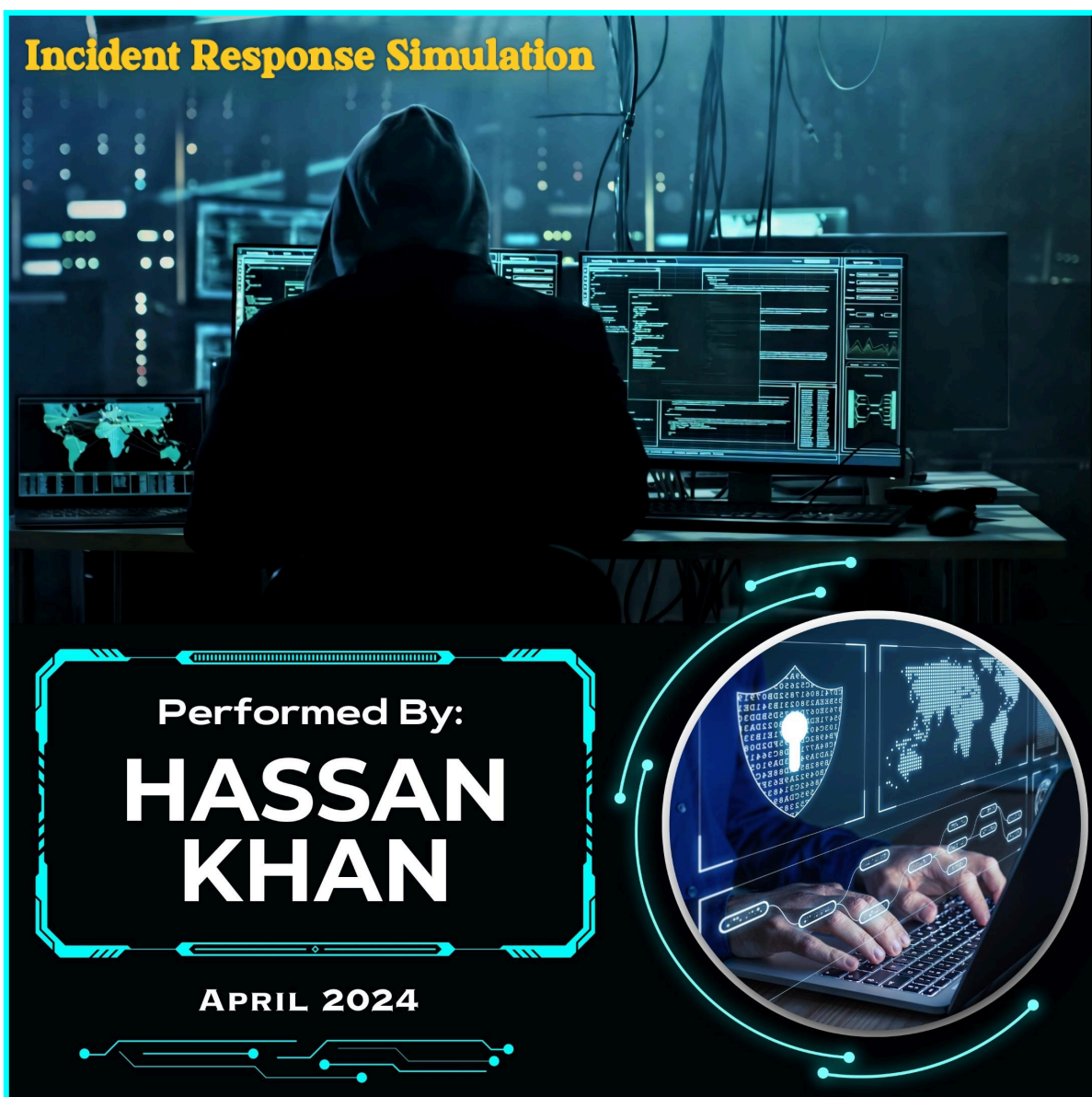


Cyber Security Internship



Incident Response Simulation

Performed By:
HASSAN KHAN

APRIL 2024

A circular inset image shows a close-up of hands typing on a laptop keyboard, with a digital shield and world map overlaying the scene.

Task 2: Incident Response Simulation

Topics To Be Covered

1. Introduction to Incident Response
2. Scenario Creation
3. Incident Detection
4. Response Plan Execution
5. Forensic Analysis
6. Post-Incident Assessment
7. Documentation & Presentation



❖ Introduction to Incident Response

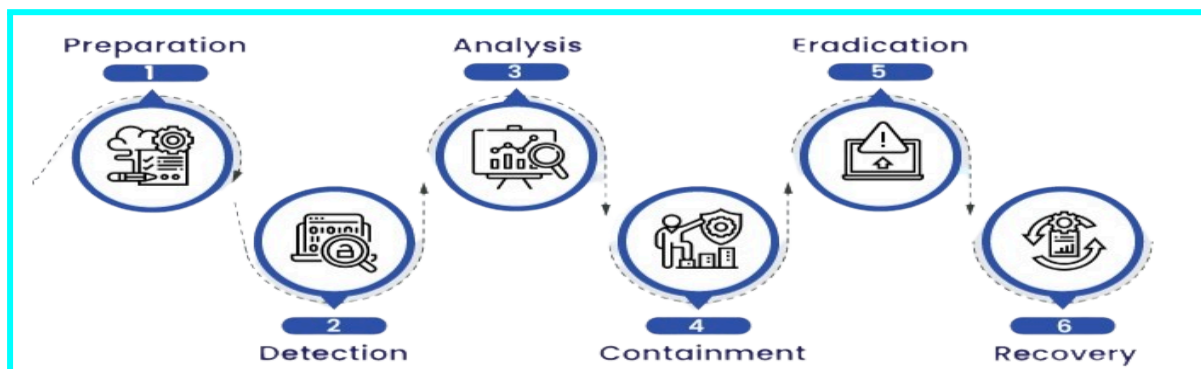
Cybersecurity incident response simulation is a way to practice responding to cyber attacks. It's like a virtual drill to test and improve your team's ability to handle security incidents. It helps identify weaknesses and develop effective strategies. Cybersecurity incident response is all about how organizations handle and respond to security breaches or cyber attacks. It's like having a plan in place to protect against and deal with any potential threats to your digital systems and data.



When a cybersecurity incident occurs, like a data breach or a malware infection, a well-defined incident response plan helps organizations respond quickly and effectively. The main goal is to minimize the impact of the incident, mitigate any damage, and get things back to normal as soon as possible.

The incident response process typically involves a few key steps:

- 1. Planning:** First, will plan out the simulation, including the scenario, objectives, and participants. This involves setting up a solid incident response plan in advance. It includes defining roles and responsibilities, establishing communication channels, and implementing security measures to prevent incidents.
- 2. Simulation Execution:** During the simulation, a realistic cyber attack scenario is simulated. This could involve things like phishing emails, malware infections, or network breaches. Participants will work together to respond to the incident and mitigate the damage.
- 3. Detection and Analysis:** This step focuses on identifying and understanding the nature and scope of the incident. It involves monitoring systems, analyzing logs, and investigating any suspicious activities or indicators of compromise.
- 4. Containment and Eradication:** Once an incident is confirmed, the next step is to contain the threat and prevent further damage. This might involve isolating affected systems, removing malware, or patching vulnerabilities.
- 5. Recovery and Restoration:** After containing the incident, the focus shifts to recovering affected systems and restoring normal operations. This could include restoring backups, repairing or replacing compromised assets, and implementing additional security measures.
- 6. Post-Incident Analysis and Lessons Learned:** Once the incident is resolved, it's important to conduct a post-incident analysis. This helps identify areas for improvement in the incident response plan, security controls, or employee training.



❖ Scenario Creation

Scenario creation is an important part of incident response planning. It involves creating hypothetical situations to test and prepare for potential cyber threats. By simulating different scenarios, organizations can identify vulnerabilities, assess their response capabilities, and develop effective strategies to mitigate risks. It's a crucial step in ensuring the security of systems and data.

Realistic cybersecurity incident scenario with a malware attack & phishing attempt.

Scenario Context:

The large multinational company that handles sensitive customer data. The company has robust cybersecurity measures in place, but attackers are constantly looking for vulnerabilities to exploit.

Objectives:

The objective of this scenario is to test the company's incident response capabilities and identify any weaknesses in their defenses against malware attacks and phishing attempts. It aims to simulate a real-life situation where an employee unknowingly falls victim to a sophisticated cyber attack.

Scope:

The scenario will focus on a targeted phishing email sent to employees within the company. The email will appear to be from a trusted source, such as the company's HR department, and will request employees to click on a link to update their personal information. Clicking on the link will lead to the download of a malware-infected file onto the employee's computer. The malware will attempt to exploit vulnerabilities in the system and gain unauthorized access to sensitive company data.

The scope of the scenario will include the initial detection of the phishing email, the response of the employee who receives it, and the subsequent actions taken by the company's IT and security teams to mitigate the attack, contain the malware, and prevent further damage.

By simulating this scenario, the company can assess their incident response procedures, train employees on identifying and reporting phishing attempts, and strengthen their overall cybersecurity posture.

❖ Incident Detection

Incident detection is a crucial part of cybersecurity incident response. It involves identifying potential security incidents by monitoring network traffic, system logs, and other indicators of compromise. It helps organizations quickly respond to and mitigate any security breaches.

Incident Response Team Roles:

In an incident response team, there are several roles related to incident detection.

1. Incident Analyst: This role involves analyzing and investigating security incidents to determine the nature, impact, and extent of the incident. They assess the severity, gather evidence, and provide recommendations for containment and recovery.

2. Security Operations Center (SOC) Analyst: SOC analysts monitor and analyze security events and alerts generated by various security systems. They identify potential incidents, investigate them, and escalate as necessary. They also maintain incident response playbooks and ensure adherence to established procedures.

3. Threat Intelligence Analyst: These analysts research and gather information about emerging threats, vulnerabilities, and attack techniques. They provide valuable insights to the incident response team, helping them stay informed and proactive in detecting and responding to incidents.

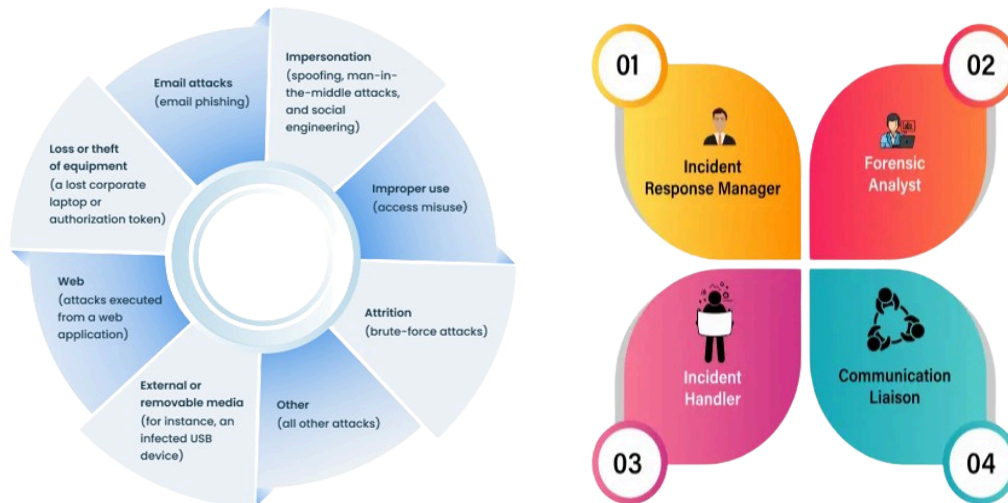
4. Forensic Analyst: Forensic analysts specialize in collecting and analyzing digital evidence related to security incidents. They use forensic tools and techniques to examine compromised systems, identify the root cause, and gather evidence for legal or investigative purposes.

5. Malware Analyst: Malware analysts focus on analyzing malicious software to understand its behavior, capabilities, and potential impact. They reverse-engineer malware samples, identify indicators of compromise (IOCs), and develop detection signatures or remediation strategies.

6. Data Analyst: Data analysts play a crucial role in incident detection by analyzing large volumes of security data, such as logs, network traffic, and user behavior. They

use data analytics techniques to identify patterns, anomalies, and potential security incidents.

These roles work together to detect and respond to security incidents effectively.



Few Examples Of Incident Detection Techniques:

- 1. Signature-based detection:** This technique uses predefined patterns or signatures to identify known malicious activities or malware. It compares network traffic or file attributes against a database of known threats.
- 2. Anomaly-based detection:** This technique focuses on identifying unusual or abnormal behavior within a system or network. It establishes a baseline of normal behavior and alerts when deviations occur.
- 3. Behavioral analysis:** This technique analyzes user and system behavior to identify potential security incidents. It looks for patterns that deviate from established norms, such as excessive failed login attempts or unusual data transfers.
- 4. Log analysis:** By analyzing system logs, organizations can identify suspicious activities, such as unauthorized access attempts, changes to critical files, or unusual network traffic.
- 5. Network traffic analysis:** Monitoring network traffic helps detect anomalies, such as unusual communication patterns, data exfiltration, or network scanning activities.
- 6. Endpoint detection and response (EDR):** EDR solutions monitor endpoint devices for signs of compromise, such as malicious processes, file modifications, or suspicious network connections.

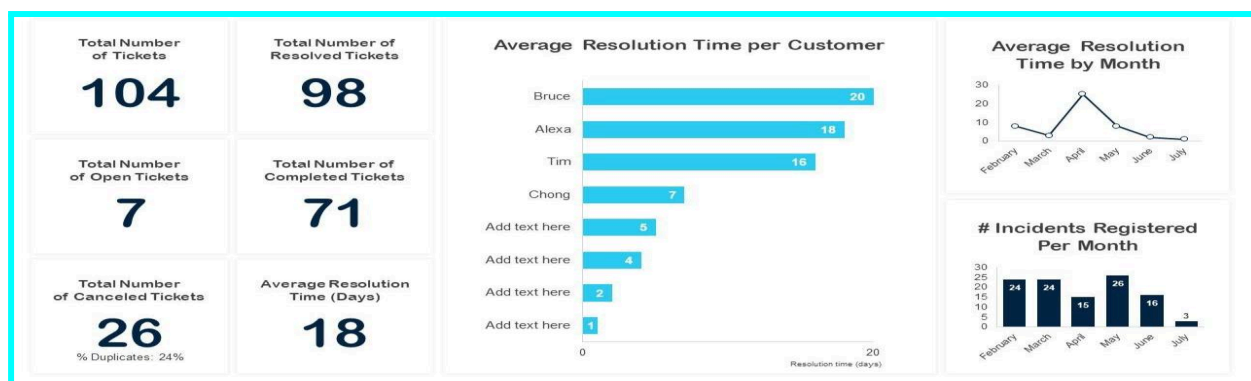
These techniques work together to provide a comprehensive approach to incident detection, allowing organizations to identify and respond to security incidents promptly.

Simulation Of Incident Detection Through Monitoring Tools:

In a typical incident detection scenario, monitoring tools continuously collect and analyze various logs and data sources to identify potential security incidents. These tools can include intrusion detection systems (IDS), log management systems, and security information and event management (SIEM) platforms.

The logs generated by systems, applications, network devices, and other sources contain valuable information about user activities, network traffic, system events, and more. By monitoring and analyzing these logs, security teams can detect indicators of compromise (IOCs), abnormal behavior, or suspicious activities that may indicate a security incident.

For example, if a log shows multiple failed login attempts from different IP addresses within a short period, it could be an indicator of a brute-force attack. The monitoring tool would raise an alert, and the incident detection team would investigate further to determine if it is indeed an attack and take appropriate actions.



There are several popular monitoring tools used for incident detection.

- 1. SIEM (Security Information and Event Management) tools:** SIEM tools collect and analyze log data from various sources to detect security incidents. They provide real-time monitoring, correlation of events, and alert generation.
- 2. IDS (Intrusion Detection System) tools:** IDS tools monitor network traffic for suspicious activities or known attack signatures. They can detect and alert on potential intrusions or unauthorized access attempts.

3. Endpoint Detection and Response (EDR) tools: EDR tools monitor and analyze activities on individual endpoints (such as laptops or servers). They can detect and respond to malicious activities, including malware infections or unauthorized access attempts.

4. Network Traffic Analysis (NTA) tools: NTA tools monitor network traffic to identify anomalies, such as unusual data transfers or communication patterns. They help detect network-based attacks and potential security breaches.

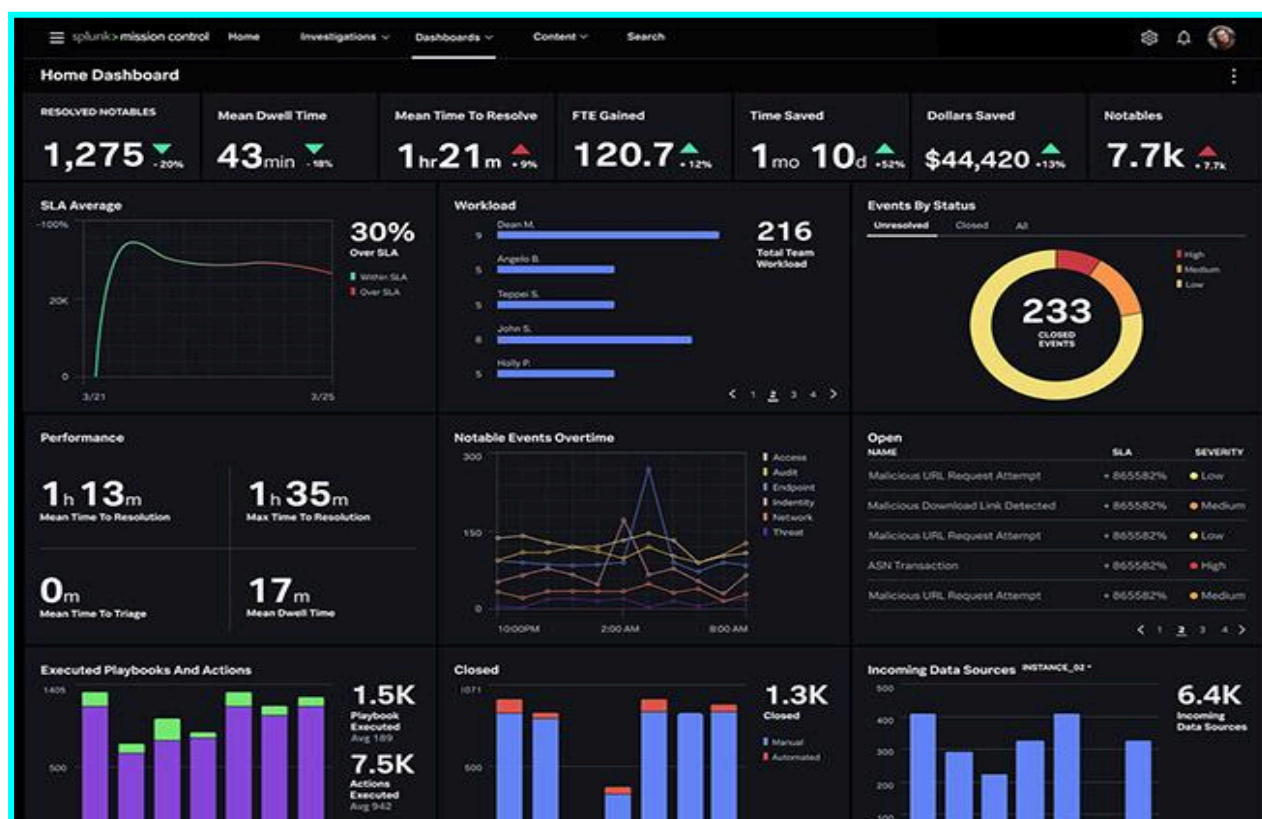
5. Log Management tools: Log management tools collect, store, and analyze logs from various systems and applications. They help identify patterns, anomalies, and potential security incidents by analyzing log data.

The key is to have a combination of tools that work together to provide comprehensive monitoring and incident detection capabilities.

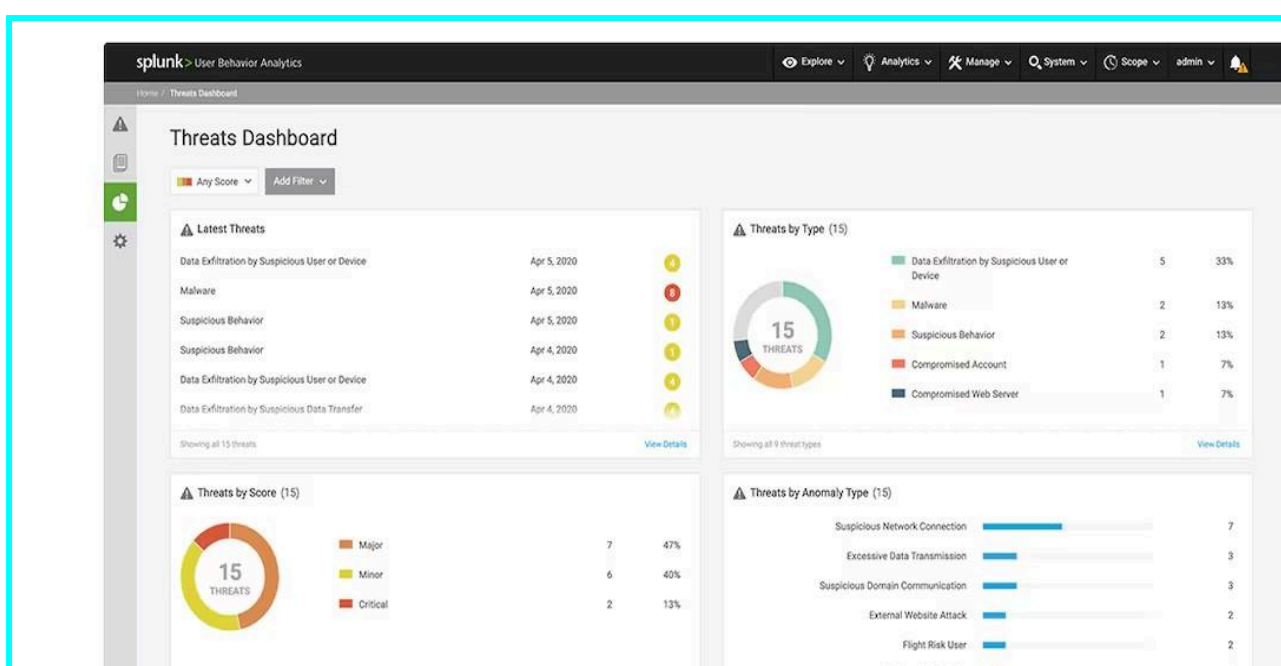
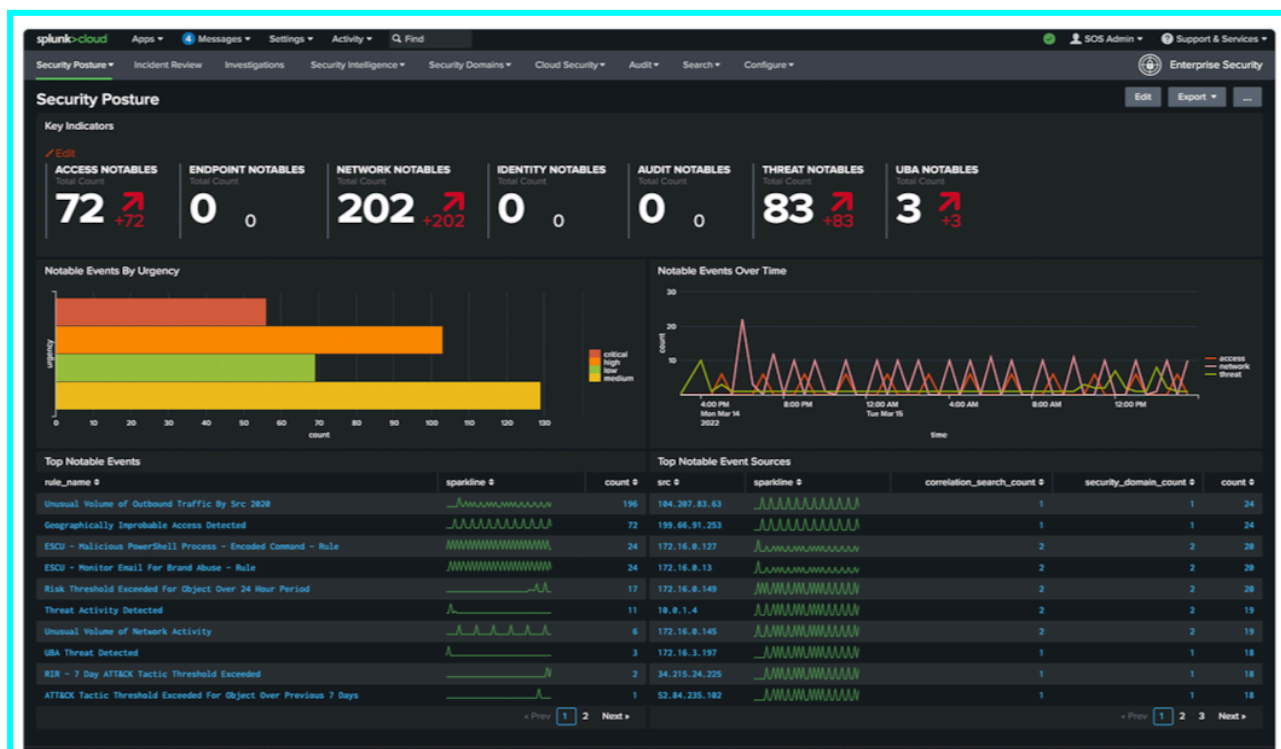
Tools used in Simulation



1. SPLUNK: It is a powerful log management and analysis platform that collects, indexes, and analyzes log data from various sources. It allows us to search, monitor, and visualize the log data in real-time. With Splunk, we can create custom dashboards and alerts to detect and respond to security incidents effectively.



Suicident response scenario involves a potential data breach. In this simulation, a security team can use SPLUNK to replay log data from a similar past incident or generate synthetic logs that mimic an actual attack. The team can then analyze the logs in real-time using SPLUNK's search capabilities to identify any suspicious activities or indicators of compromise. They can practice their incident response procedures, such as containment, eradication, and recovery, based on the insights gained from the simulation.

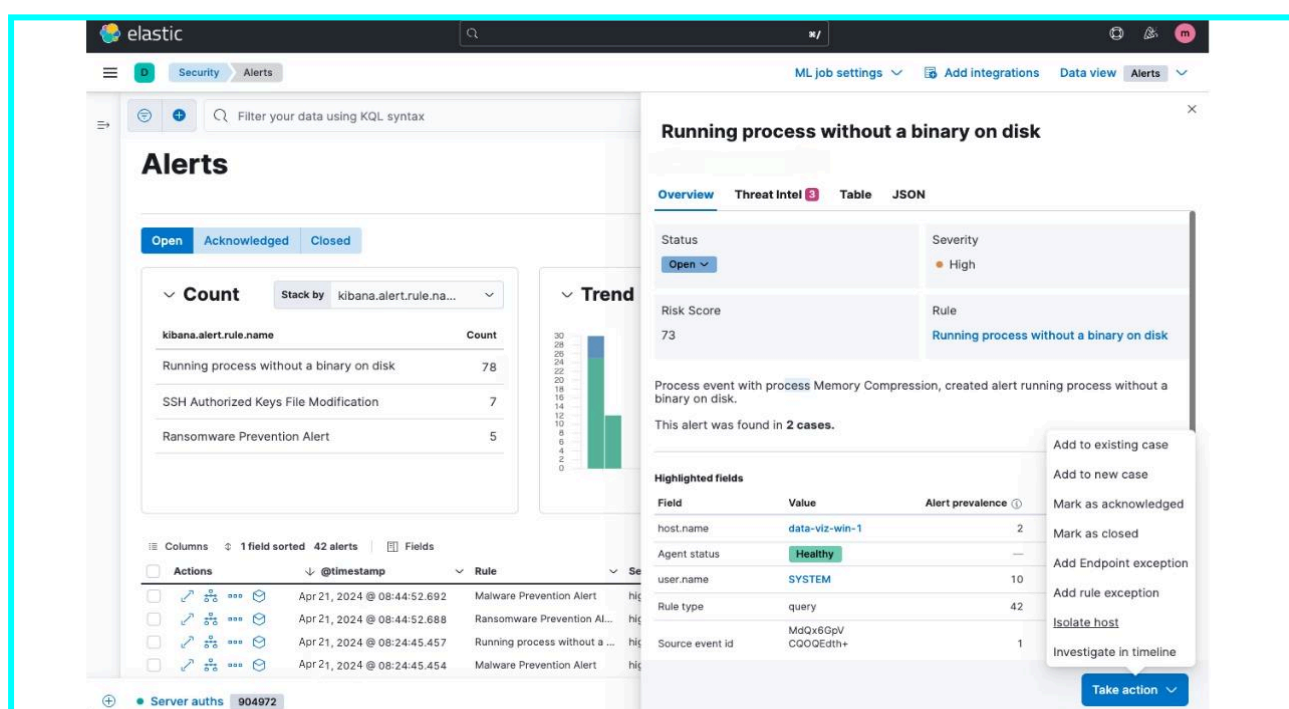
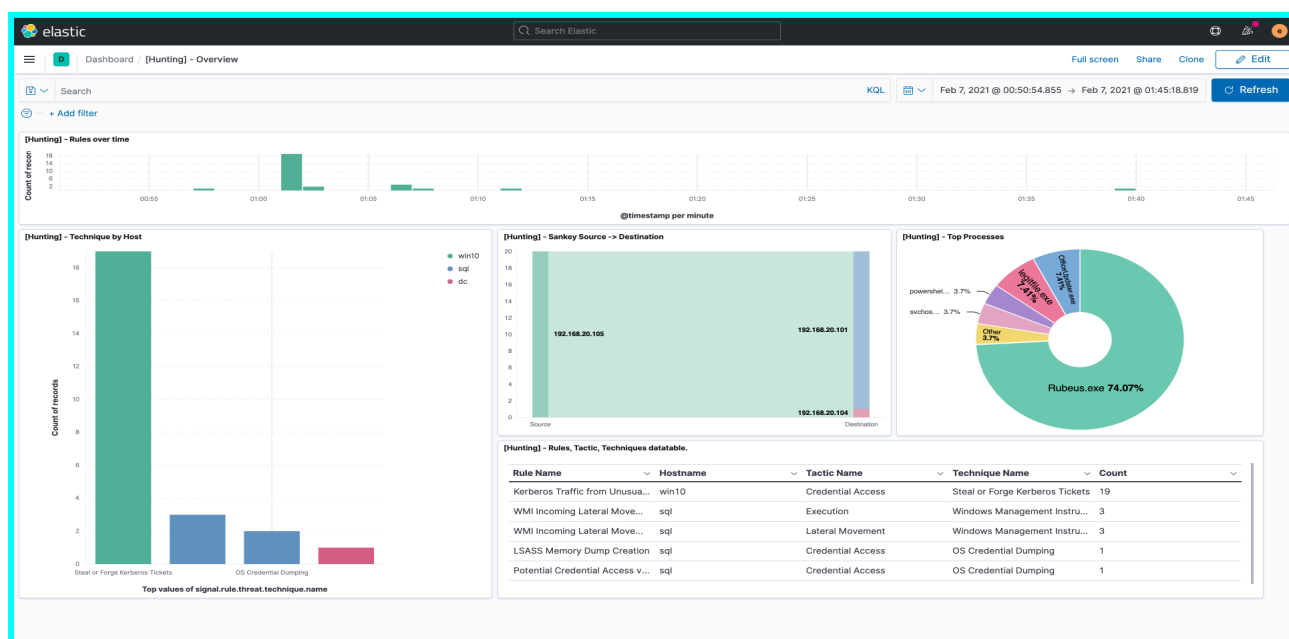


2. ELK Stack: It is an open-source solution that combines three components:

- Elasticsearch
- Logstash and
- Kibana.



Elasticsearch is a distributed search and analytics engine, Logstash is a data processing pipeline, and Kibana is a visualization tool. Together, they provide a robust log management and analysis solution. ELK Stack allows us to collect, parse, and analyze log data, and visualize it through customizable dashboards.



The screenshot shows the Elastic Security Alerts page. The top navigation bar includes 'elastic', 'Security', and 'Alerts'. The main content area displays a list of alerts for a host named 'vagrant'. The alerts are categorized by 'Process' and 'Host'. The 'Process' column shows the command executed, and the 'Host' column shows the host name. The 'Alerts' column shows the number of alerts for each process. The 'Process' column includes details like 'entity_id', 'args', 'executable', 'interactive', 'working_directory', 'pid', 'start', 'end', 'exit_code', 'user.name', and 'group.name'. The 'Host' column shows the host name. The 'Alerts' column shows the number of alerts for each process. The 'Process' column includes details like 'entity_id', 'args', 'executable', 'interactive', 'working_directory', 'pid', 'start', 'end', 'exit_code', 'user.name', and 'group.name'. The 'Host' column shows the host name. The 'Alerts' column shows the number of alerts for each process.

The screenshot shows the Elastic Security Alerts page. The top navigation bar includes 'elastic', 'Security', and 'Alerts'. The main content area displays a trend chart and a table of alerts. The trend chart shows the number of alerts over time, categorized by 'event.action'. The table shows the details of the alerts, including the signal rule name, count, and host name. The table includes columns for 'signal.rule.name', 'Count', 'host.name', and 'user.name'. The table shows the following data:

signal.rule.name	Count
Malware prevented	7,089
DLL injection	304
Ransomware prevented	161
bitsadm executed as child process	8

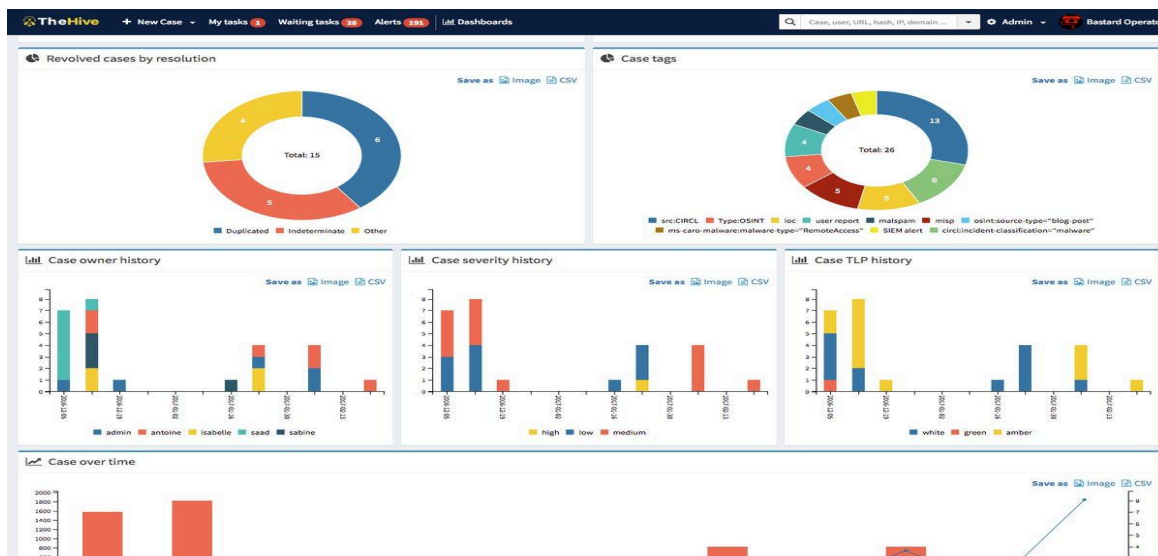
The table also includes columns for 'host.name' and 'user.name'. The table shows the following data:

host.name	user.name
Windows Laptop	SYSTEM
Finance Server	admin
Archives	reilly.hunter

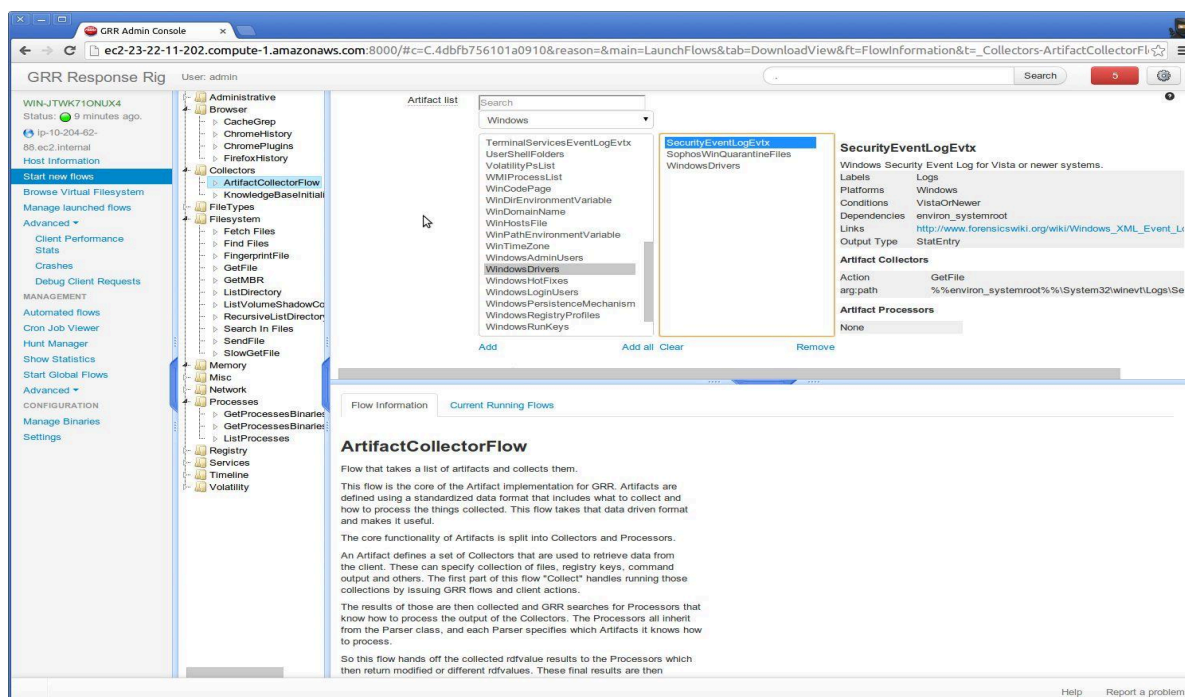
Difference between Splunk & ELK Stack:

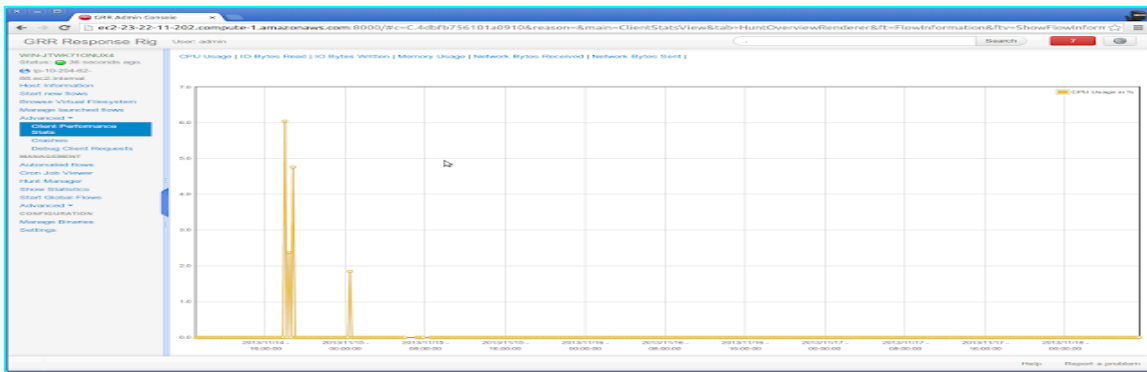
- Both Splunk and ELK Stack are popular tools used for log management and analysis, which can aid in incident detection.
- Both can be used to detect security incidents by analyzing logs for abnormal patterns, known attack signatures, or other indicators of compromise.
- They provide powerful search capabilities, correlation features, and alerting mechanisms to help identify and respond to potential incidents.
- SPLUNK is a **commercial product**, ELK Stack is an **open-source solution**.

2. TheHive: It is an open-source security incident response platform that allows us to manage and analyze security incidents. It provides a centralized interface to track and coordinate incident response activities. TheHive integrates with various security tools and allows us to automate tasks, collaborate with team members, and generate reports.



3. GRR Rapid Response: It is an open-source remote live forensics and incident response framework. It enables us to collect and analyze data from remote endpoints in real-time. GRR Rapid Response allows us to perform forensic investigations, gather evidence, and respond to security incidents remotely.





Difference between TheHive & GRR Rapid Response:

- TheHive and GRR Rapid Response are both powerful tools that can be used in incident response and investigation. By using these tools we can enhance our incident detection capabilities.
- TheHive can be used as a central hub for managing and tracking security incidents, while GRR Rapid Response can provide valuable endpoint data for investigation and response.
- When an incident is detected, GRR Rapid Response can be used to remotely collect relevant data from affected endpoints, such as memory dumps, file system snapshots, or network connections.
- This data can then be analyzed within TheHive, allowing us to correlate events, identify patterns, and take appropriate actions..

❖ Response Plan Execution

When it comes to executing a response plan in incident response, there are a few key steps to follow:



- 1. Identification:** First, we need to identify the incident and determine its scope and severity. This involves gathering information, analyzing logs, and understanding the impact on your systems and data.
- 2. Containment:** Once we've identified the incident, it's crucial to contain it to prevent further damage. This may involve isolating affected systems, disabling compromised accounts, or blocking malicious traffic.
- 3. Eradication:** After containing the incident, the next step is to eradicate the root cause. This could mean removing malware, patching vulnerabilities, or fixing misconfigurations that led to the incident.
- 4. Recovery:** Once the threat has been eliminated, we can focus on restoring affected systems and data. This may involve restoring from backups, rebuilding compromised systems, or implementing additional security measures.
- 5. Lessons Learned:** After the incident has been resolved, it's important to conduct a thorough post-incident analysis. This helps identify gaps in your security posture and allows us to improve your incident response plan for the future.



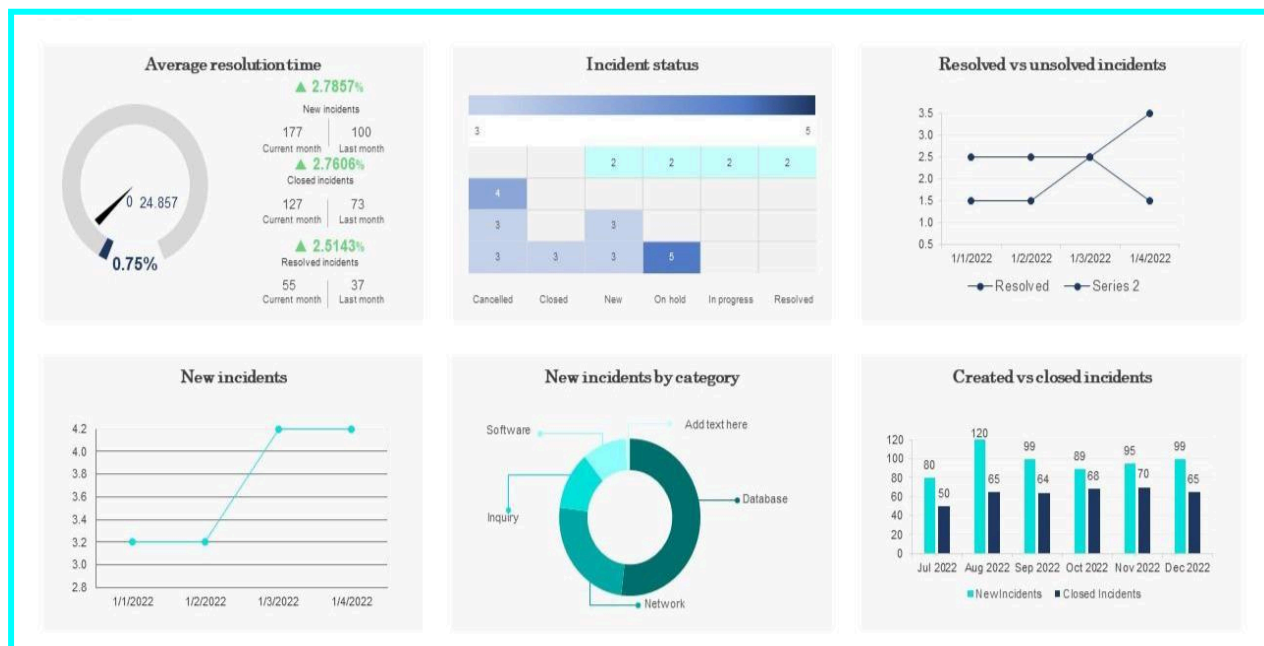
❖ Forensic Analysis

When it comes to forensic analysis in cybersecurity incident response, it plays a crucial role in understanding the nature of the incident, identifying the attackers, and gathering evidence for further investigation or legal proceedings if necessary.

Forensic analysis involves the systematic collection, preservation, and analysis of digital evidence. Here are some key steps involved in forensic analysis during incident response:

- 1. Identification:** The first step is to identify the systems, devices, or networks that are involved in the incident. This includes identifying the affected assets and potential sources of evidence.
- 2. Preservation:** Once identified, it's important to preserve the digital evidence in a forensically sound manner. This involves creating forensic images or taking snapshots of the affected systems, ensuring the integrity and authenticity of the evidence.
- 3. Analysis:** After preservation, the forensic analysis begins. This includes examining the collected evidence, such as log files, network traffic captures, memory dumps, or file system artifacts. The analysis aims to reconstruct the timeline of events, identify the attack vectors, and determine the extent of the compromise.
- 4. Reconstruction:** Based on the analysis, the forensic investigator reconstructs the attack scenario, identifying the tactics, techniques, and procedures (TTPs) used by the attackers. This helps in understanding the motives and intentions behind the incident.
- 5. Documentation:** Throughout the forensic analysis process, it's important to document all findings, methodologies, and actions taken. This documentation is crucial for reporting, legal purposes, and knowledge sharing within the incident response team.

Forensic analysis in cybersecurity incident response requires specialized tools, techniques, and expertise.



Incident Response		Forensic Analysis	
Goals			
<ul style="list-style-type: none">Focused in determining a quick response (manages events in real time).		<ul style="list-style-type: none">Completing analysis and gathering risks and impacts (part of a scheduled compliance legal discovery, or law enforcement investigation).Focused on a full understanding and thorough resolution of a breach.	
Data Requirements			
<ul style="list-style-type: none">Requires short-term data sources, often no more than a month.		<ul style="list-style-type: none">Requires much longer-lived logs and files. A well-succeeded attack is somewhere between 150 and 300 days.	
Team Skills			
<ul style="list-style-type: none">Strong log analysis and malware analysis capabilities. Ability to quickly isolate an infected device and to develop means to mitigate or quarantine the device.Interaction with other security and operations team members.		<ul style="list-style-type: none">Strong log analysis and malware analysis capabilities.Requires interaction with a much broader set of departments, including operations, legal, HR and compliance.	
Benefits			
<ul style="list-style-type: none">First line of defense in security operations.Eliminate a threat on one machine in real time.Keeping breaches isolated and limited in impact.		<ul style="list-style-type: none">Post Incident Analysis.Resolution of all threats with the careful analysis of an entire attack chain.Ability to respond judicially.	

❖ Post-Incident Assessment:

In the post-incident assessment of the cybersecurity incident response, it is important to review the effectiveness of the response plan and actions taken.

Based on the simulation in the incident response, there are a few areas for improvement and valuable lessons learned. First, it is important to ensure clear communication and coordination among the response team members. This can help streamline the decision-making process and ensure a more efficient response. Additionally, conducting regular training exercises and simulations can help identify gaps in the response plan and improve the team's preparedness. It is also crucial to regularly update and test the incident response plan to align with evolving cybersecurity threats. Lastly, documenting lessons learned from the simulation can provide valuable insights for future incident responses and help enhance the overall effectiveness of the cybersecurity incident response strategy.



❖ Documentation and Presentation

1. Incident Response Process:

- **Initial Detection:** The incident was detected through proactive monitoring and threat intelligence.
- **Incident Triage:** The response team quickly assessed the severity and impact of the incident.
- **Containment:** Immediate measures were taken to isolate the affected systems and limit further damage.
- **Investigation:** A thorough investigation was conducted to identify the root cause and extent of the incident.
- **Mitigation:** Steps were taken to mitigate the immediate risks and prevent further compromise.
- **Recovery:** Systems were restored to a secure state, and data was recovered from backups.
- **Post-Incident Analysis:** A detailed analysis was performed to understand the incident and its impact.

2. Actions Taken:

- **Isolation:** Affected systems were disconnected from the network to prevent further spread.
- **Patching and Updates:** Vulnerabilities were identified and patched to prevent future attacks.
- **Forensic Analysis:** Digital forensics techniques were used to gather evidence for investigation.
- **Communication:** Regular updates were provided to stakeholders, ensuring transparency throughout the incident.

3. Outcomes:

The incident was contained, limiting the impact on critical systems and data.

The root cause of the incident was identified, allowing for targeted remediation.

Systems were successfully restored, minimizing downtime and disruption.

Lessons learned from the incident will inform future incident response strategies.

4. Findings and Recommendations:

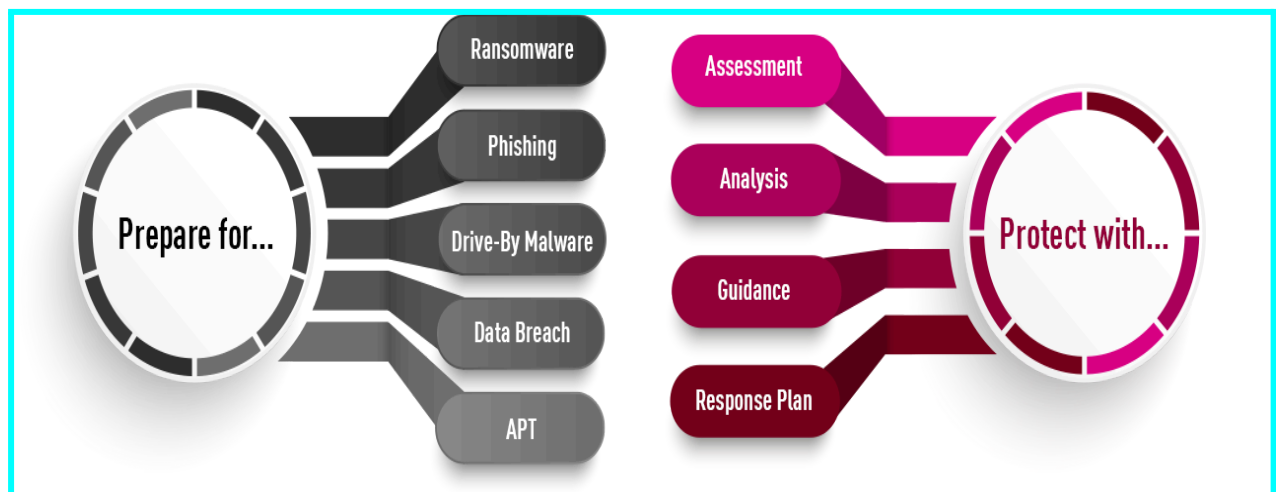
Strengthen incident detection capabilities through continuous monitoring and threat intelligence.

Enhance incident response coordination and communication channels.

Regularly update and test incident response plans to align with evolving threats.

Improve employee awareness and training to prevent similar incidents.

Invest in advanced security technologies and practices to proactively mitigate risks.



Report Prepared By:

Name: Mohd Hassan Khan | Cyber Security Intern

Internship Organization: [Intern Career](#)

Intern Email ID: hassanmuslimkhan@gmail.com

Intern LinkedIn ID: [Mohd Hassan Khan](#)

Internship Task 2 Completed Date: 22nd April 2024