INCIDENT HANDLER'S JOURNAL

Vanesa Sierra

Entry #1 — Incident Investigation (5 W's)

Date: 2025-06-10
Title: Phishing Email Investigation

Description:
Durante un ejercicio de laboratorio, identifiqué y analicé un posible intento de phishing mediante un correo sospechoso. Utilicé los 5 W para estructurar la investigación y documenté los hallazgos según el marco NIST.

5 W's:

- **Who**: Usuario final reportó el correo (empleado del departamento de Finanzas).
- **What**: Correo fraudulento con enlace malicioso simulando ser una factura pendiente.
- **When**: 10 de junio de 2025 a las 09:42h.
- **Where**: Correo electrónico corporativo (`finance@empresa.com`)
- **Why**: Intento de robar credenciales mediante una página de login falsa.

NIST Phase: Detection and Analysis
El incidente fue detectado por el usuario y analizado utilizando herramientas de sandboxing y reputación de URLs.

Entry #2 — Incident Investigation (5 W's)

Date: 2025-06-20
Title: Ransomware simulación en laboratorio de entrenamiento.

Description:
Participé en una simulación de un ataque de ransomware. Documenté cómo se propagó, qué sistemas se vieron comprometidos y cómo se ejecutó la contención y recuperación siguiendo el ciclo de NIST.

5 W's:

- **Who**: Atacante simulado accedió mediante credenciales filtradas.
- **What**: Encriptación de archivos críticos del sistema.
- **When**: 20 de junio de 2025, a las 15:10h.
- **Where**: Red interna del entorno de laboratorio.
- **Why**: Simulación para evaluar tiempos de respuesta y protocolos de recuperación.

NIST Phase: Containment, Eradication, and Recovery
Se aplicaron acciones de contención con backups, se aisló el sistema afectado y se restauraron datos.

Entry #3 — Cybersecurity Tool (Suricata)

Date: 2025-07-22
Title: Traffic inspection with Suricata

Description:
Usé **Suricata** como IDS para analizar tráfico de red en un laboratorio. Observé cómo las firmas generaban alertas, comprendí la estructura EVE JSON y aprendí a personalizar reglas.

Actions Taken:

- Se ejecutó Suricata sobre una captura `.pcap`.
- Se interpretaron logs de alerta para detectar patrones maliciosos.
- Se modificaron reglas con `sid` personalizado.

NIST Phase: Detection and Analysis
Esta herramienta permite detectar patrones maliciosos en tráfico, parte esencial de la fase de análisis.

🛠️ Entry #4 — Cybersecurity Tool (Splunk)

Date: 2025-07-24
Title: Search and correlation with Splunk SPL

Description:
Realicé consultas en **Splunk** usando SPL para analizar registros de eventos. Me centré en buscar actividad anómala como múltiples intentos fallidos de login, correlacionar logs y visualizar eventos.

Actions Taken:

- Consultas con `index`, `source`, `sourcetype`.
- Uso de filtros como `status="failed"` y `action="block"`.
- Generación de gráficos para análisis visual.

NIST Phase: Detection and Analysis
Splunk facilita la agregación y análisis de eventos para detectar amenazas en tiempo real.