Cybersituational Awareness - Appunti

Francesco Lorenzoni

Febrero 2025

Contents

Chapter 1

20 conceptos más relevantes

1.1 Fundamentos de la Ciberconciencia Situacional

1. **Ciberconciencia Situacional (CS)**
   La conciencia situacional en el ciberespacio es el concepto fundamental definido como *"la capacidad de saber lo que está sucediendo en el ciberespacio"*. Es esencial porque constituye la base para comprender y reaccionar a las amenazas cibernéticas de manera oportuna y eficaz. Además, la CS no solo es relevante para la detección de amenazas, sino también para la optimización de recursos de seguridad, permitiendo priorizar esfuerzos donde realmente se necesitan y evitar la fatiga de alertas que afecta a muchos equipos de seguridad.
   Definition 1.1 (Situational Awareness) *Situational awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*
2. **Ciclo cognitivo de la CS**
   El ciclo de la CS se compone de adquisición de datos, procesamiento, análisis, distribución y acción. Este ciclo continuo es fundamental porque representa el flujo completo de información desde su captación inicial hasta la toma de decisiones basada en ella, garantizando que la CS sea un proceso dinámico y no un estado estático. La efectividad de cada fase impacta directamente en la calidad general de la conciencia situacional, donde fallos en cualquier punto pueden crear puntos ciegos críticos para la seguridad organizacional.
   i. **Fase de percepción**
      Primera etapa del modelo de Endsley donde se capturan los datos relevantes del entorno cibernético. Esta fase es crucial porque establece la base informativa sobre la cual se construirá toda interpretación posterior. Una percepción incompleta o distorsionada inevitablemente conducirá a una CS defectuosa independientemente de la sofisticación del análisis posterior. La percepción requiere tanto amplitud como profundidad de visibilidad en el entorno digital para capturar patrones y anomalías significativas.
   ii. **Fase de comprensión**
      Segunda etapa donde se sintetizan y contextualizan los datos percibidos para crear información significativa. Su importancia radica en transformar datos aislados en un panorama coherente que revela relaciones, patrones y desviaciones significativas. Este proceso integra el conocimiento previo con los datos actuales para determinar la relevancia y el significado de los eventos observados, distinguiendo entre actividades normales y potenciales indicadores de amenaza.
   iii. **Fase de proyección**
      Tercera etapa que permite anticipar estados futuros basados en la comprensión actual de la situación. Es vital porque transforma la CS de una herramienta puramente descriptiva a una predictiva, permitiendo a las organizaciones pasar de posiciones reactivas a proactivas. La capacidad de proyectar escenarios futuros probables permite anticipar movimientos de atacantes, priorizar vulnerabilidades según la probabilidad de explotación, y asignar recursos defensivos antes de que ocurran los incidentes.

3. **Situation Understanding**
   El entendimiento situacional va más allá de la simple conciencia situacional, y se refiere a, dada una situació, comprender las posibles consecuencias y predecir eventos futuros. Es relevante porque permite anticipar las amenazas antes de que se materialicen completamente. Mientras que la conciencia situacional responde a la pregunta *"¿qué está sucediendo?"*, el *entendimiento situacional* busca responder *"¿por qué está sucediendo y qué podría ocurrir después?"*. Esta profundidad adicional de análisis es fundamental en el complejo entorno cibernético, donde las relaciones causa-efecto no siempre son evidentes y donde un solo indicador puede ser parte de un ataque multifacético más amplio.
4. **Sensemaking**
   Incluye las actividades cognitivas necesarias para desarrollar conciencia, comprensión y traducirlas en acciones. Es fundamental porque conecta la conciencia con la acción concreta en el dominio cibernético. El proceso de

sensemaking representa el puente crítico entre la observación pasiva y la respuesta activa, transformando el conocimiento abstracto en decisiones operativas tangibles. Este proceso involucra la contextualización de la información dentro de marcos mentales preexistentes, la resolución de ambigüedades y contradicciones, y la creación de narrativas coherentes que expliquen los eventos observados.

1.2 Componentes estructurales de la CS

5. **Network Awareness**
   Componente fundamental que proporciona conocimiento completo sobre los sistemas, redes y activos digitales propios. Es esencial porque establece la línea base para detectar anomalías y determinar el estado normal de operación.
   Además, un apropiado particionamento de la red y una segmentación adecuada son una de las primeras líneas de defensa contra las amenazas, y son cruciales para limitar el alcance de un ataque y contener su propagación.
6. **Threat Awareness**
   Conocimiento sobre las amenazas actuales, emergentes y potenciales que podrían afectar a la organización. Su importancia radica en proporcionar contexto sobre los actores maliciosos, sus capacidades, motivaciones y tácticas, permitiendo una defensa orientada específicamente a las amenazas más probables y peligrosas para cada entorno particular.
   Además, conocer las amenazas permite también de mejorar el Situation Understanding, y por tanto también la capacidad de predicir las consecuencias de una determinada situación.
7. **Mission Awareness**
   Comprensión de cómo los activos y procesos cibernéticos se relacionan con los objetivos organizacionales críticos. Es crucial porque alinea las actividades de ciberseguridad con el valor empresarial, permitiendo priorizar la protección de los sistemas y datos que realmente importan para la continuidad y éxito de la misión organizacional. Sin esta perspectiva, las organizaciones pueden desperdiciar recursos protegiendo activos de bajo valor mientras dejan vulnerables componentes críticos para la misión.

1.3 Colaboración y visualización en CS

8. **Common Operational Picture (COP)**

   " A single identical display of relevant (operational) information (e.g. position of own troops and enemy troops, position and status of important infrastructure such as bridges, roads, etc.) shared by more than one Command. " — wikipedia

   Es fundamental porque proporciona una base común para la conciencia situacional a todos los niveles de mando. La COP trasciende la mera representación visual para convertirse en un marco referencial compartido que asegura que todos los actores involucrados en la ciberseguridad interpreten la situación desde una misma perspectiva informativa.
   La COP se aplica tipicamente en el contexto militar, pero su concepto se ha extendido a la ciberseguridad, donde la necesidad de una visión unificada y coherente de la situación es igualmente crítica.
9. **Visualización de ciberinteligencia**
   Las técnicas de visualización son fundamentales para representar eficazmente el ciberespacio, compuesto por grandes cantidades de datos complejos y multidimensionales, ayudando a analistas y decisores a identificar rápidamente patrones y anomalías. En el contexto de la ciberdefensa, donde los conjuntos de datos pueden incluir millones de eventos por segundo, las representaciones visuales adecuadas transforman masas amorfas de datos en estructuras comprensibles. Hemos visto muchas técnicas de visualización, que no son equivalentes, y es importante también elegir la más adecuada para cada contexto, de lo contrario, los datos podrían seguir siendo incomprensibles o de poca utilidad..

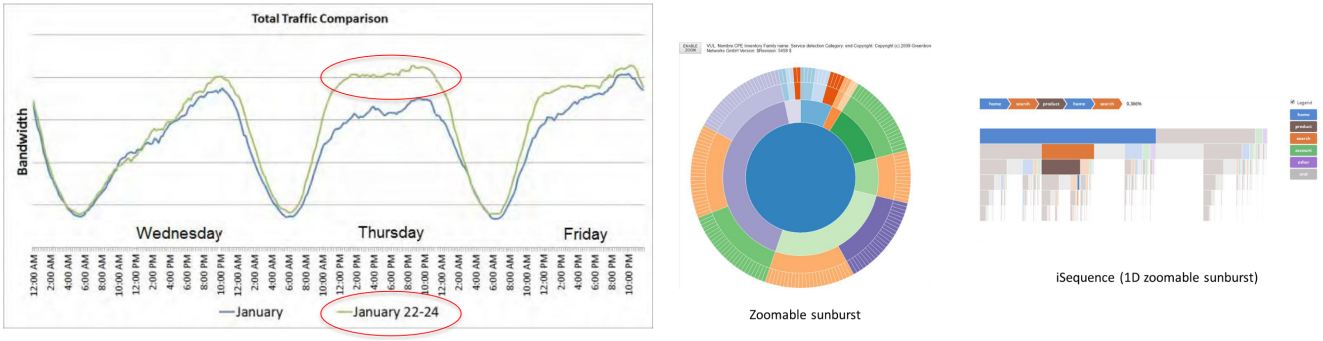

Figure 1.1: Ejemplos de visualización de datos

10. **Gestión de la sobrecarga informativa**
    Esto se refiere a la importancia de estrategias y técnicas para filtrar, priorizar y presentar solo la información relevante para cada contexto y rol.

    Los sistemas efectivos de CS implementan mecanismos de filtrado contextual, agregación inteligente y destacado adaptativo de anomalías para garantizar que cada nivel decisional reciba exactamente la información necesaria en el momento oportuno. Claro que esto incluye también técnicas de visualización, pero no se limita a eso. La *Mission Awareness*, puede ayudar a determinar qué información es relevante para cada contexto y, por tanto, también a filtrar la información con mayor eficacia.

1.4 Análisis y gestión de riesgos

11. **Factores de riesgo**
    Amenazas, vulnerabilidades, impacto, probabilidad, y condición predisponente son elementos clave para cuantificar y priorizar los riesgos en el ciberespacio. Estos cinco componentes interrelacionados forman el marco fundamental para una evaluación del riesgo cibernético, permitiendo transformar conceptos abstractos en métricas comparables y accionables. Cada uno de estos se puede descomponer en subcomponentes más específicos, proporcionando un nivel de detalle que permite una evaluación más precisa y granular de los riesgos. Por ejemplo, las amenazas pueden dividirse en fuentes de amenaza y eventos de amenaza, mientras que las vulnerabilidades pueden clasificarse según su naturaleza (técnica, humana, organizativa) o su ubicación (sistemas, procesos, infraestructura).
    El riesgo es una función de la probabilidad de que se produzca una amenaza y del impacto potencial que sufrirá un activo si se produce el suceso. El riesgo suele representarse como un valor único, normalmente decimal, o como un vector en el que se evalúan aisladamente distintos tipos de impactos.

    $$risk(e) = probability(e) \times impact(e)$$

    El impacto también puede medirse utilizando la degradación, es decir, el porcentaje % del activo afectado que se pierde

    $$impact(e) = value(asset) \times degradation(asset)$$

12. **Análisis de consecuencias**
    Las técnicas para evaluar el impacto de los ataques cibernéticos son cruciales para comprender las potenciales repercusiones operativas y estratégicas de las amenazas. Por ejemplo, hemos mencionado grafos de ataque que representan las relaciones entre vulnerabilidades y cómo los ataques pueden propagarse a través de múltiples sistemas. Estos gráficos permiten visualizar la complejidad de los ataques y sus posibles consecuencias en cascada, facilitando la identificación de puntos críticos.
    En el video sobre los sistemas idraulicos de una tarea, se menciona una herramienta para simular el estado fisico de un sistema, permitiendo de determinar diferencias entre el estado expectado y el real, y así detectar problemas.

1.5 Herramientas y tecnologías para la CS

13. **Sensores cibernéticos**
    Estos son las fuentes de datos que alimentan los sistemas CS son cruciales porque determinan la calidad y la integridad de la información disponible para el análisis.
    Estos sensores constituyen la primera fuente de ciber inteligencia de la organización, abarcando desde sistemas de detección de intrusiones de red y host, monitores de tráfico encriptado, analizadores de comportamiento de usuarios y entidades (UEBA), hasta honeypots y sistemas señuelo diseñados para atraer y estudiar actividades maliciosas.
14. **Posicionamiento de sensores**
    El posicionamiento estratégico de sensores es esencial para maximizar la cobertura y minimizar los puntos ciegos en la red.
    El diseño de la arquitectura de sensores debe considerar factores como la topología de la red, los flujos de tráfico, y las áreas críticas que requieren monitoreo intensivo.
    Un posicionamiento inadecuado puede resultar en una falta de visibilidad en áreas críticas, permitiendo que los atacantes de hacer daños graves.
15. **SIEM (Security Information and Event Management)**
    Estos sistemas centralizados son fundamentales para la recopilación, correlación y análisis de eventos de seguridad procedentes de diferentes fuentes en la red. Los SIEM actúan como el centro neurálgico de las operaciones de seguridad, proporcionando una plataforma unificada donde convergen datos estructurados y no estructurados de múltiples sistemas para crear un contexto coherente. Su capacidad para normalizar datos heterogéneos facilita la detección de patrones y anomalías que serían imposibles de percibir examinando cada fuente aisladamente.

Hemos visto que los SIEM son herramientas potentes, pero no son la solución definitiva para la CS. Aunque proporcionan una base sólida para la recopilación y análisis de datos, su eficacia depende de la calidad de los datos que reciben y de la capacidad de los analistas para interpretar correctamente los resultados.

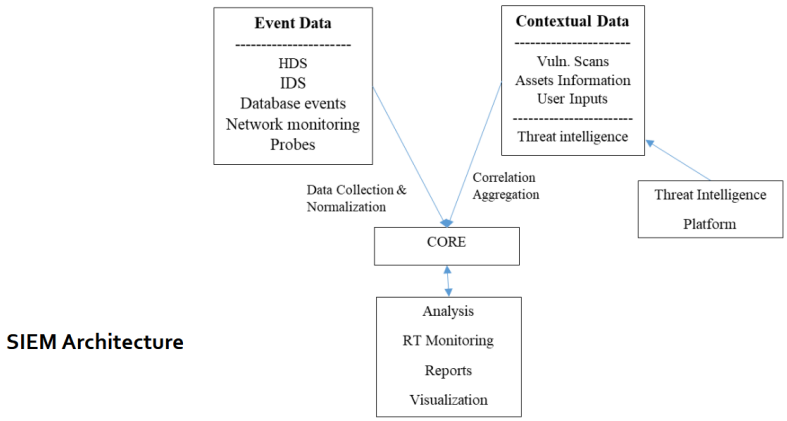

Figure 1.2: SIEM esquema

1.6 Dominios físicos y cibernéticos

16. **Cyber Hybrid Situational Awareness**
La integración de la conciencia situacional física y cibernética es esencial porque reconoce que los eventos en un dominio influyen en el otro, proporcionando una visión más completa de las amenazas modernas. Este enfoque híbrido responde a la creciente convergencia entre los mundos físico y digital, donde las fronteras tradicionales se difuminan con la proliferación de dispositivos IoT, sistemas de control industrial conectados y tecnologías operativas digitalizadas. La visión integrada permite detectar amenazas compuestas que utilizan vectores tanto físicos como digitales.
17. **Georreferenciación de activos**
La vinculación de activos cibernéticos con elementos físicos es esencial para la situational awareness híbrida, permitiendo visualizar las interdependencias entre el mundo físico y digital. Esta capacidad de localizar precisamente los recursos digitales en el espacio físico proporciona un contexto crucial para interpretar eventos de seguridad, especialmente en organizaciones con presencia geográficamente distribuida o infraestructuras complejas. La georreferenciación permite correlacionar incidentes cibernéticos con eventos físicos próximos.

1.7 Ciberinteligencia para mejorar la CS

18. **Estándares para caracterización e intercambio de información**
Los marcos estandarizados como `STIX`, `TAXII`, `OpenIOC` y `MITRE ATT&CK` son esenciales para garantizar la interoperabilidad y consistencia en la comunicación de información sobre amenazas entre diferentes organizaciones y herramientas. Estos estándares proporcionan un lenguaje común y estructuras de datos unificadas que permiten la automatización en el procesamiento e incorporación de inteligencia externa, eliminando la necesidad de conversiones manuales propensas a errores y reduciendo significativamente el tiempo entre la *identificación de una amenaza* y la *implementación de defensas correspondientes.*
19. **Fuentes de Ciberinteligencia**
La recopilación eficaz de información para la CS se basa en cuatro fuentes fundamentales de inteligencia: `HUMINT` (inteligencia humana), `OSINT` (inteligencia de fuentes abiertas), `SIGINT` (inteligencia de señales) y `TECHINT` (inteligencia técnica). Esta diversificación de fuentes es crucial porque cada una aporta una perspectiva única y complementaria sobre el panorama de amenazas. La `HUMINT` proporciona información valiosa sobre intenciones, motivaciones y capacidades de actores maliciosos a través de contactos personales y redes de informantes. La `OSINT` aprovecha la abundancia de información disponible públicamente para identificar tendencias emergentes, vulnerabilidades recién descubiertas y campañas de ataque en curso. La `SIGINT` permite detectar patrones anómalos en las comunicaciones y el tráfico de red que pueden indicar actividades maliciosas. Finalmente, la `TECHINT` analiza los artefactos técnicos de ataques (malware, exploits, infraestructura) para comprender las capacidades técnicas de los adversarios y desarrollar contramedidas efectivas.
20. **Sistemas de Respuesta a Incidentes**
Los sistemas de respuesta a incidentes son plataformas especializadas que permiten la inserción, almacenamiento y gestión centralizada de incidentes de seguridad, facilitando la coordinación de respuestas efectivas. Son fundamentales porque proporcionan un marco estructurado para el seguimiento completo del ciclo de vida de los

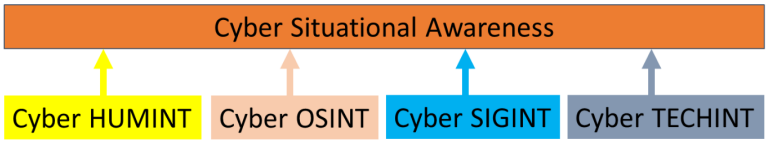

Figure 1.3: Ciberinteligencia

incidentes, desde su detección inicial hasta su resolución y el análisis posterior. Estos sistemas están diseñados para integrarse con `TIPs` (Plataformas de Inteligencia de Amenazas) y `SIEMs`, creando un ecosistema cohesivo de herramientas de seguridad. Ayudan a los miembros del *Computer Incident Response Team* (`CIRT`) a gestionar adecuadamente los incidentes, proporcionando gestión de flujos de trabajo y registros detallados sobre qué ocurrió, cuándo y cómo, tanto respecto al incidente como a la respuesta implementada. La documentación meticulosa que facilitan estos sistemas es invaluable para el aprendizaje organizacional, permitiendo refinar continuamente los procedimientos de respuesta basándose en experiencias previas y adaptarse a tácticas de ataque en evolución.

21. **Gráficos de escenarios de ataque**
    Los *attack scenario graphs* son una herramienta avanzada de visualización que representa las relaciones entre las vulnerabilidades de un sistema y muestra cómo pueden desarrollarse ataques multi-etapa. Son fundamentales para la CS porque permiten anticipar posibles rutas de compromiso antes de que sean explotadas por atacantes. Estos gráficos pueden vincularse con `software dependency graphs` para visualizar cómo un paso de ataque a un componente puede afectar a otros componentes dependientes, creando un modelo completo de la superficie de ataque. La representación visual de estas relaciones facilita la identificación de puntos críticos donde una sola vulnerabilidad podría desencadenar efectos en cascada a través de múltiples sistemas. Esta perspectiva estructurada supera las limitaciones de los enfoques tradicionales que solo consideran vulnerabilidades individuales, permitiendo priorizar defensas basadas no solo en la gravedad de vulnerabilidades aisladas, sino también en su posición estratégica dentro de posibles cadenas de ataque.
22. **Niveles de mando CS: Táctico, Operativo y Estratégico**
    La subdivisión de la conciencia situacional en los niveles táctico, operativo y estratégico es crucial porque permite adaptar la información a las necesidades específicas de los diferentes niveles decisionales. El nivel *táctico* (a veces llamado `técnico`) se enfoca en visualizar y gestionar eventos relacionados con activos específicos, requiriendo información detallada y técnica para la detección y respuesta inmediata a incidentes. El nivel *operativo* busca sintetizar los detalles del nivel táctico y contextualizarlos en términos de su impacto en la misión organizacional, facilitando la coordinación de múltiples acciones tácticas dentro de un marco temporal más amplio. El nivel *estratégico* requiere información abstracta y contextualizada sobre el panorama general de amenazas y su posible impacto en los objetivos organizacionales a largo plazo, permitiendo la planificación defensiva, la asignación de recursos y el alineamiento con requisitos regulatorios. Esta estructura jerárquica asegura que cada nivel reciba la información con el grado apropiado de detalle y abstracción.