Actividad: Reflexión y Resumen sobre la Unidad de Seguridad Informática

Nicolás Ruiz Ruiz

Incidentes de ciberseguridad

Introducción

Segunda actividad resumen del temario que hacemos en la asignatura, en esta ocasión, debo hacer una reflexión del tema de "*Detección y análisis de incidentes de seguridad*". Voy a basarme un poco en el anterior, aplicando las correcciones, pero siguiendo la estructura planteada en los criterios.

¿Qué te han parecido los temas tratados?

En general, esta unidad me ha gustado mucho más que la primera, tenía temas mucho más prácticos, también con su teoría obviamente. Voy a tratar de resumir cada tema y explicar qué he entendido de estos.

Taxonomía de incidentes

Este tema, junto con el siguiente, son los 2 temas teóricos de la unidad. Este se centra en clasificar los incidentes de una manera efectiva para lograr entenderlos y conseguir una respuesta a estos eventos. A la hora de clasificarlos, debemos tener en cuenta varios factores: tipo de amenaza, origen, sistemas afectados, usuarios afectados, impacto e implicaciones legales; estos factores determinan el tipo de incidente.

La taxonomía vista en el tema, es la usada por el INCIBE, y contiene los siguientes tipos:

1. Contenido abusivo.
   Incluye spam, delitos de odio y material explicito como pornografía infantil o violencia.
2. Contenido dañino o malicioso.
   Se refiere a virus, troyanos, botnets y malware utilizado para infectar o comprometer sistemas.
3. Obtención de información.
   Métodos como escaneo de redes, sniffing e ingeniería social para obtener datos sensibles.
4. Intento de intrusión.
   Ataques que buscan acceso no autorizado a los sistemas mediante vulnerabilidades conocidas, credenciales débiles y ataques zero day.
5. Intrusión.
   Compromiso efectivo de sistemas, cuentas o aplicaciones mediante ataques o explotación de vulnerabilidades.
6. Disponibilidad.
   Ataques (D)DoS, sabotajes y errores de configuración que afectan la disponibilidad de servicios.
7. Compromiso de la información.
   Acceso, modificación, pérdida o fuga de datos de manera no autorizada.
8. Fraude.
   Suplantación de identidad, phishing, uso no autorizado de recursos y violación de derechos de autor.

9. Vulnerable.
   Sistemas o servicios con fallos de seguridad, criptografía débil o expuestos a ataques DDoS.
10. Otros.
    Amenazas avanzadas (APT), ciberterrorismo, ataques a infraestructuras críticas y reportes que no pertenezcan a ninguna de las anteriores.

Además de clasificarlos, tenemos que darle una peligrosidad, un impacto y una prioridad, de esta forma podremos saber qué incidentes hay que solucionar en seguida, o no toman prisa. La peligrosidad va ligada al tipo de incidente, por ejemplo, **Taxonomía** Otros, **Tipo** Amenaza avanzada, tiene una **peligrosidad** crítica. El impacto va ligado a quien o que afecte, por ejemplo, si **Afecta a más del 50% de los sistemas de la organización**, tiene un **Impacto** alto. Estos datos no me los he inventado yo, vienen en la "*GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES*". Por último, la peligrosidad se calcula con la siguiente tabla:

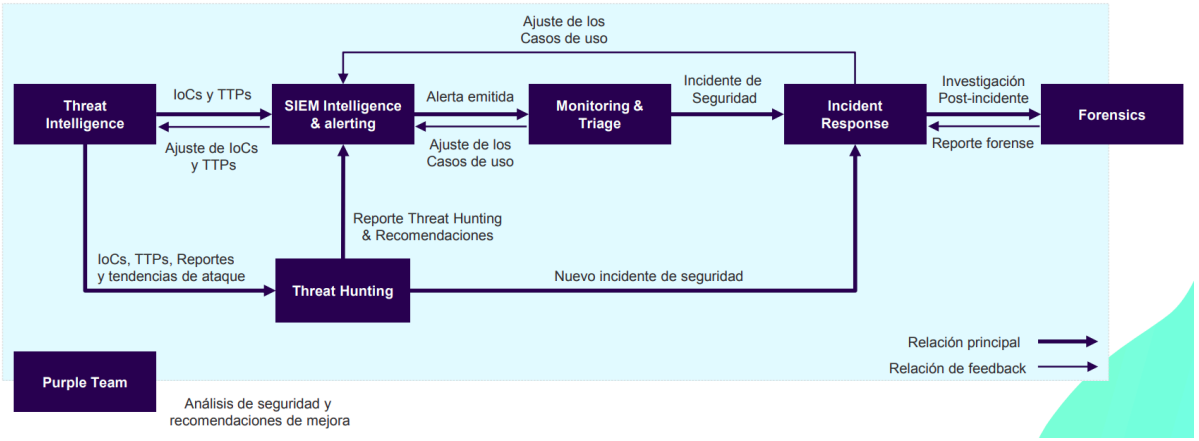
Peligrosidad Impacto	L1: Bajo	L2: Medio	L3: Alto	L4: Muy Alto	L5: Crítico
1: Bajo	Baja	Baja	Media	Media	Alta
2: Medio	Baja	Media	Media	Alta	Alta
3: Alto	Media	Media	Alta	Alta	Emergencia
4: Muy Alto	Media	Alta	Alta	Emergencia	Emergencia
5: Crítico	Alta	Alta	Emergencia	Emergencia	Emergencia

En resumen, la taxonomía de los incidentes se hace para tener un control de estos, saber cómo y cuándo actuar, además, podríamos hacer un control de que incidentes son más propensos en la organización e intentar pensar el porqué.

SOC - Servicios y herramientas

Segundo y último tema de teoría de la unidad. En este tema vemos que es un SOC y las herramientas que usa. Empecemos explicando ¿qué es un SOC? Se trata de un centro de operaciones centralizado diseñado para detectar, responder y prevenir amenazas de seguridad. Para cumplir con estos objetivos, los SOC hacen uso de varias herramientas, entre las que destacan los SIEM, para recopilar eventos; SOAR, que automatizan tareas de respuesta; Threat Intelligence, usada para recopilar información sobre amenazas; monitoreo de red; IDS, detecta intrusos; IPS, previene intrusos; ticketing, para asignar tareas; y análisis forense, para analizar equipos una vez ocurrido un evento.

Pero un SOC no solo está compuesto por herramientas, también tienen equipos encargados de varios servicios:



[Créditos a Eduardo]

En la imagen vemos 3 servicios que no expliqué antes:

- Purple Team: Una mezcla de “Red Team” y “Blue Team” que se encarga precisamente de lo mismo que estos, simular ataques y crear defensas.
- Threat Hunting: Busca complementar a las herramientas automáticas de detección de vulnerabilidades.
- Incident Response: Que gestiona incidentes para mitigar el impacto de estos.

Además de esto, en el tema se explican los siguientes términos:

- CERT: Responde ante las emergencias de ciberseguridad.
- CIRT: Se centra en la gestión de incidentes de seguridad.
- CSIRT: Es una variante del CIRT que incluye políticas de seguridad.

Es decir, son equipos que en la teoría son diferentes, pero en la práctica, todos pueden, o van a tocar los asuntos de los otros.

Me lo reservo para una de las preguntas, pero este puede ser el tema más interesante.

SIEM

No quise profundizar mucho antes para desarrollarlo aquí, un SIEM es un sistema que ayuda al SOC a detectar y analizar amenazas, de esta forma es mucho más fácil responder ante ellas antes de que afecten a la organización. Consiste en la combinación de SIM, administración de información de seguridad; y SEM, administración de eventos de seguridad. Un SIEM no vale por sí solo, se deben crear casos de uso, que en resumen, son casos específicos en el que se especifica cómo detectar, analizar y responder ante una amenaza. Para crear estos casos, debemos seguir varios varios puntos, y para explicarlos mejor, voy a utilizar como ejemplo un ataque DDoS:

- Identificar una amenaza: Ataque de denegación de servicio.
- Definir el escenario: El atacante podría usar una botnet para atacar los sistemas.
- Identificación de fuentes de datos: Registros de conexiones ICMP(hping).

- Definición de indicadores de compromiso: Conexiones masivas ICMP de varias IPs diferentes al mismo tiempo, o la misma IP.
- Creación de reglas y alertas: El propio nombre lo dice -_-
- Definición de procedimientos de respuesta: Determinar si es o no un falso positivo, y en caso de serlo, bannear las direcciones IP.
- Validación y ajuste: Probar pequeños ataques DDoS con herramientas como hping, para ver cómo se comporta el sistema.
- Monitorización continua y mejora: En caso de que ya no sea necesario, borrar la alerta.

También, montamos un SIEM nosotros mismos con snort, que nos permitía detectar comportamientos extraños en la red; filebeat, que recolectaba y enviaba las alertas creadas por el snort; y elasticsearch, que se encargaba de almacenar y mostrar gráficamente estas alertas; y, aunque costó un poco montarlo, se consiguió integrar cada una de las herramientas vistas. Además, esta práctica se complementa con una propuesta en *Bastionado de Redes* que consistía en hacer exactamente lo mismo, documentar la instalación de 2 sistemas de monitorización y añadirle un par de clientes. Yo monté Prometheus y Checkmk.

La mejor forma de entender lo que es un SIEM es con esta escena de Toy Story 3 https://www.youtube.com/watch?v=EBJOK9iAh6A

Fuentes Abiertas. OSINT

El OSINT consiste en el uso de técnicas y herramientas para recopilar información de personas u organizaciones usando fuentes públicas. OSINT no solo se usa para *stalkear* o *doxear* a la gente, si no que también lo podemos usar para:

- Auditorías de seguridad e investigación forense: Identificando información expuesta, vulnerabilidades y recolectar evidencias tras incidentes.
- Pentesting y hacking ético: Recolectar información, sin hacer escaneos(activo), haciendo uso de Google Dorking, metadatos y búsquedas en redes sociales.
- Prevenir ataques y Threat Intelligence: Ver filtraciones en la deep web, analizar ciberdelincuentes y monitorear amenazas en foros y redes.

Antes dije activo, haciendo referencia a la realización de escaneos. El OSINT no recoge ningún tipo de técnicas que interactúen directamente con la organización/persona que estamos analizando, se conoce como una técnica pasiva en la que intentamos ser lo más silencioso posible.

Tenemos un montón de herramientas para hacer OSINT, tantas que explicarlas una a una es una pérdida de tiempo, por eso mismo, la comunidad creó *OSINT Framework* una plataforma digital que recopila todas las que existen.

Por último, para llevar a cabo una buena investigación no solo basta con buscar el nombre en internet, tenemos que seguir estás 6 fases:

1. Planificación y dirección: Definir objetivos y estrategias para la recopilación de información.

2. Identificación de fuentes: Localizar los medios y plataformas donde se encuentra la información relevante.
3. Adquisición de información: Recopilar los datos de manera estructurada y eficiente.
4. Procesamiento y organización: Filtrar, clasificar y estructurar la información recopilada.
5. Análisis e interpretación: Evaluar la información, identificar patrones y extraer conclusiones.
6. Difusión y aplicación de la inteligencia: Presentar los hallazgos de manera útil y accesible.

Con todo esto en mente, se nos planteó hacerle OSINT tanto a un hospital gaditano como a un compañero de la clase, donde pudimos testear las herramientas planteadas, y creo que todos llegamos a la conclusión de que, si no pagas, hacer OSINT es muy complicado, ojo, se puede hacer perfectamente, pero las herramientas de pago te hacen el trabajo mucho más rápido.

¿Qué te ha parecido más útil para tu futuro puesto de trabajo en un equipo de seguridad?

Basándome un poco en los compañeros de años pasados que vinieron a contar sus experiencias en el sector profesional, creo que los temas relacionados con SOCs son los más importantes. Saber identificar los niveles 1,2 y 3; la retroalimentación de los equipos; como funcionan los SIEM… creo que son cosas muy importantes que, por ejemplo, en una entrevista de trabajo, deberíamos de saber cómo el padre nuestro.

¿Conocías todos los puntos tratados en la unidad?¿Cuáles no?

Sinceramente, no conocía ningún tema o, al menos, no de manera consciente. Por ejemplo, siempre he utilizado Google Dorks para mejorar mis búsquedas,o para encontrar imágenes que no estén creadas por IA, y no sabía que se trataba de una técnica OSINT.

¿Alguno te ha llamado especialmente la atención? ¿Por qué?

Si, el tema de OSINT me ha interesado muchísimo, porque explica 2 temas que me parecen interesantes. El primero es como buscar información concreta en internet, es increíble que en 2025 con coches que se manejan solos, buscar información en internet sea algo tan complicado, todo por culpa del SEO y del posicionamiento web, pero aplicando técnicas OSINT la búsqueda de información se vuelve simple y rápida. Y segundo, la huella digital que tenemos todos es más grande de lo que creemos, no sólo influye lo que publiques en internet, si no también lo que otros publiquen sobre tí, todo sirve para recopilar información.

¿Descartarías algún punto de la unidad? ¿Cuál y por qué?

No, pienso que todos los temas tratados en la unidad son importantes para nuestro desarrollo profesional. Sabiendo que es muy probable que en el futuro trabajemos en un SOC, todo lo que podamos ver en esta unidad es clave.

¿Has echado en falta algún tema?

No realmente, aunque, para no repetir lo que dije en la entrega anterior, me habría gustado profundizar en las herramientas utilizadas, muchas de ellas eran complejas de usar o ya de paso no funcionaban, o no sabía usarlas correctamente.