**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:** 06/08/23 | **Entry:** 1 | | |
| --- | --- | --- | --- |
| Description | Incident response to phishing email | | |
| Tool(s) used | None. | | |
| The 5 W's | Who: Unknown hacking group  What: Ransomware  Where: On premise  When: 06/08/23 at 0900 hrs  Why: An unknown group breached the company’s computer systems via a phishing email. The group deployed ransomware to encrypt files after gaining unauthorized access to the system(s). The group left a ransom note demanding money for the decryption key. The motivation appears to be financial. | | |
| Additional notes | Should we publicly flog Bob for clicking on the email just like we told him not to?  Pros v. cons of paying the ransom  Recent enough backups to purge and restore?  What needs to be changed to prevent this in the future? | | |

| **Date:** 06/09/23 | **Entry:** 2 | | |
| --- | --- | --- | --- |
| Description | Incident response to email with malware attachment. | | |
| Tool(s) used | Sha256: Produces a hash value for a file to allow comparison with other files. VirusTotal: Website that allows for submission, analysis, and search of threats. | | |
| The 5 W's | * Who: Unknown hacking group * What: trojan.flagpro/jaik * Where: On premise, employee computer * When: 06/09/23 at 1311 hrs: Email received   1313 hrs: Email download to employee computer, attachment executed.  1315 hrs: Multiple new executables created on computer  1320: IDS detects new executables and alerts SOC   * Why: An unknown group breached the company’s computer systems via an email with a malicious attachment. The attachment was executed by the recipient. The purpose of the malware appears to be to gain additional access and credentials. | | |
| Additional notes | Once again, should we publicly flog Bob?  Has any other systems computers beside’s Bob’s been compromised?  Can we wipe and restore with known good backups?  Why didn’t email security detect the malicious attachment?  Why didn’t endpoint security stop the malicious attachment? | | |

| **Date:** 06/09/23 | **Entry:** 3 | | |
| --- | --- | --- | --- |
| Description | Incident response to phishing email with malware attachment. | | |
| Tool(s) used | VirusTotal: Website that allows for submission, analysis, and search of threats. | | |
| The 5 W's | * Who: Unknown hacking group * What: trojan.flagpro/jaik * Where: On premise, employee computer * When: 07/20/22 at 0930 hrs * Why: Employee received email with confirmed malware attachment. Unknown if malware was executed. Escalated to T2. | | |
| Additional notes | Bob again. Literally the same thing he did last time.  Was Bob’s computer compromised?  Why didn’t email security detect the malicious attachment? | | |

| **Date:** 06/09/23 | **Entry:** 3 | | |
| --- | --- | --- | --- |
| Description | Failed SSH login attempts to ‘root’ on mailsv server | | |
| Tool(s) used | Splunk Cloud: This is a SEIM tool that collects, aggregates, and normalizes log data. It allows for searching and visualization of data. | | |
| The 5 W's | * Who: Unknown hacking group * What: Possible brute force attack * Where: Mailsv server * When: 02/27/23 at 0139 hrs through 03/05/23 at 0139 hrs * Why: Suspicious activity in authentication logs for mailsv server. 346 failed SSH login attempts to account root from multiple IP addresses and ports. There were 221 successful logins by users nsharpe, djohnson, and myuan to root. | | |
| Additional notes | Add firewall rule to autoblock IPs after a certain number of failed attempts  Determine if user accounts were compromised  Determine if mailsv was compromised  Set time and location rules for SSH login  Restore from backups if necessary | | |

| **Date:** 06/09/23 | **Entry:** 4 | | |
| --- | --- | --- | --- |
| Description | Incident response to phishing email | | |
| Tool(s) used | Chronicle: This is a SEIM tool that collects, aggregates, and normalizes log data. It allows for searching and visualization of data. | | |
| The 5 W's | * Who: Unknown hacking group * What: Malicious domain: signin.office365x24.com (known log drop server for stolen credentials) * Where: ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc * When: 01/31/23 from 1440 hrs to 1444 hrs * Why: Employees received phishing emails with malicious links. Six workstations visited the malicious URL. ashton-davidson-pc and emil-palmer-pc sent data to /login.php. Credentials likely compromised. | | |
| Additional notes | Lock affected accounts and require password change.  Confirm 2FA/MFA functioning properly  Retrain affected employees  Add rule to network firewall to block signin.office365x24.com | | |

| **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. | | |

### Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

| Reflections/Notes: The activities were well described with easy to follow step by step instructions. I felt I learned the lessons being taught. My knowledge of incident detection has improved greatly. The SEIM tools were the most interesting. |
| --- |