Milot Jeune

Lab 6

**Summary**

In this lab, I utilized Catalyst, a potent incident response platform, to manage security incidents. Using predefined forms, I documented and responded to various scenarios—malware, brute force attempts, and phishing emails. This hands-on experience strengthened my practical skills, complementing our theoretical discussions on incident detection with Splunk in Unit 5. Overall, it provided a valuable understanding of a holistic incident response strategy, encompassing both detection and effective response.

* I downloaded the phishing ir reports
* I utilized public catalyst demo in a professional setting my company has their own installation
* Created a new incident – Catalsyt
* Utilized virusTotal to analyze hash

**INCIDENT RESPONSE**

| Initial identification of the malware incident

| 14:35 | Mock user informed and advised to disconnect PC

| 14:40 | Affected system isolated from the network

| 14:45 | System backup initiated

| 15:00 | Malware analysis and identification |

| 15:15 | Malware removal and system restoration

| 15:45 | System integrity and functionality confirmed

| 16:00 | User informed and system returned to user

Created incident ticket on catalyst & report

A screenshot of a computer

Description automatically generated

Hash & IP entered omtp VirusTotal and analyzed.

On the right is a screen of the artifacts being added

A screenshot of a computer

Description automatically generated

**TLP PROTOCOL**

I chose the TLP protocol to be green which meant I was authorized to share the incident throughout the tech community but kept it anonymous and did not reveal vital information.

**Resolution**

In response to the malware incident, immediate steps were taken to contain and resolve the issue. The affected user was advised to disconnect their PC, and the compromised system was isolated. A comprehensive backup was initiated, and alongside malware removal, key artifacts like the hash and IP of the attacker were documented. This information was then shared with the tech community to enhance awareness and collaborative defenses against similar threats.

**Closed the ticket**

A screenshot of a computer

Description automatically generated

**Post-Incident Activity**

\*\*Incident Summary:\*\*

The incident unfolded as a result of a sophisticated malware infiltration, compromising the network's integrity and potentially exposing sensitive data. The impact was notable, causing disruption to normal operations and necessitating a comprehensive response. Incident identified as a true positive.

\*\*Tactics, Techniques, and Procedures (TTPs):\*\*

The attackers employed advanced phishing techniques as the initial vector, exploiting human vulnerabilities to gain unauthorized access (social engineering). Subsequent analysis uncovered their adept use of evasion tactics to circumvent traditional detection methods. The execution of fileless malware and lateral movement showcased a multifaceted approach to privilege escalation within the network.

\*\*Response Effectiveness:\*\*

As apart of the CCERT team I demonstrated efficiency in identifying the breach and promptly isolating the affected system from the network. The eradication process effectively neutralized the malware, restoring the system's functionality. The rapid response mitigated the potential impact on critical assets. Concurrently, I took the initiative to initiate the auditing process, meticulously documenting every facet of the incident. This comprehensive documentation serves as a valuable resource for post-incident analysis and future improvements.

\*\*Improvement Areas:\*\*

Despite the overall effectiveness, communication gaps during the early stages of the incident led to a minor delay in detection. Additionally, there is an opportunity for improvement in the deployment of more advanced threat detection tools to enhance early threat identification.

\*\*Future Changes:\*\*

To fortify future responses, optimizing communication protocols during the initial incident stages is paramount. Integration of advanced threat detection tools, coupled with ongoing employee training to recognize sophisticated phishing attempts, will elevate our defense posture. Regular simulations and drills should be implemented to proactively refine our incident response capabilities. Furthermore, considering the nature of the incident, the recommendation includes investing in a more advanced firewall with robust threat detection capabilities. Such an enhancement would significantly bolster our first line of defense, providing better prevention against sophisticated phishing techniques and unauthorized access attempts.