UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Ciberconciencia Situacional

2024/2025

Prof. Esteve Domingo, Manuel

Trabajo 2

Security Operation Center

Contents

Chapter 1

Trabajo 2 - SOC

Soy un estudiante italiano en Erasmus. Hablo español bastante bien, pero me resulta más natural escribir en inglés; sin embargo, decidí escribir en español para practicar, con la ayuda de algunos traductores cuando era necesario. Si hay algo mal escrito o poco claro, estoy a disposición para cualquier aclaración.

Tarea a realizar

- Visualiza este video
- Identifica las funcionalidades que en el video se atribuyen a un SOC
- Para cada una de las funcionalidades definidas, indica que posibles herramientas de ciberinteligencia podrían implementar estas funcionalidades, de entre las herramientas analizadas tanto en las clases teóricas como en las prácticas de esta asignatura y asignaturas previas.
- ¿Consideras que alguna funcionalidad propia de un SOC no ha sido incluida en el vídeo? Indica cual o cuales. Puedes utilizar el documento adjunto como apoyo a tu respuesta.

1.1 Introdución

SOC significa Security Operations Center. La finalidad de un SOC es proteger la información de una organización, detectando y respondiendo a ciberataques.

Definition 1.1 (SOC - Cyviz) *The fundamental aspects of an effective SOC is the ability to examine and **analyze** big and sensitive data flows, and to **correlate** other incidents from a cybersecurity perception. Security operations teams need appropriate tools and techniques to process, visualize and correlate the enormous amount of historical and real-time data.*

1.1.1 Costruir un SOC

Como arquitectos de seguridad, para construir un SOC, necesitamos ante todo **identificar** cuales son los datos que vamos a recoger, y con cual frequencia vamos a recogerlos, cuántos eventos por segundo/minuto/hora y cuánto storage necesitaremos.
Despues, tenemos que decidir dónde colocar los sensores (collectors) de esos datos.
Al final, deberiamos diseñar y implementar una User Interface para los analistas, que les permita visualizar los datos y tomar decisiones.

Es fundamental identificar cuales son los *crown jewels* de la organización, y protegerlos con mayor prioridad, gestionándolos lo más rápidamente posible.

*" A **crown jewel** one of the highest-value assets in your industrial control systems (ICS) and operational technology (OT) environment that, if compromised, could cause major impact to the organization "* — dragos.com

1.2 Funcionalidades más importantes de un SOC

Las funcionalidades cruciales mencionadas en el vídeo que el SOC debe implementar, son las siguientes:

1. **Agregar** datos
2. **Normalizar** datos, para que los analistas puedan escribir detecciones y reglas a partir de los datos
3. **Personalizar las detecciones**, adaptarlos a la estructura y las necesidades de la organización, para limitar el riesgo de falsos positivos y comprender la criticidad de un incidente en relación con el contexto de la organización.
4. **Proteger** datos sensibles, según un criterio de priorización.
5. **Automated responses**. Es importante minimizar el tiempo de remediación, utilizando modernas herramientas que permitan automatizar la respuesta a los eventos, en lugar de enviar una alerta a un servicio de tickets, abrir un ticket, asignarlo a un analista, etc.

Estas funcionalidades coinciden con los mencionados en el artículo de Cyviz, aunque organizados de forma ligeramente diferente. El artículo propone *"Identify", "Protect", "Detect"* and *"Respond"* como puntos clave, pero el significado es más o menos el mismo.

En el video también es mencionada la importancia de **monitorizar** constantemente el estado del SOC y de los sensores, para asegurarse de que está funcionando correctamente, evaluar disponibilidad y scalabilidad y si son apropriadas nuevas tecnologías, herramientas, dispositivos.

Vamos a ver cómo se pueden implementar estas funcionalidades con las herramientas que hemos visto en clase.

1.2.1 Agregar, normalizar datos y personalizar detecciones

Antes de agregar datos, es necesario recorgelos, pero las herramientas para hacer esto no están tratados en el video o en el artículo, que, en cambio, apuntan a la atención que debe prestarse en general al diseño de la recogida de datos, sin entrar en detalles de implementación.
Hay muchas herramientas y sensores que pueden ser fuentes de datos, por ejemplo NIDSs/HIDSs (*OSSEC*, *Snort*, *Suricata*, ...), firewalls, network monitoring tools (*Zeek*,...), EDR tools,...

En la practica de la semana pasada hemos utilizado SELKS, que es un IDS/IPS. Incluye, entre otros, Suricata y Kibana.

Es más interesante cómo **agregar** datos de diferentes fuentes, y por esto existen los SIEMs, que hemos visto en clase.
El objetivo de un SIEM es analizar registros y correlacionar eventos para detectar patterns que indiquen ataques, y tipicamente son asignados a subredes o partes de subredes.

Un SIEM muy utilizado es Splunk, pero hay otros, como QRadar, OSSIMO, o AlienVault, que pero es más viejo.

Algunos SIEMs también ofrecen la posibilidad de integrar información sobre el contexto de la organización, como la estructura de la red, las vulnerabilidades, cuales son los *crown jewels* de la organización, o asignar assets a business functions, **personalizando** el proceso de detección.
En esta manera, la severidad de un evento puede ser evaluada en relación con el contexto de la organización.

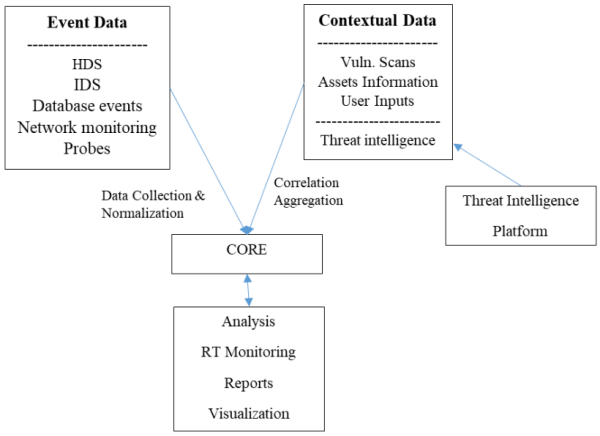

Figure 1.1: SIEM architecture

El SIEM permite "to flatten raw data", y por tanto de **normalizar**, para salir una alerta más concisa y relevante.
En el video con "normalizar" se entiende también hacer que los datos sean **visibles** para los analistas, y en este sentido hemos visto en clase diversas técnicas de **visualización**, que permiten de ver las relaciones entre los elementos.
La tipología de visualización depende de los datos que se quieren representar, y de la finalidad de la visualización.

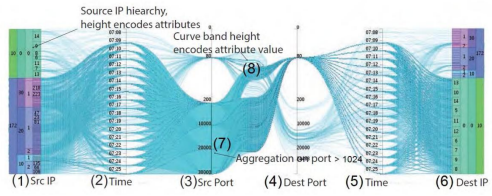

Figure 1.1: Connections flow chart

Lo más intuitivos son grafos, pero no siempre son suficiente para representar la complejidad de las relaciones entre los datos, porque los grafos tienen solo dos dimensiones (se ne pueden añadir más, utilizando el color o el tamaño de los nodos, pero son, sin embargo, limitadas en algunos casos).
En Fig. 1.1 se puede ver un ejemplo de un diagrama de flujo de conexiones, que permite de identificar rápidamente horizontal/vertical port scanning o DDoS ataques.

1.2.1.1 Herramientas de visualización

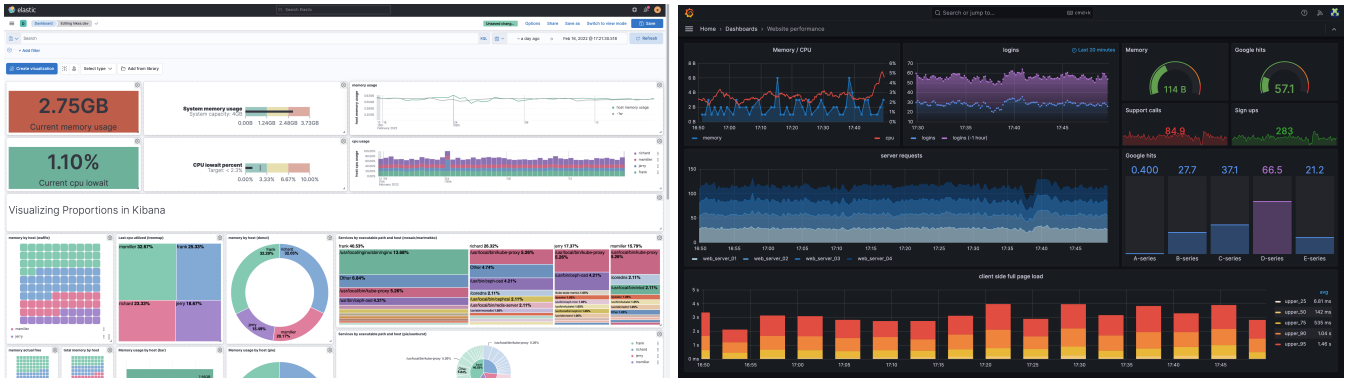

Figure 1.2: KIBANA y GRAFANA

KIBANA ofrece muchos tipos de gráficos diferentes, también algunos que no se muestran en la figura, como heatmaps y geomaps. GRAFANA es otra herramienta de visualización popular, que se centra más en los datos de series temporales, y también ofrece una amplia gama de opciones de visualización.

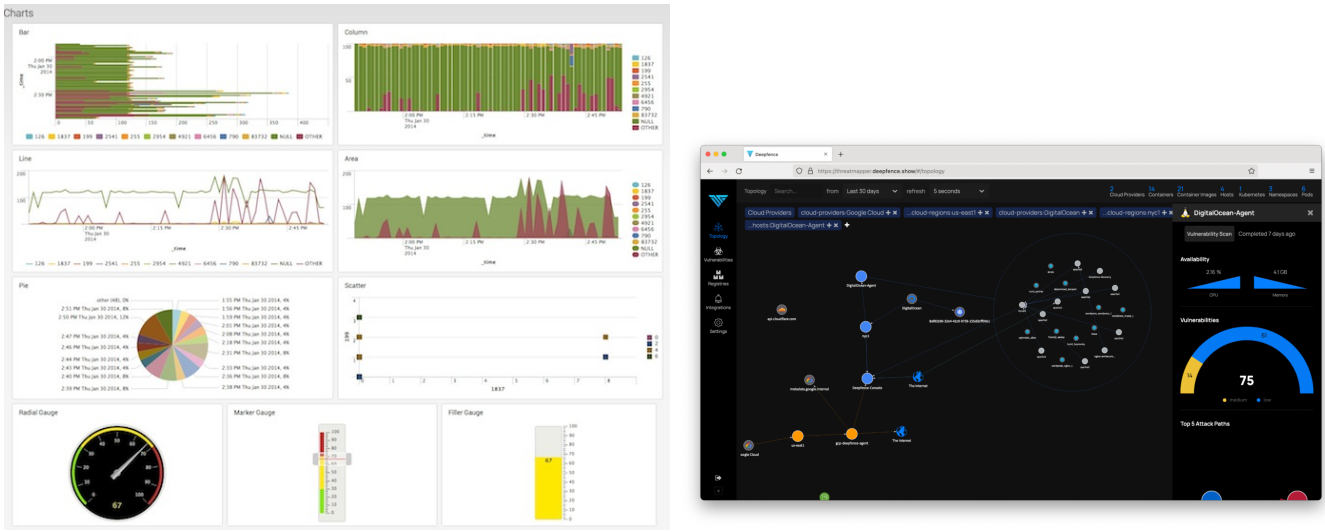

Figure 1.3: SPLUNK and THREATMAPPER

Las capacidades de visualización de SPLUNK se integran con el resto de la plataforma, y es posible crear cuadros de mando personalizados. THREATMAPPER es una herramienta que permite visualizar la superficie de ataque de una organización, y también mostrar rutas de ataque, que representan los pasos que daría un atacante para alcanzar un objetivo.

1.2.2 Proteger datos y Automated responses

Claro que la **protección** de los datos es una de las funcionalidades más importantes de un SOC, y es necesario proteger los datos más sensibles con mayor prioridad.
Gracias a los sistemas de detección y visualización, los analistas pueden identificar rápidamente las amenazas y responder adecuadamente, apoyándose posiblemente en procedimientos de remediación ya escritos y documentados. A menudo conviene integrar estos procedimientos con los standards que clasifican las vulnerabilidades y amenazas, como el MITRE ATT&CK FRAMEWORK, CVSS, CVE, STIX, que hemos mencionado en clase.

Sin embargo, para velocizar el proceso de remediación, es posible **automatizar** las respuestas a los eventos, utilizando herramientas como SOAR, que tal vez se pueden integrar con el SIEM.
El orador del vídeo presenta esto aspecto como uno de los más importantes, porque minimizar el tiempo de remediación es fundamental para limitar el daño de un ataque. Él introduce en la entrevista el concepto de **playbook** (más sobre esto más abajo), que define una secuencia de acciones que deben ser ejecutadas para realizar un objetivo, y que pueden automatizarse.

1.3 Diferencias entre el video y el artículo

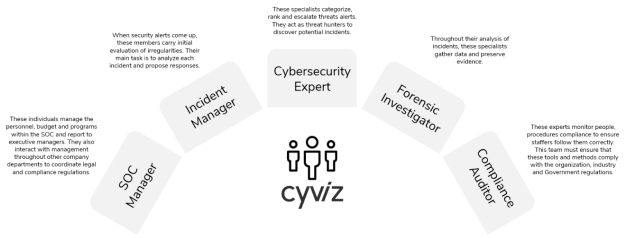

Figure 1.4: Propuesta de organización del equipo Cyviz

En el artículo hay algunas secciones sobre la estructura y la finalidad de los **equipos de seguridad**, que no se exploran en profundidad en el vídeo, que se centra más en los SOC desde el punto de vista de la arquitectura y el diseño.
También hay algunas menciones relativas a los diferentes modelos operativos del SOC, si debería ser *Internal*, *Virtual*, *Outsourced*, ...

Aunque estos aspectos no se tratan en profundidad en el vídeo, algunos se mencionan brevemente, lo que me hace pensar que el orador es consciente de ellos, pero no son el centro de la entrevista.
Por ejemplo, en el artículo se puede leer:

"An incident response team is crucial to building a functional SOC. It can decide the best way to assign and manage incidents, and act on a defined action plan. They also establish a repeatable workflow and craft essential communication between the business, legal and PR teams. They need to strictly follow a predefined response plan and/or craft new plans to address new scenarios and unknown threats"

En el video se habla de la importancia de **runbooks** y **playbooks**, y que son fundamentales —aparte de sus uso principal de automatizar las respuestas— para definir workflows repetibles que puedan enseñarse fácilmente a los nuevos miembros del equipo.

Los **runbooks** definen las acciones de alto nivel que deben emprenderse en respuesta a una alerta, y los **playbooks** definen las acciones reales que deben emprenderse, y generalmente son **automatizados**.

$$\textit{Runbook} \longrightarrow \textit{Statements}$$
$$\textit{Playbook} \longrightarrow \textit{Actions}$$

Por ejemplo, en caso de que una dispositivo se viera comprometido, el runbook diría que hay que evaluar el escenario (qué hizo el usuario, cuándo, si hay un ransomware...) y que hay que aislar la dispositivo de la red. Mientras que en el libro de jugadas está escrito cómo aislar realmente en practica la dispositivo de la red.

Y con respecto a la Fig. 1.4, el orador no habla de esos "equipos dedicados", sino que menciona las actividades que realizan, como la categorización de alertas, la investigación de una alerta o el análisis retrospectivo de un incidente, y es razonable pensar que estas las actividades se dividen y se asignan a diferentes equipos con diferentes funciones y permisos, aunque no se menciona explícitamente.