Journal du gestionnaire d'incidents

Date 2025-08-10	**Entry** #1
Description	Investigation d'un scan de ports suspect sur le serveur web. Phase NIST : **Détection et analyse** (identification via logs Splunk)
Tool(s) used	- Splunk - Nmap
The 5 W's	- **Who** : IP externe 198.51.100.25 - **What :** Scan de ports TCP sur les ports 80, 443, 8080 - **When** 10/08/2025, 14:30 UTC | - **Where** Serveur web (IP 203.0.113.5) | - **Why** Reconnaissance préalable à une attaque potentielle
Additional notes	Activité détectée par une règle Suricata. Aucune exploitation confirmée. IP bloquée au pare-feu.

Date 2025-08-12	**Entry** #2
Description	Analyse d'un fichier "invoice.exe" suspect. Phase NIST : **Éradication** (suppression du malware). Hachage SHA-256 vérifié avec VirusTotal.
Tool(s) used	- VirusTotal - CrowdStrike
The 5 W's	- **Who** : Campagne de phishing - **What :** Téléchargement d'un Emotet par un utilisateur - **When** 12/08/2025, 09:15 UTC - **Where** Poste utilisateur - **Why** Vol de données d'identification
Additional notes	Taux de détection : 58/70 sur VirusTotal. Playbook d'éradication exécuté.

Date 2025-08-13	**Entry** #3
Description	Capture de trafic réseau avec Wireshark lors d'une alerte. Phase NIST : Préparation. Filtrage des paquets pour identifier du trafic HTTP anormal.
Tool(s) used	- Wireshark - Suricata

Additional notes	Faux positif : trafic lié à un test interne. Documentation mise à jour pour affiner les règles.

Date 2025-08-15	**Entry** #4
Description	Requête Splunk pour corréler des échecs de connexion. Phase NIST : Détection (identification de tentatives de brute force).
Tool(s) used	Splunk
Additional notes	152 tentatives depuis l'IP 203.0.113.42. Comptes vulnérables réinitialisés. Alerte automatisée créée.