UNIVERSITY OF THESSALY

DIPLOMA

Cyber Threat Intelligence

Author:
Ioannis STAMOULIS

Supervisor:
Nestor EVMORFOPOULOS
Examiners:
Panagiotis KIKIRAS
Eleutherios TSOUKALAS

A thesis submitted in fulfillment of the requirements
for the degree of Diploma

in the

Department of Electrical and Computer Engineering

Volos, June 2019

"If you know the enemy and know yourself, you need not fear the result of a hundred battles."

Sun Tzu, The Art of War

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Περίληψη

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Διπλωματική Εργασία

Διαχείριση Πληροφοριών Κυβερνοεπιθέσεων

Ιωάννης Σταμούλης

Η Κυβερνοασφάλεια είναι ένα πεδίο, στο οποίο μόλις πρόσφατα εστιάστηκε η προσοχή και η σημασία του αυξάνεται συνεχώς, όσο αυξάνεται ο αριθμός διασυνδεδεμένων χρηστών και συσκευών, και κατά συνέπεια ο όγκος των δεδομένων που μεταδίδονται. Αφορά εξίσου τα άτομα καθώς και μεγαλύτερες οντότητες, όπως εταιρείες και κυβερνήσεις. Υπάρχουν μέθοδοι και εργαλεία που μπορούν να παρέχουν ένα βαθμό προστασίας από απειλές στον κυβερνοχώρο. Η παρούσα διπλωματική εργασία έχει σκοπό να διερευνήσει τα μέσα για την επίτευξη αυτής της προστασίας, περιγράφοντας αρχικά μια γενική ροή εργασίας για τον εντοπισμό συμβάντων στον κυβερνοχώρο και στη συνέχεια εξετάζοντας εργαλεία και υπηρεσίες, τα οποία μπορούν να χρησιμοποιηθούν προληπτικά ή αντιδραστικά για την εκπλήρωση αυτού του σκοπού. Οι προληπτικές επιλογές μπορούν να διακριθούν σε δύο κατηγορίες, είτε σε εργαλεία που μπορούν να εγκατασταθούν και να χρησιμοποιηθούν από μια ομάδα απόκρισης έκτακτης ψηφιακής ανάγκης (ἛΡΤ), είτε σε υπηρεσίες που παρέχουν εξωτερικές πληροφορίες σχετικά με απειλές. Η αντιδραστική προσέγγιση επικεντρώνεται στη συλλογή και βελτίωση πληροφοριών, προκειμένου να εξαχθούν πολύτιμα δεδομένα που μπορούν να βοηθήσουν στην αντιμετώπιση μιας εξελισσόμενης επίθεσης ή να αποτρέψουν τις μελλοντικές επιθέσεις από το να προκαλέσουν εκτεταμένη καταστροφή.

UNIVERSITY OF THESSALY

Abstract

Department of Electrical and Computer Engineering

Diploma

Cyber Threat Intelligence

by Ioannis STAMOULIS

Cybersecurity is a field that has only recently gained attention and becomes more relevant as the number of interconnected devices and users rises, and thus the volume of transmitted data increases. It is a concern both for individuals, as well as for larger entities, such as corporations and governments. Fortunately, there are methods and tools that can provide a degree of protection against cyber threats. In this thesis, the means to achieve this protection will be explored, first by outlining the general workflow for cyber incident detection and then by inspecting individual tools and services that can be used proactively or reactively to fulfill this purpose. The proactive options can be categorized into two groups, either tools that a Cyber Emergency Response Team (CERT) can deploy and operate, or services that provide external information about threats. The reactive approach to Cybersecurity focuses on the collection and refinement of information, in order to extract valuable data that can assist in mitigating an ongoing attack or prevent future attacks from causing extensive damage.

Contents

Περίληψη **ii**

Abstract **iii**

1 Introduction **1**

1.1 A brief history of Cyber Security Events and Regulations 1

1.1.1 First major attacks 1

1.1.2 Legislation towards better security 2

1.2 Importance of Cybersecurity 2

2 Background **5**

2.1 Log Collection 5

2.2 Log Selection and Enrichment 6

2.3 Incident Detection 7

3 Proactive techniques and tools **10**

3.1 Introduction 10

3.2 Tools for Proactive Detection 11

3.2.1 Client honeypots 11

3.2.2 Server honeypots 11

3.2.3 Sandboxes 12

3.2.4 Firewall 12

3.2.5 IDS/IPS 12

3.2.6 NetFlow 13

3.2.7 Darknet 13

3.2.8 Passive DNS monitoring 13

3.2.9 Antivirus programs 14

3.2.10 Spamtrap 14

3.2.11 Web Application Firewall 14

3.2.12 Application logs 15

3.3 Available services for Proactive Detection 15

3.3.1 DNS-BH Malware Domain Blocklist 15

3.3.2 MalwareURL 15

3.3.3 Dshield 15

3.3.4 Google Safe Browsing Alerts 16

3.3.5 HoneySpider Network . . . 16
3.3.6 AusCERT . . . 16
3.3.7 Cert.br Distributed Honeypot Project . . . 17
3.3.8 FIRE (FInding Rogue nEtworks) . . . 17
3.3.9 Team Cymru – TC Console . . . 17
3.3.10 EXPOSURE . . . 18
3.3.11 Zeus/SpyEye Tracker . . . 18
3.3.12 AMaDa . . . 18
3.3.13 Malware Domain List . . . 19
3.3.14 The Spamhaus Project (Spamhaus DNSBL Datafeed) . . . 19
3.3.15 Shadowserver Foundation . . . 19
3.3.16 SGNET Honeynet Project . . . 20
3.3.17 ARAKIS . . . 20
3.3.18 Malc0de database . . . 20
3.3.19 ParetoLogic URL Clearing House / malwareblacklist.com . . . 20
3.3.20 SpamCop . . . 21
3.3.21 Arbor ATLAS . . . 21
3.3.22 Composite Blocking List . . . 21
3.3.23 Team Cymru's CSIRT Assistance Program . . . 22
3.3.24 CERT.BR Spampots . . . 22
3.3.25 Project Honeypot . . . 22
3.3.26 Malware Threat Center . . . 23
3.3.27 Smart Network Data Services . . . 23
3.3.28 Malware Patrol . . . 23
3.3.29 Zone-H . . . 24
3.3.30 Cisco IronPort SenderBase Security Network . . . 24
3.4 Summary . . . 24

4 Reactive techniques and tools 28
4.1 Introduction . . . 28
4.2 Actionable Information . . . 28
4.2.1 Relevance . . . 29
4.2.2 Timeliness . . . 29
4.2.3 Accuracy . . . 29
4.2.4 Completeness . . . 30
4.2.5 Ingestibility . . . 30
4.3 Levels of Information . . . 30
4.3.1 Low-level Data . . . 32
4.3.2 Detection Indicators . . . 32
4.3.3 Advisories . . . 33
4.3.4 Strategic reports . . . 33
4.4 Processing Actionable Information . . . 34

4.4.1 Collection . . . 34
Sources of information . . . 34
Properties of data collection methods . . . 35
4.4.2 Preparation . . . 36
Parsing . . . 36
Normalization . . . 37
Aggregation . . . 37
Enrichment . . . 38
Automation . . . 38
4.4.3 Storage . . . 38
Retention time . . . 38
Scale . . . 39
Dataset Management . . . 39
Technologies . . . 40
4.4.4 Analysis . . . 40
Investigation . . . 40
Situational Awareness . . . 41
Metrics . . . 42
Meta-analysis and source evaluation . . . 43
4.4.5 Distribution . . . 43
Internal Entities . . . 43
External Entities . . . 44
4.5 Summary . . . 44

Bibliography **46**

List of Figures

1.1 Population of the Internet[13] 3

2.1 ATT&CK Adversarial Tactics and Techniques[32] 7
2.2 "The Pyramid of Pain"[14] 8
2.3 Detection Maturity visualized 9

4.1 Levels of Information 31
4.2 General information processing pipeline 34

List of Tables

3.1 Services Collective Evaluation Rankings 26
3.2 Tools Collective Evaluation Rankings 27

Chapter 1

Introduction

1.1 A brief history of Cyber Security Events and Regulations

1.1.1 First major attacks

Cyber Security is a field that has only recently gained widespread popular attention due to several major events happening in the last decade. However, it has existed at various levels of maturity for a long time and its history can be traced back to the early 1970's.

The earliest incident to be categorized as a cyber security breach, happened in 1971 and it was a *worm* created as an experiment by Robert (Bob) Thomas who was a researcher for BBN Technologies in Cambridge, Massachusetts . However, the worm, named *Creeper* was not malicious and its functionality was limited to moving across ARPANET terminals, printing the message *"I'm the creeper: catch me if you can"* and then deleting itself. In response the program *Reaper* was developed, which would find copies of *Creeper* and delete them from the system. *Reaper* is considered to be the earliest form of Antivirus [26, 29].

The first *Denial-of-Service (DoS) Attack* to span the entire early internet happened in 1989. It was a worm created by Robert Morris and was not intended to be harmful. Instead, it was meant to test the size of the internet by going through networks and copying itself in UNIX terminals. Since it could infect a computer multiple times and could replicate rapidly, it caused machines to progressively slow down to the point of being damaged, resulting in 6000 computers being affected, causing an estimated $10-100$ million dollars in repair bills. It also resulted in a partition of the internet lasting for several days [26, 29, 4].

Coincidentally, the first ransomware attack was also recorded in 1989. It was a malware developed by Jospeh Popp, called the *AIDS Trojan*. It was distributed by mailing floppy disks through the mail. It was not as severe as modern ransomware attacks, due to only encrypting file names, while leaving the rest of the system intact and usable. Programs like AIDS_OUT were quickly created to unlock the files [29].

1.1.2 Legislation towards better security

In 1990 the Parliament of the United Kingdom introduced the Computer Misuse Act, which was the first piece of legislation concerning cyber security. This made any unauthorized access or modification of computer material illegal. It is still in effect and has been amended several times in order to be kept up to date and effectively cover modern situations. It has become the model of similar legislation for several countries [29].

Similar legislation has been implemented in the United States in 1996, 1999 and 2002, which requires the data of health care organizations, federal agencies and financial institutions to be protected. However, these regulations have been called into question due not being specific enough, and thus open to interpretation, which hinders efforts to achieve a uniform level of security. Several bills have been proposed to bring the regulations up to date.

In the European Union the cyber security regulations are more clearly defined. Three major regulations within the EU include the ENISA, the NIS Directive and the EU GDPR.
ENISA, originally created in March 2004 is the *European Union Agency for Network and Information Security* and its operations focus on three factors [15]:

- Recommendations to member states on actions against security breaches
- Policy making and implementation support for all members states of the EU
- Direct support with ENISA taking a hands-on approach to working with operational teams in the EU

The *Directive on Security of Network and Information Systems* (NIS Directive) was set into effect in 2016 aims to improve the overall level of cyber security in the EU by requiring organizations providing essential services to report incidents to Computer Security Incident Response Teams Each member state has to implement its strategy in a way to handle security breaches with minimal impact [18].

The *EU General Data Protection Regulation* (GDPR) was set into place in 2016 and enforced in 2018 and is meant to standardize data protection across all members of the EU in order to protect EU citizens from privacy and data breaches [20].

1.2 Importance of Cybersecurity

Cybersecurity is relevant to everyone, not only to businesses and countries, but also to anyone with access to a digital device. As we move into the era of Internet-of-Things, we progressively rely more on the internet for communication and services.

The number of internet users and by extension, the number of interconnected devices containing sensitive information increases as well, as it is shown in figure 1.1. This increase introduces new weak spots to be exploited for malicious purposes. Thus the importance of Cybersecurity is made clear, as a security breach in any modern system can lead to important data being compromised. Such data include the following:

- e-mail, phone numbers, social media credentials and personal information
- tax records, licenses and official documents
- medical or insurance records
- bank accounts, checks, loan information and credit card details

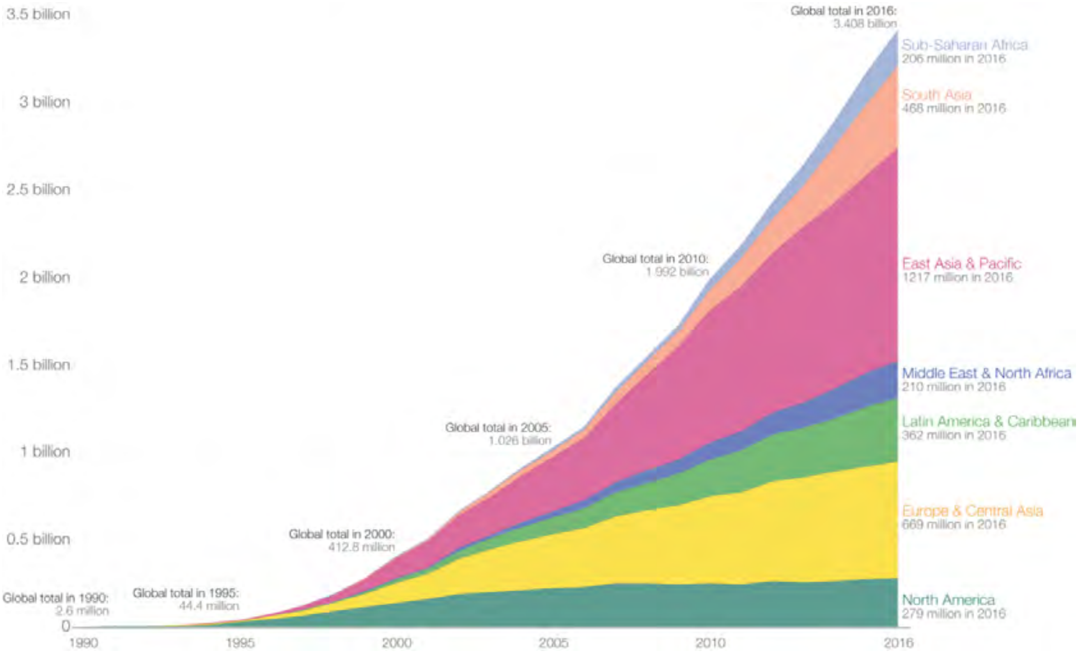


FIGURE 1.1: Population of the Internet[13]

The consequences of such data being obtained by malicious parties vary depending on the victim. If the victim is a company, it can suffer severe financial losses, technological innovations and intellectual property can be made available to competing companies and the data of its employees can be accessed. If the victim is a government official records can be accessed and altered and information that is intended to be kept secret can be exposed to the public or foreign nations, potentially leading to unrest or international incidents. If the victim is a private individual, sensitive personal information such as pictures and messages can be obtained and aside from the potential financial damage and defamation that can occur, social media profiles and e-mails can be hijacked and used to spread malware leading to further breaches in security.

Depending on the context, Cybersecurity can take several forms. Governments and large corporations can employ a Cyber Emergency Response Team (CERT) to handle its security needs, from network and system setup to responding to a cyber attack if one slips through the countermeasures already in place. Smaller institutions that may not be able to afford to employ a dedicated team should also try to have a network designed to be as secure as possible and procedures to mitigate an attack if one occurs. Individuals should also use the internet responsibly to avoid being the victim of an attack and stop it from spreading in that situation.

Chapter 2

Background

As was highlighted before, Cybersecurity is increasingly important to safeguard the extensive volumes of data that are generated and circulated daily. To achieve that, there are four key elements that define the modern Cybersecurity mindset, which is summarized in the phrase "Prevention is ideal, detection is a must" [23]. These are:

- Presumption of Compromise
- Detection Oriented Defense
- Hunt Teams
- Post-Exploitation Focus

Since the focus in on Post-Exploitation, visibility is essential. To achieve a sufficient level of visibility there are four questions that need to be answered:

- How do I collect logs?
- Which logs do I collect?
- How do I parse and enrich my logs?
- What do I look for in this mountain of data?

2.1 Log Collection

A proposition to supplement any existing Security Information and Event Management (SIEM) system is the *Elastic Stack*. It is a chain of tools such as Elasticsearch, Logstash and Kibana, that serve to collect, parse and enrich high volume logs. It also provides visualizations and dashboards to provide a quick overview of the collected data. This leads to accurate reporting, correlation and alert creation, utilizing machine learning and graph analytics. It supports horizontal scaling and provides commercial features and support, while also being compatible with third party plugins, created by an active community.

2.2 Log Selection and Enrichment

Logs that may hold value to examine after an exploitation event, in order to improve visibility can be divided into two groups, host logs and network logs. The most popular host logs fall in these categories:

- Security, System, Application
- Sysmon
- PowerShell
- Autorun items
- AppLocker
- Files, Registry

These logs, potentially, hold information about authentication, process creation, network connections initiated by suspicious processes, registry keys, autoruns and whitelisting detections.

The most popular netork logs fall in these categories:

- DNS
- HTTP
- SSL Certs
- SMTP
- NetFlow
- Host / Network Firewall & IDS
- Full PCAP

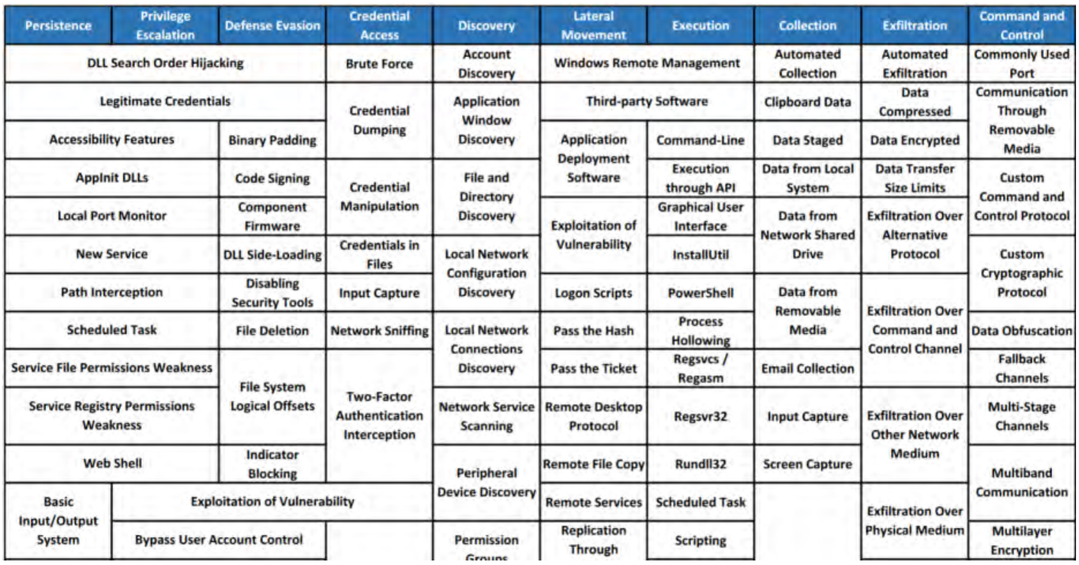
These logs, potentially, hold information about Command & Control, unexpected internal traffic, executables, SSL Certificates, password spraying, guessing and brute forcing, network share & user scanning and Internal firewall denials.

Utilizing Logstash, which is part of the aforementioned *Elastic Stack*, options become available that allow, ingestation of bulk inputs, modification of output files, as well as enrichment. Inputs are more easily received due to the availability of buffers and backpressure. Outputs can be generated in CSV, XML, Key-Value or JSON formats to make automatic parsing easier. Enrichment provides context such as domain_stats, freq, ASN, GeoIP, OUI, REST.

Collecting high value, tactical host and network logs and subsequently enriching them leads to a lower number of false positives and improves host and network visibility. This in turn improves the chance that an incident is detected. It is important to take into consideration that attackers use custom tools and try to access a multitude of protocols.

2.3 Incident Detection

In order to detect an incident, it is important to know what we are looking for in the logs. MITRE ATT&CK provides a complete suite of threat models and frameworks, as well as post-compromise behavior lists that serve as a guide in this direction.



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	
	Bypass User Account Control			Permission Groups	Replication Through	Scripting			Multilayer Encryption

FIGURE 2.1: ATT&CK Adversarial Tactics and Techniques[32]

The figure above shows MITRE's ATT&CK Navigator, which contains tactics and techniques used by attackers. Each column represents a tactic and in the rows below there are techniques used to accomplish the corresponding tactic. Techniques can belong to more than one tactic and each box is clickable and redirects to detections and mitigations for each technique. The information provided by the Navigator helps create a checklist to provide high level analytics, identify the most dangerous events to miss and measure defenses objectively. It also grants insight in the top level of the pyramid of Indicators of Compromise (IoC) regarding adversary activity (figure 2.2), which is hard to approach otherwise.

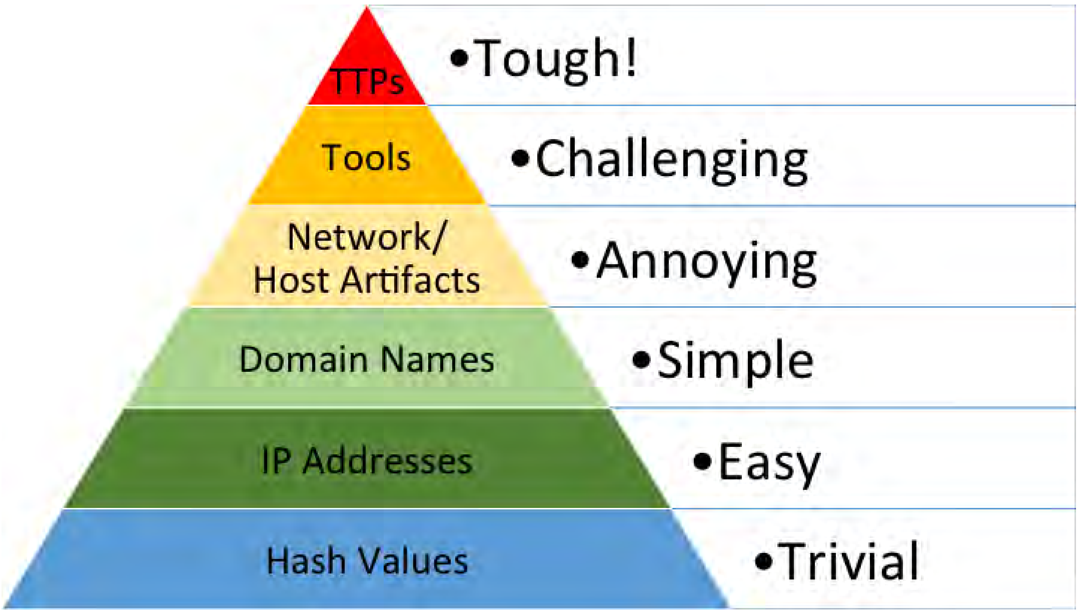


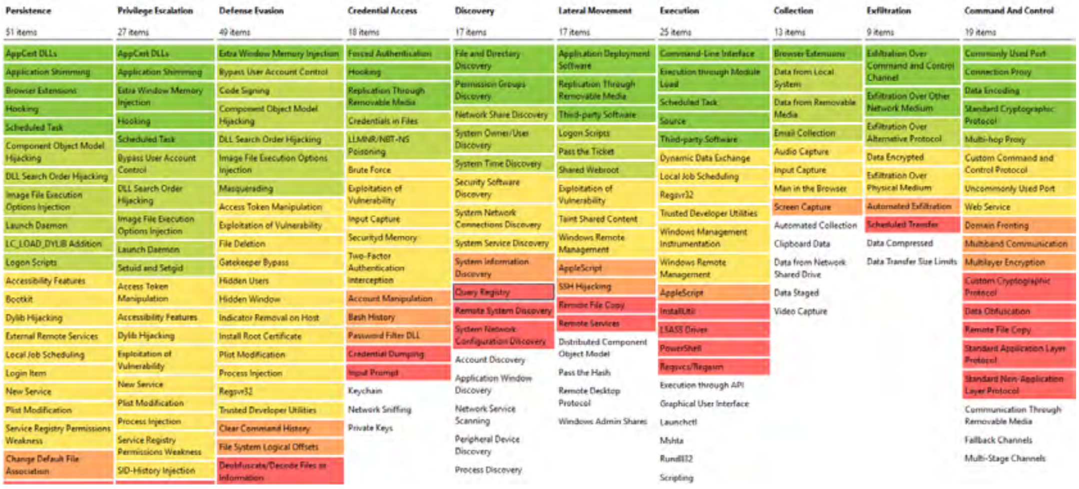
FIGURE 2.2: "The Pyramid of Pain"[14]

To implement an effective threat detection system, it is suggested that an iterative approach containing the following steps is adopted.

- Quantify detection levels
- Write analytics and track progress
- Perform red or purple teaming to repeatedly test detections and automate the process if possible

Quantifying detection maturity can be achieved by defining seven levels of maturity and rating each technique depending on the ability to detect it. These levels usually are the following and can be visualized on the ATT&CK Navigator as shown in figure 2.3:

- No Detection
- Locally Logged
- Centrally Logged
- Log Enriched/Correlated
- Report / Visualization
- Experimental / Functional Detection
- High Fidelity Detection



Persistence

51 items

- AppCert DLLs
- Application Shimming
- Browser Extensions
- Hooking
- Scheduled Task
- Component Object Model Hijacking
- DLL Search Order Hijacking
- Image File Execution Options Injection
- Launch Daemon
- LC_LOAD_DYLIB Addition
- Logon Scripts
- Accessibility Features
- Bootkit
- Dylib Hijacking
- External Remote Services
- Local Job Scheduling
- Login Item
- New Service
- Plist Modification
- Service Registry Permissions Weakness
- Change Default File Association

Privilege Escalation

27 items

- AppCert DLLs
- Application Shimming
- Extra Window Memory Injection
- Hooking
- Scheduled Task
- Bypass User Account Control
- DLL Search Order Hijacking
- Image File Execution Options Injection
- Launch Daemon
- Setuid and Setgid
- Access Token Manipulation
- Accessibility Features
- Dylib Hijacking
- Exploitation of Vulnerability
- New Service
- Plist Modification
- Process Injection
- Service Registry Permissions Weakness
- SID-History Injection

Defense Evasion

49 items

- Extra Window Memory Injection
- Bypass User Account Control
- Code Signing
- Component Object Model Hijacking
- DLL Search Order Hijacking
- Image File Execution Options Injection
- Masquerading
- Access Token Manipulation
- Exploitation of Vulnerability
- File Deletion
- Gatekeeper Bypass
- Hidden Users
- Hidden Window
- Indicator Removal on Host
- Install Root Certificate
- Plist Modification
- Process Injection
- Regsvr32
- Trusted Developer Utilities
- Clear Command History
- File System Logical Offsets
- Deobfuscate/Decode Files or Information

Credential Access

18 items

- Forced Authentication
- Hooking
- Replication Through Removable Media
- Credentials in Files
- LLMNR/NBT-NS Poisoning
- Brute Force
- Exploitation of Vulnerability
- Input Capture
- Securityd Memory
- Two-Factor Authentication Interception
- Account Manipulation
- Bash History
- Password Filter DLL
- Credential Dumping
- Input Prompt
- Keychain
- Network Sniffing
- Private Keys

Discovery

17 items

- File and Directory Discovery
- Permission Groups Discovery
- Network Share Discovery
- System Owner/User Discovery
- System Time Discovery
- Security Software Discovery
- System Network Connections Discovery
- System Service Discovery
- System Information Discovery
- Query Registry
- Remote System Discovery
- System Network Configuration Discovery
- Account Discovery
- Application Window Discovery
- Network Service Scanning
- Peripheral Device Discovery
- Process Discovery

Lateral Movement

17 items

- Application Deployment Software
- Replication Through Removable Media
- Third-party Software
- Logon Scripts
- Pass the Ticket
- Shared Webroot
- Exploitation of Vulnerability
- Taint Shared Content
- Windows Remote Management
- AppleScript
- SSH Hijacking
- Remote File Copy
- Remote Services
- Distributed Component Object Model
- Pass the Hash
- Remote Desktop Protocol
- Windows Admin Shares

Execution

25 items

- Command-Line Interface
- Execution through Module Load
- Scheduled Task
- Source
- Third-party Software
- Dynamic Data Exchange
- Local Job Scheduling
- Regsvr32
- Trusted Developer Utilities
- Windows Management Instrumentation
- Windows Remote Management
- AppleScript
- InstallUtil
- LSASS Driver
- PowerShell
- Regsvcs/Regasm
- Execution through API
- Graphical User Interface
- Launchctl
- Mshta
- Rundll32
- Scripting

Collection

13 items

- Browser Extensions
- Data from Local System
- Data from Removable Media
- Email Collection
- Audio Capture
- Input Capture
- Man in the Browser
- Screen Capture
- Automated Collection
- Clipboard Data
- Data from Network Shared Drive
- Data Staged
- Video Capture

Exfiltration

9 items

- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Alternative Protocol
- Data Encrypted
- Exfiltration Over Physical Medium
- Automated Exfiltration
- Scheduled Transfer
- Data Compressed
- Data Transfer Size Limits

Command And Control

19 items

- Commonly Used Port
- Connection Proxy
- Data Encoding
- Standard Cryptographic Protocol
- Multi-hop Proxy
- Custom Command and Control Protocol
- Uncommonly Used Port
- Web Service
- Domain Fronting
- Multiband Communication
- Multilayer Encryption
- Custom Cryptographic Protocol
- Data Obfuscation
- Remote File Copy
- Standard Application Layer Protocol
- Standard Non-Application Layer Protocol
- Communication Through Removable Media
- Fallback Channels
- Multi-Stage Channels

FIGURE 2.3: Detection Maturity visualized

To improve the incident detection capability, tools can be used to execute tests, collect data, develop detection and finally measure progress and visualize it. To speed up that process, *automated adversary emulation* tools can be utilized to achieve automation, such as Caldera and Metta, which come with accompanying datasets and analysis tools. However, this automated process generates a vast amount of data, that need to be converted to analytics that need to be easily interpreted by analysts. This has led to the development of a standardized format for analytics, named Sigma, that enables easy import and sharing accross organizations, decouples rule logic from specific implementations and eliminates SIEM tribal knowledge.

Chapter 3

Proactive techniques and tools

3.1 Introduction

As we have seen in the previous chapter, while detection of incidents is a non-negotiable goal, prevention is the ideal scenario. In this chapter we will explore tools and techniques that are being utilized by CERTs to proactively detect cyber incidents. Proactive detection of a threat by a CERT, as opposed to reactive detection, is the discovery of malicious activity before its effects become apparent to the constituency the CERT is protecting. This can be achieved by utilizing internal monitoring tools or published information about detected incidents. Proactively detecting incidents boosts the CERT's capabilities, improves situational awareness and grants greater efficiency when handling incidents.

There are two approaches when it comes to achieving effective proactive detection, depending on where the threat originates from. On one hand there are tools that the CERT can deploy to monitor internal events in its constituency. These may only cover the network that the CERT is directly responsible for. In other cases they can extend to cover a larger part of the CERT's employer's network or even be a part of a larger array with a nation-wide scope.

On the other hand, there are services that are available over the internet and can be accessed to obtain information about network security incidents detected outside the monitoring capabilities of the CERT. These can be either free, require registration, or come with a fee. The data they provide can be filtered and pre-processed and structured, or available as a raw feed in the state that it was collected.

The wide coverage that is made possible by these services offers an advantage, especially to CERTs that don't have the means to collect such data on their own and ones that are responsible for entire countries or regions.

3.2 Tools for Proactive Detection

In this section we will explore the most common types of tools used by CERTs for proactive detection of incidents and their assessment by ENISA[17].

3.2.1 Client honeypots

Client honeypots are tools that are capable of active search for malicious servers. They aim to identify whether there has been an attack after establishing contact with a server. There are three main types of honeypots:

- *High-interaction honeypots* are systems with complete functionality typically deployed as virtual machines. They operate by simulating a system belonging to the client, which in turn tries to access various servers. They have monitoring capabilities in order to observe changes and detect suspicious activity after making contact which are then reported in logs. Monitoring such a wide range of parameters comes at a cost to performance. They are, however, the most popular type used in home user cases.
- *Low-interaction honeypots* offer a different solution to the same problem. These emulate the behavior of particular pieces of software and directly observe the responses related to its activity. They can be efficient and cheap, however they are limited to mostly detecting pre-existing, known threats, as they lack the ability to observe unknown behavior.
- *Hybrid client honeypots* are an attempt to leverage the strong points of the previous two types of honeypots. Combined information of low and high interaction honeypots can give a more complete overview of an exploitation or infection providing better capability of restricting a threat.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Fair+	Fair +	Fair +	Good	Excellent	Fair

3.2.2 Server honeypots

Server honeypots are essentially traps that are set in place in order to monitor unauthorized attempts of accessing and using a network or system. They are monitored to serve as an early warning system or observe trends of suspicious activity. Many honeypots can be deployed in a network to provide wider coverage.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Good	Good	Good	Good	Good	Good

3.2.3 Sandboxes

Sandboxes are environments specifically designed to let potentially malicious code to be executed in isolation, without access to the rest of the system in order to observe its behavior without a risk of infection. All of its behavior, especially network access attempts, is then analyzed to assess whether it is malicious. Malicious code will often try to connect to the internet to download executables and tracing these connections can reveal the address of infected servers or dedicated servers distributing malware.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Fair+	Fair	N/A	Good	Fair+	Fair<

3.2.4 Firewall

Firewalls are either physical devices or software that is designed to filter network connections. They aid in proactive detection by generating an alert any time a suspicious connection is detected, either inbound or outbound. For example, attempted bulk connections to a known service can be interpreted as a hint of a worm infection. Similarly mass attempted connections to a single address may reveal a DDoS attack. Firewalls can be utilized in two ways:

- Directly generate alerts.
- Use additional tools to perform analysis on the firewall's logs.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Fair	Good	Fair+	Good	Excellent	Fair+

3.2.5 IDS/IPS

Intrusion Detection Systems (IDS) are software applications designed to observe and analyze network traffic and system behavior in order to identify possible malicious events. They typically have a passive role, generating an alert in case they detect a threat. Intrusion Prevention Systems (IPS) on the other hand share a lot of similarities but work actively to block threats. These systems can detect malicious behavior by either comparing it to known attack patterns or by comparing it to the typical behavior of the system and noticing a deviation.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Good	Good	Fair+	Fair+	Good	Fair+

3.2.6 NetFlow

Netflow is a mechanism that collects monitors and analyzes traffic based on the IP protocol. It can be effective in detecting irregular traffic and is very useful in both detecting and combating DDoS attacks. It mainly focuses on detecting compromised devices within a network.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Good	Fair	Fair+	Fair	Good+	Good

3.2.7 Darknet

Darknets are used to monitor traffic that is directed to unused IP addresses without being related to any of the other observed traffic. It works best when the number of unused IP addresses is large. They can potentially aid in the detection of worms, DDoS attacks or network devices without proper configuration, which contribute to their false positive reports.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Good	Fair	Fair+	Fair	Good	Fair

3.2.8 Passive DNS monitoring

Analyzing DNS traffic can reveal potential malicious activity. This analysis can provide information about the origin of an attack or discover a botnet. Malicious domains can be identified by comparing DNS querry results to blacklists containing known malicious domains. Additionally, monitoring DNS traffic can reveal trends that can potentially lead to the discovery of malicious activity.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Good+	Good	Fair+	Good	Good+	Fair

3.2.9 Antivirus programs

Antivirus programs are used to block, detect and delete malware from computers. They are usually built around detecting specific signatures associated with malware, which makes them most suited to detecting threats that are already known. Newer iterations have some additional capabilities, allowing them to potentially detect even unknown threats.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Good	Good	Fair+	Good	Good	N/A

3.2.10 Spamtrap

A Spamtrap is a form of honeypot that is dedicated to detecting spam. In most cases it is simply a modified email inbox that is advertised in a way that is visible to spammers with a purpose of being harvested and added to their databases. After receiving unwanted mail, the addresses of the sender can be obtained and categorized as spam.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Fair+	Fair	Fair	Good	Good	Good

3.2.11 Web Application Firewall

Web application firewalls can be devices, plugins or filters that apply a set of restrictions to HTTP connections. By modifying the set of rules, they can be customized to cover a wide range of attacks, detect them and block them in case they occur. Such customization may require significant effort however.

ENISA has rated this tool as such:

timeliness	accuracy	ease of use	coverage	resources	scalability	extensibility
Excellent	Good+	Fair	Fair	Fair	Good	Good

3.2.12 Application logs

Analysis of application logs can include logs generated by the system, databases or network activity. This way, irregular behavior, such as repeated unsuccessful log-in attempts, can be detected and the origin address of these interactions can be compared with the contents of blacklists to determine if it is actually malicious.

3.3 Available services for Proactive Detection

A study conducted by ENISA has focused on tools providing information used for proactive detection of cyber incidents [17]. In this study the tools have been evaluated in five categories and given a rank in each one. These categories are timeliness, accuracy, ease of use, coverage and required resources.

3.3.1 DNS-BH Malware Domain Blocklist

The DNS-BH project curates a list of domains related to spyware and malware. This list can be used to provide zone files and information about the blacklisted domains. Long term filters can be created to monitor traffic and create alerts when access to a blacklisted domain is attempted [38].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Fair	Good	Excellent	Excellent	Excellent

3.3.2 MalwareURL

The MalwareURL team provides a database containing up-to-date information about observed URLs and IP addresses reated to malicious activity. After registration the contents of the database can be provided in CSV and RSS formats. However it is not free for commercial use [42].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Excellent	Excellent	Excellent

3.3.3 Dshield

DShield is a distributed intrusion detection system used to collect and analyze data. The collected data is cataloged and summarized and can reveal trends in activities confirm attacks and drive forward changes in firewall design. The blocklist it provides can be used as a filter to produce alerts of attempted access to blacklisted addresses. It also supplies a list of the top 100 malicious IP addresses, which can be utilized to assess the severity of an attack [25].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Fair	Good	Excellent	Excellent

3.3.4 Google Safe Browsing Alerts

The Google Safe Browsing Alerts is a service that examines URLs, software and content of pages in an attempt to identify unsafe websites. This provides warnings to users when they attempt to access unsafe websites and allows network administrators to receive information about malicious activity on their network [21].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Fair	Good	Excellent	Good

3.3.5 HoneySpider Network

The HoneySpider Network is a system that aims to identify websites that are malicious to the end user. To achieve this goal it is designed to be modular and able to combine the outputs of multiple honeypots. After performing periodic scans it produces a report of threats, as well as the threat's sources. It can be accessed from a web browser and supports multiple users [36].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Fair	Good	Fair	Excellent

3.3.6 AusCERT

The AusCERT provides a service called malicious URL feed. It updated regularly and distributed to anyone that is a member of AusCERT. It is available in two versions, one containing the feed of the last day and one containing the feed of the last week. It provides information about several types of malicious activity and can be utilized to create blacklists and filters to aid protection [5].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Good	Good	Excellent

3.3.7 Cert.br Distributed Honeypot Project

CERT.br has deployed a distributed network of honeypots across Brazil to collect network traffic information. It provides daily statistics about activity observed by its honeypots including the most popular UDP and TCP ports. The aim of sharing this data is to improve incident detection, correlate events and detect and analyze trends. Additional information can be provided after contacting the organization and agreeing to terms of data sharing [7].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Fair	Good	Good

3.3.8 FIRE (FInding Rogue nEtworks)

FIRE (FInding Rogue nEtworks) is a system designed to identify rogue networks that consistently demonstrate malicious behavior and report the providers that are responsible for them to the public via the service's website. It can report the IP adress, server location and type of the malicious behaviors. It also keeps a record of previously detected malicious networks. [6].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Fair	Good	Good

3.3.9 Team Cymru – TC Console

The TC Console is a web-based user interface used for the visualization of malicious activity in a network developed by Team Cymru. Its aim is to improve the user's visibility by offering almost real-time information and TSV files that can be used in automated monitoring of incidents. It can also provide both a summary of previous activity on the network and quantitative information about traffic. The service allows data sharing between corporations to potentially provide the possibility of utilizing more information than what is available directly from the service. Access to the service is granted after registration and declaration of the interested party's autonomous system (AS) numbers [12].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Good	Good	Excellent	Excellent

3.3.10 EXPOSURE

EXPOSURE is a service that performs passive DNS analysis on a large scale in order to identify domains involved in malicious activity. It shares a blacklist containing domains known for past malicious activity. Historical data on previous activity is also available to allow tracking of changes over time. The contents of the list are cross referenced with other similar services and can be provided daily [27].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Excellent	Good	Excellent

3.3.11 Zeus/SpyEye Tracker

The Zeus Tracker is a service designed to monitor Zeus C&C servers and fake URLs. A blocklist is provided in several formats to aid in preventing clients infected by Zeus from accessing the C&C servers [3]. Lists of active IP addresses, as well as separate lists for removed addresses are available. The SpyEye tracker was a similar service, but is focused on the SpyEye malware instead. However it has been discontinued after not detecting any activity from SpyEye for over a year [2].

ENISA has rated this service (Zeus Tracker) as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Excellent	Excellent	Fair	Excellent

3.3.12 AMaDa

The abuse.ch Malware Database (AMaDa) is a service that provides a list of C&C servers. It gathers information by tracing malware samples giving it high quality of information. The lists are provided in multiple formats such as text, RSS or HTML [1].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Good	Excellent	Fair	Excellent

3.3.13 Malware Domain List

The Malware Domain List is a service that provides a list containing URLs that have been observed participating in malicious activity, such as infections, botnets and malware hosting. The IP addresses of the associated serves are also provided. The lists are available in numerous formats, such as CSV, text or RSS. It can be used for free, as it is a non-commercial community project [28].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Good	Excellent	Good	Excellent

3.3.14 The Spamhaus Project (Spamhaus DNSBL Datafeed)

The Spamhaus Project tracks spam operations across the internet and creates real-time lists for spam blocking purposes. It provides these lists through a professional service called the DNSBL Datafeed. It is available as either a query service or an Rsync service. The query service allows real time access to Spamhaus DNSBL's private network of servers. The Rsync service allows data synchronization between Spamhaus's servers and the client's local servers and is oriented towards high-volume users. It is available as a yearly subscription service [41].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Good	Good	Excellent	Good

3.3.15 Shadowserver Foundation

The Shadowserver Foundation is a nonprofit security organization that tracks, gathers and analyzes malicious activity. Additionally, it assists in incident response coordination. It provides the ASN & Netblock Alerting & Reporting Service which generates customized reports about adresses or specific AS numbers that are involved in malicious activity. The service is free, it updates daily and offers reports in CSV, HTML, XML, text or URL formats. [19].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Excellent	Excellent	Excellent

3.3.16 SGNET Honeynet Project

The SGNET Honeynet Project is a distributed network of honeypots. It captures the traffic from various locations across the world, stores it and enriches it with information such as location and OS information. This information is updated daily and is available to the end user in real-time through a graphical interface that can be accessed through a browser. The project relies on protocol learning and high-interaction honeypots to ensure a low false-positive rate [37].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Excellent	Good	Fair	Good

3.3.17 ARAKIS

ARAKIS is an early warning system operated by NASK / CERT Polska. Its main aim is to detect and characterize automated threats. To detect threats it relies on active scanning through a network of honeypots, firewalls, antivirus systems and adrknets. It is exclusively focused on networks in Poland. New information is available daily in CSV format, accompanied with timestamps and a daily summary is generated. Registration is needed to access the information [35].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Excellent	Good	Excellent

3.3.18 Malc0de database

The Malc0de database contains information regarding URLs that host malware. It also provides information about the IP address and AS number associated with each URL. The database is updated several times daily and the contents are available as an RSS feed, enabling automation capabilities for users. Its data collecting infrastructure is undisclosed, thus we have no information on its coverage [30].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Good	Excellent	N/A	Excellent

3.3.19 ParetoLogic URL Clearing House / malwareblacklist.com

The service malwareblacklist.com provides is information on malicious URLs that are collected by client honeypots. The honeypots try to access sites from a list of known malicious addresses, sites identified from spam messages or from malware details as well as regular sites with lower priority. However its coverage is unclear. Its information is updated daily or several times a day and can be accessed by a regular browser or collected with an automated system using an API [10].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Good	Good	N/A	Good

3.3.20 SpamCop

SpamCop is a service designed to report spam by identifying the origin of such emails and reporting it to the Internet Service Provide responisble for it via email. Additionally, it provides a Blocking List of IP addresses that have been reported by SpamCop users as having sent spam emails. There is also support for mirroring the database for free if access to the mirror is public, or for an annual fee if the mirror is private. Information about individual IP addresses is also available. The database is updated almost in real-time and data are available as email messages [39].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Good	Good	Excellent	Good

3.3.21 Arbor ATLAS

The Active Threat Level Analysis System (ATLAS) is a threat analysis network with a global scope. It provides visibility into the backbone networks that are considered the Internet's core, allowing teams to be informed about malicious traffic at a global scale. It is a publicly available resource, accessible after a free registration. Its data are updated daily, delivered in CSV, XML or IODEF formats and can be accessed through a browser or an XML/CSV parser [33].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Excellent	Excellent	Excellent

3.3.22 Composite Blocking List

the Composite Blocking List is a blackhole list of spam email senders based on DNS. It collects data from spamtraps and mail infrastructures and reports the IP address of spambots and other entities suspected of spam related activity. Information on individual addresses is available through the lookup utility it provides. The provider of the service (Spamhaus) encourages accessing CBL through the aforementioned SpamHaus DNSBL system (section 3.3.14) as it provides more results for potential queries. Its data is updated in real time and is available through Rsync or through a Mail Transfer Agent (MTA) which has to be configured [40].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Excellent	Fair	Excellent	Good

3.3.23 Team Cymru's CSIRT Assistance Program

In addition to the TC Console (section 3.3.9), Team Cymru provides lists concerning suspicious events related to a CERT's area of responsibility on a daily basis. The service is offered for free and any CERT is encouraged to join. Its information is updated daily with data for the last three days also being available. Data can be delivered via email and accessed through an HTTP client, aiding in automated collection [11].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Excellent	Excellent	Excellent	Good

3.3.24 CERT.BR Spampots

The Spampots project uses a network of low-interaction honeypots to gather spam-related data. It has deployed sensors in 11 countries across all continents. The network collects data periodically which is then analyzed by the SpamMining team and distributed to the members of the project. A web interface with can be exclusively accessed by members provides additional statistical information about the observed spam traffic. The data of the service is delivered with little delay, however, accuracy of information could not be verified due to the closed membership required to obtain it [8].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	N/A	Good	Fair	Fair

3.3.25 Project Honeypot

Project Honeypot is designed to identify spammers through a distributed network of decoy web pages. It achieves that by using custom-tagged email addresses that are set up to collect messages from spambots that happen to harvest them providing information about the time they were contacted and the IP of the sender. The full extent of the results based on the collected data are available on the service's website for registered users. However, non-members can still access the top 25 addresses identified to be engaged in spam activity. The data feeds are updated every day and can be obtained through RSS or email [43].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Excellent	Excellent	Good

3.3.26 Malware Threat Center

The Malware Threat Center service provides information on a variety of online threats by collecting data from firewall filters, antivirus reports and malware binaries to aid network administrators in protection against malware. On a daily basis, it provides a filter list that is available publicly for free in two formats, a text file and a web page which contains more detailed information [24].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Fair	Excellent	Fair	Good

3.3.27 Smart Network Data Services

Microsoft's Smart Network Data Services (SNDS) aim to enable any user that has control over an IP space to assist in the detection and neutralization of spam malware and viruses. Any user with a Microsoft Account can request access to the service regarding the IPs for which they are responsible. Data are aggregated daily and are available for 90 days after being published. Access is possible either through the dedicated website, or as a CSV file that can be utilized to aid automation [31].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Good	Good	Excellent	Excellent	Good

3.3.28 Malware Patrol

Malware Patrol is a service centered around verification of URLs for malware presence. The service is developed by community effort, it is free and is provided for non-commercial use. It provides blacklists of domains that have been identified as spreading malware. The lists are available to CERTs after an application to request access. The data is updated daily and is provided in ready-to-use form [34].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	N/A	Excellent	N/A	Excellent

3.3.29 Zone-H

Zone-H is a service that collects defacement reports for websites and maintains a historical archive of such events. It relies on its open community where anyone can anonymously submit reports related to defaced websites, which are then checked for authenticity and added to the database. The lists it provides are updated in real-time and are available through a website or RSS feed for non-commercial use [22].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Excellent	Good	Good	Fair

3.3.30 Cisco IronPort SenderBase Security Network

Recently merged with Cisco's new Talos Intelligence Group, SenderBase is a network set up to monitor email and web traffic. It examines parameters such as sending volume, country of origin, complaint levels, appearances as part of an attack and other parameters. Its database is updated in real time, information is available in text or CSV formats and its coverage is of global scope [9].

ENISA has rated this service as such:

timeliness	accuracy	ease of use	coverage	required resources
Excellent	Good	Excellent	Excellent	Good

3.4 Summary

When setting up a system aimed at proactive detection of security incidents, there are five tools that are considered essential for any CERT as a starting point, to form a core that can serve as a foundation upon which to expand as time progresses.

- Firewalls as they are present in every network and adapting them to detect security incidents is relatively easy.
- Antivirus as they are almost as ubiquitous as firewalls and offer a low false-positive rate.
- IDS/IPS to detect and block attacks against the network. They can also provide additional attack details for cases not blocked by the firewall.

- NetFlow for threat detection, post-compromise network forensics and increased situational awareness.
- Log analysis as valuable information can be gained by properly parsing and interpreting their contents.

To simplify the process of selecting the appropriate services, depending on different needs and events, ENISA recommends five specific services from the list of reviewed services in order to provide CERTs with an adequate level of coverage of security incidents occurring in their constituency.

- The Shadowserver Foundation as it provides high quality data on botnets, C&C and DDoS every day. It is free to use and easily available.
- The Zeus/SpyEye Tracker to obtain information about popular spyware. Samples of malware and IP blacklists are also available to users.
- Google's Safe Browsing Alerts as a dedicated service for malicious URL discovery backed by Google's immense processing power, despite some difficulty in obtaining access to information regarding networks outside the CERT's constituency.
- The Malware Domain List to obtain information about malicious domains that propagate malware, as well as classification information for these domains.
- Team Cymru's CSIRT Assistance Program as having access to high quality data covering a wide spectrum of incidents types is essential to any CERT. Additionally, lists of compromised devices associated with the CERT's ASNs regarding C&C server, bot infections, malware and phishing are available.

name	timeliness	accuracy	ease of use	coverage	required resources
DNS-BH Malware Domain Blocklist	Fair	Good	Excellent	Excellent	Excellent
MalwareURL	Good	Good	Excellent	Excellent	Excellent
Dshield	Excellent	Fair	Good	Excellent	Excellent
Google Safe Browsing Alerts	Good	Fair	Good	Excellent	Good
HoneySpider Network	Excellent	Fair	Good	Fair	Excellent
AusCERT	Good	Good	Good	Good	Excellent
Cert.br Distributed Honeypot Project	Good	Good	Fair	Good	Good
FIRE (FInding Rogue nEtworks)	Good	Good	Fair	Good	Good
Team Cymru – TC Console	Excellent	Good	Good	Excellent	Excellent
EXPOSURE	Good	Good	Excellent	Good	Excellent
Zeus/SpyEye Tracker	Good	Excellent	Excellent	Fair	Excellent
AMaDa	Excellent	Good	Excellent	Fair	Excellent
Malware Domain List	Excellent	Good	Excellent	Good	Excellent
The Spamhaus Project (Spamhaus DNSBL Datafeed)	Excellent	Good	Good	Excellent	Good
Shadowserver Foundation	Good	Good	Excellent	Excellent	Excellent
SGNET Honeynet Project	Good	Excellent	Good	Fair	Good
ARAKIS	Good	Good	Excellent	Good	Excellent
Malc0de database	Excellent	Good	Excellent	N/A	Excellent
ParetoLogic URL Clearing House / malwareblacklist.com	Excellent	Good	Good	N/A	Good
SpamCop	Excellent	Good	Good	Excellent	Good
Arbor ATLAS	Good	Good	Excellent	Excellent	Excellent
Composite Blocking List	Excellent	Excellent	Fair	Excellent	Good
Team Cymru's CSIRT Assistance Program	Good	Excellent	Excellent	Excellent	Good
CERT.BR Spampots	Excellent	N/A	Good	Fair	Fair
Project Honeypot	Good	Good	Excellent	Excellent	Good
Malware Threat Center	Good	Fair	Excellent	Fair	Good
Smart Network Data Services	Good	Good	Excellent	Excellent	Good
Malware Patrol	Excellent	N/A	Excellent	N/A	Excellent
Zone-H	Excellent	Excellent	Good	Good	Fair
Cisco IronPort SenderBase Security Network	Excellent	Good	Excellent	Excellent	Good

TABLE 3.1: Services Collective Evaluation Rankings

name	timeliness	accuracy	ease of use	coverage	required resources	scalability	extensibility
Client honeypots	Excellent	Fair+	Fair +	Fair +	Good	Excellent	Fair
Server honeypots	Excellent	Good	Good	Good	Good	Good	Good
Sandboxes	Excellent	Fair+	Fair	N/A	Good	Fair+	Fair+
Firewall	Excellent	Fair	Good	Fair+	Good	Excellent	Fair+
IDS/IPS	Excellent	Good	Good	Fair+	Fair+	Good	Fair+
NetFlow	Excellent	Good	Fair	Fair+	Fair	Good+	Good
Darknet	Excellent	Good	Fair	Fair+	Fair	Good	Fair
Passive DNS monitoring	Excellent	Good+	Good	Fair+	Good	Good+	Fair
Antivirus programs	Excellent	Good	Good	Fair+	Good	Good	N/A
Spamtrap	Excellent	Fair+	Fair	Fair	Good	Good	Good
Web Application Firewall	Excellent	Good+	Fair	Fair	Fair	Good	Good
Application logs	-	-	-	-	-	-	-

TABLE 3.2: Tools Collective Evaluation Rankings

Chapter 4

Reactive techniques and tools

4.1 Introduction

In the previous chapter we explored the means that aim to achieve proactive detection of Cybersecurity incidents. While they provide a strong level of protection, it is not guaranteed that they will detect and prevent all threats from entering the network and cause damage. In order to be able to combat the incidents that make it past the primary protection of the proactive defenses, *Incident Response* mechanisms and procedures need to be in place, in order to protect the victim's network against these threats, or at least mitigate the damage that is caused. The most important element to make such a secondary line of defense truly effective is high quality information. The sooner vulnerabilities are identified, the faster they can be patched to deny a point of weakness. In similar fashion, the sooner an ongoing incident is detected, the faster the reaction will be and thus the damage caused will be limited.

Even though sharing of security information is widespread, the biggest challenge faced by CERTs is extracting information in a timely fashion, so that can be immediately useful from the vast volume of data that are being received. Such information is referred to as *Actionable Information* and is at the core of any effort of successful incident response. In this chapter we will explore key properties and general techniques for an efficient pipeline that produces Actionable Information based on recommendations by ENISA [16].

4.2 Actionable Information

In general, the term *Actionable Information* can refer to market data that describe trends and other information that can be used to improve business decisions by making them more specific and strategic. To meet the criteria needed to be considered actionable, information must be timely, accurate, complete in the context of the business that receives it and ingestible. These criteria also apply to information concerning IT security, where the goal is to address current threats and reduce the impact of future ones. Whether information is considered actionable also varies depending on the recipient.

4.2.1 Relevance

Information can be considered relevant if it is applicable to the recipient's area of responsibility, depending on the network, software and hardware infrastructure of its constituents. When information is referring to compromises happening outside the area of responsibility of the recipient, it is considered irrelevant. Therefore, precisely describing one's constituency using ASNs, CIDRs and domain names is highly preferred and can be helpful in receiving relevant information through customized data feeds, or filtered data feeds based on this description.

4.2.2 Timeliness

Information can be considered timely depending on the time it is obtained, but also depending heavily on the context of the application to which it is relevant to. Due to the rapidly changing threat characteristics, even information no older than a few hours may be considered obsolete by the time it arrives. Large volumes of data being shared make ingestibility difficult, delaying the time it becomes available and actionable. Additionally, actionable information is usually a result of analysis that takes time to complete to a satisfying level. Thus timeliness may often be pursued at the cost of completeness and accuracy. Nevertheless, even information that is months old can be considered timely in the context of a post compromise damage mitigation and cleanup operation regarding a recently discovered threat. Finally it is important for the parties that provide information to correctly assess the required level of accuracy and not delay making the information available by chasing higher accuracy that may not be needed.

4.2.3 Accuracy

Information can be considered accurate if the recipient can be sure that it has been verified and checked for errors before it is received. The accuracy of information is a product of the confidence that the source asserts, the level of trust between the source and the receiver and the receiver's context. An important factor that can define the trust between the source and the recipient is the transparency on the information collection process, as it is unlikely that an important action will be made based on information of dubious origin. Accuracy can also be assessed by the track-record of the source that is established over time and by previous experience with that source by looking at indicators such as false positives and false negative rates. Feedback to the source and evaluation of received information can be helpful to improve the data feed in the future.

4.2.4 Completeness

Information can be considered complete if it can provide additional value to information that is easily available to the recipient, while being able to stand on its own. If the information provided by the source can complete gaps in the information that the recipient already has available through other means it can be considered complete. However, many information providers may decide to reduce the completeness of the information they make available in order to conceal their investigative methods or due to legal constraints regarding privacy of information. To achieve a sufficient level of completeness, the provider and the recipient need to come to a mutual understanding, both about the recipient's needs, as well as the provider's limitations and constraints. Often, standalone pieces of information that may seem incomplete, can be combined with other sources to become actionable information.

4.2.5 Ingestibility

Information can be considered ingestible if it can be imported to a organization's information management systems in a straightforward way and then easily analyzed to extract indicators. It is mostly defined by the formats and transfer protocols used for data sharing. In the most usual case, the recipient needs information which can be used immediately and quickly, in order to combat an ongoing attack, or patch security vulnerabilities. Typically information is shared between machines and human reaction can be needed at a later stage. Standardized formats are required in order to let machines effectively use the provided information.

Finally, actionable information should adopt a format that can represent it in its complete form, while allowing systems to obtain it in an automated and standardized way and provide the ability to correlate and associate it with other information. The choice of format is influenced by the number of recipients, the type of information being stored and the volume and frequency of data.

4.3 Levels of Information

Now that the definition and key characteristics of actionable information has been established, the activities related to its collection, processing and distribution will be explored and the information will be categorized. The two most prevalent ways of categorizing information within the community are:

- The data model defined by the STIX standard, which provides informal ontology that describes a variety of security information, ranging from observables to high level descriptions of entities like threat actors.
- The Pyramid of Pain[14], which defines a taxonomy organized depending on the value of indicator types, when defending against complex adversaries. These are layered according to their value, from simple indicators, such as hashes of files, to complex ones that describe the attacker's behavior, such as TTPs (Tactics, Techniques and Procedures).

Since information can exist in many types, for the purpose of protecting a network, it is convenient to categorize it in four tiers, which are low-level data, detection indicators, advisories, and strategic reports. The most commonly encountered types of information are distributed in these levels as follows:

- Low-level data include network flow records and full packet captures, application logs, including typical IDS alerts, samples of executable files, documents, and email messages.
- Detection indicators include IP addresses, DNS names, URLs, specific values of format-specific fields, for example email headers, artifacts, sequences of low-level events linked to malicious behavior.
- Advisories include ulnerabilities, exploit code, patches, patch status, high-level patterns of activity on a host, service, network or internet level.
- Strategic reports which are highly summarized threat analyses, written in prose.

As is shown in figure 4.1 as information becomes more complex and abstracted, it offers more condensed information. Typically, large volumes of low-level information are collected, which are then analyzed to obtain indicators and advisories. These are in turn assembled intohigh level conclusions and strategic reports.

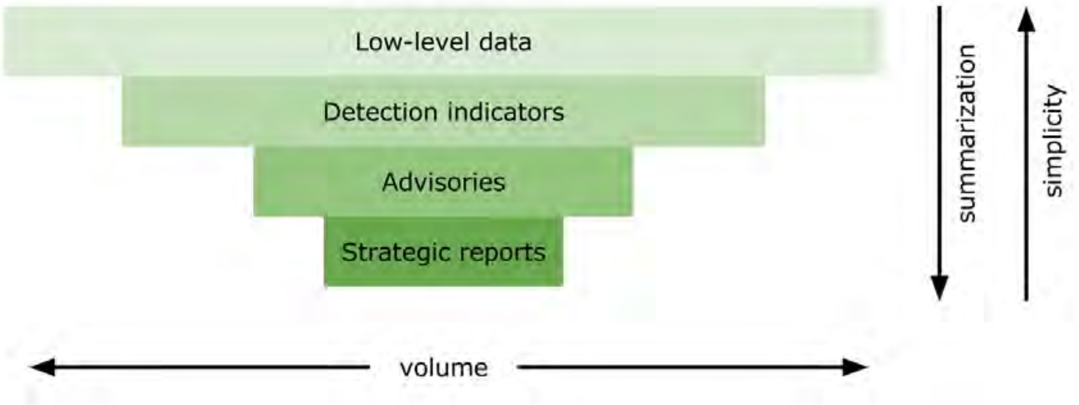


FIGURE 4.1: Levels of Information

4.3.1 Low-level Data

In order to implement an information-driven protection system, it is essential to find good data sources. Usually, CERTs can collect and monitor data related to activities that occur within their constituency, which include network traffic, actions performed by users and behavior of applications. However, without context, this data is not useful. One way to provide context is to identify potentially affected systems and, thus use the incident itself as context. Another way, which is mostly used by automated systems, is to compare the observed behavior to known patterns. Finally, anomalies in the data can also be combined with detected patterns to provide additional context. Low level data is usually produced by machines in large volumes, which leads to the need of automated processing, as it needs to be analyzed in order to become valuable, actionable information.

4.3.2 Detection Indicators

Among the various indicators that exist, that are relevant to security, detection indicators are the only ones that can be considered actionable and, as a result, are the most commonly used. Detection indicators are patterns that can be compared with low level data, in order to identify threats. They are based on network characteristics, such as IP addresses, URLs, MD5 hashes of files, as well as strings in email headers or patterns of invocations of system calls by an application, that can be observed on the protected network. Additionally, indicators provide information about the context, which may allow analysts to understand what the indicator attempts to detect in an ideal scenario. Indicators of sufficient quality, can be immediately applied for the purpose of detecting malicious behavior without additional processing other than conversion to a suitable format.

Indicators may be the result of manual analysis, or the result of automated analysis resulting from observing malware behavior using sandboxes, sinkholes, or honeypots. Indicators such as malware signatures can be used to generate alarms containing network addresses of attackers or victims, that are also indicators. The most frequently shared detection indicators are the following:

- IP addresses of infected machines
- Blocks of IP addresses historically associated with malicious activity
- DNS names for botnet C&C servers
- IP addresses of hosts performing malicious actions
- URLs of websites hosting malicious files and performing drive-by downloads
- Addresses of misconfigured services that can be abused for DoS attacks

Despite their name implying that threats can be detected after they have taken effect, detection indicators can be also used for actively blocking threats, as a threat first needs to be detected in order to be blocked. *Indicators of compromise* are a subset of detection indicators that describe behaviors related to intrusion.

4.3.3 Advisories

Advisories include several sorts of information, which, while impossible to translate directly into threat detection processes, can provide information to analysts that can lead to defensive actions. Any piece of actionable information that is not an indicator is considered an advisory. The most prevalent types are the following:

- Vulnerability advisories provide information about vulnerabilities of software or hardware, as well as context, such as attacks spotted in the wild, sample exploits and mitigation techniques. Such information is handled in a process that involves identification of affected assets, risk analysis, development and deployment of protective measures.
- High-level alerts can be interpreted by analysts in conjunction with low level data to link observations of monitoring systems, such as information on abnormal activities, to specific events.
- TTPs of adversaries characterize behavior on a higher level. By observing particular sequences of exploit approaches, or specific timing patterns for the registration, parking, and activation of malicious domains adversaries can be identified and detected even by automated monitoring systems.

Information of this type is generally unstructured, which does not allow it to easily translate into actions. It is often in text format, which requires manual analysis to obtain relevant data. As high-level information requires structured data formats for exchange, formats such as STIX are developed to meet that demand. To make advisories actionable, it is important associate them with the correct context of the organization or environment to which they are relevant.

4.3.4 Strategic reports

Strategic reports are highly summarized reports that aim to provide an overview of particular situations. Such information can be used by analysts to influence and inform the decision making and planning process in the future. Due to their high-level of abstraction, strategic reports cannot be considered immediately actionable. They can, however, be employed in a complementary fashion, in order to provide context to other forms of data and provide information to update procedures and automated control systems. The high level of abstraction that characterizes strategic reports renders automated systems unable to translate reports into actions.

4.4 Processing Actionable Information

In the next section we will explore the individual steps of the pipeline that enables information to be collected, processed, stored, analyzed and distributed. While not applicable to all situations, this process is focused on recursive tasks that are performed in incident handling, monitoring and intelligence handling. The steps of this pipeline are relevant to all levels of information with some variations, except strategic reports, due to their abstract nature, which does not allow them to be actionable without human intervention. In real-world applications within CERTs, these pipelines do not exist in isolation, as there are many other pipelines operating in parallel to accommodate the needs of different information. Ideally, data from these pipelines can be processed in one centralized system, but technical limitations make such a solution unfeasible. In figure 4.2 below, a generalized information pipeline is shown.

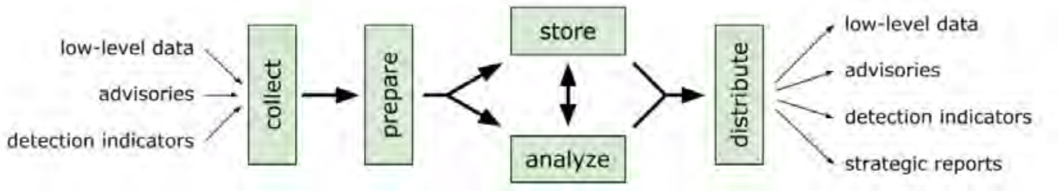


FIGURE 4.2: General information processing pipeline

4.4.1 Collection

An information processing pipeline needs a way to obtain information in order to process it and produce results. This logically leads to the observation that the first step of such a pipeline is a process of obtaining the initial data that will serve as inputs to the next stages. The collection process needs to be efficient and reliable, as it influences the quality of the data in the later stages of the pipeline.

Sources of information

One of the basic characteristics of incoming information is the source from which it was obtained. To clearly define a source we need to identify its vendor, method of delivery and format, Sources can either be internal, such as network monitoring systems, or external which can be other companies that provide their own data or any entity outside the CERT's constituency. External sources introduce an element of uncertainty about the accuracy of provided information, which is defined by the source's confidence and the level of trust towards the source. Additionally, data are sometimes processed and changed before being distributed, resulting in important information, such as the time of collection or the original source, being absent from the final product. When it comes to internal sources, such omissions can usually be avoided, as a result of the greater degree of control the CERT has over them. Internal sources are also easier to integrate and are available immediately, greatly improving timeliness. However, they vary in capability, depending on the type of organization, and are usually limited to gathering information from within the constituency and, thus, observe attacks in progress and not preemptively. Finally, what may be considered internal information to one entity, once shared, can become external to another entity.

The source's level of automation is an important factor to consider. It can vary between information produced by an entirely automated system to results of analysis performed by experts, with the middle ground being automatically generated information that has been verified by a specialist. Human analysis results in information that is more expensive, but lower in volume and more reliable, since false positives are eliminated. Typically, low-level information is the result of automated processes and advisories depend more on human actions.

Properties of data collection methods

Depending on the circumstances, the properties of data collection methods can be a defining factor of the value of the information and the way in which they are used. The three main characteristics of the collection methods are the following.

- *Recurrence* is used to describe the periodicity with which data are received. Information can be received in a singular event, such as a direct report of vulnerability, or as a regular feed of information, such as vulnerability advisories from large vendors. One time reports are considered harder to process and their handling cannot be easily automated.
- The *Consumption Model* depends on how the data source provides data. It can be either a push model, where the source sends data to the receiver, or a pull model, where the receiver can query for data. While the pull model provides more control to the receiver, allowing them to request data, it also introduces additional latency and does not scale adequately to large numbers of users. As a result, the push model is preferred for high-volume purposes, while its downside is the lack of control on the time, volume and format of the data that is sent.
- *Granularity* depends on the approach that is taken when sending data. In one hand, the individual contents of the data, such as packets, are sent separately, On the other hand, data can be sent in batches containing data grouped by topic based on indicators. The ease of implementation of batch processing is counteracted by the timeliness penalty it incurs.

There are multiple ways to collect data of each type, and each one provides some unique functionality at the cost of other elements. The large number of options of data collection methods can make it challenging to choose the correct application for each scenario. Nevertheless, choosing the correct method for the required use can be beneficial to achieving the expected result.

To alleviate the problem of choosing the correct source for each application, it is important to have an effective way of evaluating data sources, according to the quality and actionability of their data. This, in turn, will allow CERTs to effectively compare available options on a price-to-performance basis and ultimately decide on which one most effectively covers their needs, within the limitations of the resources they have. While evaluating a source can be a difficult process, that the CERTs must constantly perform on the sources they use, there are rated inventories of sources to help when choosing new sources with no previous experience with them.

4.4.2 Preparation

After data collection has been completed, the next step is to modify it, in order to make it actionable for the recipient, with the main focus being ingestibility.

Parsing

Since data can arrive in a wide variety of formats, which can range from standardized formats, that are compatible with existing tools, to proprietary or vendor specific formats, there is a need to isolate the significant contents form each one to perform analysis. To achieve that, specialized parsers are developed for each of these formats of raw input, aiming to extract the relevant information and normalize the output for further processing in the pipeline. Depending on the parser, data can either be fully normalized to represent specific types if information internally, or be preserved, allowing further parsing at a later time. Preserving the original data allows greater flexibility but it is a more difficult approach to implement. An intermediate solution is to perform normalization of the data, while also retaining the original input as a point of reference. This comes with additional computational and storage overheads, especially for high-volume data. Preserving the original format of data provides advantages even if they cannot be processed in real-time. These include the following.

- It allows a user to verify if the parsing was performed correctly, if any problems arise at a later point in time.
- When sharing data with external entities, providing the original form can increase the confidence into the received report

- If the normalized form changes then existing data can be parsed again, which should guarantee that no information is lost during conversion

Normalization

When trying to map various input formats to an internal data structure the two most prevalent problems are heterogeneity of data and a lack of common ontology. Heterogeneity stems from the large variety of different types of information that a CERT receives. Since there are multiple pipelines for different types of information, this problem is somewhat mitigated, however, designers need to balance the design of the unified internal representation between generality and specificity. Generality allows more information to be normalized and makes it more complex, resulting in higher costs when attempting further processing. Specificity makes further processing easier and cheaper at the cost of limiting the types of information that can be represented.

The lack of common ontology to form the foundation of a normalized form of information security is a problem the STIX attempts to address. A typical example where normalization of a data element is especially difficult is the case of identifiers of malicious software, since there is no common point of reference and vendors often use different names to describe the same threat. Since normalization is applied to groups of similar data, CERTs can consider a few normalized forms as standard if it fits the context of their organization. However, if an organization cannot invest in developing in-house data models, they usually have to rely on the models found in existing solutions.

Normalization difficulties leading to misinterpretation are more common in the case of one-time data exchanges, but established sources are not immune to this problem as well. Data formats may be completely overhauled, which requires the parsers to adapt in order to stay relevant. In cases of changes being applied to specific features, while the rest of the format stays backwards compatible, information can be interpreted incorrectly if the new features affect the content or the context.

Aggregation

Often, information may contain more details than what an organization needs, or contain repeated occurrences of the same event that provide no additional value. After parsing and normalizing it, this information can be aggregated in a single entry that is representative of its original form. Aggregation can be part of the information processing pipeline, or be implemented by sources, that provide already aggregated data, which is especially beneficial, if they provide high-volume, low-level data.

Enrichment

The previous steps mainly attempt to improve the ingestibility of information. Enrichment focuses on providing already existing information with additional context, in order to improve its completeness. This is achieved by correlating identifiers of the information with databases, which can be either internal or external. Additionally, if a CERT has access to otherwise inaccessible assets, it can use the additional information to make incoming data more enriched. Enrichment can also positively affect the accuracy of information by cleaning up the data and performing quality assurance. This can be achieved by verifying that data elements are well formed and the syntax is valid, eliminating artifacts that occur due to the collection method and provide no value, avoid easily identifiable false positives by using whitelists and ensure that reported values are within the expected parameters for the given institution.

Automation

The process of preparing the data is mostly automated, even for data that was collected by manual means. Even in the event of data that are provided only once, it is more efficient to utilize modified existing automated tools, rather than manually preparing it. Choosing the correct system for managing information can significantly impact the speed at which new information is integrated. New sources may be incompatible with the existing tools, which leads to infrastructure reworks or new infrastructure altogether. To avoid that, it is usually possible to modify incompatible sources to existing infrastructure, at the cost of partially losing information.

4.4.3 Storage

Storage of data is an important part of the information processing pipeline and plays an important role in how the next two steps of the pipeline will be designed. CERTs must make a choice between utilizing existing storage solutions or creating their own. It is not a clear choice to make, because existing solutions might need heavy modification to suit the needs of an institution and building a custom storage infrastructure requires significant effort and resources.

Retention time

Determining how long data should be retained in storage is an important design decision and can vary between only storing data for the time needed to analyze and distribute them and keeping them long-term for statistical analysis. Historical data can be useful in the context of operations and analysis and can become more relevant as time passes. However, the retention duration is limited by two significant factors. Legal regulations concerning personal data define a period after which the data are required to be deleted. Technical limitations limit the amount of data that can be stored and sometimes high data volume can adversely affect query performance.

Scale

Storage solutions should be designed to be able to scale according to the requirements of the user. The key areas in which a storage system must be scalable are the following.

- keep up with writing the incoming data without introducing additional delays, thus preserving timeliness
- store data for the chosen retention period
- provide read access to archived data with adequate performance

Depending on the requirements of storage volume the performance of the storage system can limit the performance of the processing pipeline. In the use case of CERTs, which tend to acquire more data over time, it is logical to choose a scalable solution to accommodate that growth in data volume. The volume of data increases for lower levels of information and is significantly smaller for higher ones as is shown in figure 4.1.

- Low-level data is usually received in large volumes and is usually not worth keeping once actionable information has been extracted from it, so it can be deleted. In case the original input is stored alongside the normalized format, the storage requirements increase substantially.
- Indicators can be a source of information that is large in volume, however, once aggregated, they become significantly more compact and can be stored more easily.
- Advisories and reports are impose insignificant storage loads compared to other types of information and can be easily stored.

Dataset Management

Due to working with multiple sets of data, efficient management of stored information is a priority for CERTs. Each source has its own requirements for management and without an appropriate solution to accommodate these needs, the complexity of such a system may become overwhelming, especially when storing information coming from one-time sources. To keep the contents of a repository under control, metadata are required, which provide additional information about the stored data and depends on the needs and infrastructure. The value of metadata increases when there are multiple sources at play, as it can provide information about the datasets that can result in a more streamlined management system.

Technologies

The storage backend technology that is chosen can significantly affect the performance and scalability of a storage system, as well as define its ability to integrate custom built software. The most commonly used technology for database management are Relational Database Management Systems (RDBMS), which rely on SQL to provide a standard way of communication across vendors and provide the ability to submit complex queries on structured data. The RDBMS is a mature and well studied technology, however in certain circumstances it cannot scale to a degree sufficient to meet the needs of certain applications that rely on semi-structured data. An alternative solution is a collection of technologies known as NoSQL, which do not rely on structured data models. The main advantage of NoSQL solutions is their ability to effectively scale to large volumes of data in the order of petabytes.

4.4.4 Analysis

After passing through the stages of collection, preparation and storage, further analysis can be performed on data before they get to the stage of distribution. Analysis is not an indispensable part of the pipeline, as information can be passed on to constituents directly. However, combining data from multiple sources can lead to additional information being discovered and provide better context and more relevance for the constituents.

The input of the analysis step is the collected and prepared information that was obtained by the previous steps of the pipeline, but is not yet considered actionable. In this step the aim is to provide additional context details that are not immediately apparent from the original data. Analysis has the potential to lead from a multitude of low-level indicators to actionable strategic reports. Additionally, by combining data from multiple sources and different levels, relationships that would otherwise go unnoticed can be observed.

Investigation

One of the typical activities of CERTs is investigative work, whether it is an investigation on an intrusion, a phishing campaign, or other threat relevant to the constituency. The main focus is analysis, but all the steps of the information processing pipeline can be included in an investigation. The result of an investigation usually is new, actionable information that can only be obtained in this manner, which justifies the effort and resources that are invested in investigations. In an investigation, typical activities include the following.

- Analysts select data with high degrees of completeness and accuracy, that is also suspected of containing relevant information
- Additional data are gathered when needed, either manually, or by the use of automated systems
- Data from multiple sources is collected and correlated
- Data is gathered from internal and external repositories to collect all the needed information, which requires infrastructure with adequate query capabilities

Investigative work revolves around correlation, which gives analysts a better understanding of the context, which leads to new observations on the already available information. Additionally, visualization techniques can improve the ability to correlate data from different sources, since visually representing the relationships between entities makes important patterns in the data easier to spot.

In the case a CERT receives a report of intrusion, either through its Intrusion Detection System, or a report by a user, an investigation is launched as a reaction. In this situation, the aim of the investigation is to minimize the damage caused by the current threat and outline the measures that need to be implemented to prevent such incidents in the future. The first step in that process is to assess the severity of the incident based on the affected machines or subnetwork. The potential threat must be verified by cross referencing the observed data with other, existing sources. After confirming a threat analysts need to assess the impact of the threat to the constituency, whether the events are isolated or part of a campaign, what information is missing and how to neutralize the threat, if possible. When a threat is active, time is critical and actionable information should be generated and put to use as soon as possible, which requires tools to enable analysts to reach that goal by minimizing the manual effort required to perform analysis. CERTs can also perform exploratory analysis to acquire a better insight of their environment, constituency and potential threats. This is an iterative process, which extracts information about potential threats in each iteration that need to be investigated, which provides the opportunity to prepare for future threats. Additionally, even if a detected anomaly in activity does not apply to the CERT's constituency, it may be relevant to the wider community.

Situational Awareness

Situational awareness, in the context of security, can be described as a CERT's understanding of the security state of its constituency and knowledge of potential threats to the constituency and their key attributes. A good level of situational awareness allows a CERT to be better prepared to react to incoming attacks or handle malware outbreaks both by preventative measures and a robust mitigation procedure. Early warning systems further increase the level of situational awareness, that is typically achieved through a continuous systematic process. Automated systems that aid in analysis are an essential part of this process, however they are not enough to provide situational awareness on their own, as human interpretation of the data they provide is required. Therefore, analysts still play an essential role in the process of situational awareness by providing an expert opinion on the actionable information provided by the automated system, in order to reach a conclusion. This information can then be used to mitigate future attacks and shared with other organizations. All types of information can be useful to improve situational awareness by performing the correct analysis on them.

Situational awareness can be divided into two categories, internal and external.

- Internal situational awareness describes the extent to which a CERT has a good understanding of the constituency it is tasked to defend. It is based on knowledge of assets and infrastructure within the organization, which adds context to any information received about a threat. Information about network infrastructure and an accurate way of profiling the activity that occurs within the network can significantly boost internal awareness, by allowing the detection of anomalies in comparison to typical behavior.
- External situational awareness concentrates on gaining knowledge about relevant threats and is usually more difficult to achieve than internal situational awareness. An effective way to achieve it is to observe the general tactics of malicious actors and the activity of malware to pinpoint the most widespread types of malware. Additionally, the infrastructure used to facilitate malicious campaigns can be identified. Despite the high value of this information, there are no automated tools that can perform the analysis required to obtain it.

Finally, visualization can be a useful tool in achieving situational awareness, as the ability of humans to identify patterns in visual data can speed up the process of spotting anomalies and new tools are being developed in order to make access to it easier.

Metrics

Quantitative information is central to data driven approaches that are used for performance evaluation and future planning. Metrics can be used to describe different areas of interest within the CERT and then compared with other CERTs to evaluate relative performance. These include:

- Number of machines infected by malware

- Number of attacks originating from the constituency
- Remediation rate –the proportion of IP addresses that are repeatedly reported in incident reports to the total number of attack sources

The results of such metrics can be used to determine the capability of a CERT against different types of attacks and detect trends in attack patterns, allowing a more targeted allocation of the CERT's resources, to counter these trends. This evaluation also aids in improving the CERT's situational awareness.

Meta-analysis and source evaluation

Since data is being collected from numerous sources, it is important to be able to determine the quality of information provided by each one, in order to reliably choose sources that can provide information that will be usable and actionable in the future. To achieve that, meta-analysis can be performed on received information to provide reports on accuracy. Finally, it is important that source evaluation is treated as an ongoing process, which can allow CERTs to identify unreliable sources and confirm the quality of trusted sources by using more objective criteria.

4.4.5 Distribution

The last step of the information processing pipeline is distribution. This is where the information that was obtained from the previous stages is applied and sent to external entities. In order to ensure that appropriate actions have been taken for the mitigation of incidents, the constituents need to be notified and act based on the provided instructions and information. Defining the method of delivering accurate and timely information requires significant effort and depends on the needs of the constituency. In cases that the CERT handles an incident itself, it still needs to distribute indicators to security systems. The last part of the distribution process is sharing information between trusted partners, to collectively analyze it. Depending on who receives the information, the characteristics that make information actionable may differ.

Internal Entities

The most usual scenario that a CERT faces is distributing information to the constituency it is responsible for, for internal consumption. In this case it is able to directly participate in incident mitigation, or closely cooperate with security related groups in the organization. In this situation, data can be easily distributed to the organization's network, with minor adjustments to the infrastructure, or the format of the data, to accommodate automated systems. The effectiveness of this relationship can be held back by the quality of information, as information of insufficient quality will not be utilized. Provided an adequate level of quality, CERTs can use information to detect threats and once a CERT is confident in the information it has at its disposal, it can deploy an automated system to improve response time.

External Entities

In cases where a CERT has no direct control over the constituency it is responsible for, it has to adopt a role of providing coordination to the efforts of threat mitigation. It is often the case, that CERTs have access to relevant information that is not directly related to the organization it is responsible for. This information should be shared with other organizations, to potentially act as an early warning, provided there are no legal restriction to doing so. This improves the effectiveness of efforts to mitigate threats, as cooperation provides better results that working in isolation. Another form of sending information to external entities, is the case of feedback sent to data providers in order to improve the quality of their data feeds.

An important consideration when sharing information is the ability of the recipient to receive and process the information in order to act upon it. There are three main categories, based on this ability.

- Low capability recipients are usually small organizations with no dedicated CERT and few automated systems in place. These may lack the capability to process advanced forms of information, such as real time feeds.
- Medium capability recipients are usually enterprises that have a basic security infrastructure and can handle security data with automated systems.
- High capability recipients have dedicated CERTs, cooperate with security vendors to provide infrastructure to store and process data and can handle real time feeds from various sources easily.

Based in the recipient's capability to receive data, CERTs can decide what data is worth being shared and what is the appropriate format to facilitate communication.

4.5 Summary

When setting up a system to respond to threats, actionable information is the most valuable resource a CERT can utilize. To obtain such information, a procedure must be established, that can enable the CERT to collect, prepare, store, analyze and finally distribute information. This process must be carefully designed to meet the demands of the CERT's constituency, given the technical capabilities it has at its disposal. If executed properly, it can yield information that is relevant to the constituency, timely, accurate, complete and easily ingestible by the organization's management systems. This information can, in turn, be used to mitigate the damage of attacks, or even prevent threats from entering the constituency altogether.

Bibliography

[1] Abuse.ch. *Welcome to AMaDa*. http://amada.abuse.ch.

[2] Abuse.ch. *Welcome to the SpyEye Tracker*. https://spyeyetracker.abuse.ch.

[3] Abuse.ch. *Welcome to the ZeuS Tracker*. https://zeustracker.abuse.ch/faq.php.

[4] ARN. *Top 10 most notorious cyber attacks in history*. https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/?fbclid=IwAR1Y6xHfc8UjCTS3sZhLveJWlSgGpu_Tm8gLNe_PBWfZ7cy904IfCNqPtTU.

[5] AusCERT. *Malicious URL Feed*. https://www.auscert.org.au/services/malicious-url-feed/.

[6] Kevin Almeroth Andreas Moser Engin Kirda Brett Stone-Gross Christopher Kruegel. *FIRE: FInding Rogue nEtworks*. https://sites.cs.ucsb.edu/~chris/research/doc/acsac09_fire.pdf.

[7] CERT.br. *Distributed Honeypots Project*. https://honeytarg.cert.br/honeypots/.

[8] Cert.br. *SpamPots Project*. https://honeytarg.cert.br/spampots/.

[9] Cisco. *Cisco Talos Intelligence Group*. https://www.talosintelligence.com.

[10] CyberDB. *Malwareblacklist.com*. https://www.cyberdb.co/vendor/malwareblacklistcom/.

[11] Team Cymru. *CSIRT ASSISTANCE PROGRAM*. http://www.team-cymru.com/CSIRT-AP.html.

[12] Team Cymru. *TC CONSOLE*. http://www.team-cymru.com/TC-Console.html.

[13] Our World in Data. *Growth of the Internet*. https://ourworldindata.org/internet.

[14] DavidJBianco. *The Pyramid of Pain*. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

[15] ENISA. *About ENISA*. https://www.enisa.europa.eu/about-enisa.

[16] ENISA. *Actionable information for security incident response*. https://www.enisa.europa.eu/publications/actionable-information-for-security.

[17] ENISA. *Proactive detection of network security incidents*. https://www.enisa.europa.eu/publications/proactive-detection-report.

[18] EUROPA. *The Directive on security of network and information systems (NIS Directive)*. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[19] Shadowserver Foundation. *Shadowserver*. https://www.shadowserver.org.

[20] EU GDPR.org. *GDPR Key Changes*. https://eugdpr.org/the-regulation/.

[21] Google. *How we identify unsafe websites*. https://transparencyreport.google.com/safe-browsing/overview?hl=en.

[22] zone h. *zone-h*. http://www.zone-h.org/disclaimer.

[23] John Hubbard. *Post-Exploitation Hunting with ATT&CK & Elastic*. https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1533071345.pdf.

[24] SRI International. *Malware Threat Center*. https://www.sri.com/newsroom/press-releases/sri-international-launches-new-malware-threat-center-tools-and-daily-updat-0.

[25] ISC. *ISC History and Overview*. https://www.dshield.org/about.html.

[26] JavaTPoint. *History of Cyber Security*. https://www.javatpoint.com/history-of-cyber-security.

[27] Christopher Kruegel Marco Balduzzi Leyla Bilge Engin Kirda. *EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis*. https://sites.cs.ucsb.edu/~chris/research/doc/ndss11_exposure.pdf.

[28] Malware Domain List. *Malware Domain List*. https://www.malwaredomainlist.com.

[29] US Cybersecurity Magazine. *A Brief and Incomplete History of Cybersecurity*. https://www.uscybersecurity.net/history/.

[30] Malc0de. *Malc0de database*. http://malc0de.com/database/.

[31] Microsoft. *Smart Network Data Service*. https://sendersupport.olc.protection.outlook.com/snds/.

[32] MITRE. *MITRE ATT&CK Navigator*. https://mitre-attack.github.io/attack-navigator/enterprise/.

[33] NETSCOUT. *ATLAS Intelligence Feed (AIF)*. https://www.netscout.com/product/atlas-intelligence-feed-aif.

[34] Malware Patrol. *Malware Patrol*. https://www.malwarepatrol.net.

[35] Cert Polska. *ARAKIS*. https://www.cert.pl/en/projekty/arakis-2/.

[36] Cert Polska. *Honeyspider Network 2.0*. https://www.cert.pl/en/news/single/honeyspider-network-2-0/.

[37] The Wombat Project. *WORLDWIDE OBSERVATORY OF MALICIOUS BEHAVIORS AND ATTACK THREATS*. http://www.wombat-project.eu/WP3/FP7-ICT-216026-Wombat_WP3_D13_V01-Sensor-deployment.pdf.

[38] RiskAnalytics. *DNS-BH – Malware Domain Blocklist by RiskAnalytics*. https://www.malwaredomains.com/?page_id=2.

[39] spamcop.net. *spamcop.net*. https://www.spamcop.net.

[40] Spamhaus. *Composite Blocking List*. https://www.abuseat.org.

[41] Spamhaus. *Spamhaus DNSBL Datafeed*. https://www.spamhaus.org/datafeed/.

[42] The MalwareURL Team. *The MalwareURL Team*. https://www.malwareurl.com.

[43] Unspam Technologies. *Project Honeypot*. https://www.projecthoneypot.org/about_us.php.