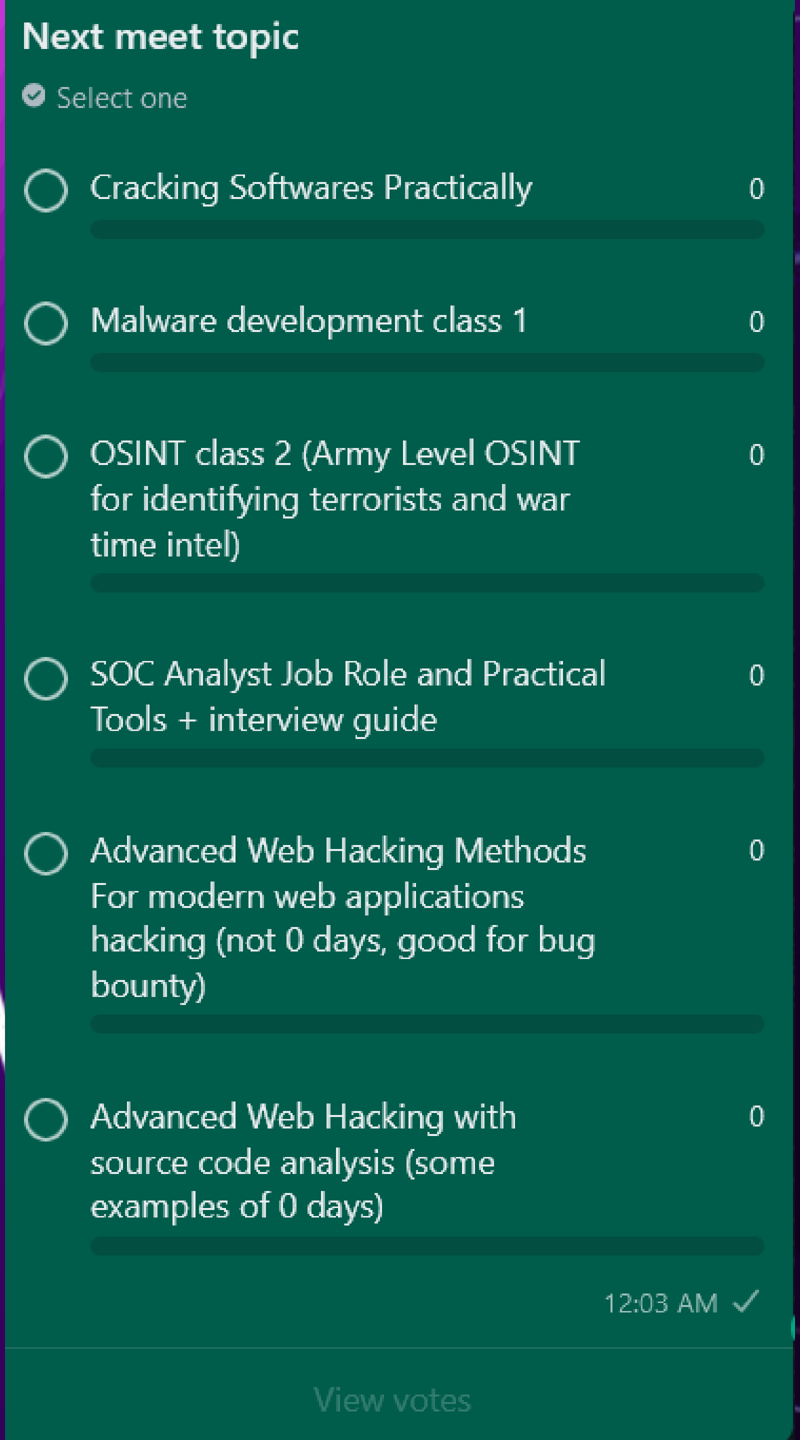


Next meet topic

Select one

○ Cracking Softwares Practically 0

○ Malware development class 1 0

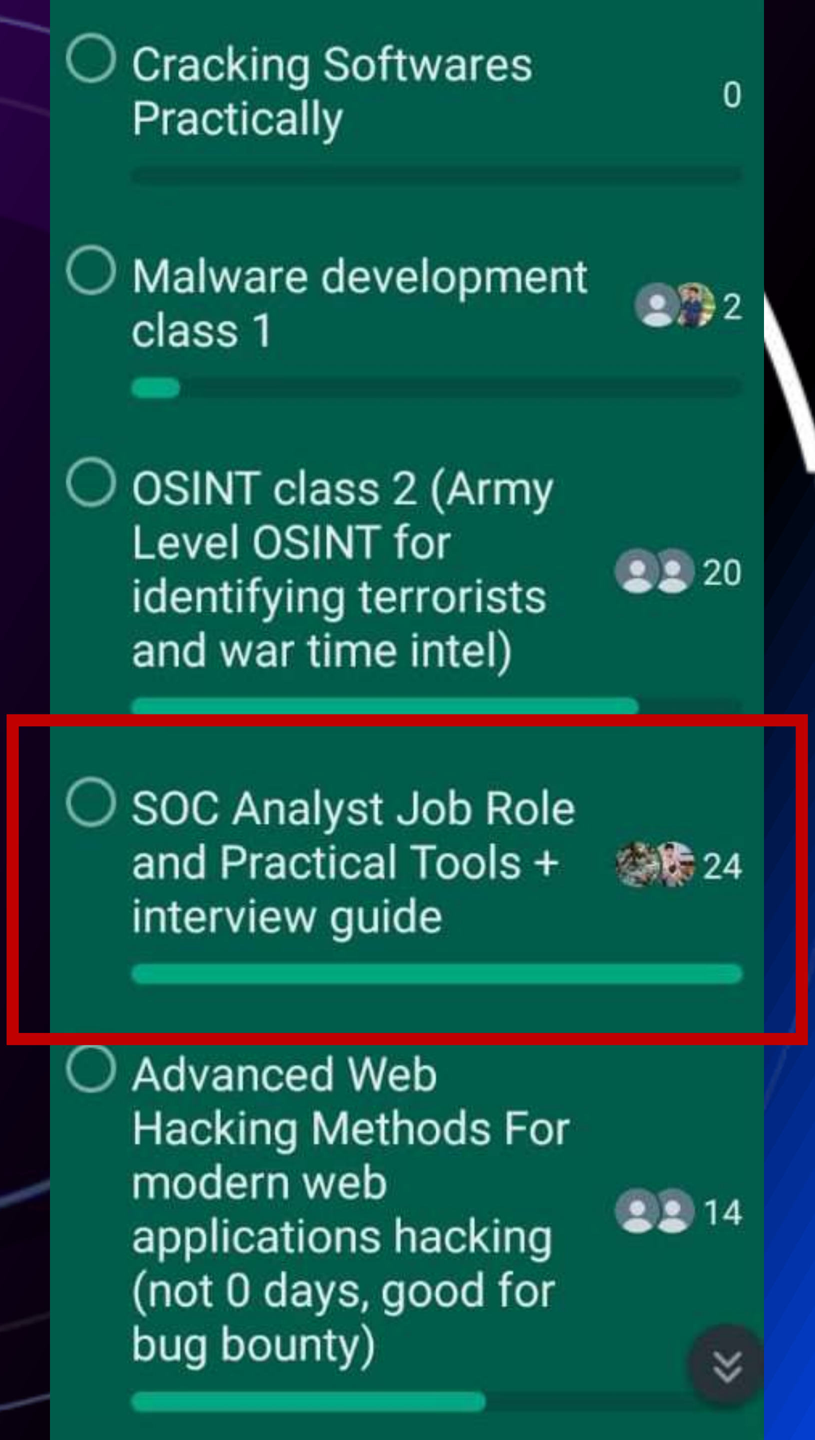
○ OSINT class 2 (Army Level OSINT for identifying terrorists and war time intel) 0

○ SOC Analyst Job Role and Practical Tools + interview guide 0

○ Advanced Web Hacking Methods For modern web applications hacking (not 0 days, good for bug bounty) 0

○ Advanced Web Hacking with source code analysis (some examples of 0 days) 0

12:03 AM ✓



○ Cracking Softwares Practically 0

○ Malware development class 1 2

○ OSINT class 2 (Army Level OSINT for identifying terrorists and war time intel) 20

○ SOC Analyst Job Role and Practical Tools + interview guide 24

○ Advanced Web Hacking Methods For modern web applications hacking (not 0 days, good for bug bounty) 14

SOC ANALYST

SHELL SQUAD

AGENDA

Cyber Kill Chain

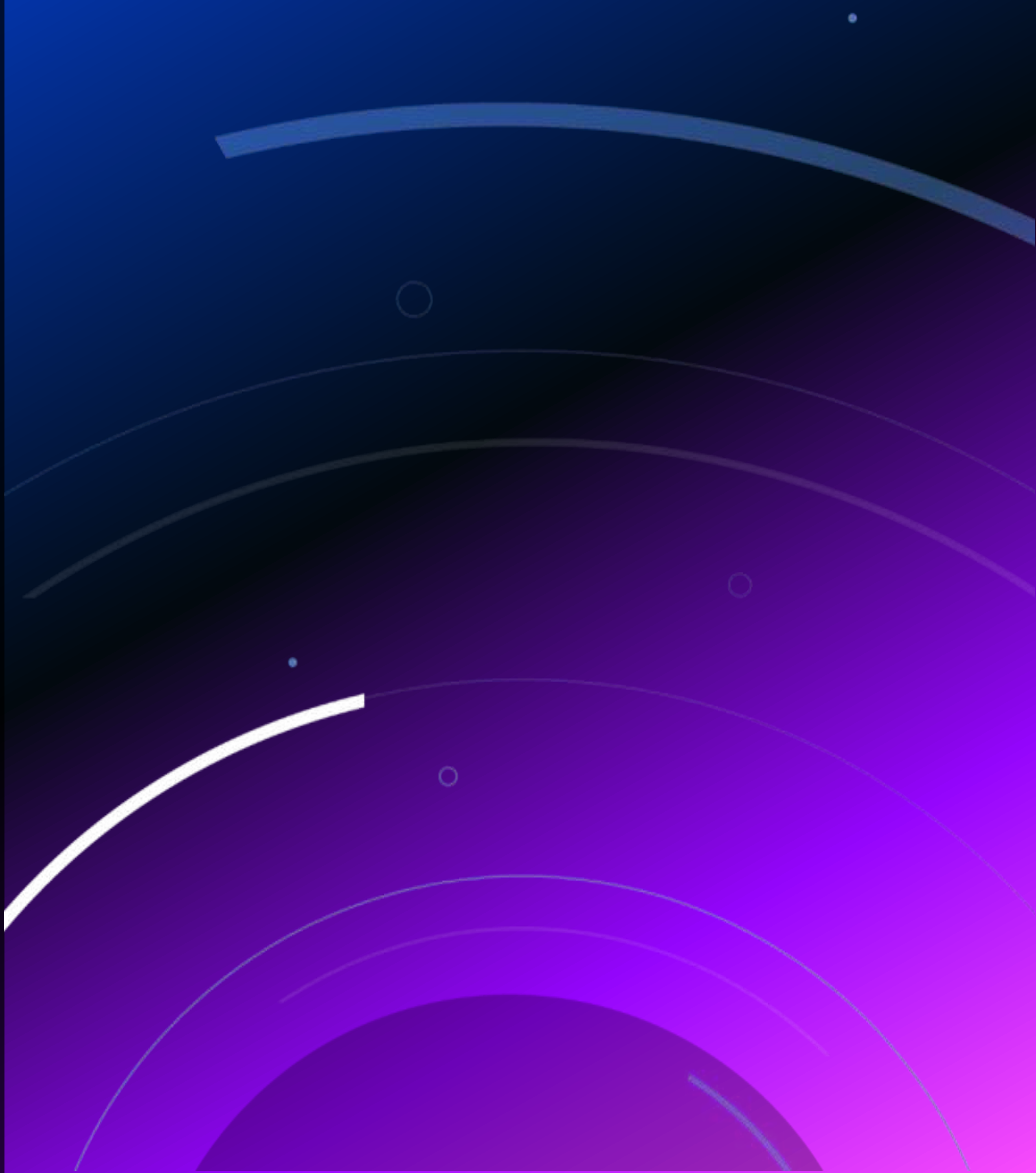
Incident Handling Process

SIEM Introduction

MITRE ATT&CK

SOC And It’s Role

Email Analysis Practical

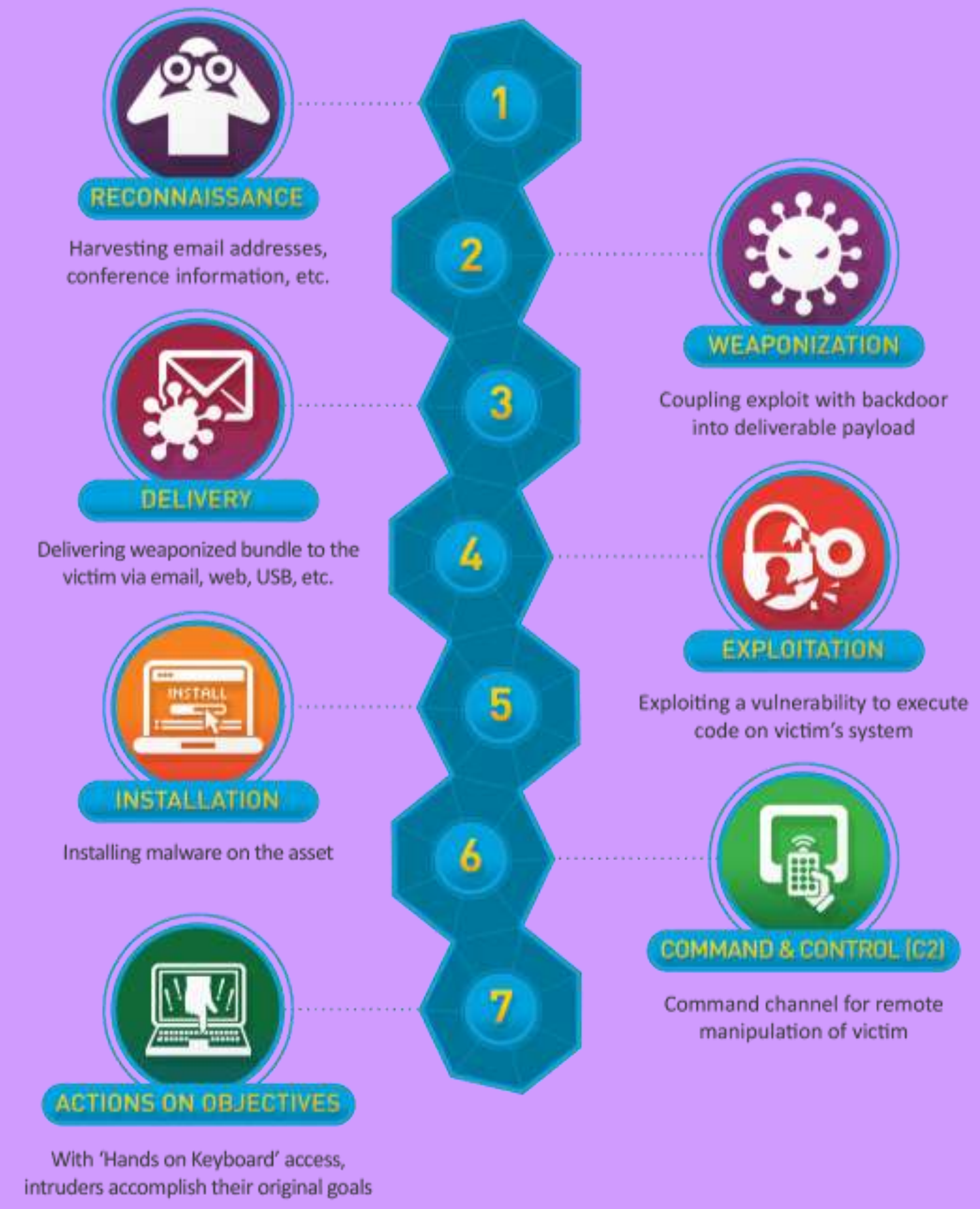


CHAPTER 1

THE CYBER KILL CHAIN

CYBER KILL CHAIN

OVERVIEW



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

MALWARE BASIC TERMS

WHAT IS A DROPPER?
WHAT IS A BACKDOOR?
WHAT IS A ROOTKIT?

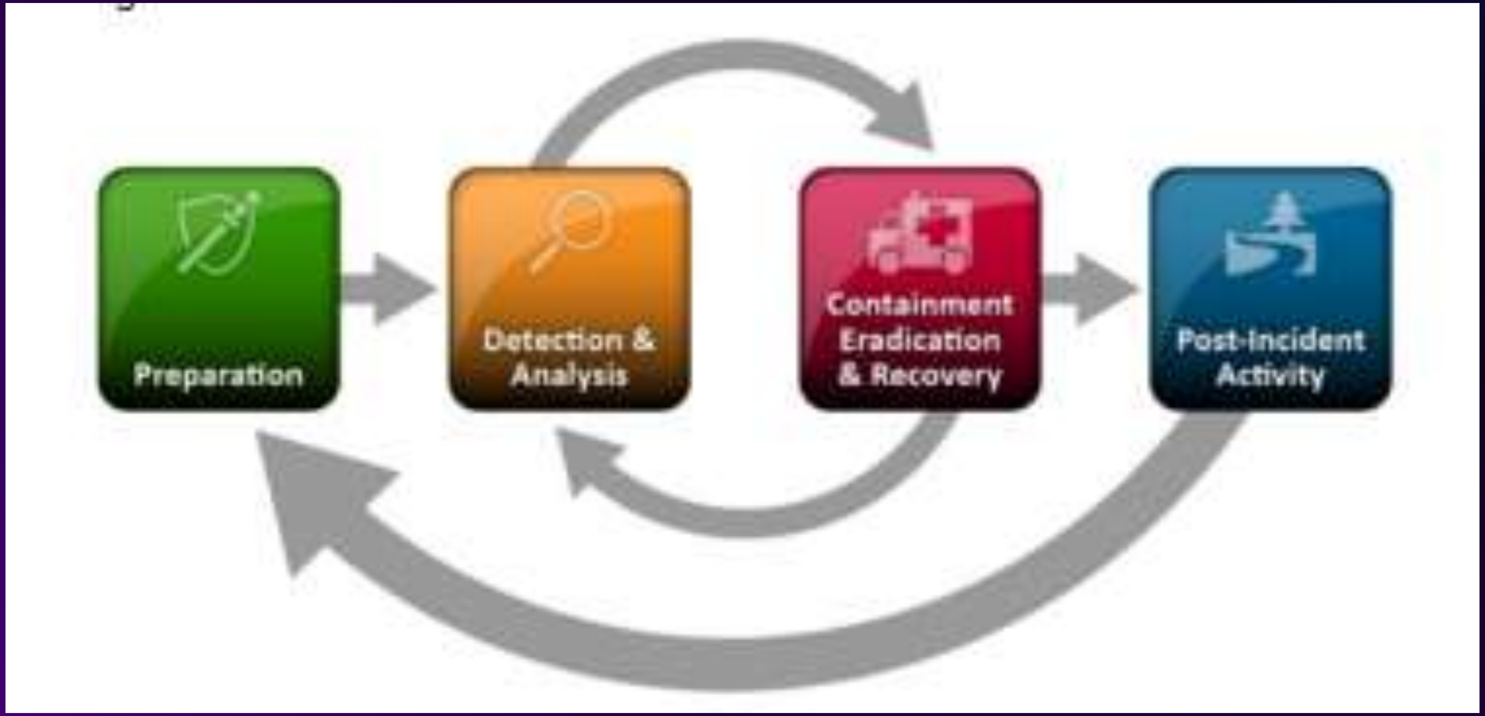
CHAPTER 2

INCIDENT HANDLING PROCESS

INCIDENT HANDLING DEFINITION & SCOPE

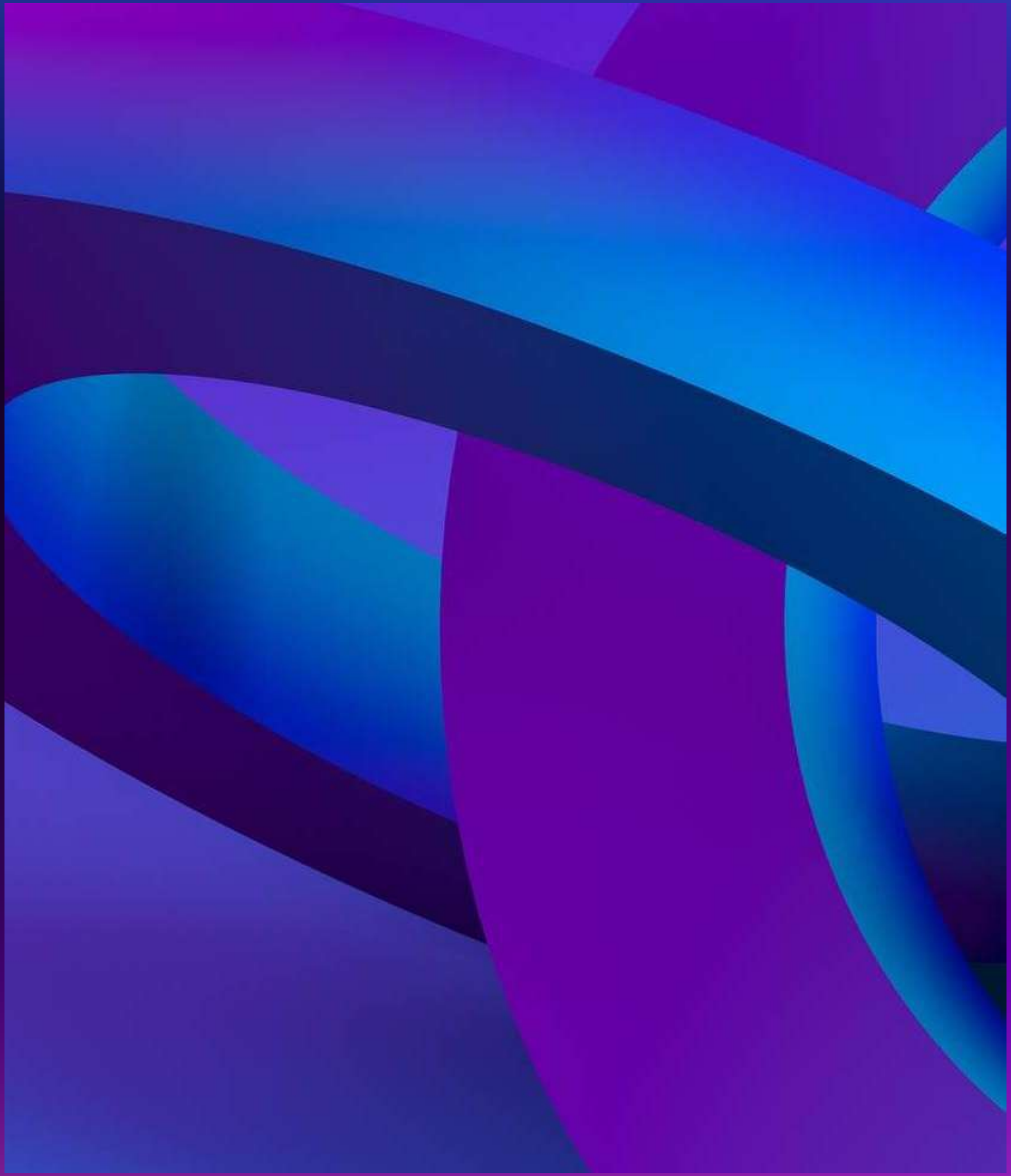
- What is an event?
- What is an Incident?
- The incident handling team is led by an incident manager. This role is often assigned to a SOC manager, CISO/CIO, or third-party (trusted) vendor, and this person usually has the ability to direct other business units as well.
- The incident manager is the single point of communication who tracks the activities taken during the investigation and their status of completion.

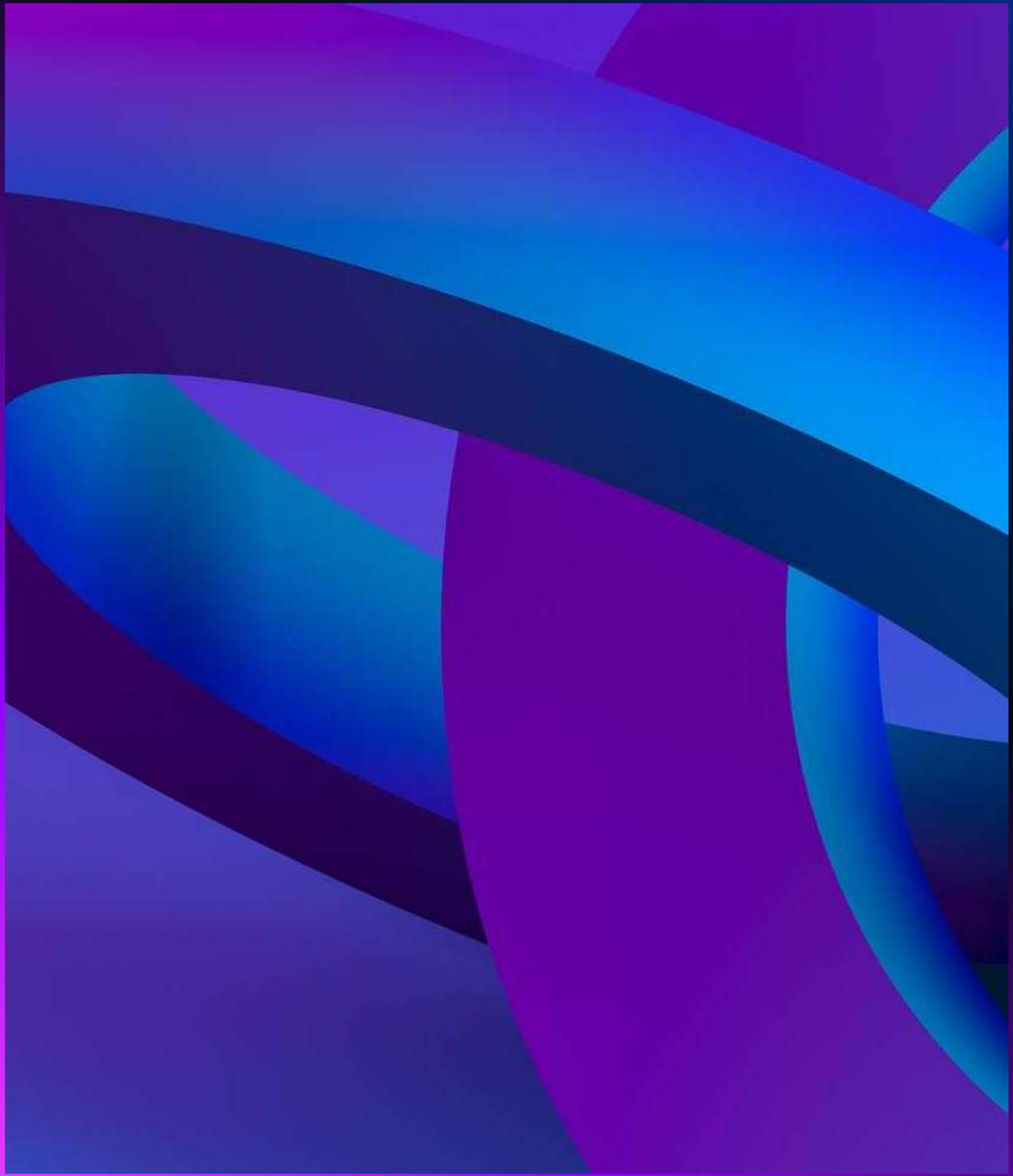
INCIDENT HANDLING PROCESS



INCIDENT HANDLING PROCESS

1. PREPARATION





WHAT TO DO?

In the preparation stage, we have two separate objectives. The first one is the establishment of incident handling capability within the organization. The second is the ability to protect against and prevent IT security incidents by implementing appropriate protective measures. Such measures include endpoint and server hardening, active directory tiering, multi-factor authentication, privileged access management, and so on and so forth. While protecting against incidents is not the responsibility of the incident handling team, this activity is fundamental to the overall success of that team.

PREPARATION PREREQUISITES

During the preparation, we need to ensure that we have:

- Skilled incident handling team members (incident handling team members can be outsourced, but a basic capability and understanding of incident handling are necessary in-house regardless)
- Trained workforce (as much as possible, through security awareness activities or other means of training)
- Clear policies and documentation
- Tools (software and hardware)

CLEAR POLICIES & DOCUMENTATION

Some of the written policies and documentation should contain an up-to-date version of the following information:

- Contact information and roles of the incident handling team members
- Contact information for the legal and compliance department, management team, IT support, communications and media relations department, law enforcement, internet service providers, facility management, and external incident response team
- Incident response policy, plan, and procedures
- Incident information sharing policy and procedures
- Baselines of systems and networks, out of a golden image and a clean state environment
- Network diagrams
- Organization-wide asset management database
- User accounts with excessive privileges that can be used on-demand by the team when necessary (also to business-critical systems, which are handled with the skills needed to administer that specific system). These user accounts are normally enabled when an incident is confirmed during the initial investigation and then disabled once it is over. A mandatory password reset is also performed when disabling the users.
- Ability to acquire hardware, software, or an external resource without a complete procurement process (urgent purchase of up to a certain amount). The last thing you need during an incident is to wait for weeks for the approval of a $500 tool.
- Forensic/Investigative cheat sheets

DMARC

DMARC is an email protection against phishing built on top of the already existing SPF and DKIM. The idea behind DMARC is to reject emails that 'pretend' to originate from your organization. Therefore, if an adversary is spoofing an email pretending to be an employee asking for an invoice to be paid, the system will reject the email before it reaches the intended recipient. DMARC is easy and inexpensive to implement, however, I cannot stress enough that thorough testing is mandatory; otherwise (and this is oftentimes the case), you risk blocking legitimate emails with no ability to recover them.

With email filtering rules, you may be able to take DMARC to the 'next' level and apply additional protection against emails failing DMARC from domains you do not own. This is possible because some email systems will perform a DMARC check and include a header stating whether DMARC passed or failed in the message headers. While this can be incredibly powerful to detect phishing emails from any domain, it requires extensive testing before it can be introduced in a production environment. High false-positives here are emails that are sent 'on behalf of' via some email sending service, since they tend to fail DMARC due to domain mismatch.

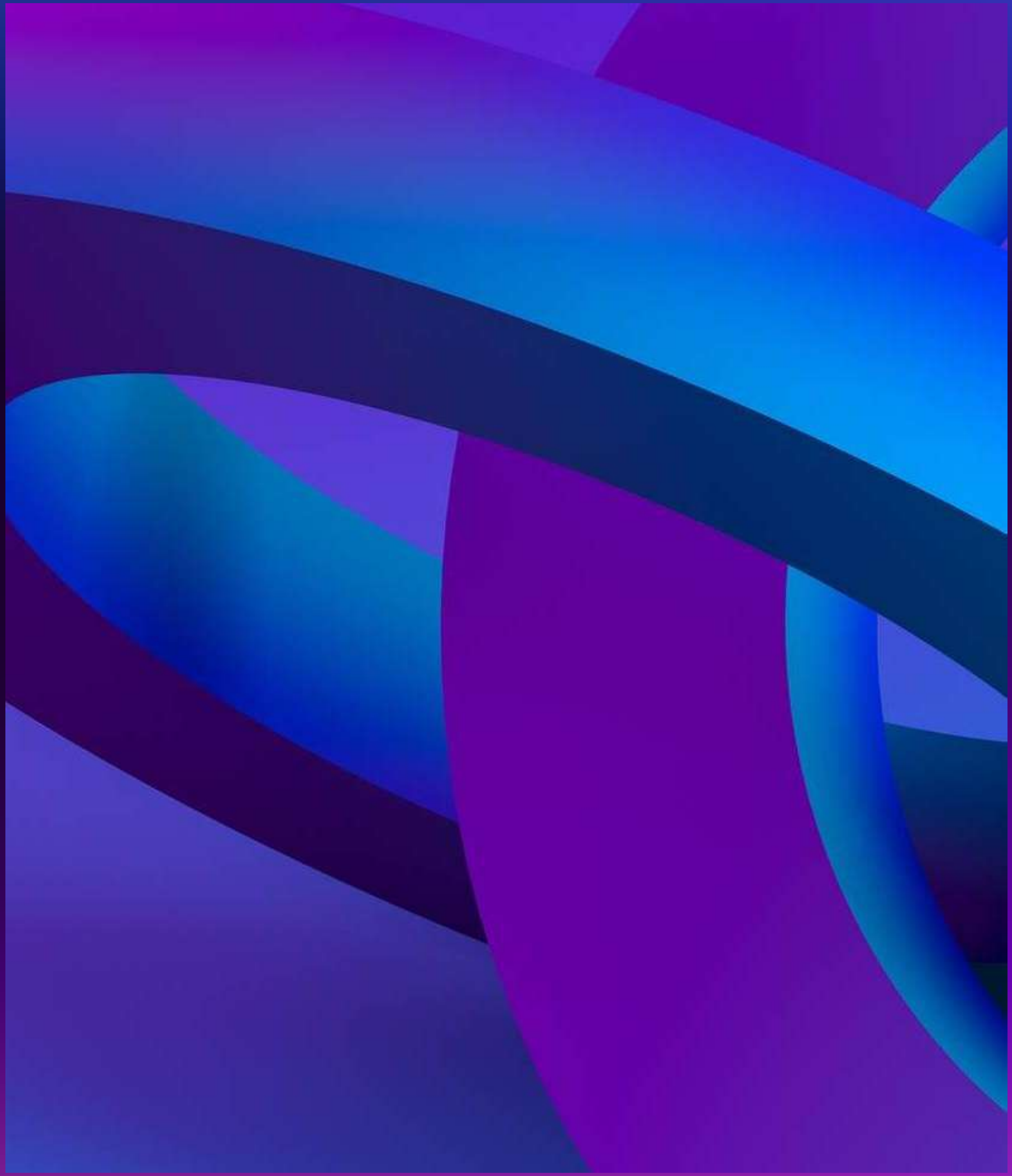
ENDPOINT HARDENING (& EDR)

Endpoint devices (workstations, laptops, etc.) are the entry points for most of the attacks that we are facing on a daily basis. If we consider the fact that most threats will originate from the internet and will target users who are browsing websites, opening attachments, or running malicious executables, a percentage of this activity will occur from their corporate endpoints. There are a few widely recognized endpoint hardening standards by now, with CIS and Microsoft baselines being the most popular, and these should really be the building blocks for your organization's hardening baselines. Some highly important actions (that actually work) to note and do something about are:

- Disable LLMNR/NetBIOS
- Implement LAPS and remove administrative privileges from regular users
- Disable or configure PowerShell in "ConstrainedLanguage" mode
- Enable Attack Surface Reduction (ASR) rules if using Microsoft Defender
- Implement whitelisting. We know this is nearly impossible to implement. Consider at least blocking execution from user-writable folders (Downloads, Desktop, AppData, etc.). These are the locations where exploits and malicious payloads will initially find themselves. Remember to also block script types such as .hta, .vbs, .cmd, .bat, .js, and similar. Please pay attention to LOLBin files while implementing whitelisting. Do not overlook them; they are really used in the wild as initial access to bypass whitelisting.
- Utilize host-based firewalls. As a bare minimum, block workstation-to-workstation communication and block outbound traffic to LOLBins
- Deploy an EDR product. At this point in time, AMSI provides great visibility into obfuscated scripts for antimalware products to inspect the content before it gets executed. It is highly recommended that you only choose products that integrate with AMSI.

INCIDENT HANDLING PROCESS

2. DETECTION & ANALYSIS



DETECTION & ANALYSIS STAGE

The detection & analysis phase involves all aspects of detecting an incident, such as utilizing sensors, logs, and trained personnel. It also includes information and knowledge sharing, as well as utilizing context-based threat intelligence. Segmentation of the architecture and having a clear understanding of and visibility within the network are also important factors.

Threats are introduced to the organization via an infinite amount of attack vectors, and their detection can come from sources such as:

- An employee that notices abnormal behavior
- An alert from one of our tools (EDR, IDS, Firewall, SIEM, etc.)
- Threat hunting activities
- A third-party notification informing us that they discovered signs of our organization being compromised.

INITIAL INVESTIGATION

- Date/Time when the incident was reported. Additionally, who detected the incident and/or who reported it?
- How was the incident detected?
- What was the incident? Phishing? System unavailability? etc.
- Assemble a list of impacted systems (if relevant)
- Document who has accessed the impacted systems and what actions have been taken. Make a note of whether this is an ongoing incident or the suspicious activity has been stopped
- Physical location, operating systems, IP addresses and hostnames, system owner, system's purpose, current state of the system
- (If malware is involved) List of IP addresses, time and date of detection, type of malware, systems impacted, export of malicious files with forensic information on them (such as hashes, copies of the files, etc.)

INCIDENT SEVERITY & EXTENT QUESTIONS

- What is the exploitation impact?
- What are the exploitation requirements?
- Can any business-critical systems be affected by the incident?
- Are there any suggested remediation steps?
- How many systems have been impacted?
- Is the exploit being used in the wild?
- Does the exploit have any worm-like capabilities?

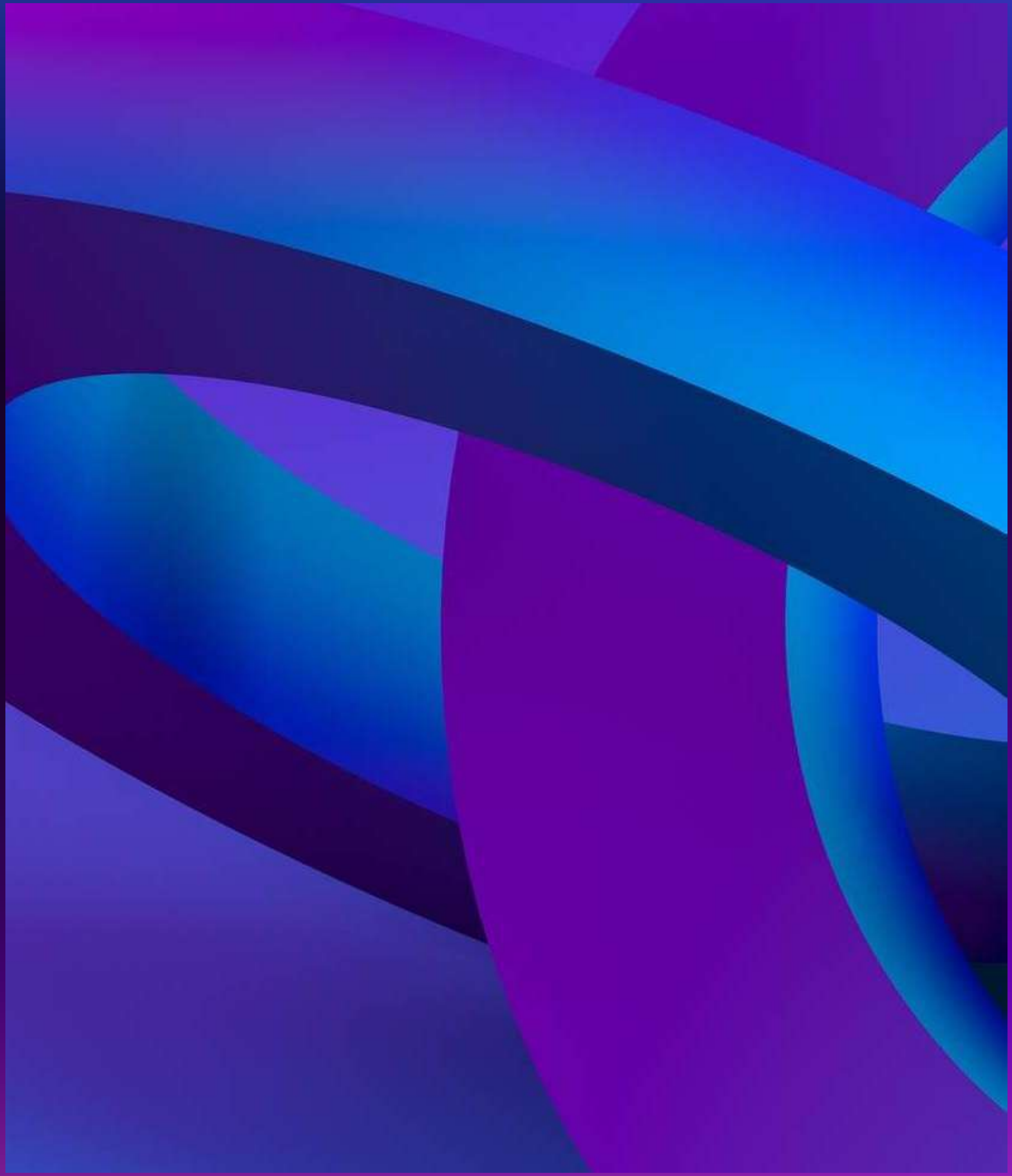
THE INVESTIGATION

The investigation starts based on the initially gathered (and limited) information that contain what we know about the incident so far. With this initial data, we will begin a 3-step cyclic process that will iterate over and over again as the investigation evolves. This process includes:

- Creation and usage of indicators of compromise (IOC)
- Identification of new leads and impacted systems
- Data collection and analysis from the new leads and impacted systems

INCIDENT HANDLING PROCESS

3.CONTAINMENT, ERADICATION, & RECOVERY



CONTAINMENT

In this stage, we take action to prevent the spread of the incident. We divide the actions into short-term containment and long-term containment . It is important that containment actions are coordinated and executed across all systems simultaneously. Otherwise, we risk notifying attackers that we are after them, in which case they might change their techniques and tools in order to persist in the environment.

In short-term containment, the actions taken leave a minimal footprint on the systems on which they occur. Some of these actions can include, placing a system in a separate/isolated VLAN, pulling the network cable out of the system(s) or modifying the attacker's C2 DNS name to a system under our control or to a non-existing one. The actions here contain the damage and provide time to develop a more concrete remediation strategy. Additionally, since we keep the systems unaltered (as much as possible), we have the opportunity to take forensic images and preserve evidence if this wasn't already done during the investigation (this is also known as the backup substage of the containment stage). If a short-term containment action requires shutting down a system, we have to ensure that this is communicated to the business and appropriate permissions are granted.

In long-term containment actions, we focus on persistent actions and changes. These can include changing user passwords, applying firewall rules, inserting a host intrusion detection system, applying a system patch, and shutting down systems. While doing these activities, we should keep the business and the relevant stakeholders updated. Bear in mind that just because a system is now patched does not mean that the incident is over. Eradication, recovery, and post-incident activities are still pending.

ERADICATION

Once the incident is contained, eradication is necessary to eliminate both the root cause of the incident and what is left of it to ensure that the adversary is out of the systems and network. Some of the activities in this stage include removing the detected malware from systems, rebuilding some systems, and restoring others from backup. During the eradication stage, we may extend the previously performed containment activities by applying additional patches, which were not immediately required. Additional system-hardening activities are often performed during the eradication stage (not only on the impacted system but across the network in some cases).

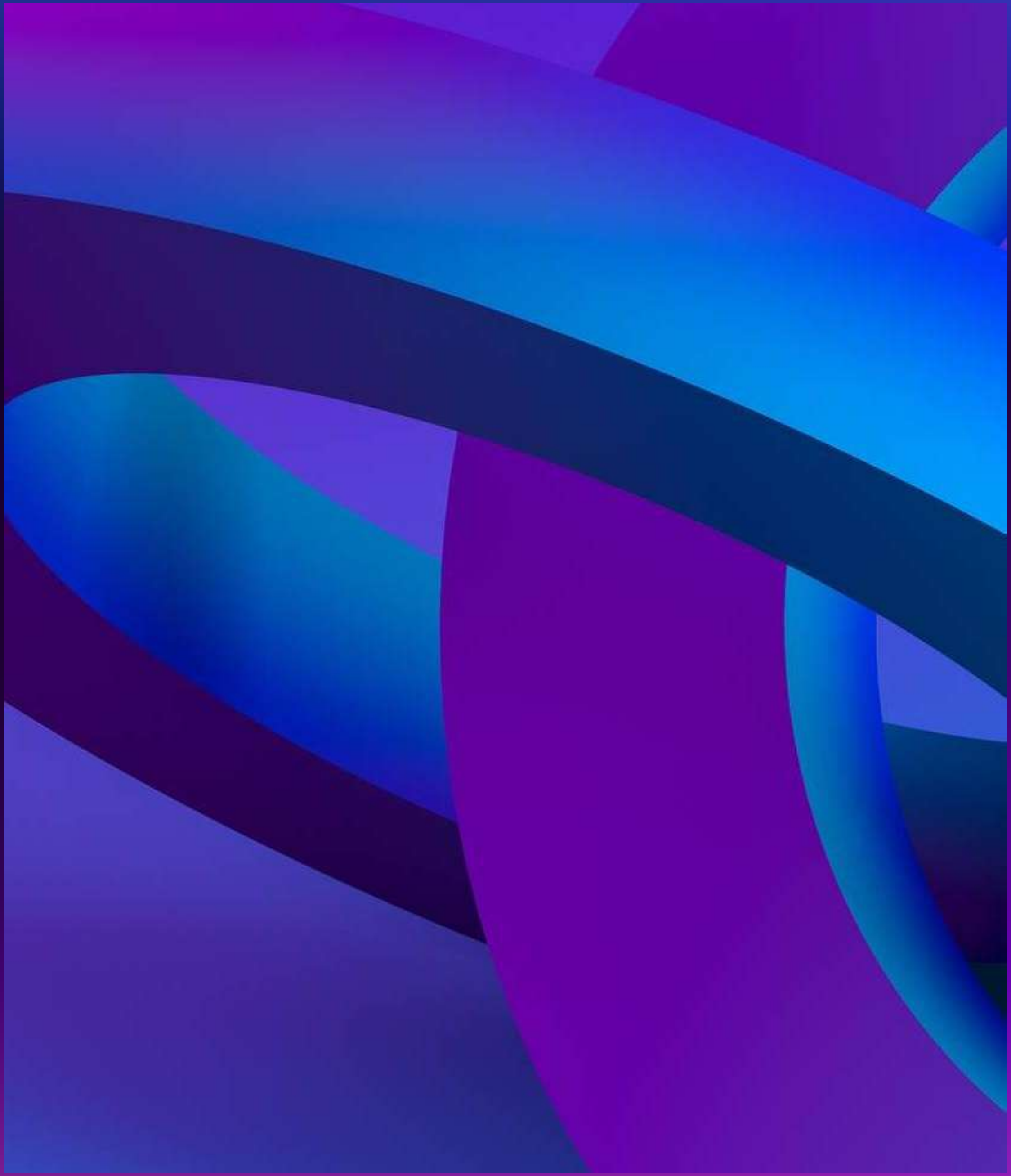
RECOVERY

In the recovery stage, we bring systems back to normal operation. Of course, the business needs to verify that a system is in fact working as expected and that it contains all the necessary data. When everything is verified, these systems are brought into the production environment. All restored systems will be subject to heavy logging and monitoring after an incident, as compromised systems tend to be targets again if the adversary regains access to the environment in a short period of time. Typical suspicious events to monitor for are:

- Unusual logons (e.g. user or service accounts that have never logged in there before)
- Unusual processes
- Changes to the registry in locations that are usually modified by malware

INCIDENT HANDLING PROCESS

4. POST-INCIDENT ACTIVITY



REPORTING

The final report is a crucial part of the entire process. A complete report will contain answers to questions such as:

- What happened and when?
- Performance of the team dealing with the incident in regard to plans, playbooks, policies, and procedures
- Did the business provide the necessary information and respond promptly to aid in handling the incident in an efficient manner? What can be improved?
- What actions have been implemented to contain and eradicate the incident?
- What preventive measures should be put in place to prevent similar incidents in the future?
- What tools and resources are needed to detect and analyze similar incidents in the future?

CHAPTER 3

SIEM INTRODUCTION

SIEM HISTORY

The acronym "SIEM" emerged from the collaboration of two Gartner analysts who suggested a novel security information framework that integrated two preceding technologies: Security Information Management (SIM) and Security Event Management (SEM). This proposition appeared in a 2005 Gartner paper titled "Enhance IT Security through Vulnerability Management."

First-generation SIM technology was developed upon conventional log collection management systems, allowing for extended storage, examination, and reporting of log data while incorporating logs with threat intelligence. Conversely, the second-generation SEM technology tackled security events by delivering consolidation, correlation, and notification of events from a range of security apparatuses, such as antivirus software, firewalls, Intrusion Detection Systems (IDS), in addition to events disclosed directly by authentication, SNMP traps, servers, and databases.

In the years that followed, vendors amalgamated the capabilities of SIM and SEM to devise the SIEM, leading to a fresh definition as per Gartner's investigation. This nascent technology gained widespread acceptance as it offered a comprehensive methodology for detecting and managing threats, including the ability to amass, preserve, and scrutinize logs and security events from various origins.

SIEM BUSINESS REQUIREMENTS & USE CASES

LOG AGGREGATION & NORMALIZATION

THREAT ALERTING

CONTEXTUALIZATION & RESPONSE

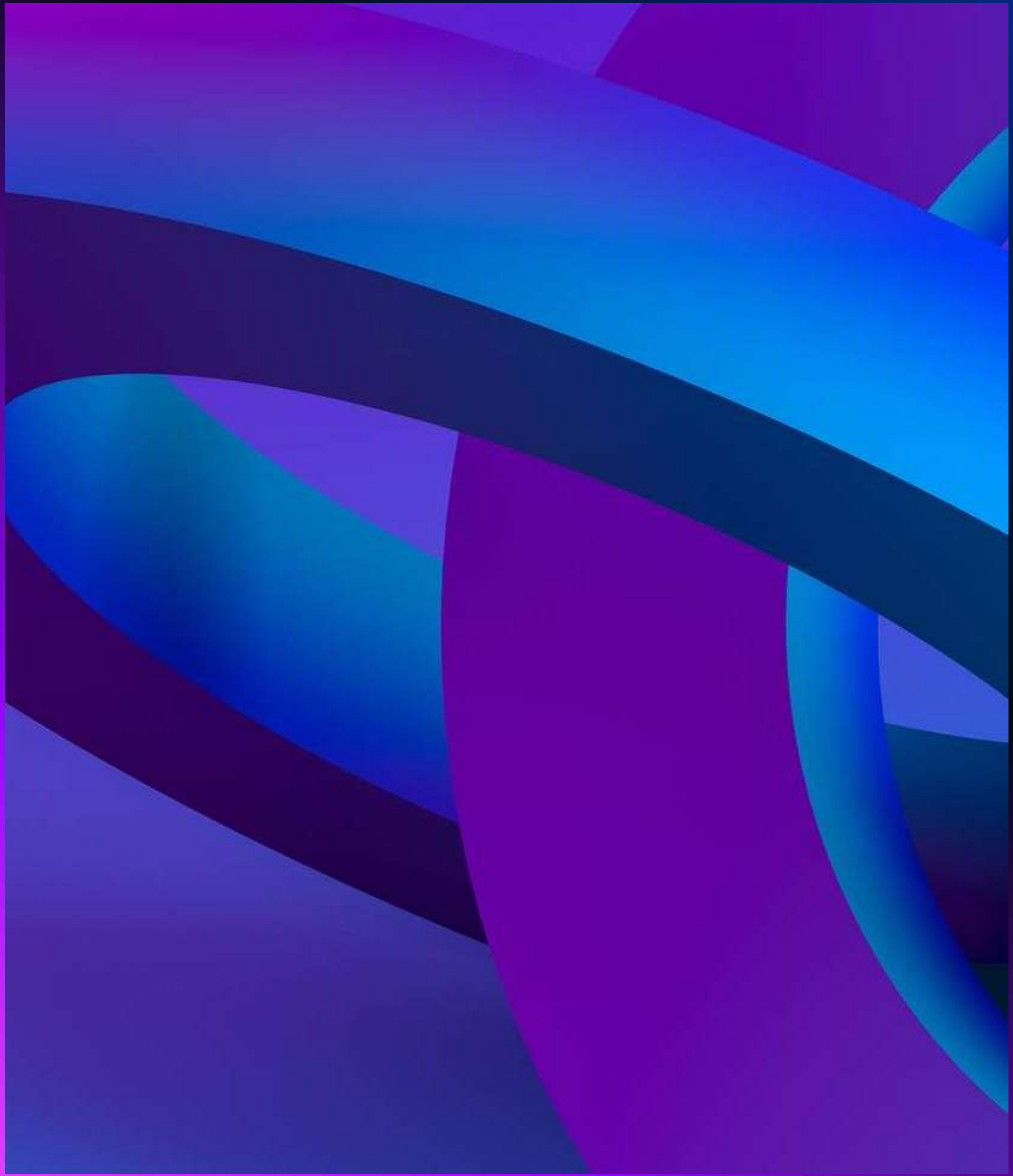
COMPLIANCE

DATA FLOWS WITHIN A SIEM

1. SIEM solutions ingest logs from various data sources. Each SIEM tool possesses unique capabilities for collecting logs from different sources. This process is known as data ingestion or data collection.

2. The gathered data is processed and normalized to be understood by the SIEM correlation engine. The raw data must be written or read in a format that can be comprehended by the SIEM and converted into a common format from various types of datasets. This process is called data normalization and data aggregation.

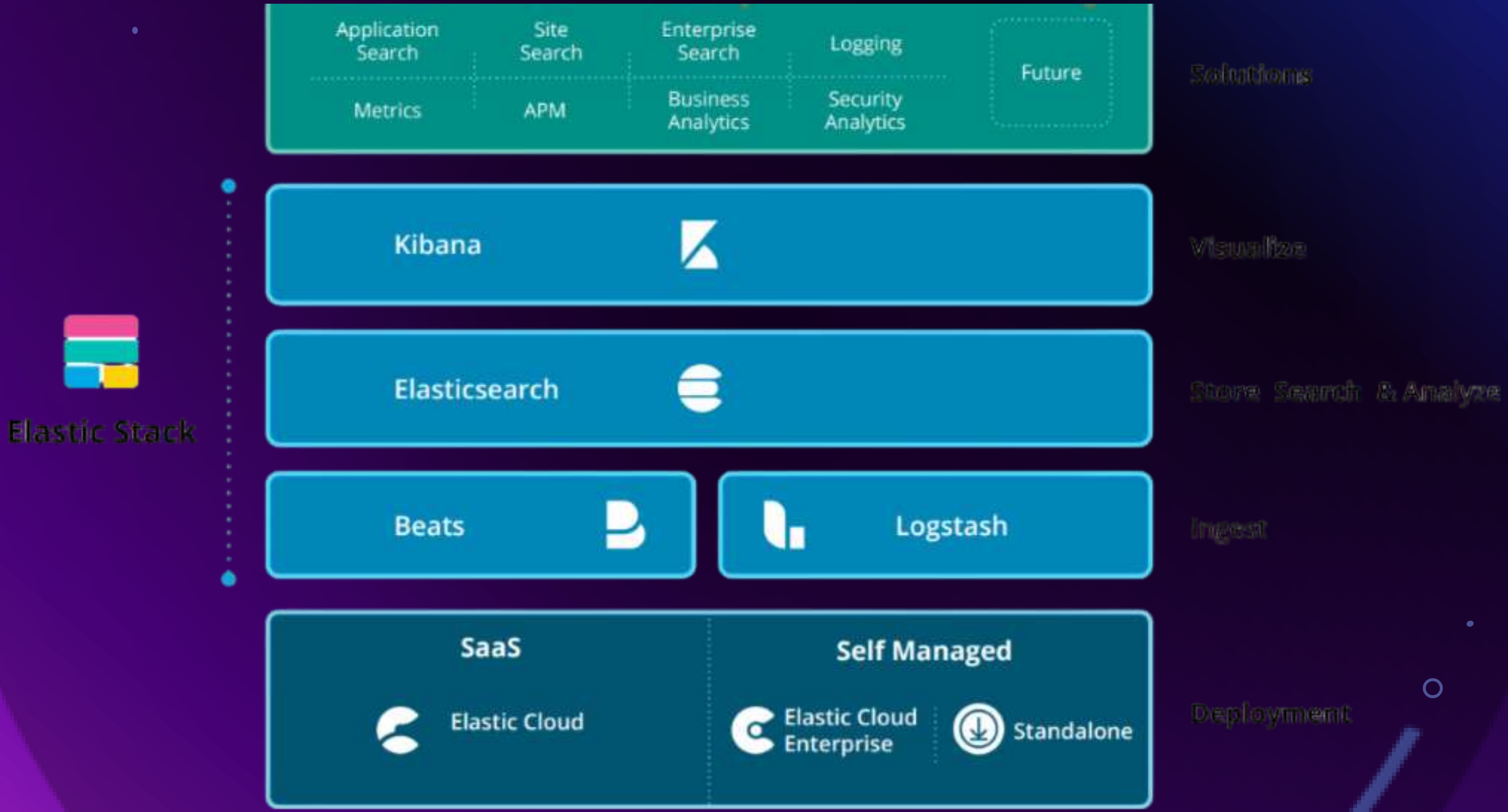
3. Finally, the most crucial part of SIEM, where SOC teams utilize the normalized data collected by the SIEM to create various detection rules, dashboards, visualizations, alerts, and incidents. This enables the SOC team to identify potential security risks and respond swiftly to security incidents.



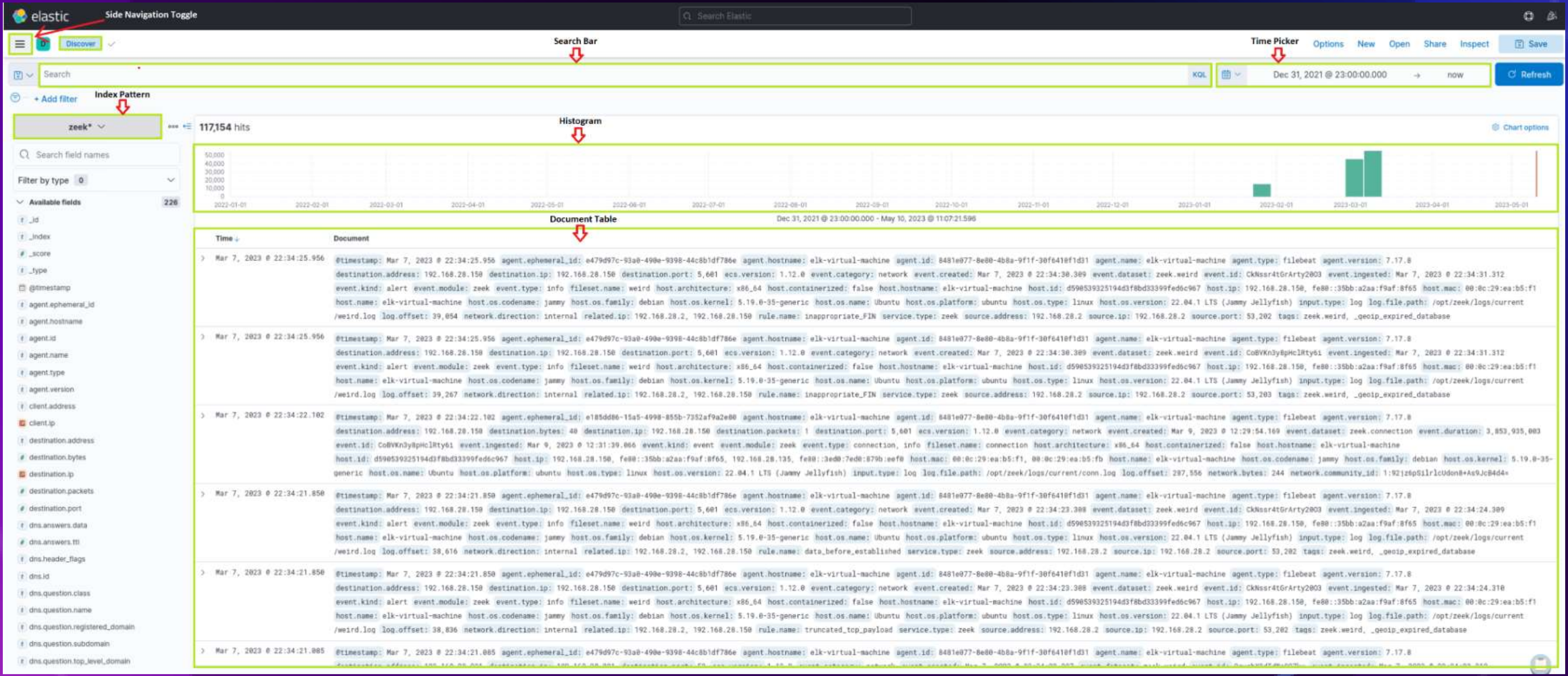
INTRODUCTION TO THE ELASTIC STACK

The Elastic stack, created by Elastic, is an open-source collection of mainly three applications (Elasticsearch, Logstash, and Kibana) that work in harmony to offer users comprehensive search and visualization capabilities for real-time analysis and exploration of log file sources.

WHAT IS THE ELASTIC STACK?

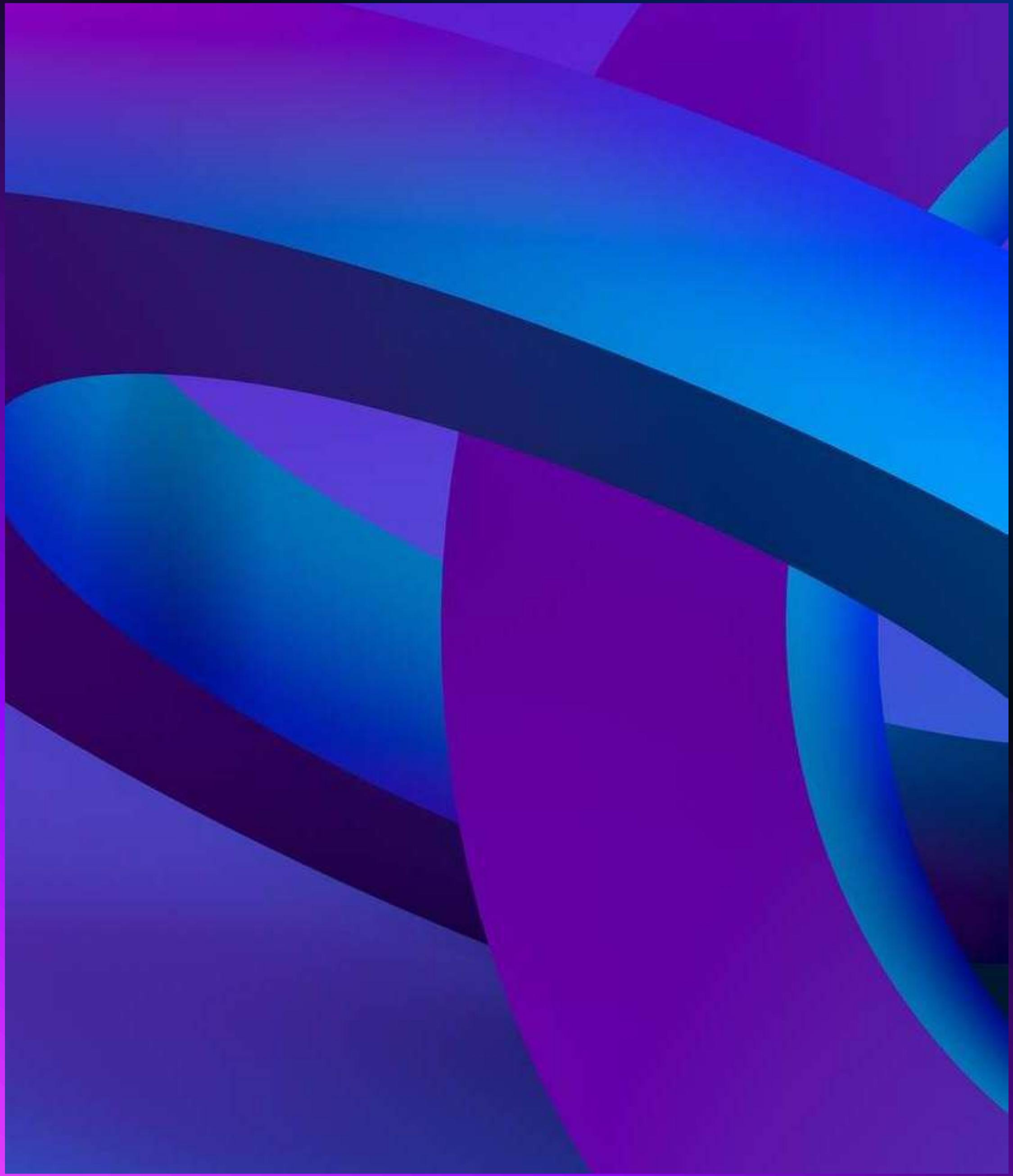


THE KIBANA



- _id
- _index
- _score
- _type
- @timestamp
- agent.ephemeral_id
- agent.hostname
- agent.id
- agent.name
- agent.type
- agent.version
- client.address
- client.ip
- destination.address
- destination.bytes
- destination.ip
- destination.packets
- destination.port
- dns.answers.data
- dns.answers.ttl
- dns.header_flags
- dns.id
- dns.question.class
- dns.question.name
- dns.question.registered_domain
- dns.question.subdomain
- dns.question.top_level_domain

```
Time ↓                       Document
> Mar 7, 2023 @ 22:34:25.956  @timestamp: Mar 7, 2023 @ 22:34:25.956 agent.ephemeral_id: e479d97c-93a0-490e-9398-44c8b1df786e agent.hostname: elk-virtual-machine agent.id: 8481e077-8e80-4b8a-9f1f-30f6410f1d31 agent.name: elk-virtual-machine agent.type: filebeat agent.version: 7.17.8
                              destination.address: 192.168.28.150 destination.ip: 192.168.28.150 destination.port: 5,601 ecs.version: 1.12.0 event.category: network event.created: Mar 7, 2023 @ 22:34:30.309 event.dataset: zeek.weird event.id: CkNssr4tGrArty2003 event.ingested: Mar 7, 2023 @ 22:34:31.312
                              event.kind: alert event.module: zeek event.type: info fileset.name: weird host.architecture: x86_64 host.containerized: false host.hostname: elk-virtual-machine host.id: d590539325194d3f8bd33399fed6c967 host.ip: 192.168.28.150, fe80::35bb:a2aa:f9af:8f65 host.mac: 00:0c:29:ea:b5:f1
                              host.name: elk-virtual-machine host.os.codename: jammy host.os.family: debian host.os.kernel: 5.19.0-35-generic host.os.name: Ubuntu host.os.platform: ubuntu host.os.type: linux host.os.version: 22.04.1 LTS (Jammy Jellyfish) input.type: log log.file.path: /opt/zeek/logs/current
                              /weird.log log.offset: 39,054 network.direction: internal related.ip: 192.168.28.2, 192.168.28.150 rule.name: inappropriate_FIN service.type: zeek source.address: 192.168.28.2 source.ip: 192.168.28.2 source.port: 53,202 tags: zeek.weird, _geoip_expired_database
> Mar 7, 2023 @ 22:34:25.956  @timestamp: Mar 7, 2023 @ 22:34:25.956 agent.ephemeral_id: e479d97c-93a0-490e-9398-44c8b1df786e agent.hostname: elk-virtual-machine agent.id: 8481e077-8e80-4b8a-9f1f-30f6410f1d31 agent.name: elk-virtual-machine agent.type: filebeat agent.version: 7.17.8
                              destination.address: 192.168.28.150 destination.ip: 192.168.28.150 destination.port: 5,601 ecs.version: 1.12.0 event.category: network event.created: Mar 7, 2023 @ 22:34:30.309 event.dataset: zeek.weird event.id: CoBVKn3y8pHclRty6i event.ingested: Mar 7, 2023 @ 22:34:31.312
                              event.kind: alert event.module: zeek event.type: info fileset.name: weird host.architecture: x86_64 host.containerized: false host.hostname: elk-virtual-machine host.id: d590539325194d3f8bd33399fed6c967 host.ip: 192.168.28.150, fe80::35bb:a2aa:f9af:8f65 host.mac: 00:0c:29:ea:b5:f1
                              host.name: elk-virtual-machine host.os.codename: jammy host.os.family: debian host.os.kernel: 5.19.0-35-generic host.os.name: Ubuntu host.os.platform: ubuntu host.os.type: linux host.os.version: 22.04.1 LTS (Jammy Jellyfish) input.type: log log.file.path: /opt/zeek/logs/current
                              /weird.log log.offset: 39,267 network.direction: internal related.ip: 192.168.28.2, 192.168.28.150 rule.name: inappropriate_FIN service.type: zeek source.address: 192.168.28.2 source.ip: 192.168.28.2 source.port: 53,203 tags: zeek.weird, _geoip_expired_database
> Mar 7, 2023 @ 22:34:22.102  @timestamp: Mar 7, 2023 @ 22:34:22.102 agent.ephemeral_id: e185dd86-15a5-4998-855b-7352af9a2e80 agent.hostname: elk-virtual-machine agent.id: 8481e077-8e80-4b8a-9f1f-30f6410f1d31 agent.name: elk-virtual-machine agent.type: filebeat agent.version: 7.17.8
                              destination.address: 192.168.28.150 destination.bytes: 40 destination.ip: 192.168.28.150 destination.packets: 1 destination.port: 5,601 ecs.version: 1.12.0 event.category: network event.created: Mar 9, 2023 @ 12:29:54.169 event.dataset: zeek.connection event.duration: 3,853,935,003
                              event.id: CoBVKn3y8pHclRty6i event.ingested: Mar 9, 2023 @ 12:31:39.066 event.kind: event event.module: zeek event.type: connection, info fileset.name: connection host.architecture: x86_64 host.containerized: false host.hostname: elk-virtual-machine
                              host.id: d590539325194d3f8bd33399fed6c967 host.ip: 192.168.28.150, fe80::35bb:a2aa:f9af:8f65, 192.168.28.135, fe80::3ed0:7ed0:879b:eef0 host.mac: 00:0c:29:ea:b5:f1, 00:0c:29:ea:b5:fb host.name: elk-virtual-machine host.os.codename: jammy host.os.family: debian host.os.kernel: 5.19.0-35-
                              generic host.os.name: Ubuntu host.os.platform: ubuntu host.os.type: linux host.os.version: 22.04.1 LTS (Jammy Jellyfish) input.type: log log.file.path: /opt/zeek/logs/current/conn.log log.offset: 287,556 network.bytes: 244 network.community_id: 1:92jz6pSilrlcUdon8+As9JcB4d4=
> Mar 7, 2023 @ 22:34:21.850  @timestamp: Mar 7, 2023 @ 22:34:21.850 agent.ephemeral_id: e479d97c-93a0-490e-9398-44c8b1df786e agent.hostname: elk-virtual-machine agent.id: 8481e077-8e80-4b8a-9f1f-30f6410f1d31 agent.name: elk-virtual-machine agent.type: filebeat agent.version: 7.17.8
                              destination.address: 192.168.28.150 destination.ip: 192.168.28.150 destination.port: 5,601 ecs.version: 1.12.0 event.category: network event.created: Mar 7, 2023 @ 22:34:23.308 event.dataset: zeek.weird event.id: CkNssr4tGrArty2003 event.ingested: Mar 7, 2023 @ 22:34:24.309
                              event.kind: alert event.module: zeek event.type: info fileset.name: weird host.architecture: x86_64 host.containerized: false host.hostname: elk-virtual-machine host.id: d590539325194d3f8bd33399fed6c967 host.ip: 192.168.28.150, fe80::35bb:a2aa:f9af:8f65 host.mac: 00:0c:29:ea:b5:f1
                              host.name: elk-virtual-machine host.os.codename: jammy host.os.family: debian host.os.kernel: 5.19.0-35-generic host.os.name: Ubuntu host.os.platform: ubuntu host.os.type: linux host.os.version: 22.04.1 LTS (Jammy Jellyfish) input.type: log log.file.path: /opt/zeek/logs/current
                              /weird.log log.offset: 38,616 network.direction: internal related.ip: 192.168.28.2, 192.168.28.150 rule.name: data_before_established service.type: zeek source.address: 192.168.28.2 source.ip: 192.168.28.2 source.port: 53,202 tags: zeek.weird, _geoip_expired_database
> Mar 7, 2023 @ 22:34:21.850  @timestamp: Mar 7, 2023 @ 22:34:21.850 agent.ephemeral_id: e479d97c-93a0-490e-9398-44c8b1df786e agent.hostname: elk-virtual-machine agent.id: 8481e077-8e80-4b8a-9f1f-30f6410f1d31 agent.name: elk-virtual-machine agent.type: filebeat agent.version: 7.17.8
                              destination.address: 192.168.28.150 destination.ip: 192.168.28.150 destination.port: 5,601 ecs.version: 1.12.0 event.category: network event.created: Mar 7, 2023 @ 22:34:23.308 event.dataset: zeek.weird event.id: CkNssr4tGrArty2003 event.ingested: Mar 7, 2023 @ 22:34:24.310
                              event.kind: alert event.module: zeek event.type: info fileset.name: weird host.architecture: x86_64 host.containerized: false host.hostname: elk-virtual-machine host.id: d590539325194d3f8bd33399fed6c967 host.ip: 192.168.28.150, fe80::35bb:a2aa:f9af:8f65 host.mac: 00:0c:29:ea:b5:f1
                              host.name: elk-virtual-machine host.os.codename: jammy host.os.family: debian host.os.kernel: 5.19.0-35-generic host.os.name: Ubuntu host.os.platform: ubuntu host.os.type: linux host.os.version: 22.04.1 LTS (Jammy Jellyfish) input.type: log log.file.path: /opt/zeek/logs/current
                              /weird.log log.offset: 38,836 network.direction: internal related.ip: 192.168.28.2, 192.168.28.150 rule.name: truncated_tcp_payload service.type: zeek source.address: 192.168.28.2 source.ip: 192.168.28.2 source.port: 53,202 tags: zeek.weird, _geoip_expired_database
> Mar 7, 2023 @ 22:34:21.085  @timestamp: Mar 7, 2023 @ 22:34:21.085 agent.ephemeral_id: e479d97c-93a0-490e-9398-44c8b1df786e agent.hostname: elk-virtual-machine agent.id: 8481e077-8e80-4b8a-9f1f-30f6410f1d31 agent.name: elk-virtual-machine agent.type: filebeat agent.version: 7.17.8
```



KIBANA QUERY LANGUAGE (KQL)

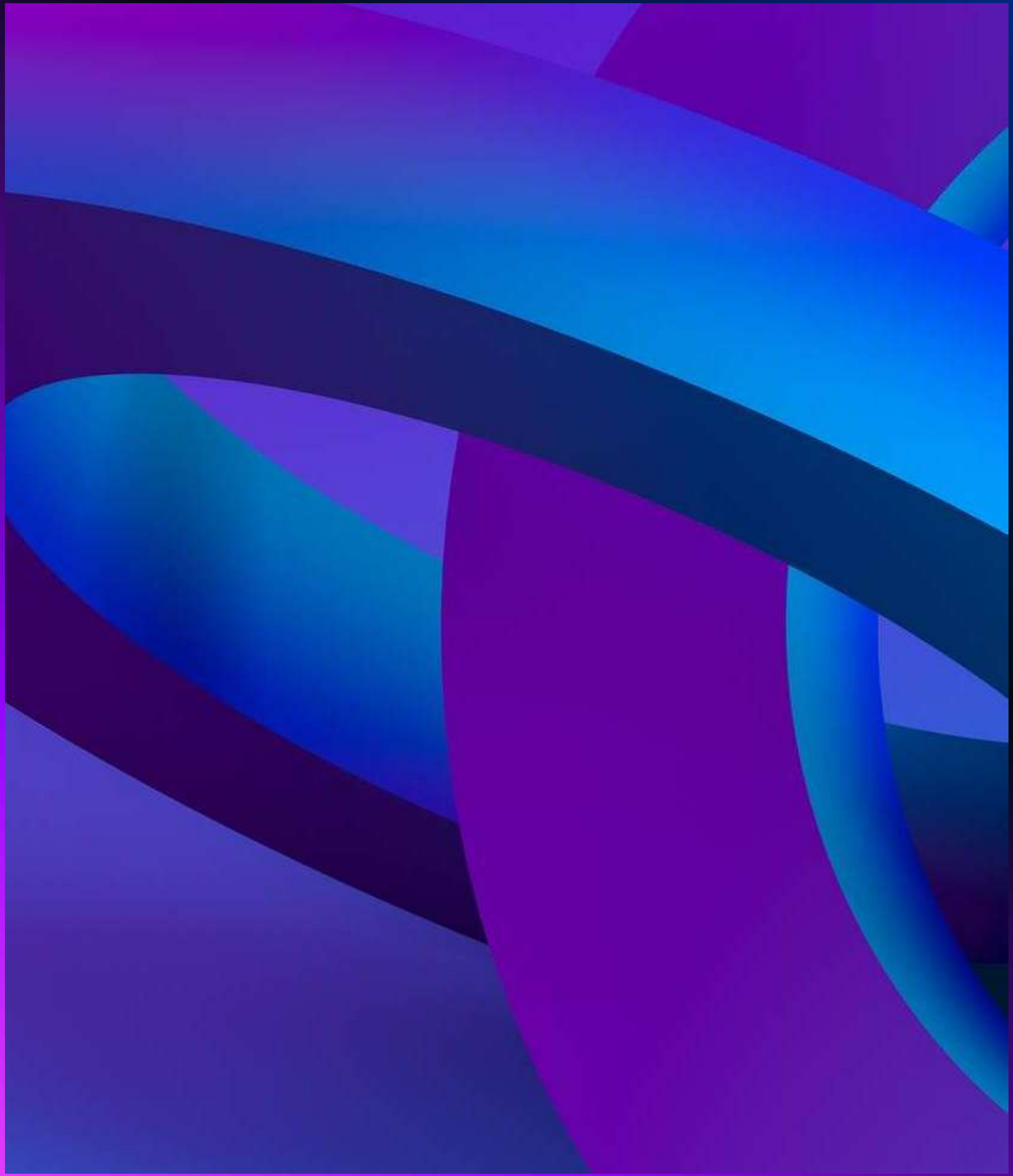
Kibana Query Language (KQL) is a powerful and user-friendly query language designed specifically for searching and analyzing data in Kibana. It simplifies the process of extracting insights from your indexed Elasticsearch data, offering a more intuitive approach than Elasticsearch's Query DSL. Let's explore the technical aspects and key components of the KQL language.

KIBANA QUERY LANGUAGE

queries
event.code:4625
"svc-sql1"
event.code:4625 AND winlog.event_data.SubStatus:0xC0000072
event.code:4625 AND winlog.event_data.SubStatus:0xC0000072 AND @timestamp >= "2023-03-03T00:00:00.000Z" AND @timestamp <= "2023-03-06T23:59:59.999Z"
event.code:4625 AND user.name: admin*

CHAPTER 4

MITRE ATT&CK



MITRE ATT&CK

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework serves as an extensive, regularly updated resource outlining the tactics, techniques, and procedures (TTPs) employed by cyber threat actors. This structured methodology assists cybersecurity experts in comprehending, identifying, and reacting to threats more proactively and knowledgeably.

Link: https://attack.mitre.org/

MITRE ATT&CK USE CASES IN SECURITY OPERATIONS

- Detection and Response : The framework supports SOCs in devising detection and response plans based on recognized attacker TTPs, empowering security teams to pinpoint potential dangers and develop proactive countermeasures.
- Security Evaluation and Gap Analysis : Organizations can leverage the ATT&CK framework to identify the strengths and weaknesses of their security posture, subsequently prioritizing security control investments to effectively defend against relevant threats.
- SOC Maturity Assessment : The ATT&CK framework enables organizations to assess their Security Operations Center (SOC) maturity by measuring their ability to detect, respond to, and mitigate various TTPs. This assessment assists in identifying areas for improvement and prioritizing resources to strengthen the overall security posture.
- Threat Intelligence : The framework offers a unified language and format to describe adversarial actions, enabling organizations to bolster their threat intelligence and improve collaboration among internal teams or with external stakeholders.
- Cyber Threat Intelligence Enrichment : Leveraging the ATT&CK framework can help organizations enrich their cyber threat intelligence by providing context on attacker TTPs, as well as insights into potential targets and indicators of compromise (IOCs). This enrichment allows for more informed decision-making and effective threat mitigation strategies.
- Behavioral Analytics Development : By mapping the TTPs outlined in the ATT&CK framework to specific user and system behaviors, organizations can develop behavioral analytics models to identify anomalous activities indicative of potential threats. This approach enhances detection capabilities and helps security teams proactively mitigate risks.
- Red Teaming and Penetration Testing : The ATT&CK framework presents a systematic way to replicate genuine attacker techniques during red teaming exercises and penetration tests, ultimately assessing an organization's defensive capabilities.
- Training and Education : The comprehensive and well-organized nature of the ATT&CK framework makes it an exceptional resource for training and educating security professionals on the latest adversarial tactics and methods.

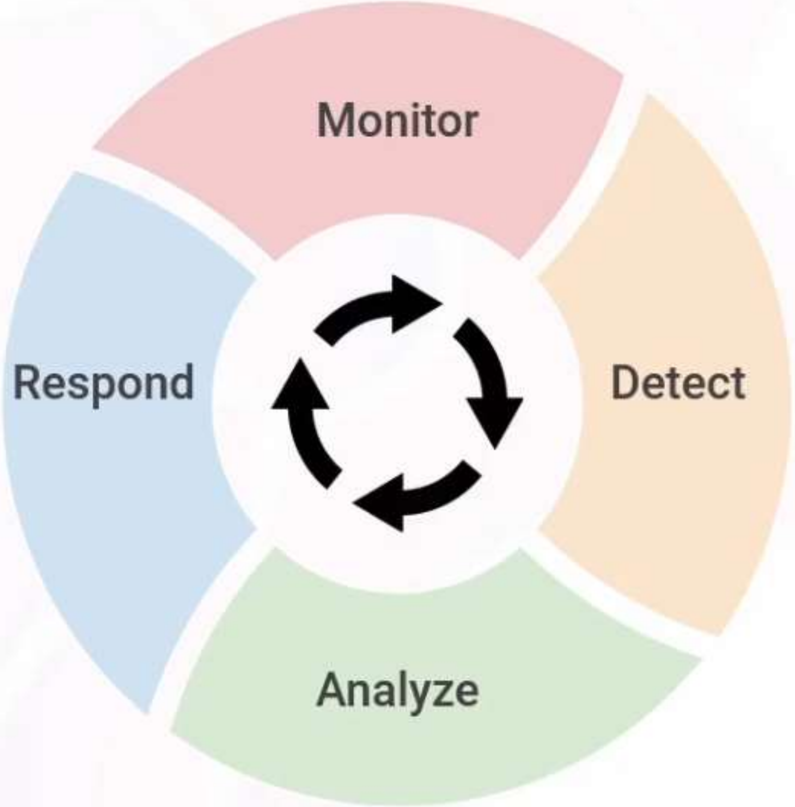
CHAPTER 5

SOC AND IT’S ROLE

The SOC and Its Role

A Security Operations Center is a centralized unit within an organization that deals with security issues, incidents, and events.

- **Monitor**
  - Continuous observation for unusual activity
  - Utilization of monitoring tools (IDS, SIEM, etc.) for real-time visibility
  - Early detections of potential security threats
- **Detect**
  - Confirm security events identified during monitoring
  - Utilize threat detection techniques
  - Identify known indicators of compromise (IOCs)
- **Analyze**
  - Perform in-depth investigations to understand security incidents
  - Examine affected systems, build a timeline of events
  - Trace tactics, techniques, and procedures (TTPs)
- **Respond**
  - Formulate a response plan based on findings
  - Contain threats, mitigate impact, and restore normal operations
  - Collaborate with internal teams and stakeholders



Key Functions of a SOC

Reactive

- **Monitoring and Detection**
    - Network and system logs, alerts
    - SIEM, IDS, log analysis
    - Alert triage
- **Incident Response**
    - Investigate, contain, and mitigate threats
    - Collect evidence and artifacts
    - Engage with stakeholders
- **Forensic Analysis**
    - In-house or third-party
    - Determine cause and scope
    - Preserve evidence and engage legal
- **Malware Analysis**
    - In-house or third-party
    - Sandbox and reverse engineer malware
    - Study malware behavior
    - Collect indicators of compromise

Proactive

- **Threat Intelligence**
    - Gather and analyze intelligence
    - Study emerging threats, vulnerabilities, and attacks
    - Feed intel into detection tools for proactive defense
- **Threat Hunting**
    - Search for malicious activity or intrusions
    - Logs, network traffic, endpoint telemetry
    - Utilize threat intelligence to hunt for known indicators
- **Vulnerability Management**
    - Identify and address vulnerabilities
    - Scan, assess, and patch
    - Coordinate remediation activity
- **Security Awareness Training**
    - Promote security awareness within the organization
    - Educate best practices, policies, and procedures

SOC Models

- **Internal SOC**
  - Owned and operated by the organization it serves
  - Monitors and defends internal networks, systems, and data
  - Requires significant upfront investment in training and resources
- **Managed SOC (MSOC)**
  - Third-party provider of security operations
  - Basic monitoring or comprehensive threat detection and response
  - Subscription-based SLAs, more cost-effective
- **Hybrid SOC**
  - Elements of internal and managed SOC services
  - Incident response, forensic analysis, malware analysis
  - Flexible compromise - call in the experts as needed

SOC Roles

SOC Analysts

- Tier 1 Analyst
- Tier 2 Analyst
- Tier 3 Analyst
- SOC Team Lead

Specialized Roles

- Incident Responder
- Threat Hunter
- Threat Intel Analyst
- Security Engineer
- Vulnerability Manager
- Forensic Analyst
- Malware Analyst

Management Roles

- SOC Manager
- Director of Security
- CISO

SOC Metrics

"If you can't measure it, you can't improve it." – ***Peter Drucker***

- **Mean Time to Detect (MTTD)**
    - Lower MTTD = faster detection
- **Mean Time to Resolution (MTTR)**
    - Lower MTTR = more efficient IR
- **Mean Time to Attend an Analyze (MTTA&A)**
    - Lower MTTA&A = reduced response latency
- **Incident Detection Rate**
    - Higher rate = better visibility and monitoring
- **False Positive Rates (FPR)**
    - Lower rate = more accurate detection
- **False Negative Rates (FNR)**
    - Lower rate = more accurate detection
- **Key Performance Indicators (KPIs)**
    - Measurable values to track performance
- **Key Risk Indicators (KRIs)**
    - Measurable values to assess risk
- **Service Level Agreements (SLAs)**

SOC Tools

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)
- Incident Management Tools
- Network Security Monitoring (NSM)
- Endpoint Detection and Response (EDR)
- Firewalls
    - Network Firewalls
    - Next-Generation Firewalls (NGFW)
    - Web Application Firewall (WAF)
- Intrusion Detection and Prevention Systems (IDS/IPS)
- Threat Intelligence Platforms (TIP)
- Forensic Analysis Tools
- Malware Analysis Tools

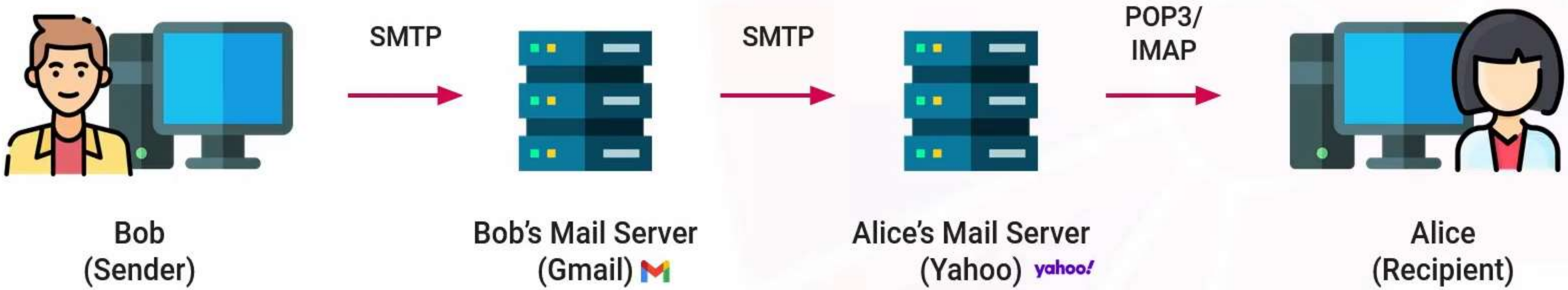
Common Threats and Attacks

- **Social Engineering**
  - Phishing
  - Spoofing
  - Vishing
  - SMiShing
  - Quishing
- **Malware**
  - Worm, Spyware, Adware
  - Ransomware
  - Trojan
  - Fileless Malware
- **Identity and Account Compromise**
  - Credential Theft
- **Insider Threats**
- **Advanced Persistent Threats (APTs)**
- **Denial-of-Service Attacks**
- **Data Breaches**
- **Zero-Days**
- **Supply Chain Attacks**

CHAPTER 6

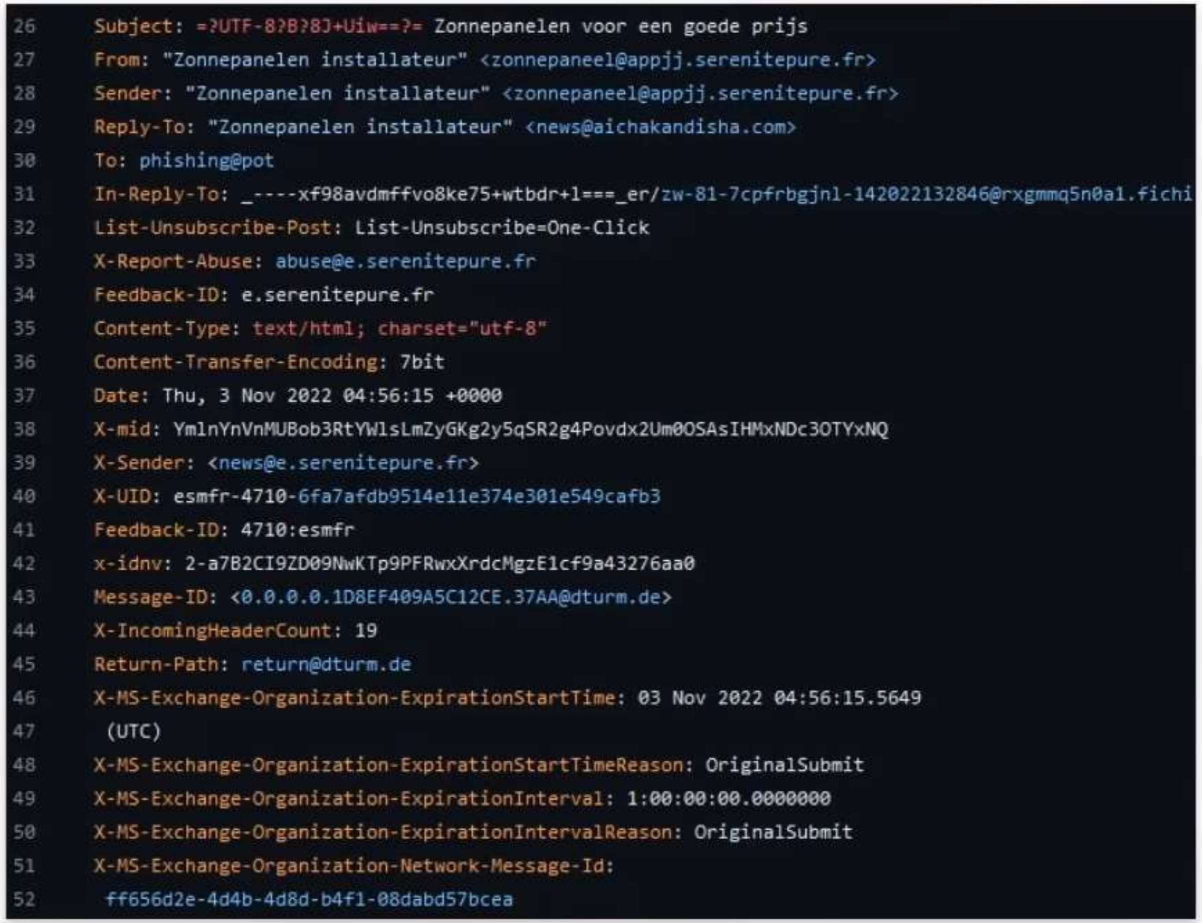
EMAIL ANALYSIS PRACTICAL

Email Fundamentals



Email Headers

Email headers are lines of metadata attached to an email and contain many useful strings of information for analysts and investigators.

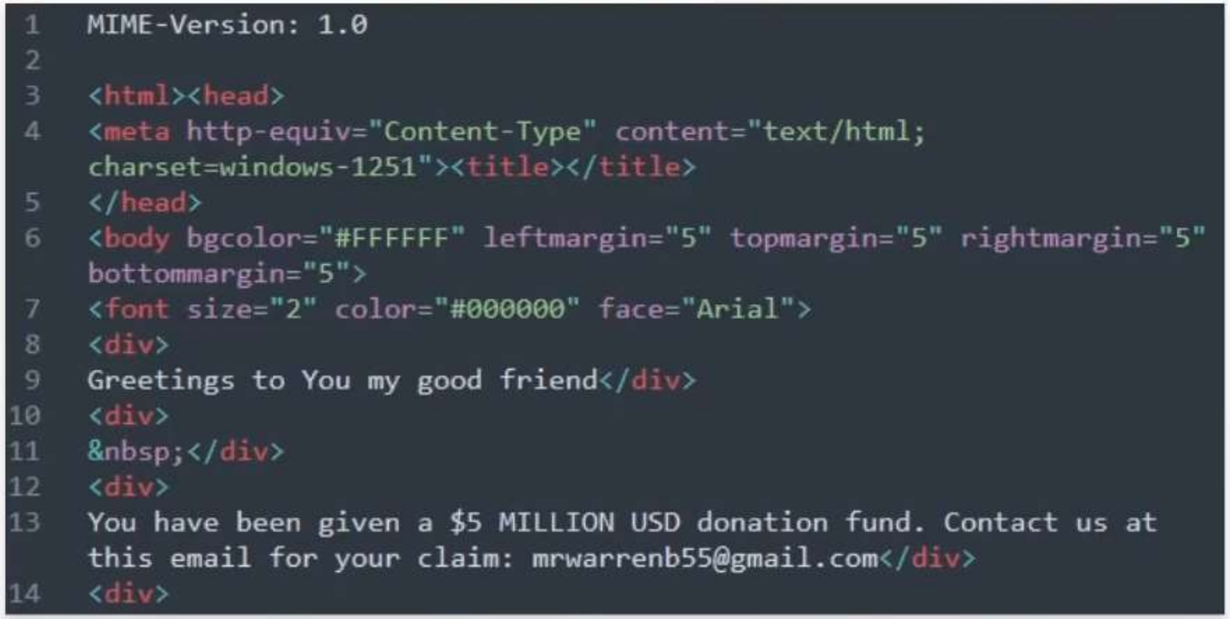


```
Subject: =?UTF-8?B?8J+Uiw==?= Zonnepanelen voor een goede prijs
From: "Zonnepanelen installateur" <zonnepaneel@appjj.serenitepure.fr>
Sender: "Zonnepanelen installateur" <zonnepaneel@appjj.serenitepure.fr>
Reply-To: "Zonnepanelen installateur" <news@aichakandisha.com>
To: phishing@pot
In-Reply-To: _----xf98avdmffvo8ke75+wtbdr+l===_er/zw-81-7cpfrbgjnl-142022132846@rxgmmq5n0a1.fichi
List-Unsubscribe-Post: List-Unsubscribe=One-Click
X-Report-Abuse: abuse@e.serenitepure.fr
Feedback-ID: e.serenitepure.fr
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: 7bit
Date: Thu, 3 Nov 2022 04:56:15 +0000
X-mid: YmlnYnVnMUBob3RtYWlsLmZyGKg2y5qSR2g4Povdx2Um0OSAsIHMxNDc3OTYxNQ
X-Sender: <news@e.serenitepure.fr>
X-UID: esmfr-4710-6fa7afdb9514e11e374e301e549cafb3
Feedback-ID: 4710:esmfr
x-idnv: 2-a7B2CI9ZD09NwKTp9PFRwxXrdcMgzE1cf9a43276aa0
Message-ID: <0.0.0.0.1D8EF409A5C12CE.37AA@dturm.de>
X-IncomingHeaderCount: 19
Return-Path: return@dturm.de
X-MS-Exchange-Organization-ExpirationStartTime: 03 Nov 2022 04:56:15.5649
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
X-MS-Exchange-Organization-Network-Message-Id:
 ff656d2e-4d4b-4d8d-b4f1-08dabd57bcea
```

Email Body

The email body is the main content of an email message that is visible to the recipient.

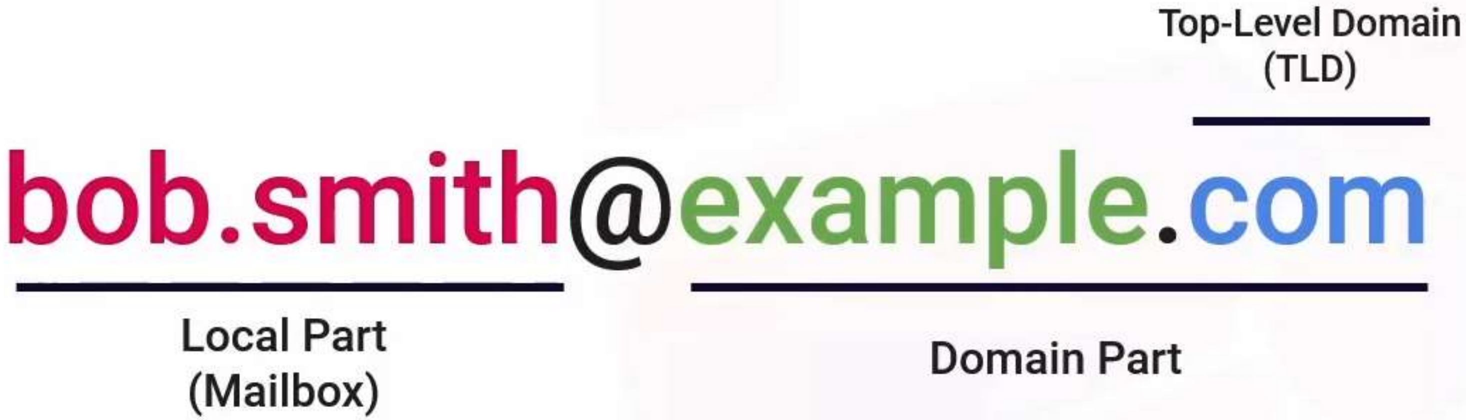
It typically contains the message that the sender wants to convey, including text, images, links, and any attachments.



```
MIME-Version: 1.0

<html><head>
<meta http-equiv="Content-Type" content="text/html;
charset=windows-1251"><title></title>
</head>
<body bgcolor="#FFFFFF" leftmargin="5" topmargin="5" rightmargin="5"
bottommargin="5">
<font size="2" color="#000000" face="Arial">
<div>
Greetings to You my good friend</div>
<div>
&nbsp;</div>
<div>
You have been given a $5 MILLION USD donation fund. Contact us at
this email for your claim: mrwarrenb55@gmail.com</div>
<div>
```

Email Addresses



Top-Level Domain
(TLD)

bob.smith@example.com

Local Part
(Mailbox)

Domain Part

Email Protocols

- SMTP
  - Simple Mail Transfer Protocol
  - Used to send outgoing mail
  - Port 25 (or 465, 587)
- POP3
  - Post Office Protocol (version 3)
  - Downloads emails, then deletes them
  - Port 110 (or 995 for POP3S)
- IMAP
  - Internet Message Access Protocol
  - Advanced email synchronization
  - Port 143 (or 993 for IMAPS)

Mail Agents

- **Mail Transfer Agent (MTA)**
  - Route and transfer email messages across mail servers
  - Determine appropriate route and relays
- **Mail User Agent (MUA)**
  - Compose, send, receive, and manage email messages
  - Gmail, Outlook, Yahoo, Thunderbird
- **Mail Delivery Agent (MDA)**
  - Accepting incoming email messages from MTAs
  - Placing the email in the recipient's inbox
- **Mail Submission Agent (MSA)**
- **Mail Retrieval Agent (MRA)**

Phishing Attack Types

- **Information Gathering**
  - Collecting data through reconnaissance
  - Verify existing accounts, craft credible phishes
- **Credential Harvesting**
  - Obtain login credentials from victims
  - Fake login pages, deceptive URLs
- **Malware Delivery**
  - Malicious attachments or links
  - Drive-by downloads
- **Spear Phishing**
  - Targeted and customized phishing
  - Research specific individuals or organizations
- **Whaling**
  - Targeting high-profile individuals (CEOs, executives)
- **Vishing, SMiShing, and Quishing**
  - Attempts to obtain information over the phone
  - SMS messages containing malicious URLs
  - QR codes leading to malicious URLs
- **Business Email Compromise (BEC)**
  - Compromising legitimate email accounts
  - Unauthorized wire transfers, invoice scams
- **Spam**
  - Unsolicited, irrelevant, and unwanted email
  - Not typically with malicious intent

Phishing Attack Techniques

- **Pretexting**
  - Fabricating a backstory
  - Manipulation under false pretense
- **Spoofing and Impersonation**
  - Email Address Spoofing
  - Domain Spoofing
- **URL Manipulation**
  - URL Shortening
  - Subdomain Spoofing
  - Homograph Attacks
  - Typosquatting
- **Encoding**
  - Obfuscate and evade detection
  - Base64, URL encoding, HTML encoding
  - Obscure JavaScript
- **Attachments**
  - Download and execute
- **Abuse of Legitimate Services**
  - Google Drive, Dropbox, etc.
  - Using trusted reputations to send malware
- **Pharming**
  - Two-step technique
  - Malware-based Pharming
  - DNS Server Poisoning