Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 29/10/2024	**Entry: 1**
Description	This entry documents a security incident which took place that compromised business operations of a small U.S healthcare clinic where computers were infected with ransomware.
Tool(s) used	-
The 5 W's	• **Who** caused the incident? The incident was caused by an organised group of unethical hackers who are known to target organisations in healthcare and transportation industries • **What** happened? Several employees reported that they were unable to access files/business documents/software which they needed to perform their jobs. It was also reported that a ransom note appeared on employees' computers stating that all files had been encrypted and a considerable sum of money would have to be paid in order to receive the description key, ultimately restoring access. This caused major disruptions in their business operations as the company was forced to shut down their computer systems. • **When** did the incident occur?

	The incident occurred on Tuesday 29th October at 09.00am. • **Where** did the incident happen? The incident occurred at the offices of a small U.S. health care clinic, however this was a ransomware attack and therefore instigated remotely. • **Why** did the incident happen? The security incident took place because employees clicked a malicious attachment sent via targeted phishing emails. This attachment installed malware on the target's computer once it was downloaded. After attackers gained access, they deployed ransomware, encrypting files on the system.
Additional notes	This attack could have perhaps been easily avoided if employees had training or better awareness when utilising email - especially of attachments/links.

Date: 20/10/2024	**Entry:** 2
Description	This entry documents a security incident which took place following a suspicious file download by an employee at a financial services company. Trojan malware had compromised the system. This was confirmed by observing results on VirusTotal.
Tool(s) used	-
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Malicious hacker. • **What** happened?

	Following an alert about a suspicious file being downloaded on an employee's computer. The employee had received an email containing a password-protected spreadsheet file. When the employee downloaded and opened the file a malicious payload was executed on their computer. • **When** did the incident occur? Between 13.1pm and 13.15pm - from receiving the email to the execution of unauthorised files. • **Where** did the incident happen? Employee was on-site but trojan malware authored remotely. • **Why** did the incident happen? Employee inadvertently downloaded a malicious payload following a phishing attack via email.
Additional notes	Investigation began by creating a SHA256 hash of the file. This was then compared with community results on VirusTotal and it was frequently reported to be malicious - a trojan that uses input capture for command and control of systems. Awareness training might be a good way to avoid input capture incidents like this.

Date: 01/11/2024	**Entry:** 3
Description	This entry documents a security incident whereby a suspicious file was downloaded on an employee's computer at a financial services company.
Tool(s) used	-

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The incident was caused by a malicious hacker. • **What** happened? An email was sent to an employee under the guise of a job application. A suspicious file was downloaded on an employee's computer, an executable under the filename "bfsvc.exe". After receiving a phishing alert, the file attachment was hashed and investigated, the results of the investigation established that the attachment has already been verified malicious. • **When** did the incident occur? Email received July 20th 2022 at 09:30 AM. • **Where** did the incident happen? Offices of the financial company, enacted remotely. • **Why** did the incident happen? The email attachment was engaged with by the employee meaning the file was able to install malware.
Additional notes	This was an example of a successful phishing incident. The employee may have benefited from additional awareness, particularly since the email demonstrated key indicators of phishing email, including spelling mistakes within subject line and the body of the text, the obscure email address and the file being .exe rather than a text format.

Date: 05/11/2024	**Entry:** 4
Description	This entry documents a security incident at a mid-size retail company, where a

	malicious actor was able to gain access to customer PII. This resulted in breach of 50,000 customers' data and had a significant impact on company finances.
Tool(s) used	-
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Malicious actor - requested cryptocurrency in exchange for non-disclosure. • **What** happened? An email was sent to an employee describing how the sender had successfully stolen customer data and in return for non-disclosure the company had to pay $25,000 dollars in cryptocurrency. The employee deleted the initial email considering it to be spam. However, a further email was sent 6 days later with a sample of the PII the sender had secured access to, as well as an increased ransom of $50,000. At this point the employee reported the incident to the security team, who subsequently began their investigation between December 28 and December 31, 2022 with the intent of establishing how the data was stolen and the extent of the theft. The security team identified that the malicious actor had managed to conduct a forced browsing attack due to a vulnerability in the e-commerce web application. • **When** did the incident occur? First email received - 15:13 p.m, December 22, 2022. Second email received - December 28, 2022. • **Where** did the incident happen? Email received on-site in company premises, attack initiated through e-commerce web application. • **Why** did the incident happen? A vulnerability within the web application meant the attacker was able to perform a forced browsing attack - access to customer transaction data was achieved by modifying the order number included in the URL string of

	a purchase confirmation page. This meant the attacker was able to gain access to purchase confirmation pages and subsequently gather and exfiltrate customers PII.
Additional notes	The company ensured that the public relations department disclosed that the data breach had occurred to its customers and offered free identity protection services to customers affected by the incident. In order to prevent future occurrences of similar incidents, it is recommended that that company perform vulnerability scans and penetration testing as standard routine. The company could also ilmplement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. Finally, the company should ensure that only authenticated users are authorized access to content.

Date: 05/11/2024	**Entry:** **5**
Description	Potential phishing incident - information investigated using Chronicle (Google Sec Ops)
Tool(s) used	Chronicle - (Now known as Google Security Operations). SIEM tool. Google Security Operations normalises, indexes, correlates, and analyses log data to provide instant analysis and context on unusual activity.
The 5 W's	Capture the 5 W's of an incident. **Who** caused the incident? Malicious actor - unknown

	What happened? Potential phishing incident **When** did the incident occur? First accessed: January 31, 2023 Last accessed: July 09, 2023 **Where** did the incident happen? Remote **Why** did the incident happen? Social engineering - employees inadvertently allowing access by engaging with malicious emails - following links, entering details, downloading files.
Additional notes	The POST information establishes that data was sent to the domain. It also suggests a possible successful phishing attack. POST requests: **2023-01-31** ● 14:40:45 ashton-davidson-pc signin.office365x24.com POST /login.php Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes) ● 14:42:45 emil-palmer-pc signin.office365x24.com POST /login.php Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes) **2023-07-08** ● 05:02:47 ashton-davidson-pc signin.office365x24.com POST /login.php Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes) ● 05:04:47 emil-palmer-pc signin.office365x24.com POST /login.php Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes) **2023-07-09**

	• 05:02:44 ashton-davidson-pc signin.office365x24.com POST /login.php Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes) • 05:04:44 emil-palmer-pc signin.office365x24.com POST /login.php Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes) Furthermore: RESOLVED IP - 40.100.174.34. **2023-01-31** 14:51:45 warren-morris-pc 40.100.174.34 POST /login.php Port:[Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes) Additional domains - signin.accounts-gooqle.com signin.office365x24.com VirusTotal - 12 security vendors flagged this domain as malicious.

Date: 05/11/2024	**Entry:** 6
Description	This log entry documents the use of Spunk to identify possible security issues with a mail server of a small games company.
Tool(s) used	Splunk - SIEM tool. Used for collecting and managing data. In this context, Splunk is used as a cybersecurity tool, but it is used broadly as well for business and web analytics, application management and compliance. Splunk correlates, captures, and indexes log data, creating alerts, dashboards, graphs, reports, and visualizations.

The 5 W's	**Who:** Unknown malicious hacker. **What:** Potential brute force login attack. **When:** 22nd February 2023 - 6th March 2023 **Where:** Remote **Why:** Access to the root account of the email server was attempted but failed. Establishing access could potentially compromise PII.
Additional notes	346 failed SSH login attempts on the root account were documented. Failed login attempts had been made in Feb and March - 287 SSH login attempts (amounting to 82.948%) were made in March alone indicating a suspicious increase in activity in march. This substantial increase in failed login attempts may indicate potential brute force attempts on login systems. It is recommended that Buttercup Games improve the security of their mail server by introducing appropriate access controls. Including authentication tools (such as MFA) or even having lockout procedures in place limiting login attempts made.

Reflections/Notes:

Were there any specific activities that were challenging for you? Why or why not?

Some activities were challenging, especially when using SIEM tools. This is not in reference to how difficult they are to use - on the contrary, I found Splunk and Chronicle quite user friendly. However, I found translating those logs into potential security incidents a bit more challenging. I believe real-world experience of security incidents and what to look for during them is fundamental to translating the data generated by these tools into an actual incident report.

Has your understanding of incident detection and response changed since taking this course?

My understanding has certainly changed, especially with regards to knowing how extensive the

toolkit security teams have at their disposal is. I feel I'm more aware of the means of incident detection and how security teams choose to respond to different incidents.

Was there a specific tool or concept that you enjoyed the most? Why?
I really enjoyed using VirusTotal. I liked how the cybersecurity community can leverage each other's current knowledge of current threats, even down to specifics such as suspect files, urls, IP's and so forth. The GUI is really user friendly and the scoring systems make it easier at a glance to know what security threat (if any) you might be dealing with.