον οποίο θα εκτελούνταν οι

επιθέσεις, όπως για παράδειγμα του να απαντηθούν κάποια ερωτήματα του τύπου: «Ποιους οργανισμούς μπορώ να στοχεύσω, βάσει των στρατηγικών του στόχων;» ή «Ποιους τρόπους και ποιες μεθόδους θα χρησιμοποιήσω στις επιθέσεις μου;». Με την βοήθεια των Red Teams, μπορούν να αποκαλυφθούν κίνητρα, προθέσεις, σημεία και δίοδοι επίθεσης, και άλλα υποθετικά σενάρια, τα οποία δεν έχουν ακόμη γίνει πραγματικότητα. Τέλος, βάσει των παρακάτω ερωτημάτων, θα μπορεί να αναπτυχθεί ένα πλαίσιο, το λεγόμενο I&W framework (Indications & Warnings framework):

- Πως ορίζονται τα περιβάλλοντα κινδύνων από τη Διοίκηση του οργανισμού, όταν η επιχείρηση λειτουργεί;
- Ποια είναι η οικονομική και η πολιτική εικόνα του οργανισμού σε κάθε ένα από τα περιβάλλοντα κινδύνων και ποιες ενδείξεις μαρτυρούν την ύπαρξη «ύποπτης» δραστηριότητας σε αυτά; Ποια αποτελέσματα στο μέλλον θα μπορούσαν να επηρεάσουν την λειτουργία της επιχείρησης;
- Η επιχείρηση, είναι ικανή στο να αποφύγει, να μετριάσει, να εξαλείψει τους κινδύνους;
- Υπάρχει κάποιος τρόπος με τον οποίο οι επιτιθέμενοι μπορούν να δημιουργήσουν πρόβλημα σε κάποια από τα περιβάλλοντα κινδύνου ή σε κάποιες λειτουργίες της επιχείρησης; Πχ πώς «στήνουν» μία απειλή, ή πως μπορούν να επιτεθούν με έμμεσο τρόπο όπως του να επιτεθούν σε έναν προμηθευτή (στην εφοδιαστική αλυσίδα) του οργανισμού; Τι τους οδήγησε στην υλοποίηση της επίθεσης και ποιες πιθανές αλλαγές στα περιβάλλοντα κινδύνου θα μπορούσαν να επηρεάσουν κάποιες άλλες αποφάσεις των επιτιθέμενων;
- Ποιες αλλαγές στην λειτουργία του οργανισμού θα μπορούσαν να αυξήσουν ή να μειώσουν την πιθανότητα επίθεσης;
- Ποιες είναι οι ικανότητες των επιτιθέμενων και ποια τα αρνητικά αποτελέσματα μίας επιτυχούς επίθεσης;

Με τη χρήση του παραπάνω πλαισίου (I&W), γίνεται εντοπισμός πιθανών μελλοντικών απειλών, οι οποίες στοχεύουν τις επιχειρηματικές δραστηριότητες της επιχείρησης. Το κλειδί εδώ είναι η ένταξη του I&W πλαισίου στο στρατηγικό και λειτουργικό/επιχειρησιακό επίπεδο. Για παράδειγμα, έστω ότι ένας οργανισμός, λόγω του αντικειμένου και των δραστηριοτήτων του, αποτελεί στόχο ακτιβιστών, για περιβαλλοντικούς λόγους. Έτσι, με τη χρήση του I&W πλαισίου, λαμβάνονται οι κατάλληλες πληροφορίες, στο στρατηγικό πλαίσιο. Επίσης, θα πρέπει να γνωρίζουμε ότι μία σωστή εφαρμογή του I&W πλαισίου ανιχνεύει διαρκώς τα περιβάλλοντα κινδύνου για «περίεργα» σημεία. Έτσι λοιπόν, ο συνδυασμός ενός I&W πλαισίου που εστιάζει στη συλλογή πληροφοριών με ένα άλλο πλαίσιο I&W σε επίπεδο λειτουργικό/επιχειρησιακό, ανιχνεύει επί καθημερινής βάσεως, τυχόν αλλαγές στο επιχειρησιακό περιβάλλον του οργανισμού.

Όλες οι δραστηριότητες του οργανισμού για την υλοποίηση του threat Assessment, δεν αποτελούν την απόλυτη και οριστική λύση, διότι δεν μπορούν να καλύψουν όλες τις πιθανές περιπτώσεις, με την απόλυτη έννοια. Όμως, είναι καλό οι ενέργειες του Threat Assessment, να συγκεκριμενοποιούνται και να στοχεύουν στην συλλογή πληροφοριών σχετικών με το αντικείμενο και τους στρατηγικούς στόχους του οργανισμού.

### 2.14.4.3.Οι μέθοδοι εκτίμησης τρωτοτήτων σύμφωνα με το NIST

Ο NIST προτείνει την εφαρμογή διαδικασιών εκτίμησης ή ανίχνευσης τρωτοτήτων στα υπολογιστικά συστήματα του οργανισμού με τη μορφή αναλύσεων, ενώ οι αναλύσεις του στρατηγικού CI, βοηθούν στην όλη διαδικασία. Με άλλα λόγια, εμπλέκονται οι ειδικοί του cyber security στην λειτουργία του οργανισμού στο επιχειρηματικό επίπεδο για να μπορέσουν να αποκτήσουν μία άποψη για τις υπάρχουσες τρωτότητες. Κύρια σημεία ενδιαφέροντος αποτελούν οι τρωτότητες του οργανισμού σε συγκεκριμένους τομείς στους οποίους δραστηριοποιείται ο οργανισμός αλλά και συνεργασίες του εν λόγω οργανισμού με άλλους. Όλα αυτά τα σημεία ενδιαφέροντος, μπορούν να καλυφθούν με την εκτίμηση της λεγόμενης «επιφάνειας επίθεσης» (“attack surface”).

Ο ορισμός της «επιφάνειας επίθεσης», σύμφωνα με τον Stephen Northcutt του Ινστιτούτου SANS είναι ***οι τρωτότητες που είναι και προσβάσιμες αλλά και εκμεταλλεύσιμες.*** Επίσης, ο ίδιος αναφέρει ότι υπάρχουν αρκετές κατηγορίες «επιφανειών επίθεσης», αλλά αυτές που πραγματικά αξίζει να ασχοληθούν οι ειδικοί της Κυβερνοασφάλειας συνοψίζονται στις εξής τρείς: Δίκτυο (Network), Λογισμικό (Software) και Άνθρωπος (Human). Υπάρχει και ένα άλλο μοντέλο «επιφάνειας επίθεσης», το οποίο χαρακτηρίζει έναν οργανισμό και είναι η «γεωγραφία» του οργανισμού. Αρκετοί οργανισμοί και φορείς έχουν υιοθετήσει το μοντέλο αυτό (δηλ τη «γεωγραφία») και μεταξύ των άλλων και ο U.S Cyber Command. Το μοντέλο της «γεωγραφίας» έχει και αυτό κάποιες εκδοχές, εκ των οποίων μία είναι η εξής: Ο Κυβερνοχώρος δεν είναι τίποτε άλλο από ένα σύνολο στρώσεων. Τα στρώματα αυτά είναι το «γεωγραφικό», το φυσικό στρώμα δικτύου, το λογικό στρώμα δικτύου, το στρώμα συσκευών, το στρώμα προσωπικοτήτων και το πραγματικό στρώμα διαφορετικών χρηστών.

Μπορούμε λοιπόν, να χρησιμοποιούμε είτε το μοντέλο SANS, ή το μοντέλο των 6 στρωμάτων. Όμως, όποιο από τα 2 και να επιλέξουμε, θα πρέπει να λάβουμε υπόψιν μας και τις «σχέσεις εμπιστοσύνης» ή «συνδέσμους» του οργανισμού με άλλους οργανισμούς, σε επαγγελματικό επίπεδο. Οι «σχέσεις εμπιστοσύνης» είναι, σύμφωνα με τον NIST, «μία πεποίθηση ότι μία ολότητα θα συμπεριφερθεί με έναν προβλέψιμο τρόπο κάτω από συγκεκριμένες συνθήκες». Στον όρο «εμπιστοσύνη», συνδέονται 3 χαρακτηριστικά: η «εμπιστοσύνη» συνδέεται με κάποια συγκεκριμένη περίπτωση, κατά γενική ομολογία δεν είναι μεταβατική και κερδίζεται ανάλογα της εμπειρίας και των μετρήσεων. Μπορούμε να πούμε ότι κατά την ανάλυση πληροφοριών στο στρατηγικό επίπεδο, θα πρέπει να λαμβάνουμε υπόψιν τους «συνδέσμους» ή τις «σχέσεις εμπιστοσύνης». Πχ οι ο οργανισμός στην περίπτωση που έχει αναπτύξει «σχέσεις εμπιστοσύνης» με μία άλλη εταιρεία, μπορεί να τεθεί σε κίνδυνο. Μετρήσεις έχουν δείξει ότι κάποιες εταιρίες, οργανισμοί ή εργοστάσια τα οποία απασχολούν λιγότερο από 1000 υπαλλήλους, αποτελούν τους πιο δύσκολους στόχους, στις περιπτώσεις επιθέσεων από τρίτους, για την υποκλοπή στοιχείων για λόγους βιομηχανικής αντικατασκοπείας. Αυτό λοιπόν το στοιχείο είναι ζωτικής σημασίας για τον οργανισμό, στην όλη διαδικασία εκτίμησης του κινδύνου.

Υπάρχει κάποιο standard το οποίο έχει θεσπιστεί και δεν είναι άλλο από το PPT’s (People, Process, Technology). Βάσει αυτού του standard, οι τρωτότητες ταξινομούνται σε Ανθρώπους, Διαδικασία και Τεχνολογία. Άρα λοιπόν, είτε χρησιμοποιήσουμε το μοντέλο της «επιφάνειας επίθεσης», ή το μοντέλο των 6 στρώσεων, θα πρέπει κάθε φορά να υπάρχει εκτίμηση των τρωτοτήτων σχετιζόμενων με τα PPT’s.Τέλος, να προσθέσουμε ότι υπάρχει και ο τριπλός στόχος “CIA”, δηλ Confidentiality (εμπιστευτικότητα), Integrity (Ακεραιότητα) και Availability (Διαθεσιμότητα) ο οποίος συνδυαζόμενος με τα PPT’s δίνει καλής ποιότητας αποτελέσματα, όσον αφορά την εκτίμηση των τρωτοτήτων.

## 2.14.4.4.Οι μέθοδοι εκτίμησης επιπτώσεων σύμφωνα με το NIST

Έως τώρα, είδαμε διάφορες μεθόδους και τεχνικές για την εκτίμηση των κινδύνων (Threat Assessment) και των τρωτοτήτων (Vulnerability Assessment). Στην 1η περίπτωση το στρατηγικό cyber intelligence αποτελούσε έναν οδηγό για την εφαρμογή συγκεκριμένων διαδικασιών ενώ στην 2η περίπτωση το στρατηγικό cyber intelligence ήταν ένα χρήσιμο εργαλείο στα χέρια των ειδικών cyber security. Μέχρι εδώ λοιπόν, όλα είναι καλά. Όμως, τι γίνεται στην περίπτωση που τελικά μία επίθεση πετύχει το στόχο της; Ποιες θα είναι οι επιπτώσεις της στον οργανισμό; Εδώ λοιπόν, το στρατηγικό cyber intelligence αποτελεί ένα εργαλείο στα χέρια της Διοίκησης, η οποία είναι και αρμόδια αλλά και υπεύθυνη για την εφαρμογή στρατηγικής και για τη διαχείριση των κινδύνων μέσω της ανάπτυξης και εφαρμογής πόρων για την υποστήριξη της. Όλες αυτές οι διαδικασίες θα πρέπει να ενημερώνονται από τις αναλύσεις του CI στοχεύοντας στη μείωση της αβεβαιότητας αλλά και στη βέλτιστη λήψη αποφάσεων. Και για να πετύχει η συνταγή, απαραίτητη προϋπόθεση είναι το να μπορεί η Διοίκηση να αντιλαμβάνεται τις επιπτώσεις μίας επιτυχούς επίθεσης, στην αποστολή αλλά και στο επιχειρηματικό επίπεδο του οργανισμού.

Μία από τις πιθανές εφαρμογές του στρατηγικού CI εδώ, είναι η ποσοτική ανάλυση κινδύνου. Σε αυτή, υπάρχουν στοιχεία του οργανισμού στα οποία «αναθέτονται» κάποια νούμερα, κάποιες αριθμητικές τιμές. Βάσει των αριθμητικών τιμών αυτών δημιουργούνται κάποια business cases με τον καλύτερο δυνατό τρόπο και από αυτά πηγάζουν διάφορες συζητήσεις για θέματα επενδύσεων.

Δεδομένου κάποιου συγκεκριμένου κινδύνου ή ρίσκου, υπάρχει ο λεγόμενος παράγοντας έκθεσης – EF (Exposure Factor) και ο λεγόμενος ρυθμός συμβάντων – ARO (Annual Rate Of Occurrence). Το EF μας πληροφορεί για την απώλεια/υποκλοπή κάποιου στοιχείου του οργανισμού σε επί τοις εκατό (%) ποσοστό σε περίπτωση επιτυχούς επίθεσης, ενώ το ARO μας πληροφορεί για το πόσες φορές μπορεί να συμβεί κάτι τέτοιο εντός του χρονικού πλαισίου ενός έτους. Υπολογίζεται η πιθανότητα εκμετάλλευσης μίας τρωτότητας, βάσει προθέσεων και ικανοτήτων των επιτιθέμενων, με τη βοήθεια αναλύσεων του στρατηγικού CI. Αφού έχει υπολογιστεί και το ARO, η Διοίκηση του οργανισμού υπολογίζει και ένα άλλο μέγεθος, το ALE-Annualized Loss Expectancy δηλ. του τι περιμένει, από στοιχεία, να χαθούν σε χρονικό διάστημα ενός έτους.

## 2.15.Το λειτουργικό/επιχειρησιακό επίπεδο του Cyber Intelligence

Σε αυτήν την παράγραφο θα μιλήσουμε για το λειτουργικό επίπεδο του Cyber Intelligence.Ας εξετάσουμε αρχικά τον ορισμό του, ο οποίος είναι ο εξής: Το λειτουργικό επίπεδο του Cyber Intelligence είναι αυτό στο οποίο υλοποιείται ο σχεδιασμός και η εφαρμογή ενεργειών οι οποίες σχετίζονται με την επίτευξη ορισμένων στόχων στρατηγικής σημασίας, εντός ορισμένου πεδίου δράσης. Ας δούμε λίγο τι μπορεί να σημαίνει αυτό και πως μπορεί να «μεταφραστεί» με τον καλύτερο δυνατό τρόπο. Στο επιχειρησιακό επίπεδο του Cyber Intelligence, έχουμε 2 αντίπαλα «στρατόπεδα»: Εκείνο των επιτιθέμενων και εκείνο των αμυνόμενων (δηλ το δικό μας). Στο αντίπαλο «στρατόπεδο», υπάρχουν διάφοροι κακόβουλοι χρήστες οι οποίοι, έχουν δικές τους διαδικασίες συλλογής πληροφοριών Intelligence,και βάσει αυτών, «χτίζουν» τα δικά τους όπλα, όπως botnets, malware, phising κλπ. Έχοντας χτίσει λοιπόν αυτά τα όπλα, κινούνται εντός του

Κυβερνοχώρου (CyberSpace) με σκοπό την επίτευξη των δικών τους στρατηγικών στόχων, δηλ την επίθεση και διείσδυση σε δίκτυα υπολογιστών άλλων οργανισμών. Τώρα, από τη μεριά του δικού μας «στρατοπέδου», το οποίο βρίσκεται σε κατάσταση άμυνας, υπάρχουν κάποιες ενέργειες Cyber Intelligence, ως απάντηση στις ενέργειες των επιτιθέμενων. Αυτές οι ενέργειες θα μπορούσαν να είναι:

- Κάποιες ειδικές αναλύσεις οι οποίες δείχνουν στο ποια είναι η κατεύθυνση στην οποία οι επιτιθέμενοι εξελίσσονται και βελτιώνουν τις γνώσεις τους, σε τεχνικό/τεχνολογικό επίπεδο.
- Κάποιες ενδείξεις, οι οποίες μας φανερώνουν κάποιες διόδους μέσω των οποίων οι hackers σχεδιάζουν να επιτεθούν στον οργανισμό (δηλ στο δικό μας «στρατόπεδο»).
- Κάποιες ενδείξεις ότι οι επιτιθέμενοι οργανώνονται και βελτιώνουν τις γνώσεις τους με σκοπό να στοχεύσουν κάποια συγκεκριμένα σημεία τρωτότητας του οργανισμού.
- Κάποια στοιχεία και πληροφορίες, τα οποία αποκαλύπτουν τις τεχνικές, τις τακτικές και τις διαδικασίες του αντίπαλου «στρατοπέδου».
- Η κατανόηση του πως λειτουργεί ο λεγόμενος επιχειρησιακός κύκλος (operational cycle) του αντίπαλου «στρατοπέδου». Αυτός ο κύκλος περιλαμβάνει λήψεις αποφάσεων, αλλά και τεχνικές τύπου command and control και έχει αναφορά και στην τεχνολογία που χρησιμοποιείται αλλά και στο προσωπικό (δηλ τις ομάδες των επιτιθέμενων).
- Η γνώση κάποιων τρωτοτήτων του αντίπαλου «στρατοπέδου», σε τεχνικό, οικονομικό, νομικό, κοινωνικό, τεχνικό ή οποιοδήποτε άλλο επίπεδο.
- Κάποιες πληροφορίες τις οποίες χρησιμοποιεί το δικό μας «στρατόπεδο» για να ασκήσει αρνητική επιρροή στους επιτιθέμενους, καθώς αυτοί κινούνται μέσα στην «αλυσίδα θανάτου» (kill chain).

Όπως έχουμε προαναφέρει, στο στρατηγικό επίπεδο του Cyber Intelligence δεν εντάσσονται οι CIO's και CISO's, κυρίως για οικονομικούς λόγους. Όμως, εντάσσονται σε αυτό το επίπεδο, δηλ. στο επιχειρησιακό/λειτουργικό επίπεδο. Οι CIO's και CISO's είναι υπεύθυνοι για μία λίστα ενεργειών όπως:

- Την υποστήριξη νέων προσπαθειών, για την βελτίωση της άμυνας του οργανισμού.
- Την σωστή διαχείριση και κατανομή των διάφορων συστημάτων και τεχνολογιών πληροφορικής (δηλ το τι θα πρέπει να κάνει ο καθένας και ποιο είναι το πεδίο δράσης του) με σκοπό την επίτευξη ορισμένων στόχων.
- Την ανάλυση των malwares. Η ανάλυση αυτή δεν έχει ως μοναδικό στόχο το ίδιο το malware (δηλ το πώς λειτουργεί) αλλά και το ποιος κρύβεται πίσω από την κατασκευή του, και ποιες οι τεχνικές/τεχνολογικές γνώσεις τον χαρακτηρίζουν. Με αυτόν τον τρόπο, θα μπορεί το αμυνόμενο στρατόπεδο να βρίσκεται ένα βήμα μπροστά από κάποια μελλοντική επίθεση.
- Ο σχεδιασμός της άμυνας, ο οποίος βασίζεται σε πληροφορίες Intelligence, αποτελεί θα λέγαμε την πρόληψη και όχι την θεραπεία, σε περιπτώσεις εμφάνισης Κυβερνοεπιθέσεων.

## 2.16.Το επίπεδο τακτικής του Cyber Intelligence

Εδώ πλέον, θα μιλήσουμε για το επίπεδο τακτικής. Πρώτα από όλα, θα πρέπει να δώσουμε τον ορισμό του, ο οποίος έχει ως εξής: Το επίπεδο τακτικής είναι αυτό στο οποίο λαμβάνουν χώρα ενέργειες επίθεσης και άμυνας, όπου και οι επιτιθέμενοι αλλά και οι αμυνόμενοι κινούνται επάνω στην «σκακιέρα» και ο καθένας εφαρμόζει τις δικές του τακτικές, επίθεσης ή άμυνας αντιστοίχως, προκειμένου να επιτευχθούν ορισμένοι στόχοι. Για παράδειγμα, οι επιτιθέμενοι χρησιμοποιούν botnets για την εξαπόλυση κάποιας επίθεσης. Ή ανακαλύπτουν κάποια τρωτότητα σε ένα δίκτυο υπολογιστών ενός οργανισμού και προσπαθούν να εκμεταλλευτούν την τρωτότητα αυτή. Ή αν καταφέρουν να διεισδύσουν εντός των υπολογιστικών συστημάτων ενός οργανισμού, αντιγράφουν τα δεδομένα, τα κρυπτογραφούν και να εξάγουν σε δικά τους υπολογιστικά συστήματα. Εδώ τονίζουμε ότι εάν στα 2 προηγούμενα επίπεδα (στρατηγικό και επιχειρησιακό/λειτουργικό) είχε δοθεί (από τη Διοίκηση) και η απαιτούμενη προσοχή αλλά και η απαιτούμενη χρηματοδότηση, κάποιες από τις επιθέσεις των κακόβουλων χρηστών θα είχαν αποκρουστεί και με αυτόν τον τρόπο ο οργανισμός θα κινδύνευε λιγότερο.

Στην «σκακιέρα» δεν υπάρχουν μόνο οι επιτιθέμενοι αλλά και οι αμυνόμενοι. Οι τελευταίοι, έχουν τα δικά τους Κέντρα Επιχειρήσεων, τα οποία δεν είναι άλλα από τα NOC's (Network Operations Centers) και SOC's (Security Operations Centers). Σε αυτά, έχουμε ενέργειες όπως η δημιουργία ειδοποιήσεων (alerts) σε συστήματα βασιζόμενα σε hosts (host-based), αναγνώριση ψηφιακών υπογραφών και σε περισσότερο πολύπλοκες περιπτώσεις, διεξάγονται αναλύσεις βάσει του kill chain είτε για περιπτώσεις γνωστών επιτιθέμενων ή για περιπτώσεις συνηθισμένων συγκεκριμένων μοτίβων.

Φυσικά, και στα 3 επίπεδα του Cyber Intelligence, γίνεται χρήση πληροφοριών CI, προκειμένου οι διαδικασίες να έχουν πετύχει το βέλτιστο αποτέλεσμα. Θα δώσουμε ένα παράδειγμα χρήσης μίας πληροφορίας CI, η οποία αποκτά πρακτικό ενδιαφέρον. Έστω ότι σε ένα NOC έχει γίνει αντιληπτή μία τρωτότητα στα υπολογιστικά συστήματα ενός οργανισμού, η οποία είναι επιρρεπής σε DDos επιθέσεις και την οποία θα μπορούσαν να εκμεταλλευτούν ορισμένοι hackers για να επιτεθούν στο δίκτυο υπολογιστών. Όμως, σε πολλές περιπτώσεις, οι hackers αυτοί είτε καταβάλουν μικρή προσπάθεια να αποκρύψουν το πότε θα ξεκινήσουν την επίθεση ενώ κάποιες άλλες ομάδες επιτιθέμενων το διαφημίζουν κιόλας! Άρα λοιπόν, το προσωπικό ενός NOC, γνωρίζει εκ των προτέρων και για την επίθεση αλλά και για το πότε θα συμβεί, δηλ γνωρίζει το λεγόμενο «παράθυρο του χρόνου» της εν λόγω επίθεσης. Έτσι, σε συνεργασία με τον αντίστοιχο πάροχο Internet (ISP-Internet Service Provider), γίνεται μία ανακατεύθυνση των «πακέτων» πληροφορίας, τα οποία προέρχονται από τους επιτιθέμενους και ουσιαστικά ο ISP μπλοκάρει ορισμένα δεδομένα και κατά αυτόν τον τρόπο, μετριάζεται η αρνητική επίπτωση μίας επίθεσης στον εν λόγω οργανισμό.

## 2.17. Αποτυχία του κλασσικού τρόπου άμυνας και η έννοια του cyber threat intelligence

Δυστυχώς, ο κλασσικός αυτός τρόπος άμυνας, αποτυγχάνει σε 3 επίπεδα: Στο επίπεδο τακτικής, στο επίπεδο λειτουργίας και στο επίπεδο στρατηγικής.

***Επίπεδο τακτικής:*** Η δημιουργία μεγάλου όγκου «συναγερμών» (alerts) έχει ως αποτέλεσμα την σύγχυση της ομάδας SOC στο να ανιχνεύσουν και να διαχωρίσουν τις επικίνδυνες απειλές από τις όχι και τόσο επικίνδυνες.
***Επίπεδο λειτουργίας:*** Καταναλώνεται αρκετός χρόνος από την IRT ομάδα για την ανεύρεση πολύτιμων πληροφοριών με τις οποίες γίνεται, όπως αναφέραμε, η ανασύνθεση των ζωτικών στοιχείων μίας επίθεσης και οι ενέργειες άμυνας για αυτή.
***Επίπεδο στρατηγικής:*** Η Διοίκηση του οργανισμού, δεν έχει την κατάλληλη πληροφόρηση για να μπορέσει να θέσει προτεραιότητες σχετικές με τη χρηματοδότηση για το που θα πρέπει να ελεγχθεί ο τραπεζικός οργανισμός και ποια σημεία της άμυνας του θα πρέπει να ενισχυθούν. Και φυσικά, υπάρχουν και υπερβολές σε ότι αφορά την ασφάλεια, στις οποίες δεν θα πρέπει να σπαταλούνται πόροι του οργανισμού.

Είδαμε ότι στο επίπεδο τακτικής υπάρχει ένας μεγάλος όγκος «συναγερμών» ο οποίος δημιουργεί αρκετά προβλήματα. Σύμφωνα με μία μελέτη του Ινστιτούτου Ponemon, έχει υπολογιστεί ότι:

- Ένας μέσος οργανισμός λαμβάνει περίπου 16.937 alerts ανά εβδομάδα.
- Από αυτά, μόνο το 19%, δηλ. τα 3.218 alerts χρήζαν περισσότερης μελέτης.
- Από τα τελευταία, μόνο τα 705, δηλ. το 4%, τέθηκε υπό έρευνα.
- Το κόστος απόκρισης σε «εσφαλμένα» alerts ανέρχεται σε 1,27 εκατομμύρια $ ανά χρόνο.

Στην «πλημμύρα» αυτή των alerts, μπορούμε να αναφέρουμε ένα περιστατικό κατά το οποίο μία εταιρεία λιανικού εμπορίου δέχθηκε επίθεση και από τα συστήματα προστασίας της παράχθηκαν περίπου 60.000 alerts σε διάρκεια περίπου 3,5 μηνών. Το ερώτημα που γεννιέται εδώ είναι γιατί η εταιρεία δεν αποκρίθηκε νωρίτερα στο συμβάν αυτό. Η απάντηση είναι ότι για να παραχθούν 60.000 alerts στην εταιρεία υλοποιήθηκαν 60.000 entries και κάθε ένα entry από αυτά δημιουργεί περίπου 100 protection log files, άρα μιλάμε για περίπου 6.000.000 log entries αρχεία, και φυσικά το πρόβλημα είναι το εξής: Σε ποιο από όλα αυτά τα log files θα μπορούσε κάποιος να ψάξει;
Στην εικόνα 2.11 βλέπουμε κλασσικά προβλήματα από τα οποία υποφέρει η Κυβερνοάμυνα και πως η cyber threat intelligence βοηθάει στην αντιμετώπιση τους.

| | Tactical Level | Operational Level | Strategic Level |
|---|---|---|---|
| IT Roles | Network Operations Center (NOC)<br>Infrastructure Operations<br>Security Operations Center (SOC) | Incident Response (IR) Team<br>Security Forensics<br>Fraud Detection | Chief Information Security Officer (CISO)<br>IT Management |
| Tasks | Feed indicators to security products<br>Patch vulnerable systems<br>Monitor, escalate alerts (triage) | Determine details of attacks<br>Remediate<br>Hunt for additional breaches | Allocate resources<br>Communicate with executive management |
| Problems | Unverified indicators cause false positives<br>Difficult to prioritize patches<br>Too many alerts to investigate | Time-consuming to reconstruct attacks from initial indicators<br>Difficult to identify damage and additional breaches | No clear priorities for investment<br>Executives do not understand technical issues |
| Value of Cyber Threat Intelligence | Validate and prioritize indicators<br>Prioritize patches<br>Prioritize alerts | Provide "context" to reconstruct attacks quickly<br>Provide data to identify damage & related breaches | Provide priorities based on business risks and likely attacks<br>"Put a face" on adversaries and threats |

(Εικόνα 2.11: Τυπικά προβλήματα Κυβερνοάμυνας και πως η cyber threat intelligence βοηθάει στην αντιμετώπιση τους)

Ουσιαστικά βλέπουμε ότι υπάρχει μία φιλοσοφία υλοποίησης προτεραιοτήτων όπως και παροχή χρήσιμων πληροφορίων, σύμφωνα με την εικόνα 4.1. Τελικά, βγαίνει ένα πολύτιμο συμπέρασμα: Είναι αδύνατη η άμυνα έναντι Κυβερνοεπιθέσεων χωρίς προηγούμενη γνώση των προθέσεων και των μεθόδων που ακολουθούν οι επιτιθέμενοι. Εδώ λοιπόν, δίνουμε τον ορισμό του cyber threat intelligence:

***Η cyber threat intelligence είναι η γνώση που περικλείει πληροφορίες για τους επιτιθέμενους και τα κίνητρα τους, τις προθέσεις τους και τις μεθόδους τους και οι οποίες πληροφορίες συλλέγονται, αναλύονται και διαδίδονται με τρόπους που βοηθούν το προσωπικό Κυβερνοασφάλειας όλων των επιπέδων να προστατεύει τους κρίσιμους τομείς ενός οργανισμού.***

## 2.18. Γενικά στοιχεία για τη συλλογή των πληροφοριών

Σε αυτό το σημείο, θα κινηθούμε σε 2 βασικούς άξονες: Θα αναφερθούμε στα τρία είδη πληροφοριών του threat intelligence αλλά και θα δούμε πως συλλέγονται πληροφορίες από κάθε είδος. Εδώ, θα παραθέσουμε και μία φράση του Sherlock Holmes, η οποία σχετίζεται με το εν λόγω κεφάλαιο: *"Data!Data!Data! he cried impatiently. I can't make bricks without clay."*

Αντιλαμβανόμαστε λοιπόν, ότι ναι μεν ότι οι πληροφορίες που μπορούμε να αντλήσουμε δεν αποτελούν οι ίδιες το ίδιο το intelligence, όμως, αποτελούν την πρώτη ύλη για αυτό. Δηλαδή, για να παραχθούν δεδομένα intelligence, χρησιμοποιούμε πληροφορίες ως πρώτη ύλη.

Οι πηγές των πληροφοριών αυτών, τις οποίες και αντλούμε, είναι κυριολεκτικά άπειρες. Υπάρχουν terabytes τέτοιων πληροφοριών ευρισκόμενα πχ σε ψηφιακές υπογραφές κακόβουλων λογισμικών και σε βάσεις δεδομένων οι οποίες περιέχουν αρχεία log. Το αρνητικό σενάριο που συνήθως συμβαίνει σε περιπτώσεις εφαρμογής threat intelligence από επαγγελματίες του είδους, είναι το ότι οι τελευταίοι δεν εκμεταλλεύονται στο έπακρο, τις παρεχόμενες σε αυτούς, πληροφορίες. Παρακάτω, στην εικόνα 2.12, παραθέτουμε τις 3 κατηγορίες αυτών των πληροφοριών.

| | Threat Indicators | Threat Data Feeds | Strategic Cyber Threat Intelligence |
|---|---|---|---|
| Content | File hashes and reputation data | Statistics, trends, survey data, and analyses of malware | Information on adversaries and their motivations, intentions, tactics, techniques, and procedures |
| Key Uses | Increase the effectiveness of blocking technologies and generate alerts | Help SOC and IR teams identify patterns associated with attacks | Help IR and forensics teams analyze attacks, hunt for breaches, and remediate; help managers improve defenses and invest strategically |
| Primary Sources | Honeypots and scanners on networks | Statistical analyses of indicators, surveys, and sandboxing products | Hacker web forums, underground marketplaces, and personal contacts |

(Εικόνα 2.12:Οι 3 κατηγορίες πληροφοριών («πρώτης ύλης»))

## 2.18.1.Το πρώτο επίπεδο: Δείκτες απειλών (threat indicators)

Στο 1° επίπεδο έχουμε λοιπόν τους δείκτες απειλών. Και θα ρωτούσε κάποιος, τι ακριβώς είναι οι δείκτες απειλών; Η απάντηση είναι ότι ένας δείκτης απειλής ή IOC (Indicator Of Compromise) είναι μία ολότητα (entity) η οποία μας δείχνει την πιθανότητα μίας επίθεσης. Εδώ υπάρχουν 2 συνήθεις υποκατηγορίες: Οι ψηφιακές υπογραφές (file hashes) και τα «δεδομένα φήμης» (reputation data). Τα τελευταία σχετίζονται με IP's και domains που έχουν υποστεί επίθεση.

Ας δούμε λίγο τι είναι ένα file hash. Ένα file hash είναι ένα αρχείο το οποίο έχει την ικανότητα να αναγνωρίζει ένα συγκεκριμένο τύπο ιού όπως για παράδειγμα rootkit, Trojan, keylogger, worm. Υπάρχουν αλγόριθμοι συνήθως του τύπου MD5 ή SHA-1, οι οποίοι εμπεριέχονται σε διάφορα αρχεία και δημιουργούν ένα μοναδικό «αποτύπωμα» (fingerprint) το οποίο βασίζεται σε μία σειρά από bytes των αρχείων αυτών. Το δε αποτέλεσμα είναι ουσιαστικά ένα text string το οποίο μπορεί να έχει τη μορφή πχ **15901ddbccc5e9e0579fc5b42f754fe8**.

Ας δούμε τώρα και τα reputation data λίγο. Αυτά αφορούν πληροφορίες, σύμφωνα με τις οποίες διάφορα sites (URL's, IP's, domains) ή υπολογιστικά συστήματα, έχουν «βαθμολογηθεί» σύμφωνα με το είδος και την έκταση της επίθεσης που έχουν υποστεί. Έχει δοθεί υψηλή «βαθμολογία» σε sites και σε υπολογιστικά συστήματα τα οποία σχετίζονται με:

- Malware και spyware
- Spam
- Phishing και άλλες απάτες
- Δίκτυα P2P και ανώνυμα εργαλεία proxy
- Servers τύπου C&C (Command and Control) οι οποίοι χειρίζονται διάφορα botnets
- Servers οι οποίοι εξάγουν ορισμένα δεδομένα
- Διευθύνσεις IP οι οποίες είναι μη ανιχνεύσιμες (το λεγόμενο darknet)

Την «βαθμολογία» που αναφέραμε προηγουμένως, δεν την λαμβάνουν μόνο τα προαναφερθέντα υπολογιστικά συστήματα και sites, αλλά και αυτά τα οποία έχουν μολυνθεί από κάποιο ιό και βρίσκονται εν μέρει υπό τις εντολές και τον έλεγχο κακόβουλων χρηστών. Μιλώντας για δείκτες, θα πρέπει να τονίσουμε ότι κάποιοι από αυτούς αποτελούν σοβαρές ενδείξεις για το ότι ένα σύστημα ή μία ιστοσελίδα έχει υποστεί επίθεση και κάποιοι άλλοι απλώς μας παρέχουν μία εικόνα πιθανοτήτων, σύμφωνα με τις οποίες μπορεί μία επίθεση να λάβει χώρα σε μελλοντικό χρόνο. Και μιλώντας για πιθανότητα, εννοούμε ότι για παράδειγμα έχοντας μία ιστοσελίδα από την οποία μπορεί ένας χρήστης να κατεβάζει διάφορα apps, τα apps αυτά μπορεί να είναι μολυσμένα από κάποιο ιό και θεωρούνται ύποπτα αλλά δεν είναι σίγουρο ότι θα είναι. Απλώς, υπάρχει μία πιθανότητα για το ότι μπορεί να περιέχουν κακόβουλο λογισμικό.

## 2.18.2.Πηγές τεχνικών πληροφοριών: Honeypots και scanners

Υπάρχουν χρήσιμα εργαλεία τα οποία κρίνονται απαραίτητα στην εφαρμογή του cyber intelligence. Εδώ λοιπόν έχουμε να κάνουμε με τα honeypots και τα scanners. Η φιλοσοφία των honeypots είναι η εξής: Στήνονται κάποια δίκτυα υπολογιστών τα οποία μιμούνται τη λειτουργία κάποιων ιστοσελίδων τα οποία προσελκύουν επιθέσεις, ενώ υπάρχουν και ειδικά προγράμματα-σένσορες, τα οποία καταγράφουν ή καλύτερα συλλέγουν δεδομένα (αρχεία και e-mails). Μετέπειτα, ακολουθούνται οι διαδικασίες scanning, κατά τις οποίες ειδικοί στον τομέα του cyber security/intelligence υποβάλουν τα αρχεία αυτά σε μία σειρά δοκιμών. Οι δοκιμές αυτές είτε

είναι σε μορφή **στατικής ανάλυσης**, όπου εξετάζεται ο κώδικας των αρχείων αυτών για να του δοθεί μία ερμηνεία στο τι λειτουργίες θα μπορούσε να εκτελέσει, είτε σε μορφή **δυναμικής ανάλυσης/ανάλυσης συμπεριφοράς**, όπου εκεί αφήνεται σκοπίμως να «τρέξει» το κακόβουλο λογισμικό για να εξεταστεί η συμπεριφορά του αλλά κα το πώς αλληλοεπιδρά με το σύστημα. Και τελικά, εάν σε κάποια από τις αναλύσεις βγει το πόρισμα ότι πρόκειται για κακόβουλο λογισμικό, τότε αυτό καταγράφεται και δημιουργείται μία ψηφιακή υπογραφή.

Από τα honeypots ουσιαστικά συλλέγονται διάφορα URL's τα οποία στη συνέχεια μελετώνται προκειμένου να διαπιστωθεί εάν οι ιστοσελίδες που σχετίζονται με αυτά έχουν μολυνθεί από κάποιο ιό ή βρίσκονται υπό τον έλεγχο κακόβουλων χρηστών. Επίσης, τα διάφορα e-mails τα οποία συλλέγονται από τα honeypots, μπαίνουν στο μικροσκόπιο και βάσει του αν περιέχουν διάφορα «περίεργα» στοιχεία, όπως ορισμένες λέξεις-κλειδιά, γνωστά links που οδηγούν σε ήδη γνωστά phising sites και τίτλους με «περίεργη» ορθογραφία, αυτομάτως βγαίνει το συμπέρασμα ότι τα e-mails αυτά είναι φορείς κακόβουλου λογισμικού. Βέβαια, υπάρχουν 2 τύποι ταξινόμησης, όσον αφορά τα honeypots.

***Η πρώτη ταξινόμηση*** διαχωρίζει τα honeypots αναλόγως με το αν έχουμε τα server-side honeypots ή τα client-side honeypots. Τα server-side honeypots έχουν αφήσει ανοικτές μία ή περισσότερες πόρτες (ports) και εκθέτουν διάφορα apps και προσπαθούν να αντιληφθούν με παθητικό τρόπο τυχόν επιθέσεις σε αυτά από κακόβουλους χρήστες και σε περίπτωση που συμβεί κάτι τέτοιο, αναλύουν τις εισερχόμενες απειλές και βρίσκουν διάφορα αρχεία, όπως worms και bots, τα οποία χρησιμοποιούνται από τους hackers για να εντοπίζουν υποψήφια θύματα. Η κατηγορία των server-honeypots ανήκει στα «κλασσικά» honeypots. Η κατηγορία των client-side-honeypots ή honeyclients για συντομία, χρησιμοποιούνται για να εντοπίζουν επιθέσεις σε εφαρμογές πελατών ή client applications αγγλιστί. Ένα client application είναι για παράδειγμα ένας web browser και γενικότερα είναι κάποιο λογισμικό το οποίο επικοινωνεί με έναν server και το οποίο μπορεί να έχει και κάποια plugins. Εδώ, τα honeyclients εντοπίζουν τυχόν περίεργη συμπεριφορά του server ή του περιεχομένου του server ο οποίος τροφοδοτεί με δεδομένα το client application. Ουσιαστικά, ανιχνεύει επιθέσεις στους browsers και στα plugins τους, οι οποίες ξεκινούν από διάφορες ιστοσελίδες.

***Η δεύτερη ταξινόμηση*** διαχωρίζει τα honeypots σε low interaction και high interaction honeypots. Τα low interaction ή «χαμηλής αλληλεπίδρασης» honeypots μιμούνται κάποια resources αλλά υπάρχει ένας περιορισμός στην μίμηση αυτή, κάτι το οποίο αποτελεί μία ειδοποιό διαφορά μεταξύ ενός resource honeypot και ενός αληθινού resource. Αυτό δυστυχώς περιορίζει και την αλληλεπίδραση του επιτιθέμενου με το honeypot και δεν αντλούνται επαρκείς πληροφορίες για αυτόν, αλλά μπορεί και ο ίδιος να αντιληφθεί ότι το resource στο οποίο επιτίθεται είναι ένα honeypot και να τερματίσει νωρίς την επίθεση του. Ένα άλλο αρνητικό είναι το ότι τα low interaction honeypots δεν μπορούν να εντοπίζουν απειλές τύπου 0-day. Στα θετικά τους στοιχεία, συγκαταλέγονται η εύκολη σύνταξη κώδικα και συντήρηση του, αλλά και η μείωση του ρίσκου του συστήματος, λόγω της χαμηλής αλληλεπίδρασης με τον επιτιθέμενο. Τα high interaction honeypots ΔΕΝ μιμούνται resources, αλλά παρέχουν αληθινά συστήματα, λειτουργικά και resources, αλλά παρόλα αυτά υπάρχουν και τρόποι να υπάρξει αλληλεπίδραση με τον επιτιθέμενο, μέσα σε ένα εικονικό περιβάλλον. Τα θετικά σημεία εδώ είναι το ότι επειδή χρησιμοποιούνται αληθινά συστήματα, παρατηρείται μία περισσότερο «αληθινή» συμπεριφορά των συστημάτων αυτών, ανιχνεύονται απειλές 0-day, και λαμβάνονται περισσότερα και αναλυτικότερα δεδομένα, σε σχέση με αυτά των low interaction honeypots. Στα αρνητικά συγκαταλέγονται ο περιορισμός στην ανίχνευση απειλών (αφού στο honeypot λειτουργεί ένα συγκεκριμένο app την συμπεριφορά του οποίου σε μία επίθεση, δεν θα μπορούσαμε να γενικεύσουμε για τις παλιότερες ή νεότερες εκδόσεις του), η πολυπλοκότητα (βάσει της οποίας δεν μπορούμε εύκολα να αποφανθούμε ποιανών στοιχείων ή συστημάτων η συμπεριφορά

χαρακτηρίζεται ως ύποπτη-πχ ενέργειες read/write σε έναν σκληρό δίσκο προέρχονται από κάποιον νόμιμο χρήστη ή είναι προϊόν επίθεσης;), και η περίπτωση του να τεθεί σε κίνδυνο το αληθινό σύστημα, καθώς ο έλεγχος του θα μπορούσε να ξεφύγει.

Υπάρχουν και τα υβριδικά honeypots τα οποία αποτελούν συνδυασμό των low και high interaction honeypots, συνδυάζοντας τα πλεονεκτήματα και των δύο. Και από αυτά, υπάρχουν και τα server-side (πχ SurfCERT IDS, SGNET) και τα client-side (πχ HoneySpider Network). Για παράδειγμα, στην περίπτωση του SGNET, υπάρχει ένα high interaction server-side honeypot, το οποίο «εκπαιδεύεται» στο πώς να διαχειρίζεται «ύποπτη» κίνηση στο δίκτυο. Αφού έχει «εκπαιδευτεί», η «ύποπτη» κίνηση, διοχετεύεται σε low interaction server-side honeypot, και με αυτόν τον τρόπο επιτυγχάνεται και καλή ανίχνευση αλλά και επίδοση.

Προσθέτουμε ένα ακόμη όπλο στη φαρέτρα των ειδικών του intelligence: Υπάρχουν διάφορα προγράμματα τα οποία εκτελούν λειτουργίες scanning σερφάροντας το Διαδίκτυο και ανιχνεύουν servers οι οποίοι δείχνουν σημάδια ότι έχουν υποστεί κακόβουλες επιθέσεις.

Τελικά, μετά από όλες τις παραπάνω διαδικασίες, οι ειδικοί «βαθμολογούν» τα διάφορα URL's, IP's και domains, βάσει των αποτελεσμάτων των άνωθι διαδικασιών.

### 2.18.3.Πηγές πληροφόρησης από τη βιομηχανία

Συνήθως, οι περισσότερες εταιρείες και οργανισμοί οι οποίοι θέλουν να συμπεριλάβουν στην όλη λειτουργία τους και διαδικασίες cyber intelligence αλλά δεν έχουν τους αντίστοιχους πόρους, καταφεύγουν σε άλλου είδους λύσεις, όπως η άντληση πληροφοριών από τις εξής πηγές:

- Εταιρείες ανάπτυξης λογισμικών antivirus
- Εταιρείες με αντικείμενο το cyber intelligence
- Εργαστήρια και ομάδες ειδικών επάνω στον τομέα του cyber security
- Πάροχοι πληροφοριών σε θέματα cyber security και malware
- Κυβερνήσεις κρατών και διάφορες βιομηχανίες οι οποίες παρέχουν πληροφόρηση αυτού του είδους

## 2.19.Το δεύτερο επίπεδο: Η τροφοδοσία πληροφοριών σχετικών με ψηφιακές απειλές

Εδώ οι πληροφορίες που λαμβάνονται συσχετίζονται με τους δείκτες απειλών αλλά και τους αναλύουν. Με αυτόν τον τρόπο, οι ομάδες IR ανιχνεύουν μοτίβα επιθέσεων και μπορούν να κατανοούν καλύτερα την συμπεριφορά των κακόβουλων λογισμικών.

### 2.19.1. Στατιστική, αναφορές και έρευνα

Στατιστική: Μπορούν να βρεθούν πολλές πηγές πληροφόρησης οι οποίες να σχετίζονται με malwares, spams, botnets κλπ. Αυτές συνήθως αφορούν την βιομηχανία αλλά και επαγγελματίες που ασχολούνται με θέματα security. Για παράδειγμα, για θέματα στατιστικής ή malware, υπάρχουν sites των διάφορων εταιρειών με προϊόντα antivirus αλλά και κάποιες ιστοσελίδες των οποίων τα στοιχεία παραθέτουμε στο Παράρτημα 1.

## 2.19.2. Αναφορές και έρευνες

Υπάρχουν διάφορες αναφορές οι οποίες άπτονται των παρακάτω θεμάτων:

- Στατιστικά στοιχεία για διαφορετικούς τύπους επιθέσεων
- Διάφορα στοιχεία από την εμπειρία των ομάδων IT, σχετικά με αποφάσεις που είχαν ληφθεί σε θέματα security
- Στοιχεία αναλύσεων από ειδικούς

Παραθέτουμε κάποιες πηγές πληροφόρησης, στο Παράρτημα 1.

Παρόλα αυτά, θα πρέπει να επισημάνουμε το ότι στις παραπάνω αναφορές υπεισέρχεται και μία δόση μεροληψίας, την οποία και θα πρέπει να λάβουμε σοβαρά υπόψιν μας. Αυτή η μεροληψία αναφέρεται κυρίως σε 2 πλαίσια: Στο δειγματοληπτικό πλαίσιο, όπου μία συγκεκριμένη αναφορά σχετίζεται με μέγεθος δείγματος εντελώς διαφορετικό από το δικό μας, και στο υποκειμενικό πλαίσιο, στο οποίο οι αναφορές καθώς γράφονται από άτομα, υπάρχει κίνδυνος απόκρυψης της αντικειμενικής αλήθειας, για να μην υπάρξει παραδοχή του πόσο επικίνδυνη μπορεί να είναι η κατάσταση σε τέτοιου είδους θέματα.

## 2.19.3.Ανάλυση malware

Υπάρχουν διάφοροι τρόποι ανάλυσης των malwares οι οποίοι στοχεύουν στη μελέτη της συμπεριφοράς τους και στην εξαγωγή συμπερασμάτων σχετικών με τις προθέσεις των επιτιθέμενων. Ένας από τους τρόπους ανάλυσης, ο οποίος είναι αυτοματοποιημένος αλλά περιέχει και αρκετή λεπτομέρεια, είναι η τεχνολογία sandboxing και η οποία ανήκει στην οικογένεια των δυναμικών τρόπων ανάλυσης. Ουσιαστικά, μελετάται η συμπεριφορά ενός «ύποπτου» αρχείου σε ένα απομονωμένο, από το κανονικό δίκτυο Η/Υ μίας εταιρείας, περιβάλλον, όπου σκοπίμως αφήνεται αυτό το αρχείο να «δράσει», και έτσι, από το sandboxing πηγάζουν χρήσιμα συμπεράσματα σχετικά με τη «δράση» του εν λόγω αρχείου, τα οποία μπορεί να είναι:

- «Είσοδοι» του αρχείου αυτού σε σημεία registry
- Απενεργοποίηση των antivirus προγραμμάτων
- Αναζήτηση αρχείων τα οποία περιέχουν λέξεις-κλειδία όπως “admin” ή “password”
- Εντολές ελέγχου για servers
- Σύνδεση με servers για άντληση πληροφοριών

Έτσι λοιπόν, έχοντας τις παραπάνω πληροφορίες όχι μόνο αναγνωρίζουμε ότι ένα αρχείο είναι κακόβουλο, αλλά ανιχνεύουμε και κατανοούμε τους σκοπούς και τους τρόπους των επιτιθέμενων. Όμως, θα πρέπει να έχουμε υπόψιν ότι τα διάφορα malwares νέας γενιάς, μπορούν να «ξεγελάσουν» την τεχνολογία sandboxing και μπαίνουν σε λειτουργία μόνο αν «καταλάβουν» την ύπαρξη ανθρώπινης δραστηριότητας (πχ mouse clicks) ή αν αναγνωρίσουν ότι βρίσκονται σε ένα desktop χρήστη και όχι σε εικονικό περιβάλλον (όπως το sandboxing). Άρα το sandboxing δεν αποτελεί την οριστική λύση για την ανίχνευση απειλών.

## 2.20.Το τρίτο επίπεδο: Ορισμένες καλές τακτικές

Η έννοια των καλών τακτικών είναι ουσιαστικά η συγκέντρωση του όγκου των πληροφοριών οι οποίες αφορούν συγκεκριμένους επιτιθέμενους αλλά τους κινδύνους που δημιουργούνται από αυτές τις επιθέσεις.

### 2.20.1.Παρακολουθώντας το Dark Web

Υπάρχει το λεγόμενο Dark Web, το οποίο αποτελεί ένα διαφορετικό και άγνωστο «κομμάτι» του Web, για τους περισσότερους και καθημερινούς χρήστες. Στο Dark Web λαμβάνουν χώρα δραστηριότητες κατά τις οποίες ανταλλάσσονται πληροφορίες για παράνομες συναλλαγές και γενικότερα υπάρχει επικοινωνία μεταξύ εγκληματικών οργανώσεων. Οι συμμετέχοντες στο Dark Web:

- Ανταλλάσσουν υλικό και ιδέες για στόχους, εργαλεία και τακτικές που χρησιμοποιούν, για την εφαρμογή επιθέσεων.
- Ανταλλάσσουν ιδέες κατασκευής διάφορων malwares, phising programs, DDos, και γενικότερα τεχνικών και λογισμικών για κακόβουλη χρήση.
- Σχεδιάζουν και συντονίζουν επιθέσεις κινούμενες από πολιτικό ή ιδεολογικό περιεχόμενο.
- Αγοράζουν και πωλούν διάφορα εργαλεία παράκαμψης των antivirus, exploit kits και γενικότερα εργαλεία επιθέσεων.
- Παρέχουν υπηρεσίες επίθεσης έναντι αμοιβής
- Αγοράζουν και πωλούν ευαίσθητα δεδομένα, όπως Αριθμούς Ασφάλισης, usernames, passwords και άλλες προσωπικές πληροφορίες.

Η επικοινωνία μεταξύ τους καθίσταται δυνατή μέσα από ειδικές πλατφόρμες, από e-mails, από μέσα κοινωνικής δικτύωσης αλλά το κύκλωμα αυτό των πληροφοριών, δεν είναι εύκολα προσπελάσιμο πχ από κάποιον ειδικό της Κυβερνοασφάλειας. Επίσης, συναντώνται γλώσσες επικοινωνίας διαφορετικές της Αγγλικής, όπως Ρώσικα, Μανδαρινικά, Βιετναμέζικα και Γερμανικά.

### 2.20.2.Κίνητρα και προθέσεις

Μέσα λοιπόν από το Dark Web, οι ειδικοί της Κυβερνοασφάλειας συλλέγουν δεδομένα που άπτονται των προθέσεων αλλά και των κινήτρων των επιτιθέμενων. Με αυτόν τον τρόπο σχηματίζεται μία εικόνα το που θα μπορούσαν να επιτεθούν (πχ σε ποιόν κλάδο εταιρειών) αλλά και ποια στοιχεία θα στόχευαν στον συγκεκριμένο κλάδο.

Φυσικά, το κίνητρο των επιτιθέμενων είναι το κέρδος και υπάρχουν διάφορες υποκατηγορίες τους. Υπάρχουν αυτοί που ανήκουν στην κατηγορία της βιομηχανικής αντικατασκοπείας, με σκοπό την υποκλοπή σχεδίων, στοιχείων πνευματικής ιδιοκτησίας και πληροφοριών στρατιωτικής βιομηχανίας. Μία άλλη κατηγορία είναι αυτή των «ακτιβιστών», οι οποίοι επιτίθενται για λόγους εντυπωσιασμού, για ιδεολογικούς και για πολιτικούς και γενικότερα

θέλουν να διαφημίσουν και να νουθετήσουν άτομα με τις δικές τους πολιτικές και ιδεολογικές απόψεις. Σε κάποιες περιπτώσεις, υπάρχει επικοινωνία μεταξύ των δύο προαναφερθέντων ομάδων και μέσα από αυτή, θα μπορούσαν οι ειδικοί του Intelligence να υποκλέψουν χρήσιμες πληροφορίες, εφόσον φυσικά έχουν ικανότητες penetration στα διάφορα forums αυτά.

## 2.20.3.Τακτικές, τεχνικές και διαδικασίες

Υπάρχει λοιπόν η έννοια των TTP's, δηλ των Tactics, Techniques and Procedures, η οποία αποτελεί ένα πολύ ισχυρό εργαλείο άμυνας διότι γνωρίζοντας εκ των προτέρων το προφίλ των επιτιθέμενων, μας βοηθάει στο να ανιχνεύουμε μελλοντικές επιθέσεις, να ισχυροποιούμε την άμυνα μας και να βελτιώνουμε τις διαδικασίες και την εκπαίδευση του προσωπικού. Υπό αυτήν την έννοια, παρακολουθώντας διάφορες δραστηριότητες κακόβουλων χρηστών στο Διαδίκτυο, μπορούμε να καταγράψουμε χρήσιμα στοιχεία, όπως:

- Συζητήσεις πάνω σε θέματα τακτικών και επιθέσεων σε διάφορα forums και μέσα κοινωνικής δικτύωσης.
- «Αγορές» εργαλείων και υπηρεσιών με προορισμό την επίθεση σε συστήματα υπολογιστών.
- Ανταλλαγή γνώσεων και απόψεων σχετικών με ανάπτυξη νέων hacking εργαλείων.
- Πώληση εργαλείων κατασκευασμένων για επιθέσεις.
- Πώληση ευαίσθητων και προσωπικών δεδομένων όπως credentials, αριθμούς πιστωτικών καρτών και άλλες πληροφορίες τέτοιου είδους.

Είδαμε λοιπόν, τους τρόπους με τους οποίους μπορούμε να συλλέξουμε τις πληροφορίες μας, οι οποίες όμως βρίσκονται σε μία πρώιμη μορφή και θα χρειαστούν περεταίρω επεξεργασία προκειμένου να εξαχθούν χρήσιμες πληροφορίες για χρήση cyber intelligence. Παρακάτω θα δούμε πως μπορούμε να επεξεργαστούμε αυτές τις πληροφορίες.

## 2.21.Πληροφορίες vs intelligence

Είδαμε λοιπόν, διάφορους τρόπους με τους οποίους μπορούμε να συλλέξουμε πληροφορίες στην «ωμή» τους μορφή και οι οποίες χρήζουν επεξεργασίας. Εάν μιλήσουμε για τους threat indicators, από μόνοι τους αποτελούν ένα κομμάτι πληροφορίας το οποίο δεν μπορεί, στην μορφή που είναι, να μας προσφέρει κάποια πορίσματα ή συμπεράσματα. Και αυτό διότι:

- Δεν υπάρχει ταξινόμηση των δεικτών ως προς την σημαντικότητα
- Αποτελούν ένα «ξερό» και απομονωμένο κομμάτι πληροφορίας
- Έχουν μια γενική μορφή η οποία δεν μπορεί να μας κατευθύνει σχετικά με ποιες επιχειρήσεις αυτοί συνδέονται

Άρα λοιπόν, δεν μπορούμε να βασιστούμε σε αυτές τις πληροφορίες, στην μορφή που βρίσκονται. Και αυτό διότι δημιουργούνται προβλήματα του στυλ:

- Δημιουργείται μία «πλημμύρα» από alerts, καθιστώντας την ομάδα SOC (Security Operations Center) ανίκανη στο να εντοπίσει ποια από τα alerts είναι σημαντικά και ποια όχι τόσο ώστε να

μπορέσει να τα ταξινομήσει ανάλογα με την επικινδυνότητα του συμβάντος στο οποίο αναφέρονται (είχαμε αναφέρει σε προηγούμενο κεφάλαιο ότι μόνο το 19% των alerts έχει νόημα να μελετηθεί περαιταίρω και από αυτό μόνο το 4% μπορεί να μελετηθεί)
• Η ομάδα IR (Incident Response) δεν μπορεί να συσχετίσει ένα alert με μία συγκεκριμένη απειλή, χωρίς να έχει προηγηθεί επιστημονική και εργαστηριακή μελέτη.

Τελικά, ποιο είναι το συμπέρασμα μετά από όλα αυτά; Το συμπέρασμα λοιπόν είναι ότι η έννοια του cyber intelligence είναι συνυφασμένη με την ταξινόμηση των δεικτών, με την ανίχνευση συγκεκριμένων απειλών για συγκεκριμένες επιχειρήσεις και για συγκεκριμένους «καταναλωτές» πληροφορίας Intelligence μέσα στις επιχειρήσεις αυτές. Επίσης, είναι συνυφασμένη με το να φιλτράρει ποιες απειλές αφορούν μία συγκεκριμένη επιχείρηση και ποιες όχι, εξοικονομώντας έτσι χρόνο.

## 2.22.Ταξινόμηση των απειλών

Υπάρχουν αρκετές ψηφιακές απειλές για τις επιχειρήσεις οι οποίες όμως χρήζουν ταξινόμησης διότι κάποιες από αυτές έχουν μικρή ή και καθόλου σχέση με την υπό προστασία επιχείρηση στα πλαίσια της τοποθεσίας της, των εφαρμογών της και του προφίλ κινδύνου της (risk profile). Επίσης, κάποιες απειλές είναι outdated ή χαμηλού κινδύνου όπως διάφορα spams και spywares.

### 2.22.1.Η «βαθμολόγηση» των κινδύνων

Προκειμένου να υπάρξει μία ταξινόμηση των threat indicators, θα πρέπει να δίνεται σε κάθε έναν από αυτούς, μία βαθμολογία ή ένα score. Αυτό γίνεται συνήθως είτε αυτοματοποιημένα μέσω κάποιων εργαλείων όπως τα SIEM (Security Information Event Management), είτε με την βοήθεια ορισμένων αναλυτών. Με αυτόν τον τρόπο, λαμβάνονται γρηγορότερες αποφάσεις για το ποιοι δείκτες είναι σημαντικοί και χρήζουν άμεσης και ιδιαίτερης προσοχής και ποιοι ανήκουν σε κατηγορία μικρής επικινδυνότητας. Τα scores παράγονται με τους εξής τρόπους:

- Μέσω αυτοματοποιημένων τεχνικών αναλύσεων – sandboxing
- Μέσω στατιστικών αναλύσεων – συσχέτιση ενός ορισμένου δείκτη με την υπό προστασία επιχείρηση
- Μέσω ανθρώπινης κρίσης και εκτίμησης τρωτότητας και συνεπειών μίας συγκεκριμένης απειλής

### 2.22.2. «Ταμπελάκια» περιεχομένου

Τα αυτοματοποιημένα συστήματα και η ανθρώπινη ανάλυση μπορούν να αποφανθούν εάν ένας δείκτης συσχετίζεται με μεμονωμένο γεγονός ή με μία περισσότερο πολύπλοκη επίθεση. Και χρησιμοποιούν διάφορα συμφραζόμενα για να χαρακτηρίσουν έναν δείκτη. Τα συμφραζόμενα περικλείονται σε «ταμπελάκια» (tags) τα οποία είναι ουσιαστικά τίτλοι ή επικεφαλίδες οι οποίοι μπαίνουν στους δείκτες, για να τους χαρακτηρίζουν. Για παράδειγμα:

- Ένα «οικονομικό» ταμπελάκι χρησιμοποιείται για να χαρακτηρίσει ένα malware το οποίο προορίζεται για επίθεση σε ATM's τραπεζών
- Ένα «ανατολικής Ευρώπης» ταμπελάκι χρησιμοποιείται για να χαρακτηρίσει ένα URL το οποίο σχετίζεται με επιθέσεις phising στην ανατολική Ευρώπη
- Ένα "Citadel οικογένεια» ταμπελάκι, συνδέεται με δείκτες σχετικούς με την υποκλοπή ευαίσθητων στοιχείων (credentials) από malwares της οικογένειας Citadel.

Γίνεται αντιληπτό πλέον ότι για παράδειγμα ένα SIEM tool μίας τράπεζας μπορεί να προγραμματιστεί για να δίνει προτεραιότητα σε «οικονομικά» ταμπελάκια. Αναλυτές SOC σε εργοστάσια κατασκευής στην Πολωνία και στην Ουγγαρία θα δίνουν προτεραιότητα σε «ανατολικής Ευρώπης» ταμπελάκια. Μία IR ομάδα βλέποντας ταμπελάκι «Citadel οικογένεια», θα αναζητήσει αμέσως πληροφορίες σχετικές με την εν λόγω «οικογένεια» των malwares.

### 2.22.3. Ανθρώπινη εκτίμηση

Το θέμα της ανθρώπινης εκτίμησης ενός κινδύνου είναι υποκειμενικής φύσεως και οι αναφορές που γίνονται σχετικά με ψηφιακά συμβάντα κληρονομούν την υποκειμενική αυτή φύση. Για παράδειγμα, μία αναφορά μπορεί να σχετίζεται με κάποιο malware το οποίο όμως να μην είναι τόσο σχετικό με την συγκεκριμένη αναφορά ή να υπάρχει ήδη αναφορά για το malware αυτό και έτσι η αναφορά να θεωρείται outdated.

## 2.23. Επεξεργασία και «μετάφραση» των πληροφοριών

Ας δούμε πως μπορούμε να επεξεργαστούμε τις πληροφορίες που συγκεντρώνουμε έτσι ώστε να προκύψουν δεδομένα σε μία μορφή η οποία έχει νόημα για τους σκοπούς του cyber intelligence.

### 2.23.1.Αναφορές

*«Ανάλυση απειλών»*

Οι ομάδες IR, διάφορες ομάδες αναλυτών και ειδικοί στην Κυβερνοασφάλεια μπορούν να εκτελέσουν με καλύτερο τρόπο το έργο τους έχοντας ως βοήθεια τις αναφορές της «ανατομίας» των επιθέσεων, οι οποίες περιλαμβάνουν:

- Συσχέτιση συγκεκριμένων επιθέσεων με συγκεκριμένες ομάδες επιτιθέμενων
- Το πότε και το που έγινε μία επίθεση αλλά και το αν υπάρχει και κάποιο ιστορικό αυτής της επίθεσης
- Κίνητρα και προθέσεις των επιτιθέμενων
- Περιγραφή των θυμάτων/στόχων ως προς την τοποθεσία και τις τρωτότητες τους
- Μια εκτίμηση της ζημιάς που προκλήθηκε στην επιχείρηση αλλά και επικείμενοι κίνδυνοι σε επιχειρήσεις άλλου είδους
- Μία ανάλυση της στρατηγικής που χρησιμοποιήθηκε , όπως για παράδειγμα τα βήματα αναγνώρισης (των τρωτών σημείων της επιχείρησης από τους επιτιθέμενους),

τεχνικές phising και αντίστροφης μηχανικής, τύποι των malware που χρησιμοποιήθηκαν, συστήματα που υπέστησαν επίθεση, τεχνικές ελέγχου και εντολών (command and control) και τρόποι υποκλοπής δεδομένων
- Ομοιότητες με άλλες απειλές
- Περιγραφές δεικτών και ψηφιακών συμβάντων οι οποίες βοηθούν στην αναγνώριση των επιθέσεων
- Ιδέες και συμβουλές για περιορισμό της έκτασης της επίθεσης και της βελτίωσης της άμυνας
- Έννοιες εγρήγορσης για τυχόν μελλοντικές επιθέσεις του ίδιου τύπου

Υπάρχουν στο web αναλύσεις των οποίων τα links αναφέρονται στο Παράρτημα 1.

*«Τοπία» απειλών»*

Μιλώντας για τοπία απειλών, αναφερόμαστε σε μία ευρύτερη, συνολική εικόνα των απειλών, οι οποίες στοχεύουν μία επιχείρηση. Αυτή η εικόνα λοιπόν, αποτελείται από:

- Μία αναφορά και ανάλυση των επιχειρηματικών κινδύνων που αντιμετωπίζει μία επιχείρηση
- Μία ανάλυση και επεξήγηση των διαφόρων τύπων malware οι οποίοι επηρεάζουν την ίδια αλλά και ιδίου τύπου επιχειρήσεις
- Μία επισκόπηση των επιτιθέμενων σχετική με τα κίνητρα τους, τις προθέσεις τους, τις τεχνικές, τις διαδικασίες και την συνολική στρατηγική τους
- Μία ταξινόμηση των προτεραιοτήτων σε θέματα ασφαλείας

## 2.23.2. Ικανότητες αναλυτών

Η ποιότητα της ανάλυσης των «ωμών» πληροφοριών και η μετατροπή τους σε χρήσιμα δεδομένα, εξαρτάται από την ικανότητα και την εμπειρία των αναλυτών. Τα άτομα που έχουν αναλάβει το έργο της ανάλυσης, θα πρέπει:

- Να έχουν τεχνικές γνώσεις στο πως λειτουργούν τα malwares
- Να έχουν γνώσεις στο πως οι hackers οργανώνονται σε ομάδες
- Να έχουν εμπειρία σε νέες τεχνολογίες cyber security
- Να έχουν ικανότητες στο να «μεταφράζουν» τις «ωμές» πληροφορίες σε χρήσιμα δεδομένα
- Να έχουν κριτικές και αναλυτικές ικανότητες και με τη βοήθεια των οποίων να μπορούν να παράγουν συμβουλές και συστάσεις πρακτικής και εφαρμόσιμης σημασίας

Εκτός από τα προαναφερθέντα, υπάρχουν ακόμη 2 σημεία ζωτικής σημασίας για τους αναλυτές: Το να μιλούν διάφορες ξένες γλώσσες (υπάρχουν forums όπου η αγγλική δεν είναι η μοναδική γλώσσα που χρησιμοποιείται) και το να διαθέτουν εξαιρετικές ικανότητες επικοινωνίας, οι οποίες, εκτός των άλλων, θα τους βοηθήσουν και στο να επικοινωνούν σωστά και με «καταναλωτές» πληροφοριών intelligence, μη τεχνολογικής εκπαίδευσης.

## 2.23.3.Πλατφόρμα intelligence

Οι αναλυτές των threats προσπαθούν να βρουν τα κομμάτια του παζλ και να ανιχνεύσουν διάφορα μοτίβα και με αυτόν τον τρόπο να ανακαλύψουν επερχόμενες επιθέσεις. Έτσι λοιπόν, η ύπαρξη μίας πλατφόρμας intelligence, θα τους ήταν ιδιαίτερα χρήσιμη στο να επιταχύνουν την άνω διαδικασία. Μία τέτοια πλατφόρμα θα μπορούσε να περιέχει τους εξής βασικούς πυλώνες:

- Μία βάση δεδομένων στην οποία θα αποθηκεύονται όλες οι πληροφορίες που άπτονται διαφόρων ψηφιακών απειλών
- Εργαλεία αυτόματης λειτουργίας τα οποία θα έχουν ως είσοδο δεδομένα τεχνικής και ανθρώπινης φύσεως και τα οποία θα επεξεργάζονται (techint, manint)
- Εργαλεία τα οποία θα συσχετίζουν πληροφορίες και θα συμπληρώνουν το παζλ
- Εργαλεία δημιουργίας και δημοσίευσης των «προϊόντων» intelligence (parsing python)[5]

## 2.23.4.Παραμετροποίηση

Η παραμετροποίηση αποτελείται από 2 πλαίσια, των επιχειρήσεων και των «καταναλωτών» πληροφοριών cyber intelligence. Ας δούμε λοιπόν τι συμβαίνει σε καθένα από αυτά.

Παραμετροποίηση επιχειρήσεων: Υπάρχει ένας τεράστιος όγκος πληροφοριών για threats, μέσα από τον οποίο οι ειδικοί του intelligence θα πρέπει να ξεχωρίζουν κάθε φορά εκείνες που αφορούν την συγκεκριμένη εταιρεία, ανάλογα με την τοποθεσία, το μέγεθος, τους κανονισμούς λειτουργίας, των applications, των mobile και cloud τεχνολογιών της.

Παραμετροποίηση των «καταναλωτών» cyber intelligence: Χρειάζεται μία ανάλυση και ένα φιλτράρισμα των πληροφοριών που προορίζονται για αυτή την κατηγορία «καταναλωτών». Οι «καταναλωτές» τέτοιων πληροφορίων μπορούν να είναι ομάδες IR (οι οποίες χρειάζονται όσο το δυνατόν περισσότερες πληροφορίες για ανίχνευση απειλών), ομάδες τακτικής αντίδρασης (οι οποίες χρειάζονται βασικές πληροφορίες για γρήγορη λήψη αποφάσεων) και για IT managers (οι οποίοι χρειάζονται γενικές πληροφορίες και περιλήψεις).

---

[5]**Jon Friedman, Mark Bouchard, CISSP, 2015, " Definitive guide to Cyber Threat Intelligence", pages v, 3-8, 10-26, 28-33**

**Intelligence and National Security Alliance, Cyber Intelligence Task Force, "Operational Levels Of Cyber Intelligence", September 2013, pages 4-10**

**Intelligence and National Security Alliance, Cyber Intelligence Task Force, "Strategic Cyber Intelligence", March 2014, pages 3-10**

**ENISA, "Proactive Detection of Security Incidents", 20-11-2012, pages 17-19**

## 2.24.Γενικά στοιχεία για τα «εργαλεία» του CTI

Όπως ήδη έχουμε δει και προηγουμένως, η αποτελεσματική χρήση του CTI (Cyber Threat Intelligence) αποτελεί ένα ισχυρό όπλο απέναντι σε διάφορους τύπους Κυβερνοεπιθέσεων. Δυστυχώς όμως, οι παραγόμενες πληροφορίες intelligence έχουν ένα μειονέκτημα: Έχουν μία «ημερομηνία λήξης». Λέγοντας αυτό, εννοούμε ότι εάν οι πληροφορίες αυτές δεν χρησιμοποιηθούν ή «καταναλωθούν» εντός ενός ορισμένου χρονικού διαστήματος, είναι άχρηστες διότι δεν είναι επίκαιρες. Και θα ρωτούσε κάποιος: Και τι σημασία έχει; Η απάντηση είναι ότι οι διάφορες επιθέσεις που συμβαίνουν στη μονάδα του χρόνου, εξελίσσονται συνεχώς ως προς τις τεχνικές, τη φιλοσοφία και την πολυπλοκότητα τους και άρα θα πρέπει να συμβαδίζει με αυτές και η κυβερνοάμυνα της επιχείρησης.

Τα τελευταία χρόνια έχει καταβληθεί μία σημαντική προσπάθεια να υπάρξει μία καλή διαχείριση του CTI και έχουν αναπτυχθεί ορισμένα εργαλεία για το σκοπό αυτό. Φυσικά, η όλη διαδικασία παραγωγής intelligence data και εξαγωγής/διαμοιρασμού τους πολλές φορές αποτελεί μία πρόκληση, εξαιτίας της πολυπλοκότητας της διαδικασίας και σε αυτό το σημείο είναι καλό να εφαρμόζονται τυποποιημένες διαδικασίες. Το ινστιτούτο PMI (Project Management Institute) παρέχει τις τυποποιημένες διαδικασίες PMBOK (Project Management Body Of Knowledge). [10,11,12,13]

## 2.25. Η διαχείριση PMBOK

Οι διαδικασίες PMBOK μπορούν να αναλυθούν σε 5 κύριους τομείς: Αρχικοποίηση, Σχεδιασμός, Εκτέλεση, Παρακολούθηση και Έλεγχος και Κλείσιμο.

Έστω λοιπόν ότι υπάρχει ένα project (σχετικό με cyber intelligence) για μία επιχείρηση το οποίο θα πρέπει να αναπτυχθεί. Οι διαδικασίες που θα ακολουθηθούν θα πηγάζουν από το PMBOK. Και για να γίνουμε περισσότερο σαφείς, επιλέγονται 3 διαδικασίες από το PMBOK, οι οποίες είναι οι πιο κατάλληλες για να μας βοηθήσουν να επιλέξουμε με τον καλύτερο δυνατό τρόπο τα εργαλεία του CTI. Παρακάτω, στην εικόνα 2.13 βλέπουμε ότι η 1η και η 2η διαδικασία προέρχονται από τον τομέα της Αρχικοποίησης και η 3η διαδικασία προέρχεται από τον τομέα του Σχεδιασμού.


(εικόνα 2.13:Διαδικασίες από τομείς)

1η διαδικασία: Ανάπτυξη καταστατικού

2η διαδικασία: Ανάπτυξη προκαταρκτικής πρότασης του έργου
3η διαδικασία: Ορισμός Πεδίου

Παρακάτω, θα δούμε αναλυτικότερα τα πορίσματα των 3 διαδικασιών αυτών.

## 2.25.1. Καταστατικό

Το πόρισμα της 1ης διαδικασίας «Ανάπτυξη καταστατικού» είναι το καταστατικό, το οποίο είναι μία αναλυτική περιγραφή του αντικειμένου του έργου και αποτελεί το πρώτο βοήθημα το οποίο δίνει μία εικόνα του πως γίνεται η αρχειοθέτηση και η διοίκηση του έργου. Παρόλο που αποτελείται από 1 μόνο σελίδα, είναι το πιο ουσιαστικό βοήθημα και βάσει αυτού αναπτύσσονται και τα υπόλοιπα βοηθήματα του συνολικού έργου. Θα πρέπει λοιπόν εδώ, να τονιστεί το γεγονός του ότι θα πρέπει το καταστατικό να συνταχθεί όσο το δυνατόν πληρέστερα και καλύτερα από την αρχή, διότι οποιαδήποτε παράλειψη ή λάθος συμβεί κατά την αρχική του σύνταξη, αυτό θα έχει αντίκτυπο και μεγενθυμένο αρνητικό αποτέλεσμα στα επόμενα βοηθήματα. Και κάτι τέτοιο θα σημαίνει επίσης χάσιμο χρόνου και πολλές επαναληπτικές ενέργειες, οι οποίες θα μπορούσαν να είχαν αποφευχθεί, με μία αρχική ποιοτική υλοποίηση του καταστατικού αυτού.

Η ποιοτική υλοποίηση του καταστατικού μπορεί να καταστεί δυνατή με ανασκοπήσεις άλλων project managers ή προσωπικού οι οποίοι δεν εμπλέκονται στο έργο αυτό.

Επίσης, κάποια βασικά συστατικά του καταστατικού είναι:

- Η περιγραφή του έργου
- Οι απαιτήσεις του έργου
- Ο manager του έργου
- Κάποια ορόσημα
- Κάποιες υποθέσεις και διάφορα σενάρια

Ας τα δούμε λίγο πιο αναλυτικά:

***Η περιγραφή του έργου:*** Η υπηρεσία CTIM (Cyber Threat Intelligence Management) θα παρέχει στην επιχείρηση ένα σύστημα με τη βοήθεια του οποίου θα είναι εφικτή η συλλογή, η διαχείριση, ο μοχλισμός και ο διαμοιρασμός δεδομένων Cyber Intelligence. Η υπηρεσία CTIM θα συνδέεται άμεσα με την συλλογή πληροφοριών σχετικών με απειλές οι οποίες μπορούν να συλλέγονται από πηγές δημόσιου ή κοινοτικού χαρακτήρα και τις οποίες θα μπορεί να μετατρέψει σε χρήσιμα δεδομένα με τα οποία θα είναι εφικτή η δημιουργία εργαλείων πρόβλεψης και ανίχνευσης επιθέσεων.

***Οι απαιτήσεις του έργου:*** Η σωστή εφαρμογή του CTIM θα έχει ως επακόλουθα:

- Ένα σύστημα συλλογής, διαχείρισης, μοχλισμού και διαμοιρασμού δεδομένων Cyber Intelligence.
- Ένα αυτόματο σύστημα συλλογής πληροφοριών σχετικών με απειλές οι οποίες μπορούν να συλλέγονται από πηγές δημόσιου ή κοινοτικού χαρακτήρα.
- Ένα αυτόματο σύστημα το οποίο θα μετατρέπει τις πληροφορίες σε χρήσιμα δεδομένα με τα οποία θα είναι εφικτή η δημιουργία εργαλείων πρόβλεψης και ανίχνευσης επιθέσεων.

***Ο manager του έργου:*** Ο κύριος Scott Moore έχει τεθεί επικεφαλής του έργου (το όνομα είναι ψεύτικο και αναφέρεται ως παράδειγμα) και ο αριθμός 409522002 είναι ο αριθμός του έργου.

***Ορόσημο:*** 25 Σεπτεμβρίου 2016, έναρξη (Kick off)
25 Ιουνίου 2017, έκδοση (release)

***Κάποιες υποθέσεις:*** Έχει υποτεθεί ότι θα υπάρχει μία εφαρμογή διεπαφής (API-Application Program Interface) για την πρόσβαση στις πληροφορίες οι οποίες προέρχονται από την πηγή.

***Σενάριο:*** Η επιχείρηση, καθώς χρησιμοποιεί το Ίντερνετ, εκτίθεται σε υψηλό κίνδυνο, επομένως επιβάλλεται χρήση κανόνων cyber intelligence και με την εφαρμογή CTIM, η επιχείρηση βελτιώνει αισθητά την άμυνά της, με την ανίχνευση ή την παρεμπόδιση απειλών ευρισκόμενων στο Web.

Αφού λοιπόν ολοκληρωθούν οι διαδικασίες του καταστατικού, σειρά έχει η Ανάπτυξη προκαταρκτικής έκτασης έργου.

## 2.25.2 Προκαταρκτική ανάπτυξη του πεδίου δράσης του έργου

Η προκαταρκτική ανάπτυξη του πεδίου δράσης του έργου αποτελεί και αυτή κομμάτι του τομέα της Αρχικοποίησης και προκύπτει από το συνδυασμό του Καταστατικού που αναφέραμε προηγουμένως και άλλων inputs. Η έκταση του έργου είναι ουσιαστικά η αναγνώριση στοιχείων σχετικών με αυτό και σε αυτή περιέχονται διαδικασίες οι οποίες περιγράφονται με μεγαλύτερη ακρίβεια από το Καταστατικό. Έτσι έχουμε την Προκαταρκτική Πρόταση εδώ η οποία θα πρέπει να έχει μεγαλύτερη ακρίβεια από το Καταστατικό αλλά να έχει μικρότερη ακρίβεια από την Τελική Πρόταση έτσι ώστε η ακρίβεια της Προκαταρκτικής Πρότασης να μην φθάνει σε σημείο υπερβολής. Τα βασικά στοιχεία αυτής της Προκαταρκτικής Πρότασης είναι το αντικείμενο του έργου, οι απαιτήσεις, τα κριτήρια αποδοχής, όρια, διαμοιραζόμενα αρχεία, περιορισμοί, κίνδυνοι της επιχείρησης, ορόσημα και κόστος. Ας τα δούμε πιο αναλυτικά:

<u>Αντικείμενο του έργου:</u> Η παράδοση του εν λόγω έργου θα γίνει στις 25 Ιουνίου 2017. Με την χρήση του CTIM θα διερευνηθούν κατά 20% λιγότερα περιστατικά.

<u>Οι απαιτήσεις:</u>

- R1: Ικανότητα εισαγωγής/εξαγωγής λεπτομερειών συναφών με δείκτες από και προς άλλα συστήματα σε ένα standard format.
- R2: Ικανότητα εισαγωγής/εξαγωγής δομημένων δεδομένων περιστατικών από και προς άλλα συστήματα σε ένα standard format.

- R3: Ικανότητα αναζήτησης, εισαγωγής, εξαγωγής και διαχείρισης δεδομένων CTI μέσω διεπαφής χρήστη (user interface).
- R4: Ικανότητα ενίσχυσης διαμοιρασμού δεδομένων βασιζόμενης σε μία λειτουργία των CTI δεδομένων.
- R5: Ικανότητα αυτοματισμού εισαγωγής και εξαγωγής των δεδομένων CTI.I
- R6: Ικανότητα παροχής πιστοποίησης και εμπιστευτικότητας στον διαμοιρασμό των δεδομένων.
- R7: Ικανότητα εξαγωγής δεδομένων τα οποία προορίζονται για ενέργειες ανίχνευσης και προστασίας έναντι επιθέσεων.
- R8: Ικανότητα επιλογής δεδομένων προς εξαγωγή βασιζόμενη σε ημερομηνίες δημιουργίας CTI δεδομένων.
- R9: Ικανότητα μέτρησης της αποτελεσματικότητας των εισερχόμενων πληροφοριών οι οποίες τροφοδοτούν το CTI.

Τα κριτήρια αποδοχής προϊόντος: Η ομάδα ελέγχου του έργου θα πρέπει να ολοκληρώνει όλα τα tests αποδοχής του.
Τα όρια του έργου: Το εύρος του έργου σχετίζεται μόνο με το cyber intelligence και όχι με άλλα αντικείμενα όπως ανίχνευση τρωτοτήτων και δεδομένα από ψηφιακά συμβάντα.
Τα ωφέλιμα στοιχεία του έργου:

- CTIM (Cyber Threat Intelligence Management)
- Στρατηγικές οι οποίες δημιουργούνται και εγκρίνονται για την διοίκηση και λειτουργία του CTIM
- Αρχειοθέτηση του σχεδιασμού και της χρήσης του συστήματος
- Εκπαιδευτικό υλικό το οποίο προορίζεται για administrators και απλούς χρήστες
- Διαδικασίες που θα πρέπει να ακολουθούνται από administrators και απλούς χρήστες

Υποθέσεις και περιορισμοί του έργου: Οι servers που θα χρησιμοποιηθούν θα πρέπει να περιλαμβάνουν συμβατό λειτουργικό σύστημα
Οργανισμός αρχικού έργου: Project Manager, Αναλυτής Επιχείρησης, Προγραμματιστής
Αρχικώς καθορισμένοι κίνδυνοι: Οι υπηρεσίες Cyber Intelligence δεν συνδέονται με συμφωνία παροχής συγκεκριμένου επιπέδου υπηρεσιών και μπορούν να διακοπούν ανά πάσα στιγμή.
Ανάλυση κόστους:

- Hardware και software -> 250.000$
- Συμβουλευτικές υπηρεσίες -> 40.000$
- Ανθρωποώρες-> 4.000$

Όλα τα παραπάνω στοιχεία της Προκαταρκτικής Πρότασης χρησιμοποιούνται ως δεδομένα εισόδου για την παρακάτω διαδικασία, η οποία δεν είναι άλλη εκτός από το Ορισμό Πεδίου.

### 2.25.3.Ορισμός του πεδίου δράσης

Ο ορισμός του πεδίου δράσης προέρχεται από τον Τομέα του Σχεδιασμού. Αυτή η διαδικασία έχει συνάφεια με τον καθορισμό του πεδίου του έργου, αλλά το να μπορέσει μία ομάδα ανθρώπων να ορίσει το πεδίο αυτό, σημαίνει ότι μπορεί να είναι ικανή να το οργανώνει και να το διοικεί και η ικανότητα να μανατζάρει σωστά το έργο αυτό έχει ως αποτέλεσμα να μπορεί να επιτύχει το στόχο του έργου. Τελικά, η διαδικασία του Ορισμού Πεδίου, έχει ως δεδομένα

εισόδου το Καταστατικό και την Προκαταρκτική Πρόταση, αλλά και άλλα inputs. Το πόρισμα της διαδικασίας του Ορισμού Πεδίου είναι η Τελική Πρόταση.

Σε όλη αυτή τη διαδικασία, θα υπάρξουν και κάποιες αλλαγές στο πεδίο αλλά το όλο σκεπτικό είναι να μην υπάρχει μεγάλη απόκλιση και αυτό είναι εφικτό με την εφαρμογή ενός καλομελετημένου σχεδιασμού του πεδίου εξαρχής. Υπάρχει μία λειτουργία εντός του PMBOK, η Διαχείριση Έργου Πεδίου, στην οποία συμπεριλαμβάνονται τεχνικές διαχείρισης σχετικές με αλλαγές του Πεδίου. Μια καλή συμβουλή θα ήταν να υπάρχει συζήτηση μεταξύ μετόχων προκειμένου να αποφευχθούν κόστη αλλαγών στο Πεδίο. Και τα κόστη αυτά έχουν μεγέθη τα οποία αυξάνονται με γεωμετρικούς ρυθμούς όσο η διαδικασία του Πεδίου πλησιάζει προς το τέλος της. Ενδεικτικά αναφέρουμε ότι μία αλλαγή, σε μεγάλα έργα software, όταν πρόκειται να συμβεί στο τέλος της διαδικασίας θα κοστίσει 100 φορές περισσότερο από ότι θα κόστιζε εάν συνέβαινε στην αρχή της διαδικασίας. Μάλιστα, υπάρχει και ένα εργαλείο εντός της διαδικασίας του Πεδίου, το οποίο ονομάζεται Ανάλυση Προϊόντος και το οποίο μπορεί να υπολογίσει, μέσα από την ανάλυση των πορισμάτων-προϊόντων μίας διαδικασίας, το πεδίο/την έκταση η οποία θα επηρεαστεί από τα προϊόντα αυτά. Με αυτό το εργαλείο, είναι εφικτές ανασκοπήσεις και αναλύσεις διάφορων εργαλείων cyber intelligence.

## 2.26. Cyber Intelligence

Το λεγόμενο CTI-Cyber Threat Intelligence, είναι ουσιαστικά τα δεδομένα τα οποία έχουν προκύψει από κατάλληλη ανάλυση πληροφοριών. Και τα δεδομένα αυτά θα πρέπει να μπορούν να εφαρμοστούν, διότι σε αντίθετη περίπτωση, δεν έχουν καμία ιδιαίτερη αξία. Επίσης, η CTI, μπορεί να χωριστεί σε 2 μεγάλες κατηγορίες: Την Στρατηγική Intelligence και την Τακτική Intelligence. Η Στρατηγική Intelligence περιλαμβάνει στοιχεία κινήτρων των επιτιθέμενων. Η Τακτική Intelligence περιλαμβάνει το τρίδυμο Τεχνικές-Τακτικές-Διαδικασίες δηλ το TTP's – Tactics-Techniques-Procedures καθώς και τους Δείκτες Διακινδύνευσης IOC'S – Indicators Of Compromise. Οι τελευταίοι έχουν πρακτική εφαρμογή και τα διάφορα εργαλεία cyber intelligence εστιάζουν σε αυτούς τους Δείκτες. Τα ευρέως χρησιμοποιούμενα IOC's είναι τα IP's, τα domains, τα URL's και τα file hashes.

## 2.27. Οδηγοί Διαχείρισης CTI

Λόγω του ότι σχεδόν όλες οι μεγάλες επιχειρήσεις χρησιμοποιούν σήμερα το Internet, έρχονται αναπόφευκτα αντιμέτωπες με μεγάλους κινδύνους επιθέσεων και το πρόβλημα εδώ είναι ότι οι επιτιθέμενοι εφευρίσκουν έξυπνους τρόπους επίθεσης, οι οποίοι συνεχώς αλλάζουν. Έτσι λοιπόν, τα εργαλεία CTI θα πρέπει να προσαρμόζονται με αυτόματο τρόπο στις αλλαγές αυτές. Ένα βασικό στοιχείο των CTI Tools είναι η συλλογή κατάλληλων πληροφοριών.

## 2.28.Πηγές CTI

Οι πηγές της CTI, χωρίζονται σε εσωτερικές, εξωτερικές και κοινότητας. Ας τις δούμε λίγο πιο αναλυτικά.

### 2.28.1. Εσωτερικές πηγές CTI

Οι πληροφορίες που συλλέγονται εδώ αφορούν το εσωτερικό της επιχείρησης και έχουν να κάνουν με εργαλεία άμυνας όπως τα Firewalls,, τα IPS-Intrusion Prevention Systems, τα Antivirus. Επίσης, γίνεται μία εσωτερική ανάλυση η οποία παράγει δεδομένα τα οποία δεν είναι άμεσα αντιληπτά όπως εργαλεία και TTP's των επιτιθέμενων τα οποία (οι επιτιθέμενοι) δεν μπορούν να αλλάξουν εύκολα, σε αντίθεση με μία IP ή ένα domain name.

### 2.28.2. Πηγές κοινότητας

Υπάρχουν κάποιες ομάδες (groups) των οποίων τα μέλη έχουν κοινά ενδιαφέροντα ή ανήκουν, για παράδειγμα, στον ίδιο βιομηχανικό τομέα. Έχουμε τα ISAC's – Information Centers And Analysis Centers, τα οποία οργανώνονται υπο την σκέπη του Διεθνούς Συμβουλίου (National Council). Για παράδειγμα, υπάρχουν ISAC's με θεματολογία τις οικονομικές υπηρεσίες ή την ανώτατη εκπαίδευση. Υπάρχει πχ το REN-ISAC (Research And Education Networking) ή το DCSIE (Defense Industrial Base Collaborative Information Sharing Environment).

### 2.28.3. Εξωτερικές πηγές

Η αναζήτηση πληροφοριών εδώ δεν αναφέρεται σε συγκεκριμένο group αλλά σε εξωτερικές πηγές, οι οποίες μπορεί να είναι είτε δημοσίου χαρακτήρα ή ιδιωτικού χαρακτήρα.

Στις πηγές δημοσίου χαρακτήρα (public) έχουν πρόσβαση όλοι, χωρίς κόστος αλλά το πρόβλημα που υπάρχει εδώ είναι η ποιότητα των πληροφοριών αυτών. Ως παράδειγμα, μπορούμε να αναφέρουμε μία τέτοια πηγή, την Malware Domains, η οποία περιλαμβάνει domains τα οποία έχουν χρησιμοποιηθεί σε παράνομες δραστηριότητες.
Στις πηγές ιδιωτικού χαρακτήρα, η πληροφορία δεν είναι δωρεάν, αλλά «αγοράζεται» έχοντας όμως το πλεονέκτημα οτι η ποιότητα της είναι μακράν καλύτερη. Οι πληροφορίες που «αγοράζονται» προέρχονται από CTI διαδικασίες, είναι συνεχώς updated και αυτό μπορεί να βοηθήσει και τα διάφορα tools άμυνας της επιχείρησης. Ως παράδειγμα αναφέρουμε το Emergency Threats ETPro RuleSet (Emerging Threats). Σε αυτό υπάρχουν υπηρεσίες για τα IDS - Intrusion Detection Systems και φήμες για ορισμένα IP's.

## 2.29.Απαιτήσεις της CTI

Αναλόγως της επιχείρησης, οι απαιτήσεις διαφέρουν. Έχουμε ήδη αναφέρει ένα παράδειγμα των απαιτήσεων R1 έως R9 στην παράγραφο 7.2.2 (Ανάπτυξη προκαταρκτικής έκτασης του έργου).

## 2.30. Εργαλεία και standards της CTI

Υπάρχουν πολλά εργαλεία και standards για την εφαρμογή διαδικασιών CTI. Ας δούμε παρακάτω ποια είναι αυτά.

## 2.30.1.Traffic Light Protocol

Σε αυτήν την περίπτωση έχουμε ένα πρωτόκολλο απλό και γρήγορο. Ανάλογα την διαμοιραζόμενη πληροφορία, «τοποθετείται» και το αντίστοιχο ταμπελάκι σε αυτή. Για παράδειγμα, πληροφορίες που μπορούν να τις βλέπουν όλοι, «χρωματίζονται» με το λευκό χρώμα. Κάποιες άλλες που μπορούν να κυκλοφορούν εντός ενός τομέα ή μίας κοινότητας αλλά όχι δημοσίως, έχουν πράσινο χρώμα. Αυτές που έχουν πορτοκαλί χρώμα, διαμοιράζονται μεταξύ μελών ενός οργανισμού και εκείνες με το κόκκινο χρώμα, δεν διαμοιράζονται. Όλα τα προαναφερθέντα αφορούν την απαίτηση R4, την οποία έχουμε ήδη αναφέρει στην παράγραφο 2.23.2. [6]

## 2.30.2.Managed Incident LightWeight Exchange (MILE)

Η ιδέα εδώ είναι η ανταλλαγή δεδομένων από διάφορα περιστατικά και υπάρχει μία ομάδα η οποία ασχολείται με το format των δεδομένων, προκειμένου να καθορίζονται δείκτες και περιστατικά. Επίσης, η ομάδα αυτή καθορίζει τα standards ανταλλαγής των δεδομένων για τους σκοπούς της CTI και κάποια από αυτά είναι τα: IODEF (Incident Object Description and Exchange Format), IODEF for Structured Cyber Security Information IODEF-SCI και Real Time Inter-Network Defense (RID).

## 2.30.3. Incident Object Description and Exchange Format (IODEF)

Το συγκεκριμένο standard προτάθηκε τον Δεκέμβριο του 2007 και βασίζεται σε αρχεία XML, τα οποία ανταλλάσσονται μεταξύ ομάδων CSIRT (Computer Security Incident Response Teams).
Γενικότερα, γίνεται ανταλλαγή δεδομένων σχετικών με την λειτουργία και με στατιστικές μετρήσεις, για περιστατικά ασφάλειας.Βάσει του standard αυτού, υπάρχουν κατηγορίες και υποκατηγορίες στις οποίες ταξινομούνται δεδομένα περιστατικών. Για παράδειγμα, τα δεδομένα περιστατικών μπορούν να ταξινομηθούν σε κατηγορίες όπως Χρόνος, Λειτουργικό Σύστημα, Εφαρμογή, Χρηματοοικονομική Επίπτωση. Και φυσικά, εμπεριέχονται έννοιες ευαισθησία δεδομένων και εμπιστευτικότητα. Θα πρέπει να προσθέσουμε ότι το standard αυτό χρησιμοποιείται από διάφορα groups, όπως το Anti-Phishing, το οποίο χρησιμοποιεί το IODEF για την αναφορά περιστατικών phishing και άλλων συμβάντων σχετικών με e-mails. Ουσιαστικά, χρησιμοποιείται ως format αποθήκευσης σε μία πλατφόρμα συλλογής δεδομένων, την CIF (Collective Intelligence Framework). Τέλος, το IODEF χρησιμοποιείται και σε άλλα προϊόντα όπως αυτά από τις εταιρείες DFLabs, Arcsite και Foundstone.

[6] **Greg Farnham, "Tools and Standards for Cyber Threat Intelligence Projects", October 14th 2013, pages 2-11**

## 2.30.4. IODEF for Structured Cyber Security Information (IODEF-SCI)

Το standard αυτό αποτελεί μία προέκταση του IODEF και το επιπλέον στοιχείο του είναι το ότι υποστηρίζει επιπρόσθετες πληροφορίες όπως μοτίβα επίθεσης, τρωτότητες, αδυναμίες συστήματος, πληροφορίες πλατφόρμας, οδηγίες για αντίμετρα σε περιπτώσεις επίθεσης, αρχεία καταγραφής (log) και επικινδυνότητα συμβάντων. Παρακάτω, παραθέτουμε τα standards, τα οποία περικλείονται στο IODEF-SCI. Αυτά είναι τα εξής:

- CAPEC-Common Attack Pattern Enumeration and Classification
- CEE-Common Event Expression
- CPE-Common Platform Enumeration
- CVE-Common Vulnerability and Exposures
- CVRF-Common Vulnerability Reporting Format
- CVSS-Common Vulnerability Scoring System
- CWE-Common Weakness Enumeration
- CWSS-Common Weakness Scoring System
- OCIL-Open Checklist Interactive Language
- OVAL-Open Vulnerability And Assessment Language
- XCCDF-Extensible Configuration Checklist Description Format
- XDAS-Distributed Audit Service
- ISO/IEC 19770

## 2.30.5. Real Time Inter-Network Defense

Αυτό το standard είναι ουσιαστικά μία προληπτική μέθοδος η οποία διευκολύνει την ανταλλαγή δεδομένων αντιμετώπισης περιστατικών με ταυτόχρονη ανίχνευση και μετριασμό για μία ολοκληρωμένη λύση χειρισμού τους. Οι πέντε λειτουργίες του RID είναι το Αίτημα, η Αναγνώριση, το Αποτέλεσμα, η Αναφορά και η Ερώτηση. Υπάρχουν διάφοροι τύποι «σχέσεων» μεταξύ των μερών στα οποία διαμοιράζονται τα δεδομένα και οι οποίες καθορίζουν μία πολιτική ανταλλαγής τους. Κάποιες από αυτές τις «σχέσεις» είναι οι:ClientTo SP (Service Provider), SPToClient, IntraConsortium, PeerToPeer και BetweenConsortiums. Εδώ δημιουργείται και μία ελαστικότητα στην επικοινωνία μεταξύ οργανισμών ή επιχειρήσεων. Για παράδειγμα, άμεση ανταλλαγή δεδομένων μεταξύ οργανισμών είναι εφικτή από την PeerToPeer «σχέση», ενώ η IntraConsortium προτείνεται για ανταλλαγή δεδομένων μεταξύ μελών μίας κοινότητας.

## 2.30.6. Περίληψη της MILE

Η ομάδα MILE-Managed LightWeight Incident Exchange Summary περικλείει τα standards IODEF, IODEF-SCI και RID. Το IODEF αναφέρεται στην R1 απαίτηση, για χρήση συγκεκριμένου format δεδομένων. Το IODEF-SCI σχετίζεται με την R2 απαίτηση ενώ το RID σχετίζεται με τις R5 και R6 απαιτήσεις.

## 2.30.7. Πλαίσιο Ανοικτών Δεικτών Διακινδύνευσης (OpenIOC)

Το standard αυτό (Open Indicators Of Compromise) προτάθηκε το 2011 και αφορά περιπτώσεις Τακτικού CTI, ενώ περιέχει τεχνικές λεπτομέρειες όρων για Δείκτες. Σε αυτούς τους όρους είναι εύκολο να προστεθούν και άλλοι, νέοι όροι, αφού οι ορισμοί τους είναι ξεχωριστοί από το κυρίως schema. Οι περισσότεροι των όρων αφορούν κυρίως έννοιες host, όπως για παράδειγμα file, driver, disk system, διαδικασία (process) και αρχειοθέτηση (registry). Ως παραδείγματα αναφέρουμε τα "File Name" και "File MD5 Hash". Όλοι οι ορισμοί αποθηκεύονται σε ένα XML schema.

Ας δούμε λίγο τον τρόπο λειτουργίας του συγκεκριμένου standard. Εδώ, με τη χρήση της λογικής Bool, συνδυάζεται ένας αριθμός IOC's, για αναγνώριση κάποιου malware ή οικογένειας αυτού. Αναφέρουμε το εξής παράδειγμα: Έστω ότι έχουμε ένα αρχείο DLL (Dynamic Link Library), το οποίο «τρέχει» μία υπηρεσία και το οποίο έχει την δική του, νόμιμη, ψηφιακή υπογραφή. Εάν βρεθεί ένα αρχείο DLL το οποίο δεν έχει μία ψηφιακή, νόμιμη, υπογραφή, αποτελεί (ως γεγονός), ένα IOC. Η διαδικασία αυτή αφορά γνωστά malwares και σχετίζεται με την ανίχνευση μεθοδολογίας ή κάποιας άλλης ένδειξης του ότι το υπολογιστικό σύστημα έχει προσβληθεί. Τα χαρακτηριστικά του συγκεκριμένου standard πληρούν τις προδιαγραφές των R1 και R2 απαιτήσεων.

Υπήρξε ένα περιστατικό σχετικό με το Nettraveler malware, το οποίο είχε πρωτίστως αναφερθεί από την Kaspersky ως ένα αρχείο IOC σε XML μορφή. Υπάρχει μία ιστοσελίδα, η ioc.forensicarftifacts.com, στην οποία διαμοιράζονται και υποβάλλονται OpenIOC αρχεία. Η εταιρεία McAfee έχει διαθέσιμα αρχεία OpenIOC για το κοινό αλλά και προϊόντα τα οποία «καταναλώνουν» αρχεία OpenIOC.

## 2.30.8. Λεξιλόγιο για καταγραφή γεγονότων και διαμοιρασμού περιστατικών (VERIS)

Το VERIS-Vocabulary for Event Recording and Incident Sharing βγήκε στην παραγωγή το 2010 και απο τον τίτλο του καταλαβαίνει κανείς ότι πρόκειται για ένα standard για τον ορισμό του πως θα ανταλλάσσονται πληροφορίες ψηφιακών συμβάντων. Η εταιρεία Verizon, μέσω της ετήσιας αναφοράς διερεύνησης περιστατικών – DBIR- Data Breach Investigation Report, δίνει ώθηση στο VERIS αλλά μπορούν και άλλες εταιρείες να συνεισφέρουν στο VERIS, και με αυτός ο τρόπος οδηγεί στον σχηματισμό ενός μεγάλου σετ δεδομένων, από το οποίο είναι εφικτή η άντληση πληροφοριών οι οποίες θα προορίζονται για ανάλυση και για αναφορές. Ουσιαστικά μιλάμε για ένα σετ δεδομένων, στο οποίο υπάρχει μία γλώσσα επικοινωνίας για πλήρη περιγραφή περιστατικών σε μία δομημένη και επαναλήψιμη μορφή. Και ο τελικός σκοπός του VERIS είναι η απόκτηση πολύτιμης γνώσης μέσα από τις εμπειρίες και η οποία οδηγεί σε υλοποίηση καλύτερων τακτικών διαχείρισης ρίσκου.

Υπάρχουν 5 κατηγορίες στις οποίες διαιρείται το schema του VERIS: Ιχνηλάτηση, Δημογραφικά Στοιχεία Θύματος, Περιγραφή Περιστατικού, Ανακάλυψη και Ανταπόκριση και Εκτίμηση Επίπτωσης. Σε κάθε κατηγορία υπάρχουν στοιχεία με συγκεκριμένους τύπους δεδομένων και ονομάτων μεταβλητών. Για παράδειγμα υπάρχουν στοιχεία με ονομασίες "Incident Summary", Confidence Rating", Primary Industry" και "Hacking Variety". Κάποια από αυτά τα στοιχεία απαριθμούν αλλά και ονοματίζουν κάποιες λίστες υπο-στοιχείων. Πχ το στοιχείο "Hacking Variety" , περιέχει μία λίστα με 64 «ποικιλίες» τρόπων hacking και για τον κάθε τρόπο από

αυτούς υπάρχει και μία ονομασία όπως “Brute Force”, “Buffer Overflow”, “Cache Poisoning” κλπ. Η αρνητική πλευρά του VERIS είναι το ότι έχει περιορισμένη δυνατότητα του να συμπεριλάβει IOC’s, αλλά την συγκεκριμένη λειτουργία την έχει ένα απλό στοιχείο IOC (αποθήκευση και σχολιασμός μίας πληροφορίας). Ας μην ξεχνάμε ότι το VERIS χρησιμοποιείται για στρατηγική χρήση πληροφοριών και όχι για τακτική χρήση αυτών.

Η εταιρεία Verizon παρέχει στο κοινό μία βάση δεδομένων με 1200 περιστατικά από το τμήμα HHS-Health and Human Services αλλά και από άλλα περιστατικά και αυτή η βάση είναι σε JSON format. Επίσης, η εν λόγω εταιρεία χρησιμοποιεί το standard VERIS για να παράγει DBIR δεδομένα. Και τέλος, το 2013, 19 οργανισμοί τροφοδότησαν το κοινό με δεδομένα περιστατικών με τους εξής τρόπους: Κατευθείαν από το VERIS, μπαίνοντας σε κάποιες εφαρμογές του VERIS ή μετατρέποντας δεδομένα από άλλα schemas.

Το VERIS καλύπτει τις R2 απαιτήσεις και είναι σχεδιασμένο για χρήση πληροφοριών με στρατηγικό και όχι τακτικό τρόπο.

## 2.31.Mitre Standards CyBOX, STIX, TAXII

Έχουμε 3 standards σε αυτήν την περίπτωση, όπου το καθένα χρησιμοποιείται για την κάλυψη διαφορετικών αναγκών, για κάποιο σύστημα CTI. Ας τα δούμε από την αρχή. Το CyBOX-Cyber Observable eXpression αποτελεί ένα standard το οποίο καθορίζει κάποιες λεπτομέρειες των δεικτών, τις οποίες λεπτομέρειες τις ονομάζει “observables”. Το STIX-Structured Threat Information Expression, είναι ένα standard το οποίο καθορίζει την εμφάνιση μοτίβων των observables σε ένα γενικό πλαίσιο και το standard TAXII-Trusted Automated Exchange of Indicator Information, έχει να κάνει με την ανταλλαγή δεδομένων Cyber Intelligence. Τα 3 standards αυτά λειτουργούν μαζί, ως μία μονάδα, αφού έτσι είχαν σχεδιαστεί από την αρχή.

### 2.31.1. Το CyBOX-Cyber Observable eXpression

Το CyBOX παρέχει λεπτομέρειες σχετικά με κάποια περιστατικά τα οποία μπορούν να μετρηθούν και με κάποιες ιδιότητες. Στο CyBOX παράγονται ορισμένα «αντικείμενα» (objects), τα οποία χρησιμοποιούνται σε υψηλότερο επίπεδο λειτουργίας, όπως για παράδειγμα στο STIX. Το CyBOX βγήκε στην παραγωγή το 2010, αφού είχε προηγηθεί, το 2009, η σχετική πρόταση.

Ο στόχος του CyBOX είναι να παρέχει μία αυτόματη διαδικασία διαμοιρασμού δεδομένων CTI και το κάνει αυτό, παράγοντας 70 διαφορετικά «αντικείμενα», τα οποία χρησιμοποιούνται για κάποια περιστατικά τα οποία μπορούν να μετρηθούν αλλά και για κάποιες ιδιότητες. Μπορούμε να αναφέρουμε ως παραδείγματα «αντικειμένων» τα: File, HTTP Session, Mutex, Network Connection, Network Flow και X509 Certificate. Υπάρχει παράδειγμα χρήσης του object Network Connection στο site του CyBOX.

Για την εκμετάλλευση των δεδομένων του CyBOX, υπάρχουν διάφοροι τρόποι. Ο ένας είναι κάποιες «βιβλιοθήκες» (libraries) της γλώσσας Python, τα λεγόμενα bindings, οι οποίες μας παρέχουν έναν τρόπο σύνδεσης με ορισμένους τύπους δεδομένων Python. Ένας άλλος τρόπος είναι μέσω των API’s-Helper Application Programmer Interfaces, δηλ κάποιων εφαρμογών διεπαφής, οι οποίες χρησιμοποιούνται για «διάβασμα» (parsing), δημιουργία (creating) και επεξεργασίας (editing) των «αντικειμένων» του CyBOX. Τελικά, το CyBOX χρησιμοποιείται στο STIX, το οποίο θα δούμε αμέσως μετά.

## 2.31.2. Structured Threat Information eXpression (STIX)

Η πρώτη έκδοση του STIX , η 1.0, υπήρξε τον Απρίλιο του 2013, ενώ έως τώρα βρίσκεται σε εφαρμογή η έκδοση 1.1. Το συγκεκριμένο standard έχει ως στόχο 4 σημεία: Την ανάλυση των ψηφιακών απειλών, τον καθορισμό των μοτίβων των δεικτών και την διαχείριση ενεργειών πρόληψης, αντιμέτρων και διαμοιρασμού δεδομένων cyber intelligence. Καθορίζει, χρησιμοποιώντας αρχεία XML, κάποια στοιχεία σχετικά με ψηφιακές απειλές, όπως συντονισμένες επιθέσεις, εκμετάλλευση στόχων, περιστατικά, δείκτες, παράγοντες κινδύνου και TTP's, αλλά μπορεί και να συσχετίσει τα παραπάνω, πχ να συσχετίσει έναν παράγοντα κινδύνου με TTP. Στο site του STIX υπάρχει ένα παράδειγμα στο οποίο, μέσω της χρήσης ενός δείκτη, παρακολουθείται μια λίστα «ύποπτων» domains.

## 2.31.3. Μια βαθύτερη ματιά στο STIX

Η ανάγκη διαμοιρασμού πληροφοριών CTI (Cyber Threat Intelligence), οδήγησε στην επινόηση του εργαλείου STIX. Ουσιαστικά, το STIX αποτελεί μία, από κοινού, προσπάθεια, να μπορούν οι πληροφορίες που συλλέγονται, να είναι όσο το δυνατόν περισσότερο ευανάγνωστες, να μπορούν να προστεθούν σε αυτές και άλλες πιο φρέσκες (να είναι δηλ. επεκτάσιμες) και να παράγονται και να καταναλώνονται με αυτοματοποιημένο τρόπο. Υπάρχει λοιπόν η κοινότητα του STIX, στην οποία μπορούν να συμμετέχουν όλοι οι ενδιαφερόμενοι. Σε αυτή, παράγονται ή καταναλώνονται πληροφορίες (από τα SOC'S-Security Operation Centers), υπάρχουν οι CERT ομάδες, ειδικοί του cyber security, και άλλα groups, και όλοι αυτοί μπορούν να ανταλλάσσουν μεταξύ τους μέσω διάφορων μοντέλων επικοινωνίας.

Ουσιαστικά, το STIX θα λέγαμε ότι είναι μία γλώσσα επικοινωνίας, η οποία χρησιμοποιείται για την συγκέντρωση, την συγκεκριμενοποίηση, και τον διαμοιρασμό τυποποιημένης πληροφορίας CTI και αυτό γίνεται μέσω συγκεκριμένων και δομημένων διαδικασιών για τη διασφάλιση της αυτοματοποίησης και της υποστήριξης διαδικασιών διαχείρισης για περιπτώσεις κινδύνων (cyber threat). Η πληροφορία αυτή λοιπόν που διαμοιράζεται, οδηγεί στην δημιουργία ορισμένων περιπτώσεων μελέτης (use cases), οι οποίες μπορεί να είναι οι εξής:

Η ανάλυση των κινδύνων

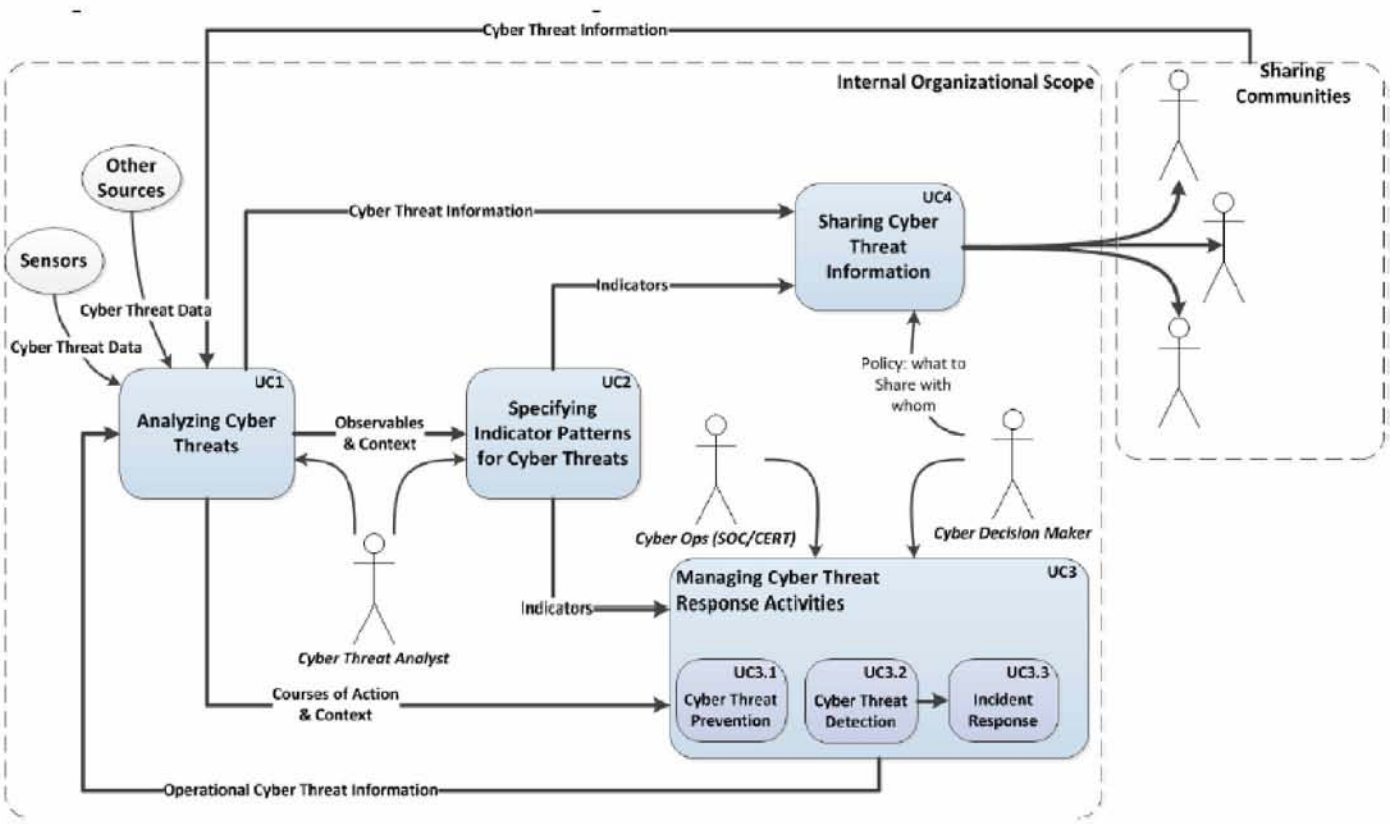
- Για κάθε έναν από τους κινδύνους, η συγκεκριμενοποίηση τους με την αντιστοιχία σε αυτούς, ορισμένων δεικτών μοτίβων
- Η διαχείριση ορισμένων δραστηριοτήτων με τις οποίες υλοποιούνται αντίμετρα σε επιθέσεις
- Ο διαμοιρασμός των πληροφοριών CTI

Επίσης, το STIX είναι δομημένο με τέτοιον τρόπο, με τον οποίο συγκεντρώνονται και συσχετίζονται μεταξύ τους, πληροφορίες CTI από διαφορετικές περιπτώσεις, οι οποίες μπορεί να είναι:

- Πληροφορίες τύπου Cyber Observables
- Δείκτες
- Ψηφιακά συμβάντα

- Τα TTP's των επιτιθέμενων (Tactics, Techniques and Procedures), όπως για παράδειγμα εργαλεία, kill chains, malware, μοτίβα επίθεσης κλπ
- Τρωτότητες μέσω των οποίων οι επιθέσεις κατέληξαν στους στόχους τους
- Διάφορα αντίμετρα άμυνας, ,όπως ενέργειες τύπου Incident Response ή μετριασμός των επιπτώσεων σε έναν οργανισμό
- Διάφορα campaigns για επιθέσεις
- Ομάδες επιτιθέμενων

Όπως βλέπουμε, συνωστίζεται ένας μεγάλος όγκος πληροφορίας, ο οποίος προέρχεται από διάφορα πεδία. Ένα θετικό στοιχείο του STIX, είναι ότι εάν ένας χρήστης-μέλος του θελήσει να αντλήσει στοιχεία για ένα συγκεκριμένο use case, θα βρει τις κατάλληλες πληροφορίες για αυτό και δεν θα χρειάζεται να ψάχνει σε όλα τα use cases, δηλ υπάρχει το κατάλληλο «φιλτράρισμα» για το σκοπό αυτό. Παρακάτω, στην εικόνα 2.14 βλέπουμε μία γενική εικόνα στην οποία εμπεριέχονται διάφορα βασικά use cases (μελέτες περιπτώσεων) και πως αυτά διαχειρίζονται από το STIX.




(εικόνα 2.14: Διάφορα use cases και η διαχείριση τους από το STIX)

Όπως παρατηρούμε στην εικόνα 2.14, οι εισερχόμενες πληροφορίες αναλύονται αρχικά από έναν ειδικό αναλυτή και μετά, κάποιες από αυτές καταλήγουν σε ομάδες SOC ή CERT και κάποιες άλλες διαμοιράζονται σε άλλες ομάδες ή κοινότητες. Ας δούμε λίγο πιο αναλυτικά το κάθε ένα στάδιο από αυτά.

Σε πρώτη φάση λοιπόν, λαμβάνει χώρα η ανάλυση των εισερχόμενων πληροφοριών. Αυτές οι πληροφορίες προέρχονται από κάποιες πηγές και έχουν συλλεχθεί είτε «χειροκίνητα» ή με αυτοματοποιημένο τρόπο. Ο αναλυτής, έχοντας στα χέρια του τις πληροφορίες αυτές, τις ταξινομεί, αναλόγως του τύπου της απειλής, σε ομάδες, όπου σε κάθε ομάδα βάζει έναν «τίτλο» με τέτοιο τρόπο έτσι ώστε όλη η υπάρχουσα γνώση για τον «τίτλο» αυτό να μπορεί να εκφραστεί και να αναπτυχθεί. Η υπάρχουσα γνώση για κάθε ένα «τίτλο» ή ομάδα απειλών, συνήθως περιέχει προθέσεις, ενέργειες και μοτίβα επιθέσεων και ικανότητες των κακόβουλων χρηστών. Από εκεί και μετά, ο αναλυτής μπορεί να ορίσει κάποιους δείκτες, οι οποίοι συνδέονται άρρηκτα με κάποια μοτίβα και φυσικά να στείλει τις κατάλληλες πληροφορίες στο αντίστοιχο «κανάλι»: Κάποιες από αυτές θα σταλούν σε Response Teams, ενώ κάποιες άλλες θα σταλούν για την ενημέρωση διάφορων κοινοτήτων και ομάδων. Για παράδειγμα, στην περίπτωση ενός phising e-mail, ο αναλυτής θα εξετάσει τυχόν «ύποπτα» attachments, θα δει σε ποια links μπορεί να οδηγούν αυτά τα attachments, εάν τα links είναι «ύποπτα» και εάν έχουν ακολουθηθεί, σε ποιους έγινε προώθηση το e-mail αυτό και φυσικά κρατάει ένα αρχείο για κάθε στάδιο ανάλυσης.

Σε δεύτερη φάση, κάποια χαρακτηριστικά των διάφορων απειλών τα οποία παρατηρούνται από τον αναλυτή, συγκεκριμενοποιούνται με διάφορα μοτίβα με τα οποία αντιπροσωπεύονται και κάθε ένα μοτίβο από αυτά, προσδίδεται ένα «περιεχόμενο» και κάποια μεταδεδομένα, με σκοπό την περαιτέρω «μετάφραση» και το χειρισμό τους, και αυτό γίνεται είτε χειροκίνητα, είτε με αυτοματοποιημένο τρόπο με τη χρήση διάφορων εργαλείων. Έστω ότι έχουμε μία επίθεση phising. Εδώ, ο αναλυτής θα πρέπει να βάλει στο μικροσκόπιο όλα τα παρελκόμενα και παρατηρούμενα στοιχεία του e-mail αυτού, όπως διευθύνσεις αποστολής και λήψης, τύποι των attachments και κάποια ενσωματωμένα URL's, για την ανάλυση του. Και αυτό το κάνει για να ανακαλύψει τα TTP’s τα οποία βρίσκονται πίσω από την phising αυτή επίθεση, να εντοπίσει το kill chain, να παρέχει συγκεκριμένες οδηγίες χειρισμού, να προσδώσει έναν δείκτη για αυτό, να παράξει ορισμένα μοτίβα για τον δείκτη αυτό (πχ Snort, YARA, OVAL), να προτείνει τρόπους αντιμετώπισης και όλες αυτές τις πληροφορίες να τις «πακετάρει» και να τις στείλει διαμοιράζοντάς τες και έτσι δημιουργείται και μία εγγραφή η οποία θα μπορεί να χρησιμοποιείται και στο μέλλον.

### 2.31.3.1 Η διαχείριση των ενεργειών άμυνας

Οι ενέργειες της άμυνας μπορούν να περιλαμβάνουν ανίχνευση μίας απειλής, διερεύνηση της και υλοποίηση αντίστοιχων ενεργειών. Για παράδειγμα, στην περίπτωση μίας επίθεσης phising, η οποία αντιπροσωπεύεται από έναν δείκτη, οι ειδικοί της Κυβερνοασφάλειας προσπαθούν να κατανοήσουν το πώς λειτουργεί η επίθεση αυτή, δηλ. το πώς εγκαθίσταται και δρα το malware στα υπολογιστικά συστήματα, να υπολογίσουν το συνολικό κόστος και την αποτελεσματικότητα των αντίμετρων και τελικά να εφαρμόσουν τα κατάλληλα αντίμετρα πρόληψης ή ανίχνευσης.

Τα προληπτικά μέτρα, εφαρμόζονται με σκοπό να προστατεύσουν τα υπολογιστικά συστήματα, πριν συμβεί κάποια επίθεση σε αυτά. Αυτό γίνεται με τη βοήθεια των δεικτών, δηλ. με τη «μετάφραση» τους, η οποία βοηθά σε ενέργειες πρόληψης ή μετριασμού των επιπτώσεων μίας επίθεσης. Έστω πχ ότι έχουμε μία επίθεση phising, στην οποία έχει προσδοθεί ένας συγκεκριμένος δείκτης. Οι ειδικοί της Κυβερνοασφάλειας θα πρέπει να προτείνουν ορισμένα αντίμετρα (πχ «κλείσιμο» μίας διόδου στην λήψη των e-mails) και να υπολογίζουν κάθε φορά το κόστος και το ρίσκο αυτών.

Τα μέτρα ανίχνευσης, περιλαμβάνουν ενέργειες κατά τις οποίες είτε εξετάζεται το ιστορικό επιθέσεων (για να εντοπιστούν τυχόν ίδιες επιθέσεις), είτε «μεταφράζονται» οι δείκτες, ή υπάρχει μία συνεχής εγρήγορση η οποία στοχεύει στον εντοπισμό νεών απειλών. Πχ σε επίθεση phising, οι ειδικοί του cyber security αποκομίζουν από τον δείκτη πληροφορίες για το μοτίβο της εν λόγω επίθεσης και το οποίο εφαρμόζουν σε λειτουργικό περιβάλλον για να μελετήσουν το πώς δρα η επίθεση phising αυτή.

Τα μέτρα άμυνας ή άμεσης ανταπόκρισης, περιλαμβάνουν ενέργειες οι οποίες απαντούν σε ήδη εντοπισμένες απειλές ή επιθέσεις, και προσπαθούν να ανιχνεύσουν την φύση των απειλών αυτών, με ταυτόχρονη προσπάθεια επανόρθωσης των συστημάτων ή μετριασμού της επίπτωσης της επίθεσης. Στην περίπτωση μίας επίθεσης phising, γίνεται έρευνα για το αν πχ το malware όντως εγκαταστάθηκε και έδρασε επιτυχώς, και αν ναι, ποια συστήματα επηρεάστηκαν, ποια δεδομένα υποκλάπηκαν κλπ. Μετά, αποφασίζονται ενέργειες επανόρθωσης ή μετριασμού όπως «καθαρισμός» των συστημάτων από το malware, μπλοκάρισμα των διόδων εξαγωγής δεδομένων κλπ.

### 2.31.3.2.Ο διαμοιρασμός των πληροφοριών

Όπως είδαμε και προηγουμένως, εκτός των άλλων ενεργειών, υπάρχει και ο διαμοιρασμός των πληροφοριών ο οποίος ακολουθεί κανόνες όπως συνέπεια, έλεγχος και περιεχόμενο, ενώ ανταλλάσσονται πληροφορίες ή δείκτες.Πχ στην περίπτωση επίθεσης phising, η οποία έχει χαρακτηριστεί από ορισμένους δείκτες, οι ειδικοί της άμυνας, επιτρέπουν τον διαμοιρασμό των δεικτών αυτών και σε άλλα μέλη ή σε κοινότητες, με σκοπό την ενημέρωσή τους και την απόκτηση της γνώσης αυτής.

## 2.32.Trusted Automated eXchange of Indicator Information

Το TAXII χρησιμοποιείται για την ανταλλαγή δεδομένων CTI και πιο συγκεκριμένα καθορίζει τον τρόπο του πως θα διαμοιράζονται τα δεδομένα του CTI. Η πρώτη εφαρμογή του TAXII προτάθηκε το 2012.

Η φιλοσοφία του TAXII εδράζεται στα λεγόμενα «μοντέλα» διαμοιρασμού δεδομένων, όπως τα “hub and spoke”, “peer to peer” κλπ. Στην μορφή αυτή επικοινωνίας, τα «μοντέλα» δίνουν την δυνατότητα αμφίδρομης ανταλλαγής δεδομένων στους χρήστες, ενώ υποστηρίζονται από 4 βασικές υπηρεσίες: Ανακάλυψη, Διαχείριση Τροφοδότησης, Εισερχόμενα και Εγγραφές.

Η κάθε μία υπηρεσία αποτελείται από διάφορα μέρη. Για παράδειγμα, η Διαχείριση Τροφοδότησης αποτελείται από τα: υπογραφή, διαγραφή, παύση, διανομή, τροποποίηση συνδρομής, κατάσταση ερωτήματος. Τα Εισερχόμενα λαμβάνουν πληροφορίες από ανατροφοδοτήσεις. Οι Εγγραφές υποστηρίζονται από άτομα τα οποία παράγουν πληροφορίες και τις οποίες ζητούν οι «καταναλωτές» δεδομένων, σε μία χρονική στιγμή. Τέλος, η Ανακάλυψη έχει να κάνει με την αναγνώριση των διαφόρων υπηρεσιών και το πώς αυτές λειτουργούν.

Για τη μεταφορά μηνυμάτων και περιεχομένου, χρησιμοποιούνται XML και HTTP, ενώ χρησιμοποιούνται μηχανισμοί οι οποίοι διαφυλάσσουν την ακεραιότητα, την εμπιστευτικότητα και την απόδοση.

Το TAXII χρησιμοποιείται από μεγάλες εταιρείες και οργανισμούς, όπως η Microsoft. Η Microsoft έχει εντάξει σε ένα πρόγραμμα της, το “Microsoft Active Protections Program” (MAPP),

στο οποίο, μέλη του MAPP μπορούν να ανταλλάσσουν μεταξύ τους CTI δεδομένα. Ένας άλλος φορέας ο οποίος χρησιμοποιεί το TAXII είναι το Κέντρο Διαμοιρασμού και Ανάλυσης Πληροφοριών Χρηματοοικονομικών Υπηρεσιών (Financial Services Information Sharing Analysis Center-FS/ISAC, όπου μέλη του εν λόγω οργανισμού μπορούν να έχουν πρόσβαση σε δεδομένα CTI, χρησιμοποιώντας τα STIX και TAXII.

## 2.33.Open Threat Exchange

Το OTX-Open Threat Exchange, επινοήθηκε από τον Alien Vault το 2012 και ο σκοπός του είναι η ανταλλαγή δεδομένων σχετικών με ψηφιακές απειλές. Είναι ένα σύστημα το οποίο συλλέγει δεδομένα CTI από συσκευές cyber security και τα οποία επικυρώνει και δημοσιεύει. Έχει τη δυνατότητα συνεργασίας και με άλλα συστήματα, όπως τα SIEM (Security and Information Event Management), τα οποία είναι δωρεάν για τους χρήστες. Οι τελευταίοι ρυθμίζουν τα συστήματα τους, προκειμένου να κάνουν upload τα δικά τους δεδομένα CTI και τα οποία επικυρώνονται από τον Alien Vault. Μετά, τα δεδομένα αυτά διαμοιράζονται σε όλους τους χρήστες οι οποίοι συνεισφέρουν και αυτοί στο OTX. Παρακάτω, παραθέτουμε ένα παράδειγμα «φήμης» δεδομένων (εγγραφών) από κάποια IP's:

64.202.163.216 # Malware Domain US,Scottsdale,33.6119003296,-111.890602112
50.22.225.203 # Scanning Host US,Dallas,32.929901123,-96.8352966309
189.4.93.167 # Scanning Host „32.929901123,-96.8352966309
217.107.219.76 # Malware IP RU„60.0,100.0
198.56.193.26 # Scanning Host US„38.0,-97.0
174.122.148.162 # C&C US,Houston,29.7523002625,-95.3669967651
75.127.114.52 # C&C;Malware IP US,Atlanta,33.7257003784,-84.4309005737

Επίσης, οι χρήστες του CIF (Collective Intelligence Framework), το οποίο θα δούμε παρακάτω, έχουν πρόσβαση στο OTX.

Ο σκοπός του OTX είναι ένας αυτοματοποιημένος τρόπος διαμοιρασμού CTI δεδομένων στο κοινό και έτσι ικανοποιείται η R5 απαίτηση.

Το μειονέκτημα του OTX είναι ότι έχουν πρόσβαση και μέλη κοινοτήτων και γενικότερα οποιοσδήποτε χρήστη και έτσι δεν υπάρχει κανένας έλεγχος του ποιος έχει πρόσβαση στα δεδομένα αυτά.

## 2.34.Collective Intelligence Framework (CIF)

Το Collective Intelligence Framework αναπτύχθηκε από το Research and Education Network Information Sharing and Analysis Center (REN-ISAC) το 2009 και είναι ένα σύστημα τύπου client/server και το οποίο χρησιμοποιείται για τον διαμοιρασμό δεδομένων cyber intelligence. Τα δεδομένα που συλλέγονται είναι διευθύνσεις IP, e-mails, domains, ASN νούμερα και URL's. Υπάρχουν προγράμματα πελατών (clients) με τα οποία είναι εφικτή η πρόσβαση στον server και ένα κλασσικό client πρόγραμμα είναι ένα command line σε γλώσσα Perl.

Οι πληροφορίες που περιέχονται στο CIF περιλαμβάνουν και στοιχεία όπως τον τύπο της απειλής, την σοβαρότητα μίας επίθεσης και την εμπιστευτικότητα των δεδομένων. Επίσης, υπάρχει η δυνατότητα για περιορισμένη πρόσβαση σε δεδομένα με την χρήση ενός API-Key και

τέλος, τα δεδομένα αποθηκεύονται σε IODEF format, ενώ μπορούν να εξαχθούν για να χρησιμοποιηθούν και από άλλα εργαλεία security.

Παρακάτω, παραθέτουμε ένα παράδειγμα κατά το οποίο χρησιμοποιείται ένας command line client για URL'' με «ύποπτο» υλικό, μεσαίας επικινδυνότητας.

```
$ cif -q url/malware -s medium
restriction |severity|address
need-to-know|medium |http://derts3563d.net/old_files/root/bin/config.bin
need-to-know|medium |http://yyyaanve.ru/b.bin
```

Προσθέτουμε ότι ο CIF έχει χρησιμοποιηθεί από μέλη REN-ISAC, και ως προς την λειτουργία του, με την χρήση του command line, είναι εύκολη η εξαγωγή και χρήση δεδομένων CTI καθώς γίνεται με αυτοματοποιημένο τρόπο. Το CIF καλύπτει τις απαιτήσεις R1, R3, R4, R5, R6, R7, και R8.[7]

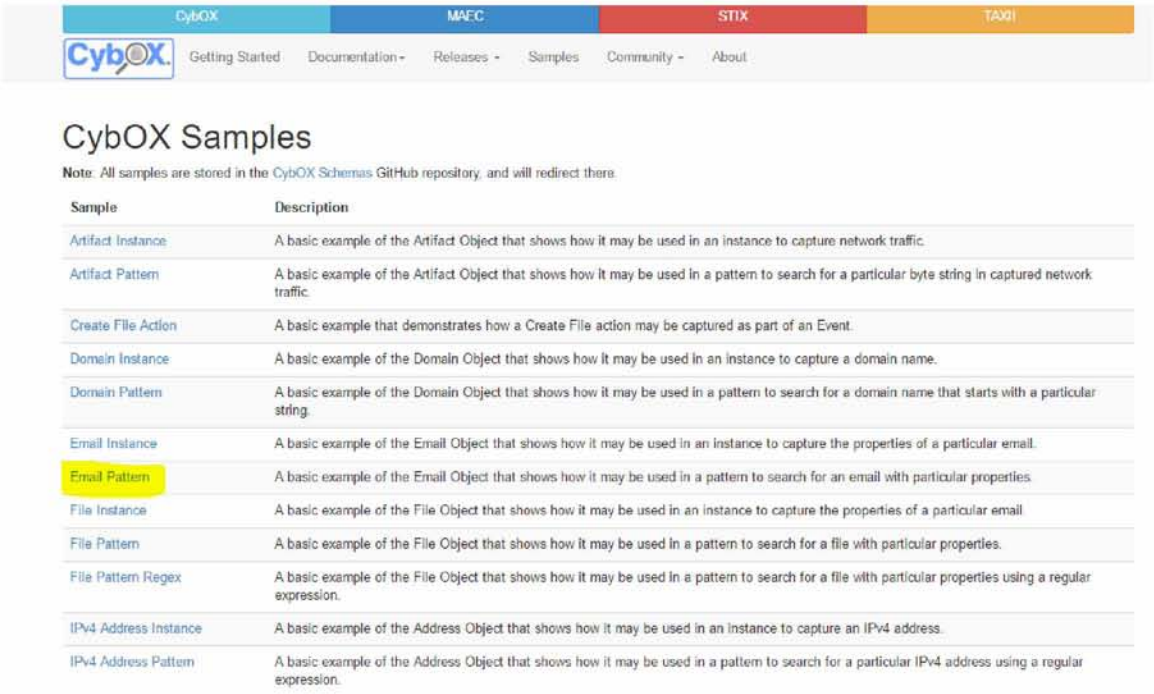
## 2.35.Παραδείγματα αρχείων από CyBOX, STIX και TAXII

Στο link https://cyboxproject.github.io/samples/ υπάρχουν κάποια παραδείγματα περιπτώσεων και αρχείων από διάφορα περιστατικά. Στην παρακάτω εικόνα βλέπουμε το περιβάλλον του CyBOX:

[7] **Greg Farnham, "Tools and Standards for Cyber Threat Intelligence Projects", October 14th 2013, pages 11-20**

**Sean Barnum, "Standardizing Cyber Threat Intelligence Information with The Structured Threat Information eXpression (STIX)", February 20, 2014, pages 2,4,7-11**

**ENISA, "Standards and tools for exchange and processing of actionable information", November 2014, pages 8,10,17,18,20**




(εικόνα 2.15: Το περιβάλλον του Cybox)

Στην εικόνα 2.15 βλέπουμε κάποια παραδείγματα στο link του CyBOX και πατώντας σε ένα από αυτά, έστω στο “Email Pattern”, έχουμε την εξής εικόνα:

3 contributors

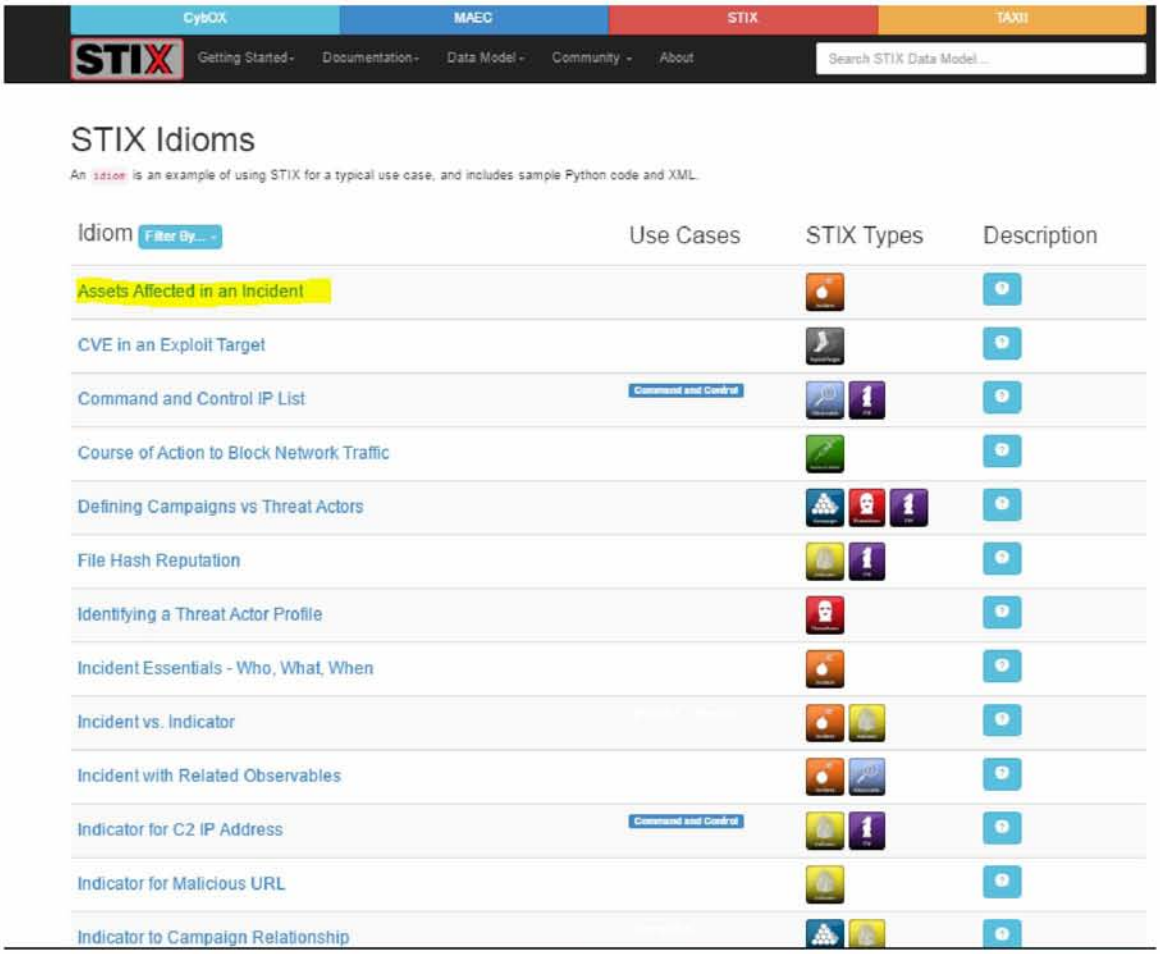
Executable File | 31 lines (30 sloc) | 1.97 KB | Raw | Blame | History

```
<?xml version="1.0" encoding="UTF-8"?>
<cybox:Observables
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:cybox="http://docs.oasis-open.org/cti/ns/cybox/core-2"
    xmlns:cyboxCommon="http://docs.oasis-open.org/cti/ns/cybox/common-2"
    xmlns:AddrObj="http://docs.oasis-open.org/cti/ns/cybox/objects/address-2"
    xmlns:URIObj="http://docs.oasis-open.org/cti/ns/cybox/objects/uri-2"
    xmlns:FileObj="http://docs.oasis-open.org/cti/ns/cybox/objects/file-2"
    xmlns:cyboxVocabs="http://docs.oasis-open.org/cti/ns/cybox/vocabularies-2"
    xmlns:EmailMessageObj="http://docs.oasis-open.org/cti/ns/cybox/objects/email-message-2"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://docs.oasis-open.org/cti/ns/cybox/core-2 ../cybox_core.xsd
    http://docs.oasis-open.org/cti/ns/cybox/objects/file-2 ../objects/File_Object.xsd
    http://docs.oasis-open.org/cti/ns/cybox/objects/email-message-2 ../objects/Email_Message_Object.xsd
    http://docs.oasis-open.org/cti/ns/cybox/vocabularies-2 ../cybox_default_vocabularies.xsd"
    cybox_major_version="2" cybox_minor_version="1" cybox_update_version="1">
    <cybox:Observable id="example:Observable-298376a2-cf65-4778-9894-ed9a95b5441d">
        <cybox:Object id="example:Object-f9769431-db6b-448f-b34e-72eb3c3e07d1">
            <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
                <EmailMessageObj:Header>
                    <EmailMessageObj:From category="e-mail">
                        <AddrObj:Address_Value condition="Equals" apply_condition="ANY">attacker@example.com##comma##attecker1@example.com#
                    </EmailMessageObj:From>
                    <EmailMessageObj:Subject condition="Equals" >New modifications to the specification</EmailMessageObj:Subject>
                </EmailMessageObj:Header>
            </cybox:Properties>
        </cybox:Object>
    </cybox:Observable>
</cybox:Observables>
```

(εικόνα 2.16: Αρχείο XML για τη συγκεκριμένη περίπτωση)

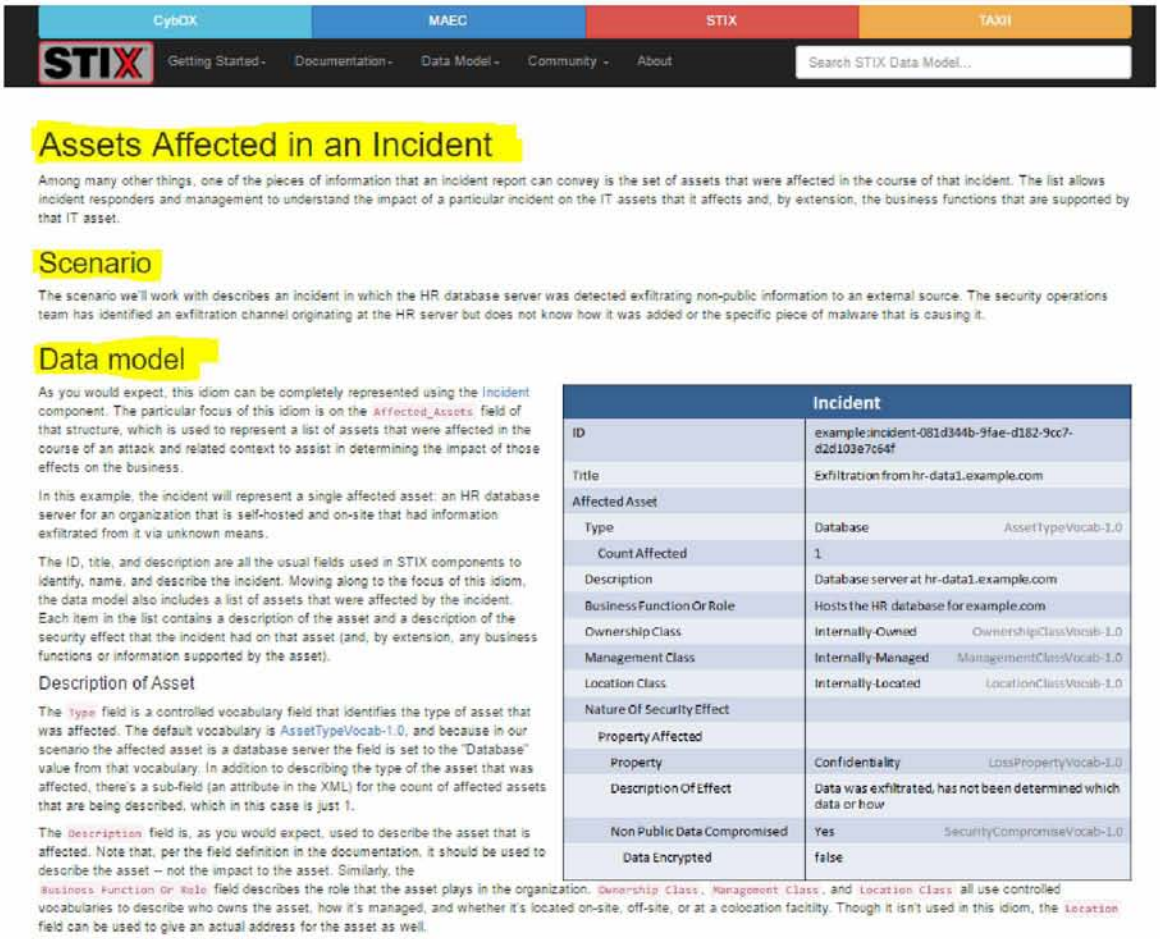
Για το συγκεκριμένο αρχείο έχουν συνεισφέρει 3 χρήστες και αφορά ένα μοτίβο το οποίο ανιχνεύει e-mails με συγκεκριμένες ιδιότητες.

Παρακάτω, στην εικόνα 2.17 βλέπουμε το περιβάλλον του STIX.




(εικόνα 2.17: Περιβάλλον του STIX)

Πατώντας έστω το πρώτο link (Assets Affected In an Incident), έχουμε την παρακάτω εικόνα:




(εικόνα 2.18: Περίπτωση μελέτης σε περιβάλλον STIX)

Στην συγκεκριμένη περίπτωση, περιγράφονται τα στοιχεία που επηρεάστηκαν σε ένα συμβάν, το γενικό σενάριο (κατά το οποίο υπήρξε υποκλοπή δεδομένων από server), το μοντέλο δεδομένων. Αν ζουμάρουμε στον πίνακα δεξιά της σελίδας, θα δούμε το εξής:

| Incident | | |
|---|---|---|
| ID | example:incident-081d344b-9fae-d182-9cc7-d2d103e7c64f | |
| Title | Exfiltration from hr-data1.example.com | |
| Affected Asset | | |
| Type | Database | AssetTypeVocab-1.0 |
| Count Affected | 1 | |
| Description | Database server at hr-data1.example.com | |
| Business Function Or Role | Hosts the HR database for example.com | |
| Ownership Class | Internally-Owned | OwnershipClassVocab-1.0 |
| Management Class | Internally-Managed | ManagementClassVocab-1.0 |
| Location Class | Internally-Located | LocationClassVocab-1.0 |
| Nature Of Security Effect | | |
| Property Affected | | |
| Property | Confidentiality | LossPropertyVocab-1.0 |
| Description Of Effect | Data was exfiltrated, has not been determined which data or how | |
| Non Public Data Compromised | Yes | SecurityCompromiseVocab-1.0 |
| Data Encrypted | false | |

(εικόνα 2.19: Ανάλυση συμβάντος)

Στην εικόνα 2.19, βλέπουμε έναν πίνακα με τα στοιχεία ενός συμβάντος. Τα πιο βασικά είναι τα εξής:

- Το ID του περιστατικού
- Ο τίτλος ο οποίος έχει αποδοθεί στο περιστατικό
- Η περιγραφή του περιστατικού
- Η περιγραφή των στοιχείων που επηρεάστηκαν κατά το περιστατικό αυτό
- Ο τύπος του στοιχείου που επηρεάστηκε αλλά και τυχόν υπο-στοιχεία (count affected) τα οποία συνδέονται με το στοιχείο αυτό (εδώ είναι μόνο 1)
- Ο ρόλος που παίζει το στοιχείο στην λειτουργία του οργανισμού
- Ο ιδιοκτήτης του στοιχείου αυτού
- Ποιος διαχειρίζεται το στοιχείο αυτό
- Η τοποθεσία του στοιχείου αυτού
- Η επιρροή σε στοιχεία ασφάλειας (Nature Security Effect)
- Property Affected- Τα στοιχεία της ασφάλειας που επηρεάστηκαν - confidentiality, integrity, and availability
- Η διαρροή ή όχι δεδομένων τα οποία δεν προορίζονται για δημόσια χρήση
- Η κρυπτογράφηση ή όχι των δεδομένων που κλαπήκαν

Παρακάτω στις εικόνες 2.20, 2.21 και 2.22 βλέπουμε ότι έχουμε 3 tabs: Το αρχείο XML, τον αλγόριθμο παραγωγής του αρχείου XML και τον αλγόριθμο «κατανάλωσης» του αρχείου XML.

Implementation

XML | Python Producer | Python Consumer

```
<stix:Incident id="example:incident-081d344b-9fae-d182-9cc7-d2d103e7c64f" xsi:type='incident:IncidentType' timestamp="2014-02-20T09:00:00.000000Z">
    <incident:Title>Exfiltration from hr-data1.example.com</incident:Title>
    <incident:Affected_Assets>
        <incident:Affected_Asset>
            <incident:Type count_affected="1">Database</incident:Type>
            <incident:Description>Database server at hr-data1.example.com</incident:Description>
            <incident:Business_Function_Or_Role>Hosts the database for example.com</incident:Business_Function_Or_Role>
            <incident:Ownership_Class xsi:type="stixVocabs:OwnershipClassVocab-1.0">Internally-Owned</incident:Ownership_Class>
            <incident:Management_Class xsi:type="stixVocabs:ManagementClassVocab-1.0">Internally-Managed</incident:Management_Class>
            <incident:Location_Class xsi:type="stixVocabs:LocationClassVocab-1.0">Internally-Located</incident:Location_Class>
            <incident:Nature_Of_Security_Effect>
                <incident:Property_Affected>
                    <incident:Property xsi:type="stixVocabs:LossPropertyVocab-1.0">Confidentiality</incident:Property>
                        <incident:Description_Of_Effect>Data was exfiltrated, has not been determined which data or how.</incident:Description_Of_Effect>
                        <incident:Non_Public_Data_Compromised data_encrypted="false">Yes</incident:Non_Public_Data_Compromised>
                </incident:Property_Affected>
            </incident:Nature_Of_Security_Effect>
        </incident:Affected_Asset>
    </incident:Affected_Assets>
</stix:Incident>
```

(εικόνα 2.20: Αρχείο XML)

Implementation

XML | Python Producer | Python Consumer

```
affected_asset = AffectedAsset()
affected_asset.description = "Database server at hr-data1.example.com"
affected_asset.type_ = "Database"
affected_asset.type_.count_affected = 1
affected_asset.business_function_or_role = "Hosts the database for example.com"
affected_asset.ownership_class = "Internally-Owned"
affected_asset.management_class = "Internally-Managed"
affected_asset.location_class = "Internally-Located"

property_affected = PropertyAffected()
property_affected.property_ = "Confidentiality"
property_affected.description_of_effect = "Data was exfiltrated, has not been determined which data or how."
property_affected.non_public_data_compromised = "Yes"
property_affected.non_public_data_compromised.data_encrypted = False

affected_asset.nature_of_security_effect = property_affected
incident = Incident(title="Exfiltration from hr-data1.example.com")
incident.affected_assets = affected_asset

print incident.to_xml()
```

Full XML | Python Producer | Python Consumer

(εικόνα 2.21: Αλγόριθμος παραγωγής αρχείου XML)

Implementation

XML Python Producer Python Consumer

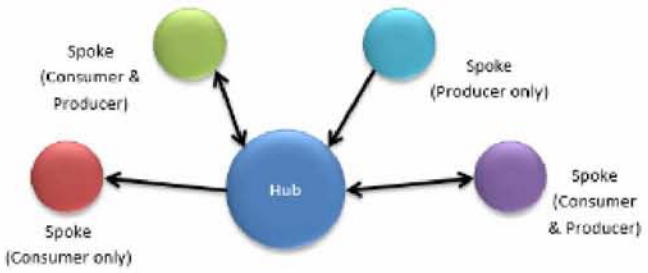
```
print "== INCIDENT Assets Impacted =="
for inc in pkg.incidents:
    print "---"
    print "Title: "+ inc.title
    for asset in inc.affected_assets:
        print "---"
        print "Description: "+ str(asset.description)
        print "Type: "+ str(asset.type_)
        print "How many: "+ str(asset.type_.count_affected)
        print "Role: " + str(asset.business_function_or_role )
        print "Owner: " +str(asset.ownership_class )
        print "Manager: " +str(asset.management_class )
        print "Location: " +str(asset.location_class )

        for effect in asset.nature_of_security_effect:
            print "---"
            print "Lost:" + str(effect.property_ )
            print "Effect:" + str(effect.description_of_effect )
            print "Was private data stolen?: " + str(effect.non_public_data_compromised )
            print "Was it encrypted?: " + str(effect.non_public_data_compromised.data_encrypted )
```

(εικόνα 2.22: Αλγόριθμος «κατανάλωσης» του αρχείου XML)

Παραθέτουμε και κάποιες επιπλέον πληροφορίες για την βιβλιοθήκη PYTHON-STIX στη συνέχεια της εργασίας, παρακάτω. Όσον αφορά το TAXII, στην σελίδα http://taxiiproject.github.io/documentation/sample-use/ έχει αρκετά παραδείγματα με κώδικα, ενώ παρατηρώντας τις εικόνες 2.23, 2.24 και 2.25 βλέπουμε τα «μοντέλα διαμοιρασμού» του TAXII.

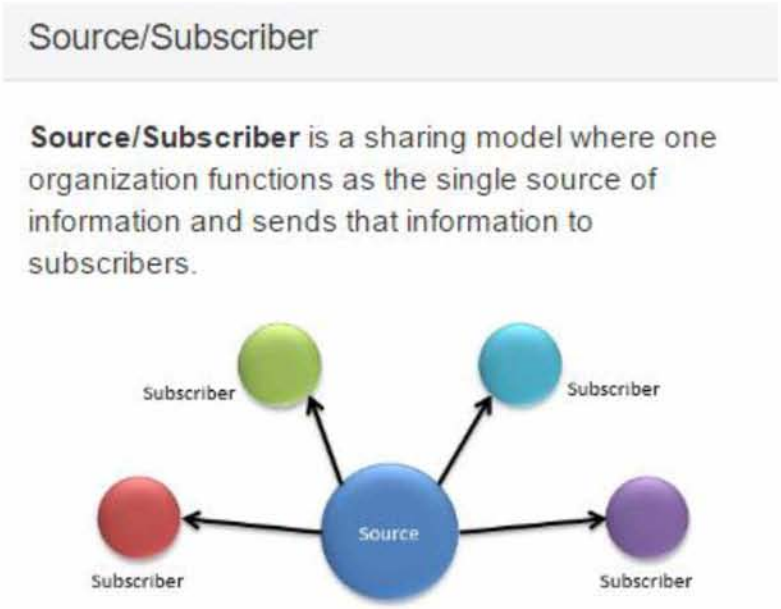
## Hub and Spoke

**Hub and Spoke** is a sharing model where one organization functions as the central clearinghouse for information, or hub, coordinating information exchange between partner organizations, or spokes. Spokes can produce and/or consume information from the Hub.



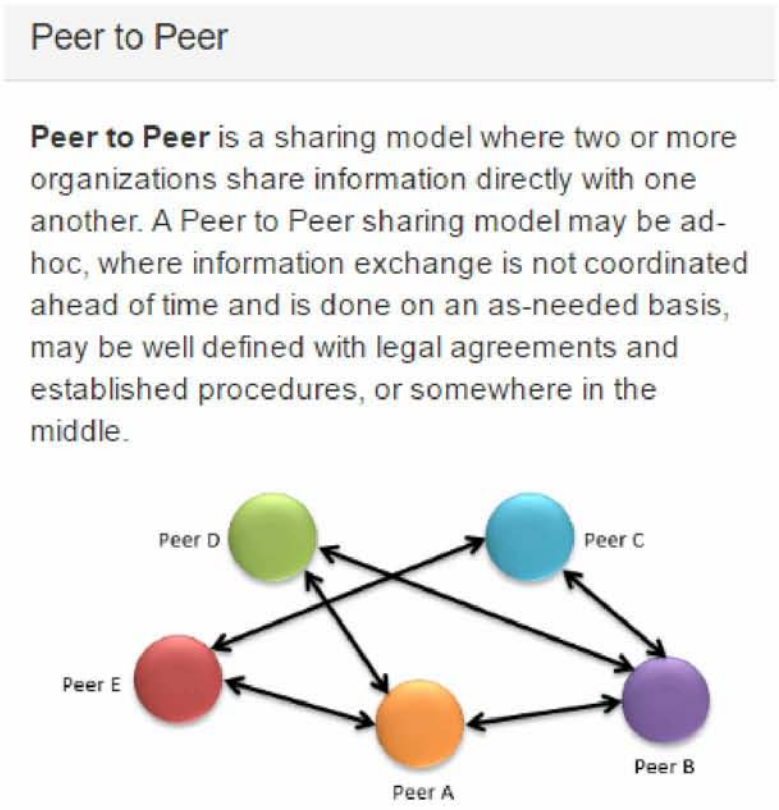
(εικόνα 2.23: Μοντέλο Hub And Spoke)

Στο μοντέλο Hub And Spoke ένας χρήστης μπορεί να είναι είτε «παραγωγός» είτε «καταναλωτής» δεδομένων.




(εικόνα 2.24: Μοντέλο Source/Subscriber)

Στο μοντέλο Source/Subscriber ένας οργανισμός ο οποίος μοιράζει σε όλους τους «καταναλωτές» τα δεδομένα.




(εικόνα 2.25: Μοντέλο Peer To Peer)

Στο μοντέλο Peer To Peer, δύο ή περισσότεροι οργανισμοί μπορούν να ανταλλάσσουν δεδομένα μεταξύ τους. [8]

## 2.36.Πληροφορίες για την βιβλιοθήκη PYTHON-STIX

Ας δούμε κάποιες βασικές πληροφορίες για την βιβλιοθήκη STIX-PYTHON. Δίνουμε τον ορισμό του API.

---

[8] **The MITRE CORPORATION, Copyright 2016, [Online]. Available: https://cyboxproject.github.io/samples/**

**Greg Back, 2016, Cybox Simple e-mail Pattern, [Online].Available: https://github.com/CybOXProject/schemas/blob/master/samples/CybOX_Simple_Email_Pattern.xml**

**The MITRE CORPORATION, Copyright 2016, [Online]. Available:http://stixproject.github.io/documentation/idioms/**

**The MITRE CORPORATION, Copyright 2016, [Online]. Available:http://taxiiproject.github.io/about/**

**The MITRE CORPORATION, Copyright 2016, [Online].Available:http://taxiiproject.github.io/documentation/sample-use/**

**API (Application Programming Interface):** Η Διεπαφή Προγραμματισμού Εφαρμογών είναι ουσιαστικά ένα σύνολο αποτελούμενο από εργαλεία και ορισμούς και μέσω των οποίων υλοποιούνται διάφορα softwares και εφαρμογές (με τη βοήθεια προγραμματιστών φυσικά). Η Διεπαφή είναι αυτή που ορίζει και διατυπώνει τις λειτουργίες πχ μίας βιβλιοθήκης ή ενός λειτουργικού συστήματος σε άλλα προγράμματα. Για παράδειγμα, ένας ιδιώτης Α θέλει να στείλει ένα γράμμα μέσω ταχυδρομείου σε έναν άλλο ιδιώτη Β. Για να μπορέσει να στείλει το γράμμα ο Α στον Β, θα πρέπει να ακολουθήσει συγκεκριμένους κανόνες (πχ αναγραφή διεύθυνσης, γραμματόσημο κλπ) οι οποίοι ναι μεν καλώς υπάρχουν, αλλά πίσω από αυτούς κρύβεται ένας τεράστιος μηχανισμός ανθρώπων, υπολογιστών και οχημάτων, ο οποίος υπάρχει για τον σκοπό αυτό:Την αποστολή του γράμματος. Άρα λοιπόν, εδώ η διεπαφή είναι οι υπηρεσίες του ταχυδρομείου, δηλ το «συμβόλαιο κλήσης» μεταξύ καλούντα (ιδιώτης Α) και καλούμενου (ταχυδρομείο).

Έτσι λοιπόν, η βιβλιοθήκη PYTHON-STIX αποτελεί και αυτή ένα API, το οποίο μπορεί να χρησιμοποιηθεί για την παραγωγή και «κατανάλωση» περιεχομένου STIX, όπως έχουμε προαναφέρει. Ουσιαστικά, αυτή η κατηγορία προγραμματιστών, η οποία θέλει να παράγει, να «καταναλώνει», και να «μεταφράζει» περιεχόμενο STIX, έχει στη διάθεσή της ένα πολύ καλό εργαλείο, την PYTHON-STIX βιβλιοθήκη.

Υπάρχουν αντιστοιχίες εκδόσεων python-stix με εκδόσεις stix γλώσσας, για να μπορεί να υπάρχει συμβατότητα στην λειτουργία μεταξύ τους. Αυτές έχουν ως εξής:

| **STIX Version** | **PYTHON-STIX Version** |
|---|---|
| 1.2 | 1.2.0.0 (PyPI) (GitHub) |
| 1.1.1 | 1.1.1.5 (PyPI) (GitHub) |
| 1.1.0 | 1.1.0.6 (PyPI) (GitHub) |
| 1.0.1 | 1.0.1.1 (PyPI) (GitHub) |
| 1.0 | 1.0.0a.7 (PyPI) (GitHub) |

Το python-stix για να λειτουργεί σωστά, δηλ για να μπορεί να επεξεργάζεται αρχεία STIX, είναι απαραίτητο το να υπάρχουν κάποιες βιβλιοθήκες οι οποίες δεν ανήκουν στις standard βιβλιοθήκες python οι οποίες είναι οι: **lxlm** (binding για τις C βιβλιοθήκες libxml2 και libxstl), **python-cybox** (βιβλιοθήκη για παραγωγή και «κατανάλωση περιεχομένου CybOX), **python-dateutil** (βιβλιοθήκη για λειτουργίες parsing/διαβάσματος δηλ, πληροφοριών ημερομηνίας και ώρας).

Για να παράξει κάποιος αρχεία XML (δηλ STIX XML αρχεία), θα πρέπει να έχει γνώση των μεθοδολογιών git και GitHub pull request, των οποίων η ανάλυση δεν είναι επί του παρόντος αλλά και να είναι εξοικειωμένος με την python γλώσσα προγραμματισμού.

Παρακάτω, στην παρακάτω εικόνα 2.26, παραθέτουμε ένα απλό παράδειγμα δημιουργίας και «κατανάλωσης» αρχείου STIX:

**Creating a STIX Package**

```
from stix.core import STIXPackage                          # Import the STIX Package API
from stix.report import Report                             # Import the STIX Report API
from stix.report.header import Header                      # Import the STIX Report Header API

stix_package = STIXPackage()                               # Create an instance of STIXPackage
stix_report = Report()                                     # Create a Report instance
stix_report.header = Header()                              # Create a header for the report
stix_report.header.description = "Getting Started!"        # Set the description
stix_package.add(stix_report)                              # Add the report to our STIX Package

print(stix_package.to_xml())                               # Print the XML for this STIX Package
```

**Parsing STIX XML**

```
from stix.core import STIXPackage          # Import the STIX Package API

fn = 'stix_content.xml'                    # The STIX content filename
stix_package = STIXPackage.from_xml(fn)    # Parse using the from_xml() method
```

(εικόνα 2.26: Δημιουργία και «κατανάλωση» αρχείου STIX) [9]

# ΚΕΦΑΛΑΙΟ 3Ο: CASE STUDY:ΥΛΟΠΟΙΗΣΗ ΜΕΘΟΔΟΛΟΓΙΩΝ CI ΣΤΟΝ ΤΡΑΠΕΖΙΚΟ ΤΟΜΕΑ

## 3.1.Η έννοια του CBEST

'Εχουμε λοιπόν το πλαίσιο διαδικασιών και κανόνων του CBEST, το οποίο και αντιπαραβάλουμε με τα κλασσικά penetration tests. Η βασικότερη και ουσιαστική διαφορά μεταξύ των δύο αυτών συστημάτων Κυβερνοασφάλειας είναι το ότι τα tests τα οποία υπάγονται

[9] **The MITRE Corporation, Release 1.2.0.1 dev.2, July 19, 2016, pages 1, 3, 5-7)**

**Wikipedia, (2016, September 30), [Online].**

**Available:https://en.wikipedia.org/wiki/Application_programming_interface**

**Wikipedia Βικιπαίδεια, (2015, Οκτώβριος 27), [Online].**

**Available:https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B5%CF%80%CE%B1%CF%86%CE%AE_%CF%80%CF%81%CE%BF%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1%CF%84%CE%B9%CF%83%CE%BC%CE%BF%CF%8D_%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CF%8E%CE%BD**

στο πλαίσιο του CBEST, «οδηγούνται» από ορισμένου τύπου πληροφορία, οπότε μπορούμε να μιλάμε για intelligence-led tests. Δηλαδή, εδώ εισάγουμε την έννοια της πληροφορίας αυτής, η οποία «οδηγεί» τα tests του CBEST και η οποία χαρακτηρίζεται γενικότερα ως intelligence. Ένα από τα βασικότερα προτερήματα των intelligence-led tests σε σύγκριση με τα κλασσικά penetration tests είναι ότι προσομοιάζουν και προσεγγίζουν καλύτερα τον τρόπο με τον οποίο θα μπορούσε να λάβει χώρα μια Κυβερνοεπίθεση, σε πραγματικές συνθήκες.

Οι CBEST διαδιακασίες υλοποιούνται από την Κυβέρνηση της Αγγλίας σε συνεργασία με φορείς παροχής Κυβερνοασφάλειας. Τα tests που διεξάγονται εντός του πλαισίου του CBEST, έχουν σκοπό την δοκιμασία του προσωπικού, των συστημάτων και της τεχνολογίας ενός τραπεζικού οργανισμού, κάτι που θα ήταν ανέφικτο με ένα απλό penetration test. Χρησιμοποιούνται οι λεγόμενοι δείκτες, οι οποίοι μας δίνουν μία εικόνα της ετοιμότητας, της ικανότητας και της ωριμότητας των τραπεζικών συστημάτων ως προς την ασφάλεια τους. Η εικόνα αυτή που αποκομίζουμε από τους δείκτες, μπορεί να μας ωφελήσει μελλοντικά, προετοιμάζοντας το τραπεζικό σύστημα για πιθανές μελλοντικές Κυβερνοεπιθέσεις. [10]

## 3.2.Η έννοια του CREST

Ο CREST είναι ένας μη-κερδοσκοπικός οργανισμός, ο οποίος παρέχει τεχνικές/τεχνολογικές πληροφορίες και οδηγίες σχετικές με την Κυβερνοασφάλεια. Πιο συγκεκριμένα:

- Αποδεικνύει έμπρακτα το γεγονός του ότι υπάρχει ένα επίπεδο κατά το οποίο τυποποιούνται και διασφαλίζονται standard διαδικασίες των οργανισμών-μελών, οι οποίοι ανήκουν στον CREST
- Επικυρώνει την αρμοδιότητα του τεχνικού προσωπικού Κυβερνοασφάλειας
- Παίζει συμβουλετικό και εκπαιδευτικό ρόλο, παρέχοντας οδηγίες, standards και ευκαιρίες για διανομή γνώσεων και διαφόρων tips για θέματα Κυβερνοασφάλειας
- Παρέχει επαγγελματικές πιστοποιήσεις σε αναγνωρισμένο τεχνικό προσωπικό για τον τομέα της Κυβερνοασφάλειας αλλά και υποστήριξη σε άτομα ή εταιρείες τα οποία εισέρχονται στην βιομηχανία του Cyber Security

Κάτω από την «ομπρέλα» του CREST, υπάρχουν φορείς παροχής Κυβερνοασφάλειας, οι οποίοι αποτελούνται από άτομα καταρτισμένα, πιστοποιημένα και εκπαιδευμένα σύμφωνα με τις συνταγές του πλαισίου του CBEST και τα οποία έχουν τις γνώσεις, την αρμοδιότητα αλλά και τις απαράιτητες ικανότητες για την αντιμετώπιση επιθέσεων πολύπλοκης φύσεως.

Το πλαίσιο του CBEST, όπως αναφέρθηκε προηγουμένως, περιέχει ελεγχόμενα, κατά παραγγελία, tests Κυβερνοασφάλειας «οδηγούμενα» από ορισμένες πληροφορίες (intelligence-led cyber security tests). Υπάρχουν οι λεγόμενες STAR (Simulated Target Attack and Response) διαδικασίες, οι οποίες προπορεύονται των διαδικασιών CBEST, και οι οποίες αποτελούνται από 2 κύρια μέρη, από τα penetration tests και από τις υπηρεσίες cyber intelligence, οι οποίες τροφοδοτούν τον οργανισμό με τις απαράιτητες, intelligence, πληροφορίες. Οι STAR διαδικασίες

[10] **CREST Organization, (2013), "An introduction to CBEST",[Online]. Available**: https://www.crest-approved.org/wp-content/uploads/2014/05/CBEST-OVERVIEW.pdf

χρησιμοποιούνται για ρεαλιστικές αναπαραστάσεις επιθέσεων σε τραπεζικά συστήματα και για την προστασία και διαφύλαξη βασικών ευαίσθητων πληροφοριών των πιο κρίσιμων τομέων των χρηματοπιστωτικών υπηρεσιών της Αγγλίας.

Ο ρόλος του CREST είναι να προμηθεύει ενδιαφερόμενες εταιρείες ή οργανισμούς οι οποίοι είτε θέλουν να εντάξουν την φιλοσοφία του CBEST στην λειτουργία τους ή έχουν ήδη δεχθεί κάποια επίθεση και θέλουν να μειώσουν τις πιθανότητες επανάληψης τέτοιων επιθέσεων, με φορείς κατάλληλους για το σκοπό αυτό. Έτσι λοιπόν, ο CREST μπορεί να προτείνει κάποιους, μέσα από μία εκτενή λίστα φορέων οι οποίοι έχουν φυσικά πιστοποιηθεί και έχουν επιδείξει ότι ακολουθούν συγκεκριμένες διαδικασίες και πολιτικές για την παροχή υπηρεσιών προς τους πελάτες τους , στον σχεδιασμό, στην διαχείριση και στην επαναφορά συστημάτων τα οποία έχουν υποστεί επίθεση. Οι λίστες φορέων που ανήκουν στον CREST είναι:

- Φορείς που παρέχουν υπηρεσίες tests διεισδύσεων (Members Supplying Penetration Testing Services)
- Φορείς που παρέχουν υπηρεσίες τύπου STAR tests διεισδύσεων και τύπου STAR υπηρεσιών πληροφόρησης απειλών (Members Supplying STAR Penetration Testing And Star Threat Intelligence Services)
- Φορείς που παρέχουν εγκεκριμένες τύπου CBEST υπηρεσίες (Members Supplying CBEST Approved Services)
- Φορείς που παρέχουν υπηρεσίες απόκρισης Κυβερνοασφάλειας σε ψηφιακά συμβάντα (Members Supplying Cyber Security Incident Response Services)

Φορείς που παρέχουν υπηρεσίες ασφάλειας αρχιτεκτονικής πληροφοριακών συστημάτων (Members Supplying Security Architecture Services) [11]

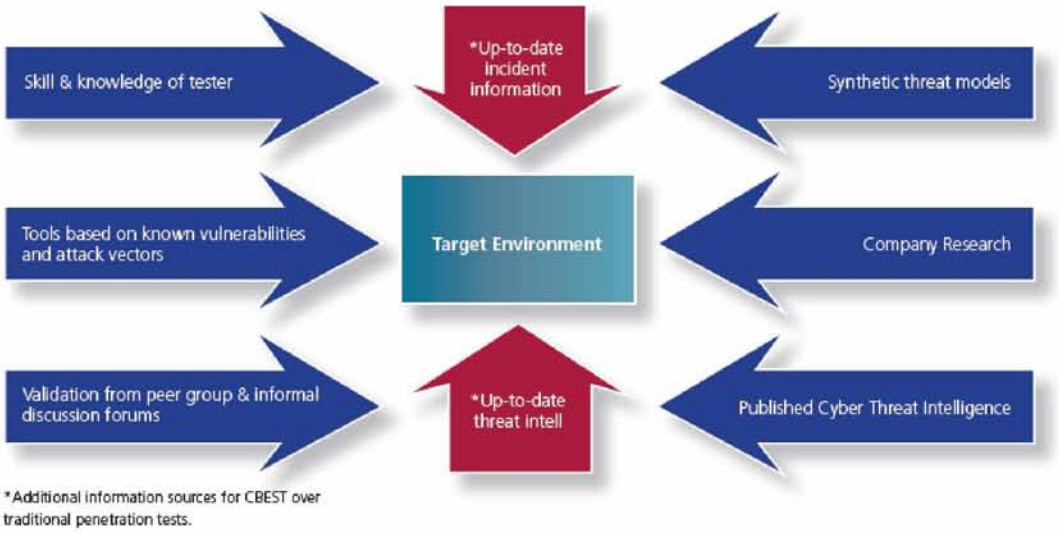
## 3.3. Γενικά στοιχεία για τις διαδικασίες CBEST

Ρίχνοντας μία γενική ματιά στο πλαίσιο εφαρμογής και λειτουργίας των κανόνων και των διαδικασιών CBEST, μπορούμε να πούμε ότι το τελευταίο απαρτίζεται από 2 βασικά μέρη. Το ένα μέρος περιλαμβάνει penetration tests τα οποία υλοποιούνται από κατάλληλα εκπαιδευμένο προσωπικό, το οποίο έχει στη διάθεση του και πληροφορίες που έχουν προκύψει από διαδικασίες cyber intelligence και με αυτόν τον τρόπο τα tests βελτιώνονται αισθητά, παρέχοντας ένα καλύτερο επίπεδο ασφάλειας. Επίσης, για την διεξαγωγή των tests αυτών χρησιμοποιούνται αυτοματοποιημένες και μη, διαδικασίες, με την βοήθεια των οποίων το τραπεζικό σύστημα δοκιμάζεται σε συνθήκες πραγματικών Κυβερνοεπιθέσεων οι οποίες προέρχονται είτε από εξωτερικούς παράγοντες (πχ.απο hackers), ή από εσωτερικούς παράγοντες (πχ εφαρμογή τεχνικών phising από κακόβουλους χρήστες σε προσωπικό ή σε πελάτες της τράπεζας/του οργανισμού). Το άλλο μέρος αποτελείται κυρίως από τεχνικές ανάλυσης

[11] **CREST International, (2016), "Assurance in Information Security", [Online]. Available: http://crest-approved.org/**

πληροφοριών οι οποίες σχετίζονται με ενδεχόμενες ψηφιακές απειλές τραπεζικών συστημάτων (Cyber Threat Intelligence Analysis). Σε αυτό το μέρος, πραγματοποιείται συλλογή πληροφοριών από διάφορες πηγές, έχοντας υπόψιν φυσικά κάποιο νομικό πλαίσιο εντός του οποίου γίνεται η συλλογή αυτή αλλά και βάσει του να είναι έγκυρες και έγκαιρες.

Θα πρέπει να προσθέσουμε ότι οι διαδικασίες συλλογής και επεξεργασίας πληροφοριών κατά την εφαρμογή κανόνων cyber intelligence, έχει εξελιχθεί αρκετά, καθώς αποτελεί μία αναπτυσσόμενη βιομηχανία. Σε αυτό το γεγονός βοήθησαν αρκετά και οι οικονομικές αρχές της Αγγλίας (Financial Authorities). Αναλυτικότερα, αυτοί οι κανόνες είναι προσβάσιμοι στο www.crest-approved.org. Στην παρακάτω εικόνα (εικόνα 3.1) βλέπουμε σχηματικά πως λειτουργεί η διαδικασία του testing σε συνδυασμό/συνεργασία με την διαδικασία του threat intelligence.




(εικόνα 3.1: Συνδυασμός των testing και threat intelligence)

Από την εικόνα 3.1 διαπιστώνουμε ότι παίζουν ρόλο η εμπειρία κα οι γνώσεις του tester, τα διάφορα «εργαλεία» που χρησιμοποιούνται, τα forums από τα οποία μπορεί να αντληθεί χρήσιμη γνώση, η έρευνα της εταιρείας ή του οργανισμού που έχει αναλάβει την εφαρμογή των διαδικασιών CBEST, τα διάφορα «μοντέλα» επίθεσης και η γνώση που έχει αποκτηθεί και δημοσιευθεί, σχετική με διαδικασίες CTI (Cyber Threat Intelligence).

## 3.4.Ωφέλη που αποκομίζονται από την εφαρμογή του CBEST

Τελικά ποιο είναι το όφελος με την εφαρμογή των κανόνων και διαδικασιών CBEST; Η όλη ιδέα αφορά την αισθητή βελτίωση των penetration tests, τα οποία πλέον έχουν ως οδηγό τις πληροφορίες που έχουν συλλεχθεί και επεξεργαστεί, βάσει διαδικασιών CTI και με αυτόν τον τρόπο, η άμυνα του οργανισμού οργανώνεται πολύ πιο αποτελεσματικά, καθώς τα penetration tests που λαμβάνουν χώρα προσεγγίζουν πολύ περισσότερο τις πραγματικές συνθήκες επίθεσης. Και θα ρωτούσε κάποιος:Πως γίνεται αυτό; Η απάντηση βρίσκεται στο γεγονός του ότι οι πληροφορίες από τις διαδικασίες CTI, θα λέγαμε ότι μας αποκαλύπτουν που (δηλ σε ποια σημεία) υπάρχει μεγάλη πιθανότητα να υποστεί ένας οργανισμός ή το τραπεζικό σύστημα μία, μεγάλης έντασης και πολυπλοκότητας, επίθεση, και έτσι, μπορεί να οργανωθεί καλύτερα και η αντίστοιχη άμυνα, πριν ακόμη να λάβει χώρα η επίθεση αυτή. Βλέπουμε λοιπόν, ότι μπαίνουμε σε μία τελείως διαφορετική φιλοσοφία, όπου γίνονται προσπάθειες για να μπορεί η άμυνα να βρίσκεται πάντοτε ένα βήμα μπροστά σε σχέση με την επίθεση.

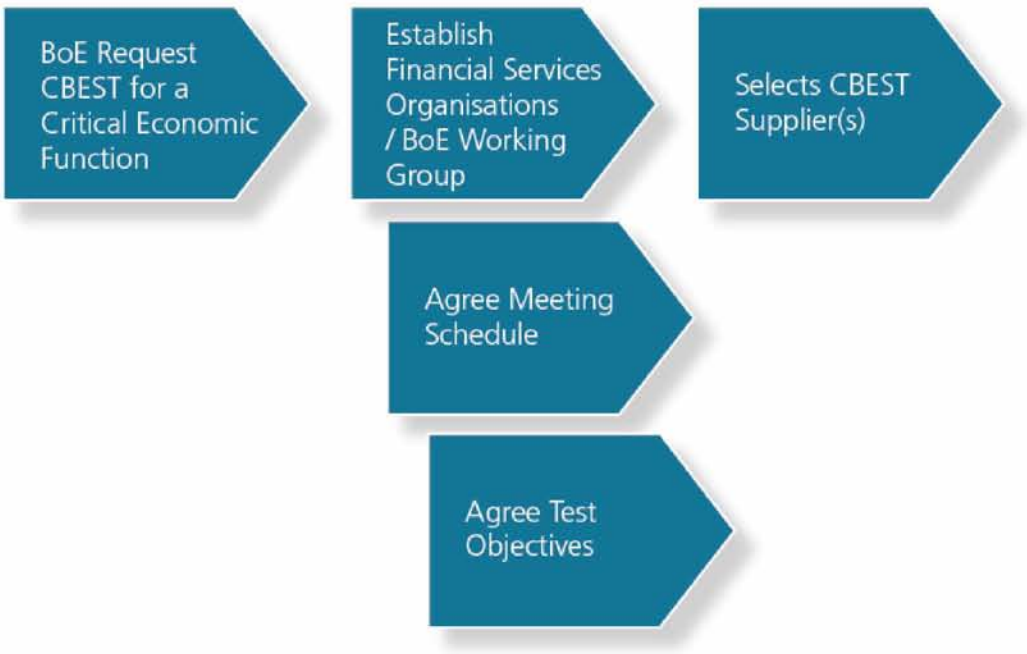
Δεν θα πρέπει φυσικά να παραλείψουμε το ότι οι ομάδες των pen tests θα πρέπει να έχουν λάβει την κατάλληλη εκπαίδευση και πιστοποίηση από τον CREST, ενώ οι ενέργειες τους παρακολουθούνται από τον CREST για να διασφαλιστεί το ότι συμμορφώνονται με τον κώδικα δεοντολογίας του CREST.

## 3.5.Διαδικασίες πριν την εφαρμογή του CBEST

Δεν θα μπορούσε να φανταστεί κανείς, τι θα συνέβαινε στην περίπτωση που μία επίθεση, η οποία στόχευε ένα τραπεζικό σύστημα, πετύχαινε τον σκοπό της, δηλ εάν τελικά κάποιοι κακόβουλοι χρήστες μπορούσαν να ανακτήσουν τον έλεγχο, έστω και μερικό, τραπεζικών συστημάτων μίας χώρας (πχ αγγλικών τραπεζικών συστημάτων). Το μόνο σίγουρο είναι το ότι θα δημιουργούνταν ένα κύμα σε μορφή ντόμινο, το οποίο θα μπορούσε να συμπαρασύρει και να έχει αρνητικό αντίκτυπο και σε τραπεζικά συστήματα άλλων χωρών και αυτό θα αλλοίωνε και την γενικότερη μορφή της οικονομίας και των χρηματοπιστωτικών συστημάτων της.

Πρώτα από όλα λοιπόν, πριν την εφαρμογή κανόνων και διαδικασιών CBEST, ξεκινάμε από το σημείο μηδέν, στο οποίο επιλέγεται ένα τραπεζικό σύστημα, το οποίο χρήζει προστασίας από τέτοιου είδους επιθέσεις.

Αφού επιλεχθεί το σύστημα αυτό, σειρά έχουν κάποιες προκαταρκτικές ενέργειες. Αυτές περιλαμβάνουν κυρίως την εγκαθίδρυση κάποιων Οικονομικών Υπηρεσιών, οι οποίες ορίζονται από την Τράπεζα της Αγγλίας (BoE-Bank of England), το πρόγραμμα συναντήσεων και τελικά την επιλογή κάποιου φορέα, πιστοποιημένου από τον CREST, ο οποίος θα παρέχει και θα εφαρμόζει τις διαδικασίες CBEST. Όλα αυτά που αναφέραμε, φαίνονται και στην εικόνα 3.2.




(εικόνα 3.2: Προετοιμάζοντας το έδαφος για την εφαρμογή του CBEST)

Ας αναλύσουμε περαιτέρω την εικόνα 3.2. Θα πρέπει να σχηματιστεί μία ειδική ομάδα εργασίας (working group) η οποία θα έχει την κατάλληλη εμπειρία και γνώση των ευαίσθητων στοιχείων, των συστημάτων και των οικονομικών λειτουργιών του τραπεζικού συστήματος, ενώ θα πρέπει να έχει μια εικόνα του κινδύνου να διαρρεύσουν ευαίσθητες πληροφορίες τραπεζικών και χρηματοοικονομικών δραστηριοτήτων ενώ θα πρέπει να είναι παρούσα σε όλες τις εφαρμοζόμενες διαδικασίες του CBEST. Οι συναντήσεις που καθορίζονται έχουν το νόημα του να ορίζονται κάποιοι στόχοι των tests ενώ οι Οικονομικές Αρχές (Financial Authorities) της Αγγλίας θα έχουν τη δυνατότητα να αναβαθμίσουν την όλη διαδικασία παρέχοντας νέες πληροφορίες από διαδικασίες CTI. Οι στόχοι των tests (Test Objectives) προσπαθούν να βελτιώσουν διάφορες διαδικασίες, να ενισχύσουν τα τραπεζικά συστήματα και να εντάξουν την έννοια της εκπαίδευσης του προσωπικού που εργάζεται σε ένα τέτοιο τραπεζικό σύστημα. Εκτός αυτών, αυτοί οι στόχοι προδιαγράφουν τις κατάλληλες ενέργειες σε περίπτωση που μία επίθεση καταφέρει να διεισδύσει στα τραπεζικά συστήματα, οι οποίες δεν είναι άλλες από την επαναφορά των συστημάτων αυτών σε λειτουργία αλλά και η διατήρηση της ακεραιότητας και της εμπιστευτικότητας τους.

Φυσικά, υπάρχουν διαφόρων ειδών τραπεζικά συστήματα και εδώ ένα θετικό στοιχείο είναι το ότι ναι μεν οι πληροφορίες από διαδικασίες CTI θα παρέχονται από πιστοποιημένους και κατάλληλα εκπαιδευμένους παρόχους, όμως οι πληροφορίες αυτές θα προσαρμόζονται ανάλογα με τις εκάστοτε ανάγκες του τραπεζικού συστήματος και έτσι υπάρχει μία καλύτερη ευελιξία στην ανίχνευση των ειδικών αναγκών των συστημάτων, άρα και μεγαλύτερη ακρίβεια στα penetration tests.

## 3.6.Πεδίο δράσης και αρχικοποίηση του σχεδίου

Όπως είδαμε, θα πρέπει αρχικά να επιλεχθεί ένας φορέας CBEST ο οποίος θα αναλάβει την διεκπεραίωση του έργου. Το αμέσως επόμενο βήμα είναι να υπάρξει μία ρύθμιση όσον αφορά το πεδίο δράσης αλλά και τα αντικείμενα των test (Test Objectives). Φυσικά, θα πρέπει να σχηματιστεί και η Ομάδα Εργασίας (Working Group), όπως είχαμε αναφέρει και προηγουμένως. Ας δούμε λίγο την εικόνα 3.3.


(Εικόνα 3.3:Αρχικοποίηση του σχεδίου)

Βλέποντας την εικόνα 2.3, πρώτα από όλα στην Ομάδα Έργου (Working Group), θα πρέπει να συμπεριληφθούν οι ομάδες οι οποίες θα εφαρμόσουν τις CBEST διαδικασίες. Αυτές είναι η ομάδα του penetration testing αλλά και η ομάδα των CTI διαδικασιών. Έτσι λοιπόν, έχουμε μία εκτενή Ομάδα Έργου. Μετά από αυτό, θα πρέπει να συμφωνηθεί, μέσω κάποιου ειδικού «εργαστηρίου» το πεδίο δράσης, το οποίο δεν είναι τίποτα άλλο από την σύνταξη κάποιων εγγράφων σχετικών με την εκτίμηση του κινδύνου (όπως για παράδειγμα η έκθεση και διαρροή ευαίσθητων τραπεζικών πληροφοριών σε κακόβουλους χρήστες) αλλά και το έγγραφο αρχικοποίησης του έργου αυτού.

Εν συνεχεία, έχουμε μία συμφωνία η οποία καθορίζει κάποιες διαδικασίες και κάποια standards βάσει των οποίων θα υλοποιούνται οι αναφορές από τα tests, ενώ η διαδικασία ολοκληρώνεται με μία κοινή συμφωνία επί του σχεδίου βάσει του οποίου θα διεξαχθούν τα tests

και τελευταίως, έχουμε και μία κοινή συμφωνία από όλα τα εμπλεκόμενα μέρη, για ενέργειες άμεσης ανταπόκρισης, σε περίπτωση που διαπιστωθεί κάποιο ψηφιακό συμβάν.

Γενικά μιλώντας, μπορούμε να πούμε ότι αρχικά καταστρώνεται ένα σχέδιο το οποίο ορίζει το πώς θα διεξαχθούν τα penetration tests. Αυτό το σχέδιο υλοποιείτα από την ομάδα/τον φορέα του penetration test. Στη συνέχεια, το σχέδιο αυτό προωθείται στις Οικονομικές Αρχές και μετά στην Ομάδα Εργασίας (Working Group). Ύστερα από όλα αυτά τα στάδια, εάν το σχέδιο αυτό εγκριθεί, η ομάδα του penetration test το ενισχύει προσθέτωντας του και κάποια άλλα στοιχεία. Το τελικό και εμπλουτισμένο σχέδιο πλέον, αποτελεί σημείο αναφοράς και ένα πρότυπο σχέδιο για το πεδίο δράσης αλλά και για τις δραστηριότητες που σχετίζονται με τα tests. Ουσιαστικά, το πρότυπο αυτό σχέδιο αποτελεί έναν οδηγό ο οποίος ξεκαθαρίζει το τι ακριβώς θα πρέπει να συμπεριληφθεί στις διαδικασίες του CBEST. Τελικώς, το πρότυπο αυτό σχέδιο θα πρέπει να καλύπτει και τους 4 εμπλεκόμενους (την τράπεζα της Αγγλίας/BoE-Bank Of England, τον Οργανισμό των Οικονομικών Υπηρεσιών, τον φορέα του Penetration Testing και τον φορέα του Threat Intelligence), στα παρακάτω εξής σημεία:

- Θα πρέπει να συμφωνηθεί από κοινού το πεδίο δράσης του test, με την έννοια του ποια συστήματα και ποια όχι, θα πρέπει να συμπεριληφθούν στην εφαρμογή του. Και το ερώτημα είναι, ποιοι παράγοντες θα καθορίσουν την έκταση αυτή; Η απάντηση είναι ο συνδυασμός των πληροφοριών που πηγάζουν από τις CTI διαδικασίες πριν την εφαρμογή του CBEST με τις πληροφορίες που έχουν συνάφεια με σύγχρονους τρόπους στοχοποίησης τραπεζικών και μη, συστημάτων. Έτσι λοιπόν, ο συνδυασμός των 2 αυτών όγκων πληροφορίας μας οδηγεί σε μία εκτίμηση του πόσο καλά ή όχι λειτουργούν οι μηχανισμοί ανίχνευσης και διαχείρισης ψηφιακών συμβάντων στο τραπεζικό σύστημα αυτό.
- Θα πρέπει να υπάρχει ένας συντονιστής cyber threat intelligence, ο οποίος θα συντονίζει τις λειτουργίες των Οικονομικών Αρχών, τον φορέα των Penetration Tests αλλά και τον συντονιστή των διαδικασίων CBEST.
- Θα πρέπει να συμφωνηθεί από κοινού η εικόνα και ο τρόπος υλοποίησης των tests. Πιο συγκεκριμένα, θα πρέπει να υιοθετηθεί η μεθοδολογία, ο/οι τύπος/τύποι και το επίπεδο ασφάλειας του test.
- Θα πρέπει να καθοριστεί ο βαθμός πρόσβασης σε εσωτερικά (ευαίσθητα) στοιχεία του τραπεζικού συστήματος, διότι το test που θα υλοποιηθεί, θα περιέχει χαρακτήρα «εξωτερικής απειλής». Μία εξωτερική απειλή, έχει ένα βαθμό πρόσβασης, εάν πετύχει, σε ευαίσθητα δεδομένα άρα εδώ γίνεται μία προσπάθεια προσομοίωσης μίας τέτοιας επίθεσης.
- Ο καθορισμός ενός ατόμου ενταγμένου στο τραπεζικό σύστημα το οποίο θα αποφασίζει, κατά την διενέργεια του test, ποιο τμήμα του test αντικατοπτρίζει μία «πραγματική επίθεση» και το οποίο θα παίζει το ρόλο του συντονιστή, κατά την άμυνα του τραπεζικού συστήματος, όταν ή εάν αυτό συμβεί (στην πραγματικότητα).
- Ο καθορισμός του χρονικού διαστήματος υλοποίησης του test εσωτερικών διαδικασιών οι οποίες έχουν συμφωνηθεί στο να γίνουν και κατά τις οποίες τεστάρονται συστήματα εντός του πεδίου δράσης του σχεδίου.
- Υπάρχει ένας κανόνας (βάσει των διαδικασιών CBEST) ο οποίος καθορίζει, σε μία πιστοποιημένη-κατά CBEST-ομάδα test, των αριθμό της ομάδας των testers αλλά και το ποιο άτομο θα ηγείται αυτής της ομάδας, εκτελώντας καθήκοντα επίβλεψης, κατά την όλη διάρκεια του test.

- Καθορίζονται τόσο ο αριθμός των ημερών, όσο και οι ημέρες στις οποίες θα διενεργείται το test. Δεδομένου ότι οι διαδικασίες CBEST προσεγγίζουν το σενάριο μίας «αληθινής επίθεσης», αυτό συνεπάγεται ότι ο χρόνος υλοποίησης του test μπορεί να είναι μεγαλύτερος από το χρόνο υλοποίησης ενός κλασικού test.
- Οι οικονομικές αρχές έχουν καθορίσει την μορφή του εντύπου αναφοράς στο οποίο θα καταγράφονται όλες οι πληροφορίες και τα πορίσματα των tests αλλά μπορούν να υπάρξουν και τροποποιήσεις σε αυτό το έντυπο, διότι μπορεί να χρειαστεί να προστεθούν και άλλες πληροφορίες χρήσιμες για το τραπεζικό σύστημα.
- Η ύπαρξη συμφωνίας για την ημερομηνία παράδοσης του εντύπου αναφοράς.
- Η ύπαρξη συμφωνίας για τον τρόπο παράδοσης του εντύπου αναφοράς, ο οποίος θα διασφαλίζει την επίτευξη κατάλληλου επιπέδου ασφαλείας.
- Η ύπαρξη πληροφορίας σχετικής με συχνές συναντήσεις πελατών. Είναι ζωτικής σημασίας οι διενέργειες συναντήσεων με τους διάφορους testers, προκειμένου να οι πρόοδοι των tests αλλά και κάποια στοιχεία που έχουν έρθει στην επιφάνεια (είτε ανακαλύψεις είτε προβλήματα), να συζητούνται από κοινού για την επίτευξη λύσεων.
- Περιπτώσεις κατά τις οποίες ανακαλύπτεται μία τρωτότητα (vulnerability) στο σύστημα θα πρέπει να υπάρχει άμεση ενημέρωση σε όλους τους εμπλεκόμενους, λόγω του κινδύνου στον οποίο εκτίθεται ο φορέας.
- Σε περιπτώσεις που το test συμπεριλαμβάνει και μέρη τρίτων, τότε θα πρέπει να υπάρχει πληροφόρηση, σχετική με το test, και στους τρίτους. Για παράδειγμα, εάν το test περιλαμβάνει ένα website, τότε θα πρέπει να υπάρχει αδειοδότηση από τους τρίτους (δηλ απο αυτούς που κάνουν το hosting) στην ομάδα που θα κάνει το test.
- Θα πρέπει να μπορεί η ομάδα που θα διεξάγει το test να μπορεί να αποδεικνύει, με την επίδειξη επίσημων εγγράφων και στοιχείων, την αληθινή της ταυτότητα, διότι η τελευταία θα έρχεται σε επαφή με ευαίσθητα στοιχεία, πράγμα το οποίο εγκυμονεί κινδύνους.
- Θα πρέπει να υπάρχουν ευκαιρίες κατά τη διάρκεια του test όπου θα μπορούν να καταγράφονται κάποιες χρήσιμες λεπτομέρειες.
- Θα πρέπει να καθοριστεί τόσο ή προσέγγιση όσο και το ποιος θα είναι υπεύθυνος για τη διαχείριση των ψηφιακών συμβάντων.
- Η ύπαρξη σημείων ελέγχου μεταξύ των φάσεων του test καθώς και εναλλακτικά σχέδια συνέχισης του test, σε περίπτωση διακοπής κάποιας φάσεως.
- Η ύπαρξη κάποιων λεπτομερειών σχετικών με δραστηριότητες οι οποίες θα μπορούσαν να συμπληρώσουν την όλη υλοποίηση του test, όπως για παράδειγμα επαναλαμβανόμενα test τα οποία θα ελέγχουν τις πρωτίστως ευρεθείσες τρωτότητες, με σκοπό την διαπίστωση της πλέον μη ύπαρξης τους.

## 3.7.Αξιολόγηση και μετριασμός του κινδύνου

Έχουμε ήδη αναφέρει ότι ένα μελανό σημείο στις διαδικασίες του CBEST είναι η πιθανότητα έκθεσης και διαρροής ευαίσθητων τραπεζικών πληροφοριών σε κακόβουλους χρήστες, αφού στις διαδικασίες αυτές υπάρχει πρόσβαση, για λόγους δοκιμής, στις πληροφορίες αυτές. Άρα έχουμε από την μία μεριά την απαραίτητη εκτίμηση του κινδύνου αυτού (δηλ του να διαρρεύσουν ευαίσθητες πληροφορίες) και τις αντίστοιχες ενέργειες της μείωσης του κινδύνου

αυτού, και από την άλλη μεριά την προσπάθεια να μην επηρεαστούν καθόλου οι οικονομικές λειτουργίες του φορέα. Όσον αφορά την εκτίμηση και την μείωση του κινδύνου, θα πρέπει να πούμε ότι όλοι οι εμπλεκόμενοι στις διαδικασίες CBEST να γνωρίζουν στοιχεία εκτίμησης κινδύνου και να υιοθετούν στρατηγικές μείωσης κινδύνου και επίσης, κατά τη διάρκεια των διαδικασιών CBEST θα πρέπει να γίνεται ανασκόπηση της εκτίμησης του κινδύνου. Τέλος, θα πρέπει να τονίσουμε κάτι σημαντικό: Τα διάφορα ευαίσθητα στοιχεία που χρησιμοποιούνται για τους λόγους των tests, δεν θα πρέπει να στοχοποιούνται με άμεσο τρόπο, σε μία εικονική, «ρεαλιστική» επίθεση, διότι υπάρχει κίνδυνος η όλη διαδικασία της εικονικής επίθεσης να την εκμεταλλευτούν κακόβουλοι χρήστες, οι οποίοι δεν θα έχουν καμία σχέση με την ομάδα του penetration test και να την χρησιμοποιήσουν προς όφελος τους, ανακτώντας με αυτόν τον τρόπο πραγματική πρόσβαση στα ευαίσθητα στοιχεία αυτά.

## 3.8.Ο φαύλος κύκλος των διαδικασιών CBEST

Θα μπορούσαμε να πούμε ότι οι διαδικασίες CBEST αποτελούν έναν φαύλο κύκλο, του οποίου η σύνθεση είναι τα μέρη της πληροφόρησης (πληροφορίες που πηγάζουν από τις CTI διαδικασίες), τα tests διείσδυσης (penetration tests), της «τρέχουσας ωριμότητας» current maturity) – δηλ κατά πόσο είναι ώριμο είναι το τραπεζικό σύστημα (πόσο ευάλωτο ή όχι είναι σε περίπτωση επίθεσης) και το σχέδιο βελτίωσης (improvemet plan). Σε κάθε ένα από τα παραπάνω μέρη, υπάρχουν και οι αντίστοιχες αναφορές αλλά επίσης θα πρέπει να προσθέσουμε ότι το κάθε ένα από αυτά τα μέρη απαρτίζεται και από κάποια αναλυτικότερα στοιχεία όπως σκοπός, σύνθεση, δραστηριότητες, κριτήρια ποιότητας, ανασκόπηση και απαιτήσεις αποσύνδεσης (sign off).

## 3.9.Ενδείξεις σημαντικών στοιχείων κατά τη διάρκεια του test

Θα πρέπει κατά την διεξαγωγή tests, να είναι παρόντα όλα τα εμπλεκόμενα μέρη, διότι με αυτόν τον τρόπο μειώνονται οι πιθανότητες να μην παρατηρηθούν κάποιες ενδείξεις από τα αποτελέσματα των tests αυτών και έτσι μειώνονται δραματικά οι πιθανότητες να βρεθούν σημεία τρωτότητας σε μελλοντικό χρόνο.

Και τι προβλεπεται στην περίπτωση που βρεθούν σημεία τρωτότητας κατά την διεξαγωγή των tests; Η απάντηση είναι ότι θα πρέπει να έχει προβλεφθεί από πρίν, ένας σωστός δίαυλος επικοινωνίας και ανταλλαγής πληροφορίων μεταξύ του φορέα penetration test και της Ομάδας Εργασίας, με στόχο τον διαμοιρασμό των πληροφοριών.

## 3.10. Έγγραφο αρχικοποίησης του έργου

Τυποποιώντας την διαδικασία του test, κρίνεται απαραίτητη η υλοποίηση ενός εγγράφου, σχετικού με την περιγραφή του οργανισμού, τον σχεδιασμό και τον έλεγχο του έργου. Θα πρέπει επίσης να περιέχει τις διαδικασίες πριν από την εφαρμογή του CBEST καθώς επίσης και το πεδίο δράσης. Φυσικά, αυτό το έγγραφο συνυπογράφεται από τον Οργανισμό, από τις Οικονομικές Αρχές αλλά και από τα άτομα που ρυθμίζουν την συνεργασία των ομάδων του penetration testing και cyber intelligence. [12]

## 3.11.Τα test του CBEST

Έχουμε πλέον καταλάβει ότι οι Κυβερνοεπιθέσεις που λαμβάνουν χώρα και στοχεύουν άτομα, οργανισμούς και επιχειρήσεις, έχουν μία πολυσύνθετη και πολύπλοκη μορφή με ταυτόχρονη επίθεση σε περισσότερα του ενός συστήματα. Το «αντίδοτο» σε τέτοιου τύπου επιθέσεις είναι η εφαρμογή κανόνων και διαδικασιών CBEST και οι οποίες μας δίνουν μία πολύ καλή εικόνα του πόσο καλή άμυνα διατηρεί ένας οργανισμός έναντι τέτοιων ψηφιακών απειλών και οι οποίες περιλαμβάνουν κάποια tests. Το κάθε ένα από αυτά τα tests «σπάει» σε πολλά βήματα και το κάθε βήμα έχει μία ορισμένη χρονική διάρκεια. Η χρονική διάρκεια του κάθε βήματος εξαρτάται από έναν ορισμένο αριθμό παραγόντων όπως το πεδίο δράσης, τα σημεία ζωτικής σημασίας, και θέματα ασφάλειας και οι παράγοντες αυτοί σχετίζονται με τη φύση του οργανισμού (πχ του τραπεζικού συστήματος) ο οποίος εντάσσεται στις διαδικασίες CBEST. Φυσικά, δεν θα μπορούσαν να παραλειφθούν και τρόποι εφαρμογής διαχείρισης κινδύνου. Παρακάτω, παραθέτουμε μία συγκεκριμένη μεθοδολογία, η οποία αποτελεί αναπόσπαστο κομμάτι της εκτέλεσης του CBEST test:

- Αναγνώριση: Σε αυτό το σημείο, υλοποιείται συλλογή πληροφοριών σχετικών με την στοχοποίηση του οργανισμού, κυρίως από πηγές οι οποίες σχετίζονται με διάφορους χρήστες του Internet και με αυτόν τον τρόπο σχηματίζεται μία εικόνα της «επιφάνειας» του οργανισμού, στην οποία μπορούν να υπάρξουν επιθέσεις από κακόβουλους χρήστες ή hackers. Έτσι λοιπόν, εφαρμόζονται διαδικασίες cyber threat intelligence (C TI)και φυσικά η ομάδα που αναλαμβάνει την συλλογή αυτών των πληροφοριών είναι κάποιος πιστοποιημένος φορέας (από CREST) ο οποίος παρέχει αυτού του τύπου την υπηρεσία.
- Υλοποίηση σταδίων: Αφού λοιπόν συλλεχθούν οι παραπάνω πληροφορίες βάσει της αναγνώρισης, δημιουργούνται διάφορα στάδια. Στο κάθε ένα στάδιο δημιουργείται μία πλατφόρμα για την κατάλληλη προσομοίωση διάφορων «απειλών» για τον οργανισμό και φυσικά η κάθε μία πλατφόρμα αποτελεί και μία βάση από όπου θα ξεκινούν και άλλες «επιθέσεις», στα πλαίσια της προσομοίωσης αυτής.

[12] **CBEST/CREST STAR/CBEST Implementation Guide, 2016, pages 3-4, 8-12**

• Εκμετάλλευση: Σε αυτό το σημείο, πραγματοποιούνται διάφορες διαδικασίες, τεχνικές και τακτικές σχετικές με τις «απειλές» (τις οποίες αναφέραμε παραπάνω, στην υλοποίηση σταδίων) προκειμένου να ανακαλυφθούν τρωτότητες στον οργανισμό και μέσω αυτών, να επιτευχθεί εξουσιοδοτημένη «πρόσβαση» στο «στόχο» (δηλ. στον οργανισμό). Όλη αυτή η διαδικασία θα πρέπει φυσικά να εναρμονίζεται με το τι έχει συμφωνηθεί σε ότι αφορά για το πεδίο δράσης αλλά και για το ρίσκο κινδύνου του εν λόγω οργανισμού.
• Έλεγχος και κυκλοφορία: Εφόσον λοιπόν, από το σημείο της εκμετάλλευσης (ή τρωτότητας), αποκτηθεί «πρόσβαση» στο «στόχο», το επόμενο σημείο είναι η περαιτέρω «διείσδυση» σε περισσότερα συστήματα, ή του ίδιου επιπέδου ασφάλειας, είτε σε συστήματα υψηλότερου επιπέδου ασφάλειας αλλά και αξίας. Για παράδειγμα, γίνεται προσπάθεια μεταπήδησης (το λεγόμενο "hoping") μεταξύ εσωτερικών συστημάτων, η οποία έχει ως σκοπό την ολοένα αυξανόμενη απόκτηση πρόσβασης στα συστήματα του οργανισμού και εν τέλει τον εξ ολοκλήρου έλεγχο των συστημάτων αυτών.
• Ενέργειες επάνω στον στόχο: Αφού επιτευχθεί ολοκληρωτικός έλεγχος των συστημάτων του οργανισμού (όπως είδαμε προηγουμένως), γίνεται εφικτή η πρόσβαση σε ευαίσθητα δεδομένα του οργανισμού. Και εδώ πάλι, η διαδικασία που ακολουθείται σχετίζεται με το τι έχει συμφωνηθεί ως προς το πεδίο δράσης του test αλλά και την εκτίμηση κινδύνου, στοιχεία που εγκρίνονται από τον οργανισμό «στόχο».
• Επιμονή και έξοδος: Εδώ, έχοντας ως σημείο αναφοράς, την προσομοίωση επιθέσεων ενός καλού hacker, το δίκτυο του οργανισμού θωρακίζεται ενώ απορρέουν φιλτραρισμένες πληροφορίες σε περιβάλλον προσομοίωσης, από κάθε στάδιο, δηλ τα πορίσματα των tests. Και πάλι, η άντληση των πληροφοριών αυτών, εναρμονίζεται με την εκτίμηση κινδύνου του οργανισμού, έτσι ώστε να αποφευχθεί τυχόν διαρροή απόρρητων πληροφοριών.

Τελικά, η όλη φιλοσοφία του CBEST test είναι να εκτιμηθεί κατά πόσο είναι ικανός ο οργανισμός που ελέγχεται στο να εντοπίζει αλλά και να διαχειρίζεται διάφορες ψηφιακές απειλές, οι οποίες είναι εξελιγμένες και πολύπλοκες και προέρχονται από άτομα ή ομάδες ατόμων οι οποίες είναι συνυφασμένες με τις έννοιες του hacking.

## 3.12. Μοντέλο ωριμότητας και δείκτες επίδοσης

Σε όλα αυτά τα στοιχεία που έχουμε ήδη αναφέρει, θα πρέπει να προσθέσουμε και την υλοποίηση της εκτίμησης της ωριμότητας του οργανισμού, η οποία θα γίνει από την ομάδα του penetration testing. Αυτό φυσικά δεν θα δείξει μόνο τον τρόπο με τον οποίο ο οργανισμός ανταποκρίνεται στο test του CBEST αλλά και κάτι ακόμα πιο ουσιαστικό: το πώς ο οργανισμός ανταποκρίνεται σε πραγματικές συνθήκες μίας αληθινής επίθεσης, ως προς την οργάνωση του στην διαχείριση των επιθέσεων αυτών, από το άλφα έως το ωμέγα, δηλ. από τις πρώτες δραστηριότητες μέχρι και την ανάκτηση του ελέγχου και το ποια εμπειρία και χρήσιμες γνώσεις αποκτήθηκαν. Η Ρυθμιστική Αρχή Οικονομικών καθορίζει το επίπεδο ωριμότητας ενώ από την εκτίμηση της προκύπτουν οι δείκτες επίδοσης (KPI's-Key Performance Indicators) οι οποίοι χρησιμοποιούνται εν συνεχεία από την Ρυθμιστική Αρχή αυτή για να μπορεί και να δει σε τι επίπεδο ετοιμότητας βρίσκεται το εν λόγω τραπεζικό σύστημα αλλά και να να συγκρίνει το επίπεδο αυτό με άλλα επίπεδα, άλλων τραπεζικών συστημάτων.

Η εφαρμογή αυτή παρέχεται δωρεάν στην ομάδα του penetration testing μέσω της ιστοσελίδας του CBEST (www.crest-approved.org).

## 3.13. Εργαστήριο ευρημάτων

Κατά τη διάρκεια των tests της εφαρμογής του CBEST πλαισίου, ανακαλύπτονται διάφορες τρωτότητες (vulnerabilities) του τραπεζικού συστήματος. Για την υλοποίηση των tests αυτών, προβλέπεται ένα κοινό έδαφος συνεργασίας της ομάδας που υλοποιεί το penetration testing και των ατόμων που είναι αρμόδιοι για τις οικονομικές υπηρεσίες, το οποίο είναι τα «εργαστήρια», που έχουμε αναφέρει και προηγουμένως. Στα εργαστήρια αυτά επιτυγχάνεται ένα κατάλληλο επίπεδο ελέγχου καθώς και μία διεξοδική μελέτη και ανάλυση των διάφορων τρωτοτήτων (vulnerabilities) του συστήματος. Και τι εννοούμε κοινό έδαφος συνεργασίας; Εννοούμε το ότι, σε αντίθεση με τα απλά penetration tests, στα tests του CBEST, υπάρχει ενεργός συμμετοχή των ατόμων των οικονομικών υπηρεσιών, όπου κρίνεται απαραίτητο, για υποστήριξη και για βελτίωση των διαδικασιών του test. Φυσικά, κατά τη διάρκεια των εργαστηρίων αυτών, καταγράφονται λεπτομέρειες οι οποίες περιλαμβάνουν πληροφορίες για διάφορες ενέργειες, χρονοδιαγράμματα και τομείς ευθυνών.

## 3.14.Αναφορές

Οι αναφορές αποτελούν αναπόσπαστο κομμάτι για τις διαδικασίες του CBEST. Παρακάτω, στην εικόνα 3.4 απεικονίζονται τα 4 βασικά συστατικά της πρότασης CBEST.


(εικόνα 3.4: Τα 4 βασικά συστατικά της πρότασης CBEST)

Παρατηρώντας την εικόνα 3.1 βλέπουμε ότι αρχικά, διανέμονται οι αναφορές στα άτομα των Οικονομικών Υπηρεσιών και στην Ομάδα Διοίκησης, εξετάζονται σφάλματα και παραλείψεις, επινοούνται τεχνικές μετριασμού των σφαλμάτων και των τρωτοτήτων και μελετώνται διάφορες διαδικασίες βελτίωσης. Εν συνεχεία, οι αναφορές οδηγούνται στην Τράπεζα της Αγγλίας και συστήνεται Εργαστήριο Ποιότητας και εν τέλει, συμφωνείται σχέδιο δράσης και βελτίωσης. Καταλαβαίνουμε λοιπόν, ότι οι αναφορές αποτελούν ένα εργαλείο επικοινωνίας και βελτίωσης των διαδικασιών CBEST. Παρακάτω, στην εικόνα 3.5, βλέπουμε τα στάδια της αναφοράς CBEST.


(εικόνα 3.5: Τα στάδια της αναφοράς CBEST)

Στο στάδιο 1, υπάρχει μία περιγραφή του πεδίου δράσης αλλά και της εκτέλεσης του test. Στο στάδιο 2, έχουμε την αναφορά threat intelligence, η οποία εμπεριέχει λεπτομέρειες κατά την αρχή του Project και βελτιώνεται κατά τη διάρκεια του. Στο στάδιο 3, ακολουθεί η αναφορά του security testing, όπου θίγονται θέματα τρωτοτήτων και αποτελεσμάτων από το test. Εδώ, όπου κρίνεται απαραίτητο, συμπεριλαμβάνονται και θέματα τεχνικού ελέγχου, εκπαίδευσης του προσωπικού και διαδικασιών. Στο στάδιο 4, έχουμε πλέον στοιχεία για το πόσο «ώριμα» μπορεί να αντιδράσει το εν λόγω τραπεζικό σύστημα, δηλ σε τι επίπεδα βρίσκεται η ετοιμότητα του, σε περίπτωση ψηφιακού συμβάντος, κάτι που μπορεί να υπολογιστεί μέσω δεικτών «ωρίμανσης». Στο τελικό και 5° στάδιο, προβλέπεται ένα σχέδιο βελτίωσης του επιπέδου ετοιμότητας, δηλ του επιπέδου ασφαλείας.

## 3.15.Διαδικασία ανασκόπησης

Αφού λοιπόν συλλεχθούν και διανεμηθούν τόσο οι αναφορές αλλά και όσο τα πορίσματα και στις Οικονομικές Αρχές αλλά και στον οργανισμό, υλοποιείται μία ανασκόπηση και συντάσσονται διάφορες κριτικές. Το τραπεζικό σύστημα δεν έχει, σε καμία περίπτωση, το δικαίωμα είτε να καθυστερήσει την ανασκόπηση, είτε να αλλοιώσει τα αποτελέσματα των tests. Οι κριτικές που γίνονται θα πρέπει να συνδέονται με θέματα λαθών και παραλείψεων, έχοντας ως σκοπό τον μετριασμό ή καλύτερα την εξάλειψη των τρωτοτήτων του τραπεζικού συστήματος.

Από την άλλη μεριά, οι Οικονομικές Αρχές είναι αρμόδιες να οργανώσουν ένα εργαστήριο ανατροφοδότησης, σύμφωνα με το οποίο οι αναφορές και τα πορίσματα συζητούνται και συμφωνείται η υλοποίηση απαραιτήτων ενεργειών αλλά και η επανάληψη διαφόρων διαδικασιών-test για να ελεγχθεί το ότι οι συμφωνημένες βελτιώσεις έχουν όντως πραγματοποιηθεί. Φυσικά, κάποιες από τις αναφερθείσες προτεινόμενες ενέργειες είναι απλές

στην εφαρμογή τους και κάποιες άλλες είναι περισσότερο πολύπλοκες στην υλοποίηση τους. Και προσθέτουμε εδώ ότι, δίνεται μεγάλη σημασία σε κρίσιμες τρωτότητες, οι οποίες θέτουν σε κίνδυνο τον οργανισμό και οποιαδήποτε επαναληπτική διαδικασία-test, ακολουθεί ακριβώς την αρχική φιλοσοφία CBEST.

Θα πρέπει εδώ να τονίσουμε ότι ο έλεγχος ασφάλειας (security testing) δεν αποτελεί ενέργεια μίας και μόνο φοράς. Θα πρέπει ο οργανισμός να συμπεριλάβει στην λειτουργία του, ένα σετ από tests CREST STAR, το οποίο και θα εντάξει στο ευρύτερο πλαίσιο του penetration testing.

## 3.16.Η χρηματοδότηση του CBEST

Η χρηματοδότηση του CBEST βασίζεται στους εξής 3 πυλώνες:

- Στο τραπεζικό σύστημα ,το οποίο θα ελεγχθεί σύμφωνα με τις διαδικασίες CBEST και το οποίο φυσικά θα πληρώσει ένα μεγάλο μέρος των χρημάτων για την εφαρμογή των διαδικασιών και κανόνων CBEST
- Στις Οικονομικές Αρχές και στον CREST οργανισμό οι οποίοι συμμετέχουν ενεργά στην επιδότηση ενός τέτοιου έργου και της οποίας επιδότησης το ύψος έχει συμφωνηθεί.
- Σε ορισμένες μεμονωμένες περιπτώσεις, είναι δυνατή και η μερική χρηματική υποστήριξη από την Τράπεζα της Αγγλίας.

## 3.17. Επιλέγοντας κατάλληλο πάροχο υπηρεσιών

Η παροχή υπηρεσιών CBEST μπορεί να υλοποιηθεί βάσει των κάτωθι:

- Με την επιλογή πιστοποιημένης ομάδας threat intelligence. Η ομάδα αυτή θα συνεργάζεται με την ομάδα του penetration testing.
- Με την επιλογή πιστοποιημένης ομάδας penetration testing. Η ομάδα αυτή θα συνεργάζεται με την ομάδα threat intelligence.
- Η παροχή υπηρεσιών CBEST μπορεί να αποτελείται από διαφορετικές αλλά πιστοποιημένες ομάδες για penetration testing και threat intelligence.

Το ερώτημα που τίθεται εδώ είναι τελικά ποιες από τις ομάδες, από μία μεγάλη λίστα που παρέχει ο οργανισμός CREST, οι οποίες παρέχουν είτε penetration testing ή threat intelligence υπηρεσίες, θα επιλέξει το τραπεζικό σύστημα; Η απάντηση είναι ότι θα πρέπει (το τραπεζικό σύστημα) να λάβει υπόψιν του τα εξής 3 κύρια σημεία:

Α. Η κατανόηση των πραγματικών αναγκών του οργανισμού

Το άτομο το οποίο θα οριστεί υπεύθυνο για την επιλογή των κατάλληλων ομάδων για την εφαρμογή του CBEST, θα πρέπει να λάβει υπόψιν του τις πραγματικές ανάγκες του οργανισμού, οι οποίες σχετίζονται με την διοίκηση, το σχεδιασμό και τις διάφορες άλλες προετοιμασίες.

Β. Η θέσπιση κριτηρίων επιλογής των ομάδων CBEST

Έχοντας ως κεντρικό άξονα τις πραγματικές ανάγκες του οργανισμού, το επόμενο βήμα είναι η αναζήτηση των κατάλληλων ομάδων οι οποίες θα πρέπει:

- Να παρέχουν αξιόπιστες και αποτελεσματικές υπηρεσίες threat intelligence και penetration testing.
- Να καλύπτουν τις απαιτήσεις του CBEST test.
- Να είναι ικανές στο να μπορούν να συλλέξουν και να «μεταφράσουν» τις πληροφορίες του threat intelligence, οι οποίες άπτονται των αναγκών του οργανισμού, των χρησιμοποιούμενων τεχνολογιών, της κουλτούρας και των γεωπολιτικών θεμάτων του οργανισμού, και φυσικά να διαθέτουν κατάλληλες γλωσσικές ικανότητες.
- Να είναι ικανές να διεξάγουν, μέσω της προσομοίωσης, αποτελεσματικά penetration testings, καλύπτοντας ένα μεγάλο φάσμα πιθανών στόχων του οργανισμού.
- Να μπορούν να ανακαλύπτουν τις πιο επικίνδυνες τρωτότητες του οργανισμού και να αναλύουν τα βασικά σημεία του test.
- Να αναπτύσσουν στρατηγικές βελτίωσης με τη μορφή αντίμετρων τα οποία θα καλύπτουν τις τρωτότητες και θα εμποδίζουν την εμφάνιση τους.
- Να συντάσσουν πρακτικές και ευανάγνωστες αναφορές, έχοντας συνεργαστεί με την Διοίκηση του οργανισμού, έχοντας επιλύσει θέματα με τους παρόχους Πληροφορικής και έχοντας διευθετήσει θέματα risk management.
- Να συμβουλεύουν τον οργανισμό, σε μακροχρόνια βάση, για την διοίκηση διαφόρων συστημάτων.
- Να παρέχουν υπηρεσίες threat intelligence και alert.

Γ. Η ανάθεση έργου στον κατάλληλο πάροχο

Θα πρέπει ο πάροχος υπηρεσιών να αποτελείται από τα εξής κύρια συστατικά: Να είναι έμπιστος, να παρέχει ένα ικανοποιητικό επίπεδο ασφάλειας και να είναι ικανός να ιεραρχεί τις προτεραιότητες του έργου που θα του ανατεθεί. Εάν μιλάμε για πάροχο σε θέματα penetration testing, θα μπορούσαν να συμπεριλαμβάνονται στη λίστα διάφοροι οργανισμοί οι οποίοι εξειδικεύονται στο penetration testing, ή σύμβουλοι ασφαλείας πληροφοριών με δικές τους ομάδες penetration testing, ή εξωτερικοί συνεργάτες με δικές τους ομάδες penetration testing, αλλά και κάποιες επιχειρήσεις που προσφέρουν επαγγελματικές υπηρεσίες οι οποίες εσωκλείουν και λογιστικές επιχειρήσεις. Εάν τώρα μιλάμε για πάροχο σε θέματα threat intelligence, ο τραπεζικός οργανισμός θα μπορούσε να έχει στη λίστα του οργανισμούς οι οποίοι εξειδικεύονται σε θέματα cyber intelligence, συμβούλους με εξειδίκευση σε θέματα cyber intelligence, οργανισμούς των οποίων το αντικείμενο σχετίζεται με ανάλυση μεγάλου όγκου δεδομένων αλλά και κάποιες ομάδες οι οποίες θα έχουν πρόσβαση λεπτομερειακά σε μεγάλο όγκο δεδομένων.

Φυσικά, την απόφαση του ποιες ομάδες θα προσληφθούν από τον οργανισμό για την εφαρμογή του CBEST πλαισίου, εξαρτάται από τον ίδιο τον τραπεζικό οργανισμό, έχοντας ως σημείο αναφοράς, τον εξής απλό κανόνα: ***Θα πρέπει να ελέγχονται τα κατάλληλα συστήματα με την βοήθεια των κατάλληλων ατόμων, για τους σωστούς λόγους την κατάλληλη χρονική στιγμή***. Ο οργανισμός θα πρέπει να επιλέξει με σύνεση τις ομάδες για την εφαρμογή των κανόνων CBEST. Και θα το πράξει αυτό, λαμβάνοντας υπόψιν του και το ***κατάλληλο κόστος***- δεν θα επιλέξει πάροχο ο οποίος θα μπορεί να προσφέρει υπηρεσίες που ενώ εντυπωσιάζουν,

κοστίζουν αρκετά και το κυριότερο μπορεί να μην σχετίζονται ή να είναι περιττές σε σχέση με τις πραγματικές ανάγκες του οργανισμού. [13]

# ΚΕΦΑΛΑΙΟ 4$^{Ο}$: ΕΠΙΛΟΓΟΣ

## 4.1. Συμπεράσματα-προτάσεις

Στην παρούσα Διπλωματική Εργασία μέσα από την διεξοδική μελέτη του ποια είναι η έννοια του Cyber Intelligence και πως εφαρμόζεται, μπορεί εύκολα να διαπιστωθεί ότι μιλάμε πλέον για κάτι σχετικά καινούργιο, το οποίο θα πρέπει να συμπεριλαμβάνεται στην λειτουργία ενός οργανισμού, για την καλύτερη δυνατή προστασία και διαφύλαξη πολύτιμων και ευαίσθητων δεδομένων. Και φυσικά, θα πρέπει πρώτα η ίδια η Διοίκηση του οργανισμού να είναι σε θέση να μπορεί να αντιληφθεί την σπουδαιότητα του CI αλλά και την απαραίτητη εμπλοκή της σε θέματα εφαρμογής του, διότι αυτή είναι που θα αποφασίσει και θα εγκρίνει ενέργειες τέτοιου τύπου. Και όσον αφορά το ίδιο το Cyber Intelligence, υπάρχουν πολλοί τομείς με τους οποίους θα μπορούσε να ασχοληθεί κανείς. Για παράδειγμα, ζούμε στην εποχή του IoT (Internet of Things), όπου ένας τεράστιος αριθμός υπολογιστών, οχημάτων, κτηρίων, αισθητήρων, δικτύων και λογισμικών συνδέονται μεταξύ τους, ανταλλάσσοντας πληροφορία. Βάσει αυτού του γεγονότος, γεννιέται η ανάγκη για την διαφύλαξη των δεδομένων που υπάρχουν σε:

- Υπηρεσίες Διαδικτύου
- Υπηρεσίες cloud
- Διεπαφές κινητών τηλεφώνων
- Λογισμικά
- Λειτουργίες πιστοποίησης στοιχείων (authentication/authorization)
- Διεπαφές Web
- Ελλείψεις κρυπτογράφησης σε μεταφορές δεδομένων
- Προσωπικά δεδομένα (σε κινητές ή σταθερές συσκευές)
- Smart Houses («έξυπνα σπίτια»), όπου όλες οι συσκευές και λειτουργίες του σπιτιού ελέγχονται από ένα κινητό ή έναν υπολογιστή

Σε όλες τις παραπάνω περιπτώσεις, τα δεδομένα χρειάζονται προστασία και φυσικά ο τρόπος που προτείνουμε είναι η εφαρμογή διαδικασιών και τεχνικών cyber intelligence. [14]

---

[13] **CBEST/CREST STAR/CBEST Implementation Guide, 2016, pages 13-19**

[14] **Omner Barajas, (2014, September 17), "How the Internet Of Things (IoT) is changing the CyberSecurity Landscape", [Online]. Available: https://securityintelligence.com/how-the-internet-of-things-iot-is-changing-the-cybersecurity-landscape/**

**Wikipedia, (2016, September 30), "Internet of Things", [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things**

## Παράρτημα 1:Ιστοσελίδες σχετικές με θέματα στατιστικής και malware

Στοιχεία στατιστικής: http://av-test.org/en/statistics/malware/

Για στατιστική ή spam: http://av-test.org/en/statistics/spam/

Για στατιστική ή phising: http://apwg.org/resources/apwg-reports/ (Anti-Phising Working Group)

http://verizonenterprise.com/DBIR/, όπου αναφέρονται στατιστικά στοιχεία για το πόσο ικανά ανταπεξέρχονται διάφορες εταιρείες σε ψηφιακές απειλές αλλά και στοιχεία ανάλυσης των πιο κοινών ψηφιακών απειλών.

http://www.ponemon.org/library , όπου αναφέρονται στοιχεία για τα κόστη που δημιουργήθηκαν σε εταιρείες, λόγω διαφόρων επιθέσεων που έλαβαν χώρα σε αυτές.

http://microsoft.com/sir (MIcrosoft Security Intelligence Report), http://cisco.com/web/offers/lp/2015-annual-security-report/index.html (Cisco Annual Security Report) και http://symantec.com/security_response/publications/threatreport.jsp (Symantec Internet Security Threat Report)

https://www.scribd.com/document/274055078/CyberEdge-2015-CDR-Report (σχετικό με απειλές, άμυνες από ένα σύνολο περίπου 800 ατόμων και ειδικών που ασχολούνται με θέματα Κυβενοασφάλειας)

Αναλύσεις στο link: https://www.fireeye.com/

# ΒΙΒΛΙΟΓΡΑΦΙΑ

## Δημοσιεύσεις:


Jon Friedman, Mark Bouchard, CISSP, 2015, " Definitive guide to Cyber Threat Intelligence", pages v, 3-8, 10-26, 28-33

Intelligence and National Security Alliance, Cyber Intelligence Task Force, "Operational Levels Of Cyber Intelligence", September 2013, pages 4-10

Intelligence and National Security Alliance, Cyber Intelligence Task Force, "Strategic Cyber Intelligence", March 2014, pages 3-10

ENISA, "Proactive Detection of Security Incidents", 20-11-2012, pages 17-19

Greg Farnham, "Tools and Standards for Cyber Threat Intelligence Projects", October 14th 2013, pages 2-20

Sean Barnum, "Standardizing Cyber Threat Intelligence Information with The Structured Threat Information eXpression (STIX)", February 20, 2014, pages 2,4,7-11

ENISA, "Standards and tools for exchange and processing of actionable information", November 2014, pages 8,10,17,18,20

The MITRE Corporation, Release 1.2.0.1 dev.2, July 19, 2016, pages 1, 3, 5-7

CBEST/CREST STAR, "CBEST Implementation Guide", 2016, pages 3-4, 8-19


## Ιστοσελίδες:


University of Maryland, 2016, "About Cyber Security".[Online]. Available: http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfmhttp://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Robert M.Lee, "An Introduction To Cyber Intelligence", (2014, Jan 16), [Online]. Available:http://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/

Wikipedia, (2016, February 29), "Cyberhumint", [Online]. Available: https://en.wikipedia.org/wiki/Cyber-HUMINT

InfoSec Institute, (2016), [Online]. Available: http://resources.infosecinstitute.com/osint-open-source-intelligence/

Wikipedia, (2016, September 26), [Online]. Available: https://en.wikipedia.org/wiki/Signals_intelligence

Wikipedia (2016, September 16), "Measurement and Signature Intelligence", [Online]. Available: https://en.wikipedia.org/wiki/Measurement_and_signature_intelligence

**Robert M. Lee, (2014, January 16), "An introduction to Cyber Intelligence", [Online]. Available: http://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/**

**The MITRE CORPORATION, Copyright 2016, [Online]. Available: https://cyboxproject.github.io/samples/**

**Greg Back, 2016, "Cybox Simple e-mail Pattern", [Online]. Available:https://github.com/CybOXProject/schemas/blob/master/samples/CybOX_Simple_Email_Pattern.xml**

**The MITRE CORPORATION, Copyright 2016, [Online]. Available:http://stixproject.github.io/documentation/idioms/**

**The MITRE CORPORATION, Copyright 2016, [Online]. Available:http://taxiiproject.github.io/about/**

**The MITRE CORPORATION, Copyright 2016, [Online].Available:http://taxiiproject.github.io/documentation/sample-use/**

**Wikipedia, (2016, September 30), [Online]. Available:https://en.wikipedia.org/wiki/Application_programming_interface**

**Βικιπαίδεια, (2015, Οκτώβριος 27), [Online]. Available:https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B5%CF%80%CE%B1%CF%86%CE%AE_%CF%80%CF%81%CE%BF%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1%CF%84%CE%B9%CF%83%CE%BC%CE%BF%CF%8D_%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CF%8E%CE%BD**

**CREST Organization, (2013), "An introduction to CBEST", [Online]. Available: https://www.crest-approved.org/wp-content/uploads/2014/05/CBEST-OVERVIEW.pdf**

**CREST International, (2016), "Assurance in Information Security", [Online]. Available: http://crest-approved.org/**

**Omner Barajas, (2014, September 17), "How the Internet Of Things (IoT) is changing the CyberSecurity Landscape", [Online]. Available: https://securityintelligence.com/how-the-internet-of-things-iot-is-changing-the-cybersecurity-landscape/**

**Wikipedia, (2016, September 30), "Internet of Things", [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things**