**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:** 06-26-2024 | **Entry: 01** | | |
| --- | --- | --- | --- |
| Description | Primary Care Company Ransomware Event | | |
| Tool(s) used | IDS & Packet Sniffers | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An organized group of unethical hackers who target healthcare and transportation systems * **What** happened? Encrypted critical files in efforts for a ransom via a phishing attack * **When** did the incident occur? 9:00 am Tuesday morning * **Where** did the incident happen? In the email of a company employee * **Why** did the incident happen? To collect a ransom | | |
| Additional notes | How does the team recover files? Backups? copies? | | |

| **Date: 07-24-2024** | **Entry: 02** | | |
| --- | --- | --- | --- |
| Description | Potential Phishing Incident. Alert Ticket # A-2703 | | |
| Tool(s) used | IDS tool and community shared reports via VirusTotal.com | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> * **What** Phishing attack * **When** Wednesday, July 20, 2022 09:30:14 AM * **Where** SERVER - MAIL <hr@inergy.com> <176.157.125.93> * **Why** Gain unauthorized access into an employee account. | | |
| Additional notes | **Known malicious file hash**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b | | |

| **Date: 7-24-2024** | **Entry: 03** | | |
| --- | --- | --- | --- |
| Description | Forced browsing Data Exfiltration | | |
| Tool(s) used | IDS Tool, SIEM Tool | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** Individual Threat Actor * **What** Forced browsing data exfiltration via E-commerce web application vulnerability * **When** December 28, 2022, at 7:20 p.m * **Where** E-commerce web application * **Why** vulnerability in the url string of the E-commerce web application | | |
| Additional notes | Individual was able to force their order number into the url sting of the web application and steal customer PII and financial information. | | |

| **Date: 7-29-2024** | **Entry: 04** | | |
| --- | --- | --- | --- |
| Description | Creating and analyzing a Chronicle search query | | |
| Tool(s) used | Chronicle | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** **signin.office365x24.com 40.100.174.34** * **What** Phishing * **When** 2023-01-31 14:40:45 * **Where** Employee inbox principal.asset.hostname["ashton-davidson-pc"](https://demo.backstory.chronicle.security/search?query=principal.asset.hostname+%3D+%22ashton-davidson-pc%22+nocase&startTime=2023-01-31T14%3A10%3A45.000Z&endTime=2023-01-31T15%3A10%3A45.000Z&alertsSnapshotQuery=feedback_summary.status+%21%3D+%22CLOSED%22&snapshotStartTime=2023-01-31T14%3A38%3A15.000Z&snapshotEndTime=2023-01-31T14%3A43%3A15.000Z&eventTimestamp=2023-01-31T14%3A40%3A45Z&eventIds=AAAAAB0d%2BzKEY%2B49MfdASOHrJRgAAAAABQAAAAEAAAA%3D&overviewEntity=Cg00MC4xMDAuMTc0LjM0EMkBIhAKBgjo0OSeBhIGCIHW5J4G&tab=events) principal.asset.ip[0]["10.200.1.11"](https://demo.backstory.chronicle.security/search?query=principal.asset.ip+%3D+%2210.200.1.11%22&startTime=2023-01-31T14%3A10%3A45.000Z&endTime=2023-01-31T15%3A10%3A45.000Z&alertsSnapshotQuery=feedback_summary.status+%21%3D+%22CLOSED%22&snapshotStartTime=2023-01-31T14%3A38%3A15.000Z&snapshotEndTime=2023-01-31T14%3A43%3A15.000Z&eventTimestamp=2023-01-31T14%3A40%3A45Z&eventIds=AAAAAB0d%2BzKEY%2B49MfdASOHrJRgAAAAABQAAAAEAAAA%3D&overviewEntity=Cg00MC4xMDAuMTc0LjM0EMkBIhAKBgjo0OSeBhIGCIHW5J4G&tab=events) * **Why** Gain unauthorized access into company accounts | | |
| Additional notes | Chronicle uses (UDM) Unified Data Model for normalized logs data format or syntax.  Chronicle uses YARA-L for raw logs data format or syntax  Chronicle can utilize virustotal.com vendor scores, detections, graphs, IoC’s and more for context from within it’s own UI.  POST logs where issued from the principal (employee: ashton davidson) to the target (threat actor).  Target location is in the United Kingdom  Target IP address has alternate IP addresses related to the parent IP.  Target Domain has alternate domains related to the parent Domain | | |

| **Date: 9-28-2024** | **Entry: 05** | | |
| --- | --- | --- | --- |
| Description | Chronicle Search Practice Exercises | | |
| Tool(s) used | Chronicle. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** phishing domain out of United Kingdom / England * **What** Phishing emails were sent out * **When** July 9th 2023 * **Where** [signin.office365x24.com](https://demo.backstory.chronicle.security/domainResults?domain=signin.office365x24.com&selectedList=DomainViewDistinctAssets&whoIsTimestamp=2024-10-09T20%3A00%3A47.932Z) and other resolved domains/ip addresses * **Why** The individual wasn't aware of threat surface. | | |
| Additional notes | Observed sibling ip addresses and domain names.  Checked for GET and POST requests inside of the Expand All timeline view.  Viewed the list of assets in the Legacy View.  Compared VT Context for other ip addresses and events. | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Reflections/Notes:**   1. Were there any specific activities that were challenging for you? Why or why not?   I like to think I have a grasp of the concepts in the course. The packet sniffers and IDS activities weren’t as easy as they might seem. Understanding the syntax of each tool takes the most time i’d say.   1. Has your understanding of incident detection and response changed since taking this course? I don't think my understanding has changed. I don't think I was led astray as to what to expect out of incident detection and response. I like to think of it as a puzzle and I had most of the perimeter finished with a few interior pieces already in the right place. The course just filled in the gaps of knowledge that was missing as well as broadened my perimeter and overall understanding. 2. Was there a specific tool or concept that you enjoyed the most? Why? WireShark as a packet sniffer is really cool. I love how it can monitor within the network and you can customize the configuration however you please. Chronicle is probably my favorite tool so far. |
| --- |