



Diário de incidentes

Date: July 23, 2024	Entry: #1
Description	<p>Documenting a cybersecurity incident</p> <p>This incident occurred in the two phases:</p> <ol style="list-style-type: none">1. Detection and Analysis: The scenario outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance.2. Containment, Eradication, and Recovery: The scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance.
Tool(s) used	None
The 5 W's	<ul style="list-style-type: none">• Who: An organized group of unethical hackers• What: A ransomware security incident• Where: At a health care company• When: Tuesday 9:00 a.m.• Why: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	<ol style="list-style-type: none">1. Should the company pay the ransom to retrieve the decryption key?

Date: July 25 2024	Entry: #2
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.
The 5 W's	<ul style="list-style-type: none"> • Who: N/A • What: N/A • Where: N/A • When: N/A • Why: N/A
Additional notes	

Date: July 25 2024	Entry: #3
Description	DDoS incident
Tool(s) used	<p>A malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.</p> <p>Response using NISTcsf and by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.</p>
The 5 W's	<ul style="list-style-type: none"> • Who: An unknown malicious actor • What: ICMP Flood DDoS attack • Where: Multimedia company • When: 8:00 AM • Why: Take down the services

Additional notes	
------------------	--

Date: July 27 2024	Entry: #4
Description	Investigate a suspicious file hash
Tool(s) used	<p>For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious.</p> <p>Investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.</p>
The 5 W's	<ul style="list-style-type: none"> • Who: An unknown malicious actor • What: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • Where: An employee's computer at a financial services company • When: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file • Why: An employee was able to download and execute a malicious file attachment via e-mail.