Universidad del Rosario | Escuela de Ingeniería, Ciencia y Tecnología | MACC Matemáticas Aplicadas y Ciencias de la Computación | HINNT Hub de INNovación y Transferencia

Computer Incident Response

Daniel Díaz-López

Líder de Ciberseguridad - MACC
Profesor principal de carrera

danielo.diaz@urosario.edu.co

@MACC_URosario @MACC.URosario macc_ur

Computer Incident Response

Categorize incidents
Identify the impact to request timely remediation

Find the root cause -> Identify weak controls
Eliminate traces left by the threat

Document lessons

Define procedures, formats and guides

Understand what happened
Block the threat

Identify remediation steps
Recover lost data or restaure systems

Containment, eradication and recovery should be specific for each type of category

Computer Incident Response

Internal Incident Communication: It is important to keep personnel informed, reduce stress related to the incident, and reinforce policies and standards for external communication.

This reinforcement of external communication is necessary because personnel may forget the external communication policy during an incident and unintentionally disclose harmful or erroneous information.

Depending on the type of incident, inappropriate disclosures from employees can make the situation worse. For example, improper communication on social media about a breach or incident could result in unnecessary and additional attention from external regulators.

Computer Incident Response

External Incident Communication: Organizations should develop a strategy that addresses communication with law enforcement to support any legal action or criminal investigations associated with an incident. Organizations should also plan communication with the media to support an effective public relations strategy related to an incident.

Law Enforcement: Law enforcement can provide intelligence resources to investigate incidents and provide intelligence information. Examples:

1. Federal Bureau of Investigation (FBI)
2. Secret Service
3. District Attorneys
4. Variety of state and local law enforcement agencies
5. International Criminal Police Organization (Interpol) and the Law Enforcement Intelligence Unit (LEIU)
6. Country's law enforcement agencies

Computer Incident Response

External Incident Communication: Organizations should develop a strategy that addresses communication with law enforcement to support any legal action or criminal investigations associated with an incident. Organizations should also plan communication with the media to support an effective public relations strategy related to an incident.

Media Relations: Some incidents may attract media attention and require procedures for handling media inquiries, press releases, and interviews. Improper media communication can create problems for public relations and legal proceedings when released information is incomplete, incorrect, or misunderstood. A single spokesperson with input from: the CISO, technical personnel, legal counsel, and public relations should interface with the media.

Computer Incident Response

- Post-incident analysis provides an opportunity to evaluate the effectiveness of event management and incident response procedures.

- A meeting held after the event allows staff to document root cause, lessons learned, and revise processes for continuous improvement.

- The CISO should ensure that new information gained from incident response activity is incorporated into the policy and procedures to improve the process.

Tools that support the process of Computer Incident Response

- Security information and event management (SIEM)
- Laptops with security analyzer software
- Packet sniffers
- Protocol analyzers

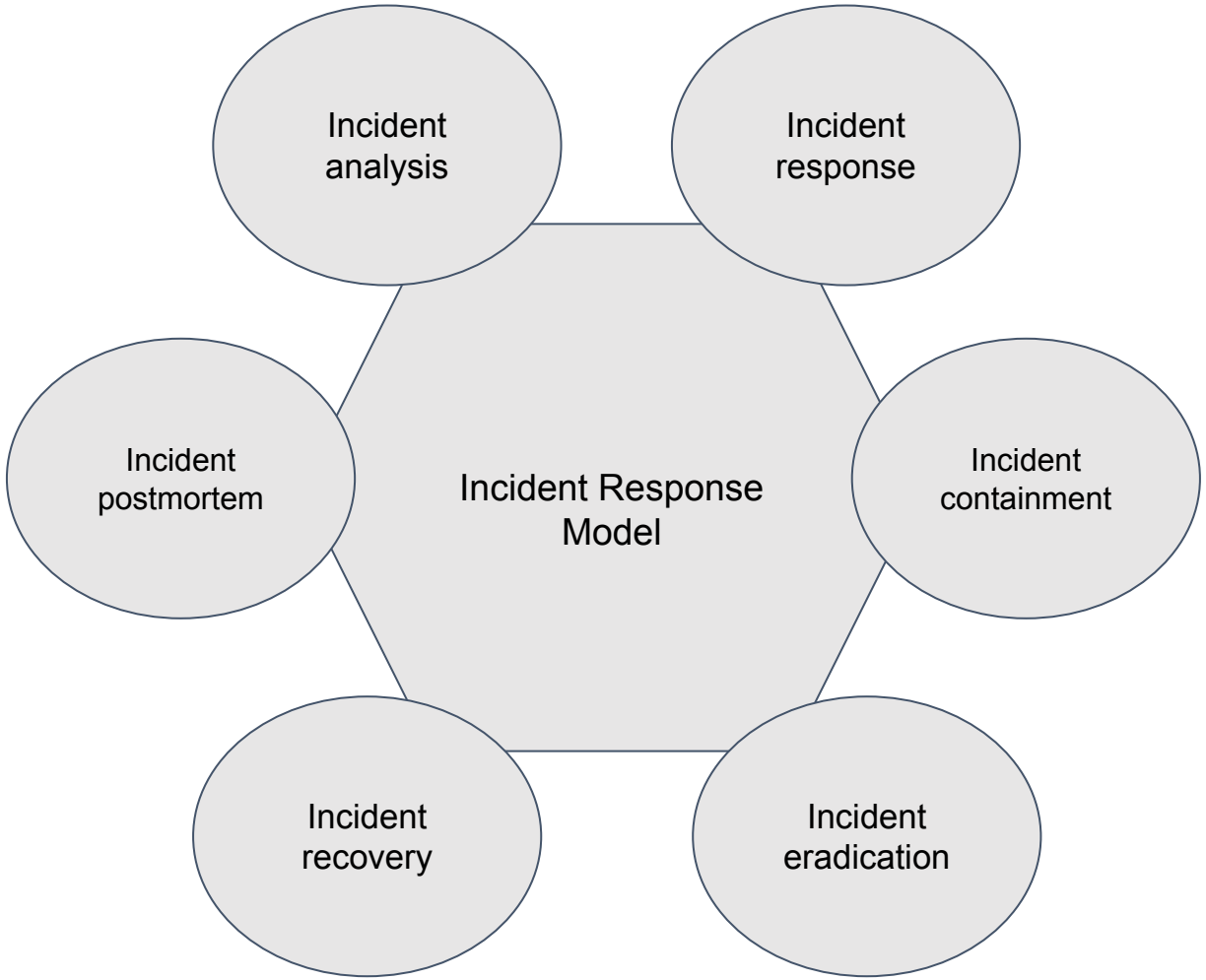
- Static & Dynamic Forensic: Forensic workstations
- Storage and replication solutions
- Networking equipment to test scenarios and provide means to restore files
- Notebooks
- Evidence tape
- Tags
- Bags to support response and investigation activities

Testing an Incident Response Procedure

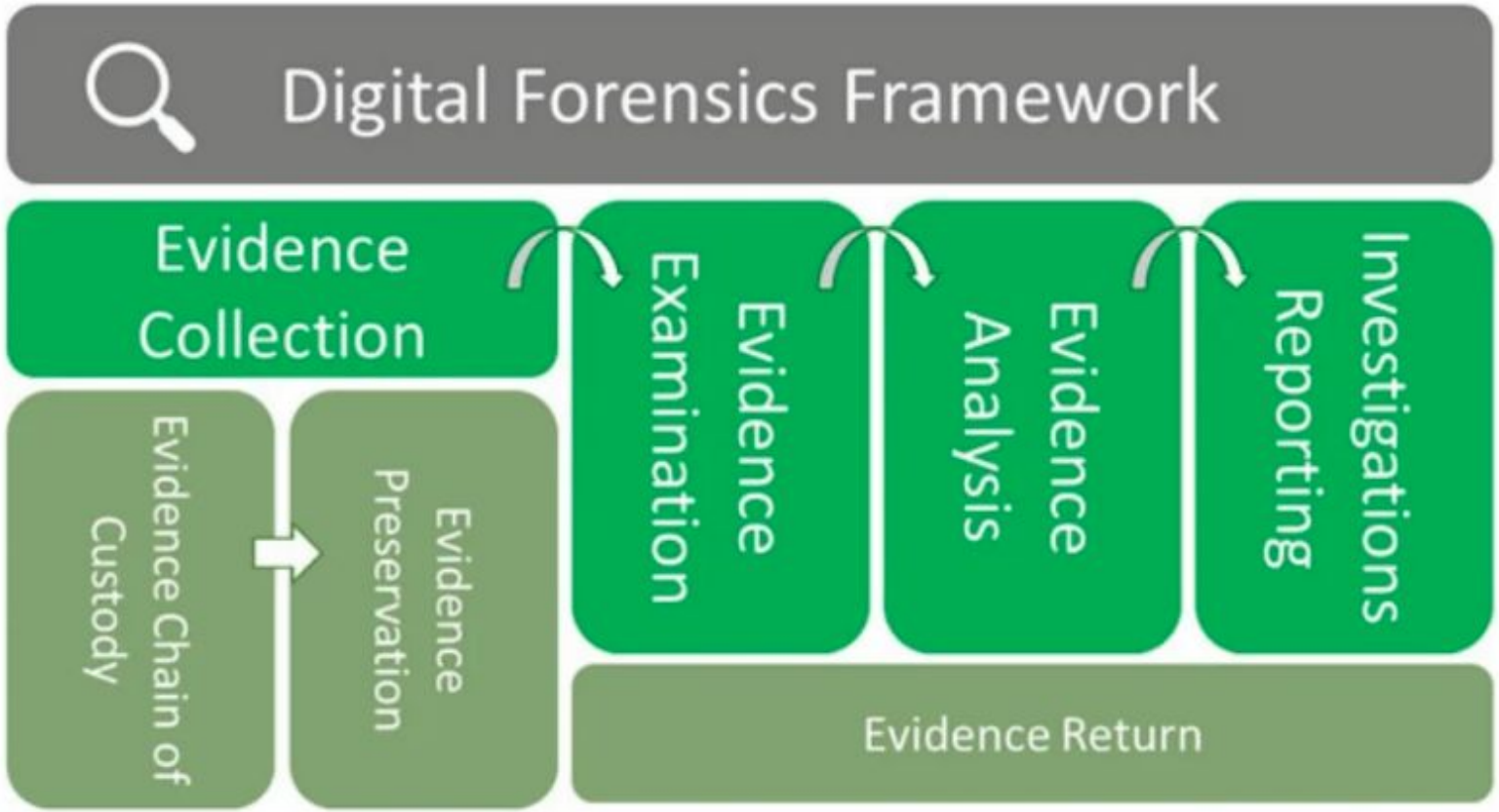
The following **checklist** can aid in the formulation and execution of an incident response test:

1. Select a scenario that poses the greatest risk to the organization.
2. Add as much realism as possible to the test.
3. Ensure members of the incident response team only use procedures documented in the incident response plan.
4. Document plan changes identified during the test.
5. Determine if cross-training is necessary to ensure the plan does not rely on a single person.

Incident Response Model



Digital Forensic Lifecycle



Digital Forensic Lifecycle

The following describes each of the components of the digital forensics' framework:

Evidence Collection:

- It is the **most important** phase of the digital forensic investigation process.
- The organization must determine the **intent of the investigation** before starting the collection process.
- **Preservation of evidence** and **chain of custody** constitute the base of the forensic investigation structure.
- The information to be collected is **refined,** while moving through the rest of the process, to find what is most relevant.
- The investigation cannot be improved at later phases if there are problems with the collection or the chain of custody at the onset of the investigation.

Digital Forensic Lifecycle

Chain of Custody:

- Each collection step and all interactions with the evidence **must be recorded** to maintain chain of custody.
- **Chain of custody** refers to the documented record that provides accountability for each step of the handling process.
- The forensic investigation process must demonstrate that information handling procedures and actions performed **did not alter** the original data throughout the custody chain.
- This may include the following:
  - Recording the **name** of person in charge of maintain the chain of custody.
  - Details of **the timing** of the event
  - **Purpose** for moving the data
  - Identification of evidence through recording of **serial numbers** and other details
  - **Sealing** the evidence with evidence tape
  - Documenting the **location** of storage
  - Documenting the **movement** of the information

Evidence must be **reliable** to support legal proceedings or root-cause analysis. Policies, procedures, and training are recommended to ensure the chain of custody is understood and applied correctly to each investigation.

Digital Forensic Lifecycle

Evidence Preservation:

- The key to collection and preservation is to collect data in a way that **prevents inadvertent changes**.
- Plans should exist that define **how to acquire data** and the **method used to copy data**.
- The data should be copied using defined processes and tools to ensure the original evidence is **not** modified.
- Logs should be kept of observations, as well as pictures or videos of the collection process to provide **further verification** that tampering was not introduced to the evidence.
- **Severing network connections** and **powering down** the affected host must be done carefully to ensure these activities do not destroy valuable data required to support investigations.
- The process must prove that data collected on day one has not changed when it is analyzed later—nonrepudiation.
- The **file format** used for collecting evidence should make it hard to change it without destroying the file. i.e. to create evidence containers (logical file structure) that prevent the data from changing once it is in the container.

Digital Forensic Lifecycle

Evidence Examination:

- The second phase of the digital forensics process is examination.
- **Not** all the information collected will be of value!
- The evidence examination is done using **a copy** of the original data.
- **Tools are used to search and locate** documents with key phrases or patterns.
- The data may have to **be restored** to another device from the backups to perform this analysis.
- Special issues arise with encrypted files. The encryption method may need to be determined from the **file header**, and the file may be decrypted if the encryption method is weak or if the decryption key is located on other media.
- The primary objective of this phase is to **reduce** the available evidence.

Digital Forensic Lifecycle

Evidence Analysis:

- The third phase of the digital forensics process is analysis.
- The analyst inspects data during this phase with the goal to determine the activities that occurred in terms of the following:
  - **Who** was involved?
  - **What** occurred?
  - **When** did the events occur?
  - **Where** did the action originate and where was the impact?
  - **How** was it accomplished?
- The analyst's job is to gather information by examining and **correlating** disparate sources of information.
- **SIEM** tools can automatically correlate some of this information, using the logs of the systems.
- **Intrusion detection systems** can assist analysis: network activity, events performed by users through their account or email system.
- The forensic analyst can review documents, spreadsheets, graphics files, and other information to construct a **timeline of events**.

Digital Forensic Lifecycle

Investigation Reporting:

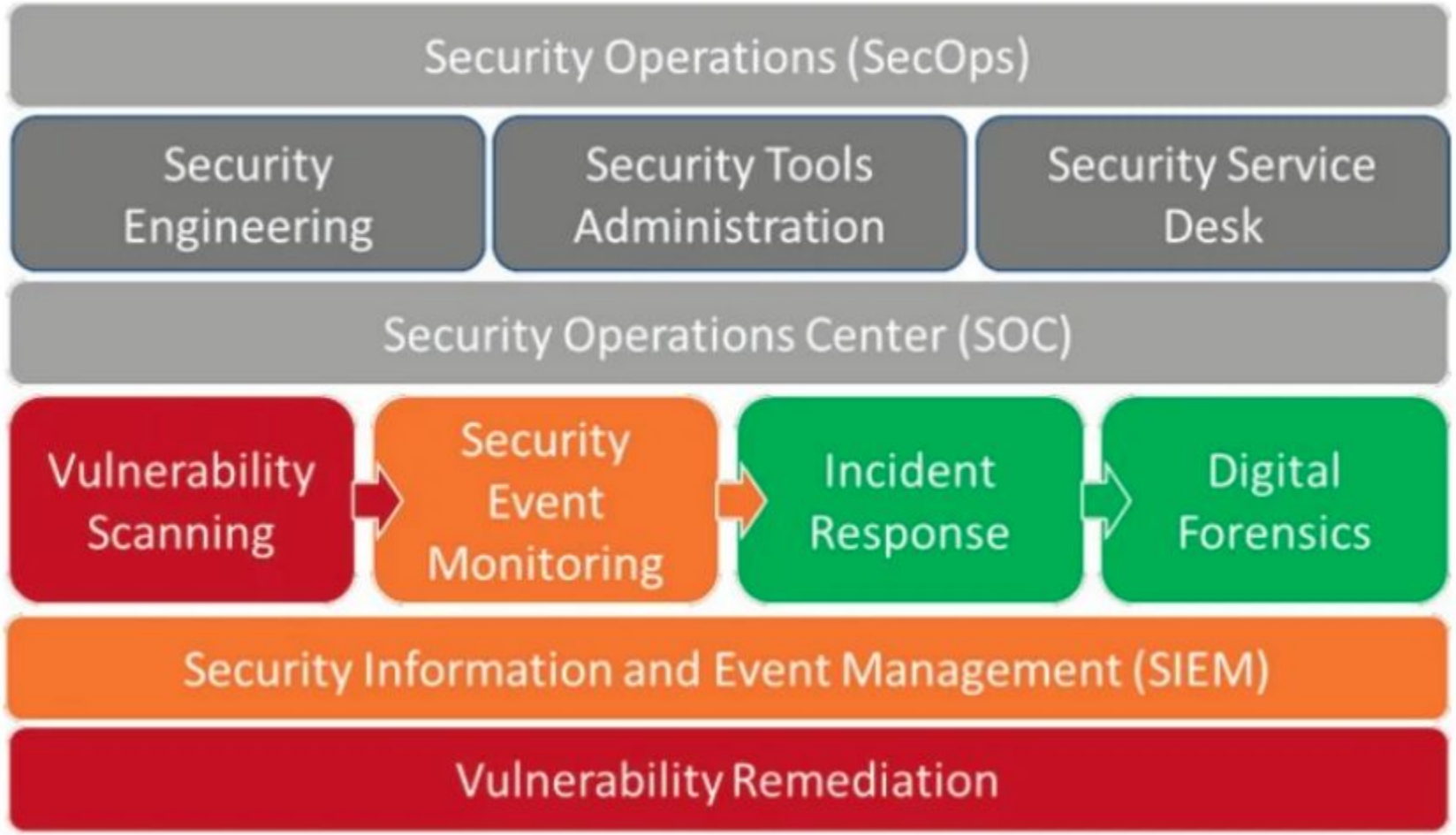
- The final phase of the digital forensics process is **reporting**.
- In this phase, **a report** with the information that was collected with event descriptions is created.
- The conclusions are supported by the **analysis steps** and the report is written clearly so it can be understood by the audience receiving it.
- The **methodology** used to perform analysis and determine the results should be provided.
- Recommendations of **improvements** to mitigate issues found during the analysis should also be noted.
- Reviews can be conducted to discuss **improvements** to policies and procedures and additional investments to the infrastructure in support of the program.
- This could include the **capability to capture more source data**, purchasing additional forensic tools, adding file retention capabilities, increasing storage, or providing additional forensics training.

Digital Forensic Lifecycle

Evidence Return:

- The returning of digital evidence requires returning of the physical and digital sources back to the rightful owner.

ESTABLISHING AND OPERATING A SECURITY OPERATIONS (SecOps) Framework



Universidad del Rosario | Escuela de Ingeniería, Ciencia y Tecnología | MACC Matemáticas Aplicadas y Ciencias de la Computación | HINNT Hub de INNovación y Transferencia

Event Management

Daniel Díaz-López

Líder de Ciberseguridad - MACC
Profesor principal de carrera

danielo.diaz@urosario.edu.co

@MACC_URosario @MACC.URosario macc_ur

La norma ISO 27001 define la forma como se debe implementar un Sistema de Gestión de Seguridad de la Información (SGSI)

ISO 27001

Information technology - Security techniques - Information security management systems - Requirements

En el sector público colombiano existe el MSPI para las Entidades públicas:

MINTIC

Modelo de Seguridad y Privacidad de la Información (MSPI)
(Basado en la norma ISO 27001)

La norma ISO 27001 define el dominio A.12: Seguridad de la Operaciones

Dominio A.12: Seguridad de la Operaciones

- **A.12.4.1. Registro de eventos:** Indica que se debe **generar**, mantener y revisar con regularidad los registros de eventos de las actividades de los usuarios, excepciones, faltas y eventos de seguridad de la información.
- **A.12.4.2. Protección de la información de registro:** Indica que las instalaciones de registro y la información de registro se deben **proteger** contra alteraciones y accesos no autorizados.
- **A.12.4.3. Registros del administrador y del operador.** Indica que se deben registrar las **actividades del operador** y del administrador del sistema, los registros se deben proteger y revisar con regularidad.

¿La gestión de eventos podría realizarse de manera manual?

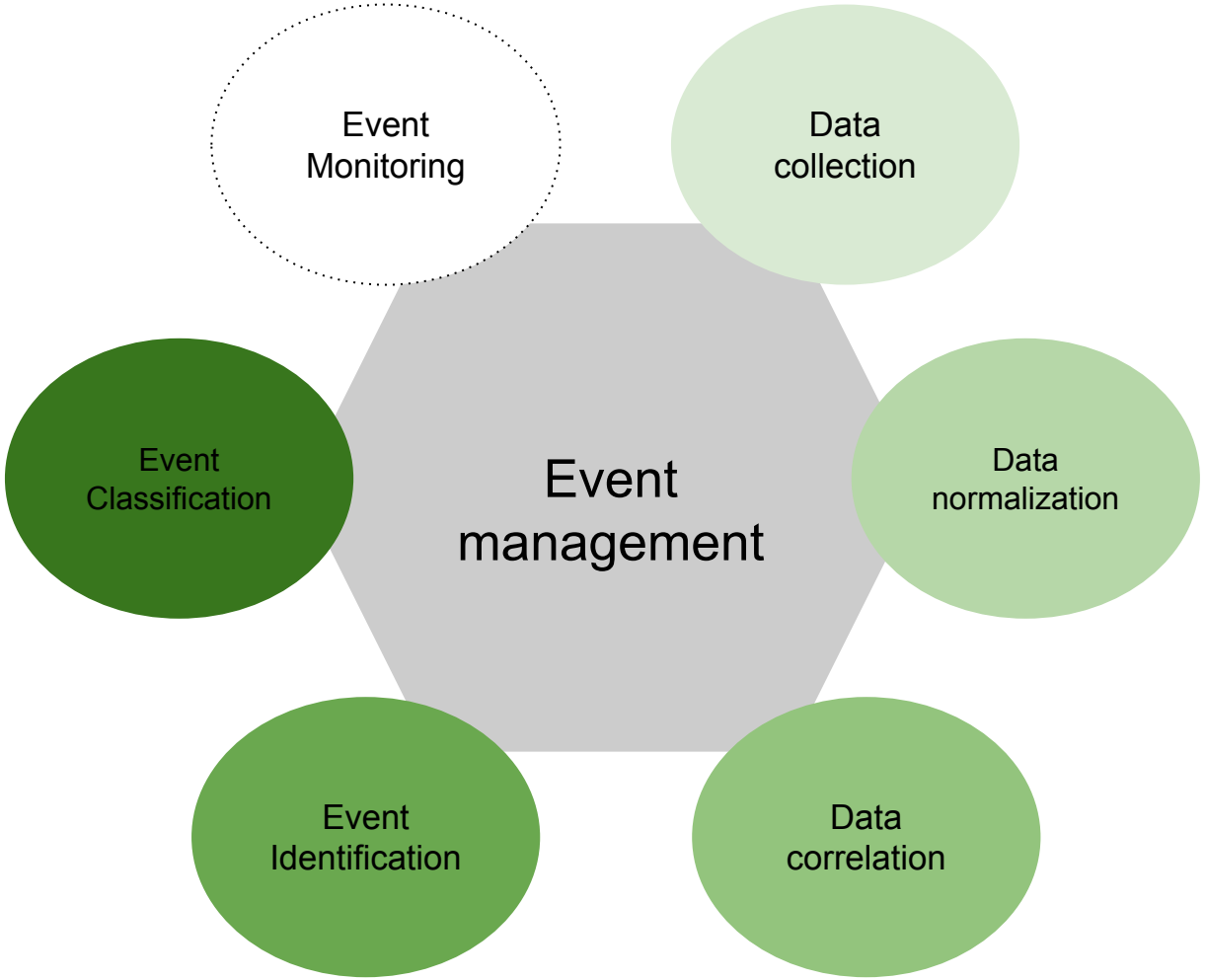
Instrumento de Evaluación MSPI para Entidades públicas

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA
T.4.4.1	Responsable de SI	Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	**A.12.4.1**	Modelo de madurez gestionado cuantitativamente	PR.PT-1 DE.CM-3 RS.AN-1	Revisar los registros de eventos que incluyan: a) **identificar los usuarios**; b) establecer las **actividades del sistema;** c) definir las **fechas, horas y detalles de los eventos clave**, (entrada y salida); d) identificar el **dispositivo o ubicación**, si es posible, e identificador del sistema; e) tener registros **de intentos de acceso al sistema exitosos y rechazados;** e) definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos; g) establecer los **cambios a la configuración** del sistema; h) definir el **uso de privilegios;** i) establecer el **uso de utilitarios y aplicaciones** del sistema; j) definir los archivos a los que se tuvo acceso, y el **tipo de acceso**; k) establecer las **direcciones y protocolos de red**; l) definir las **alarmas accionadas** por el sistema de control de acceso; m) activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión; n) registrar **las transacciones ejecutadas** por los usuarios en las aplicaciones.	
T.4.4.2	Responsable de SI	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	**A.12.4.2**		PR.PT-1	Revisar los procedimientos y controles dirigidos a **proteger contra cambios no autorizados** de la información del registro y contra problemas con la instalación de registro, que incluya: a) verificar todas **las alteraciones** a los tipos de mensaje que se registran; b) establecer **los archivos log que son editados o eliminados**; c) verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.	
T.4.4.3	Responsable de SI	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se debe registrar, y los registros se deben proteger y revisar con regularidad.	**A.12.4.3**		PR.PT-1 RS.AN-1	**Revisar los registros** de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad.	

Event Management Model

Event Monitoring

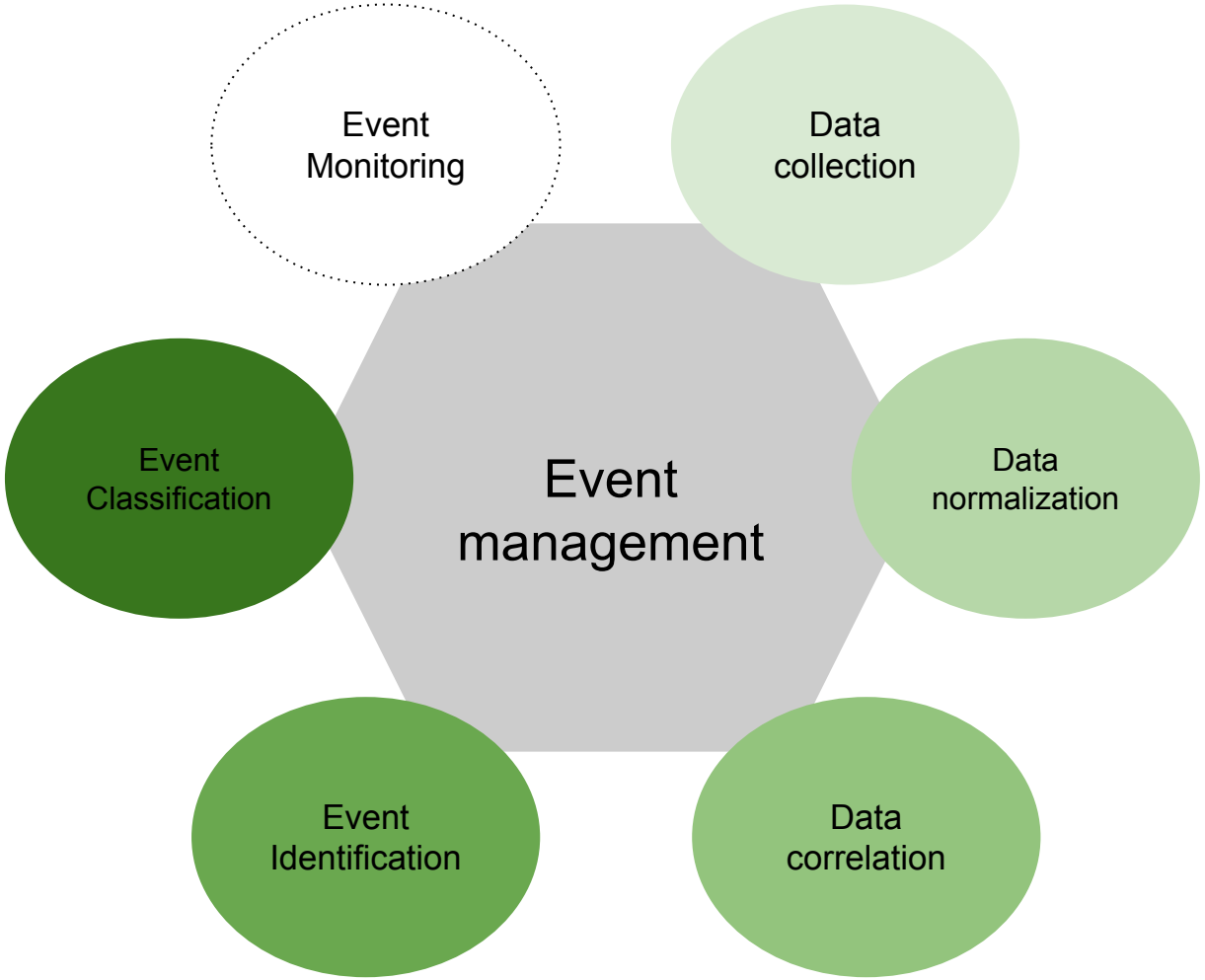
- Event management is one of the activities of a SOC
- Event monitoring may be considered a problem of Big Data
- Tools in the Event Monitoring:
  - Security logs aggregators
  - Logs filters
  - Identification of a event normalized baseline (normal activities)
  - Generation of alerts that conduces to individual responses



Event Management Model

Data collection

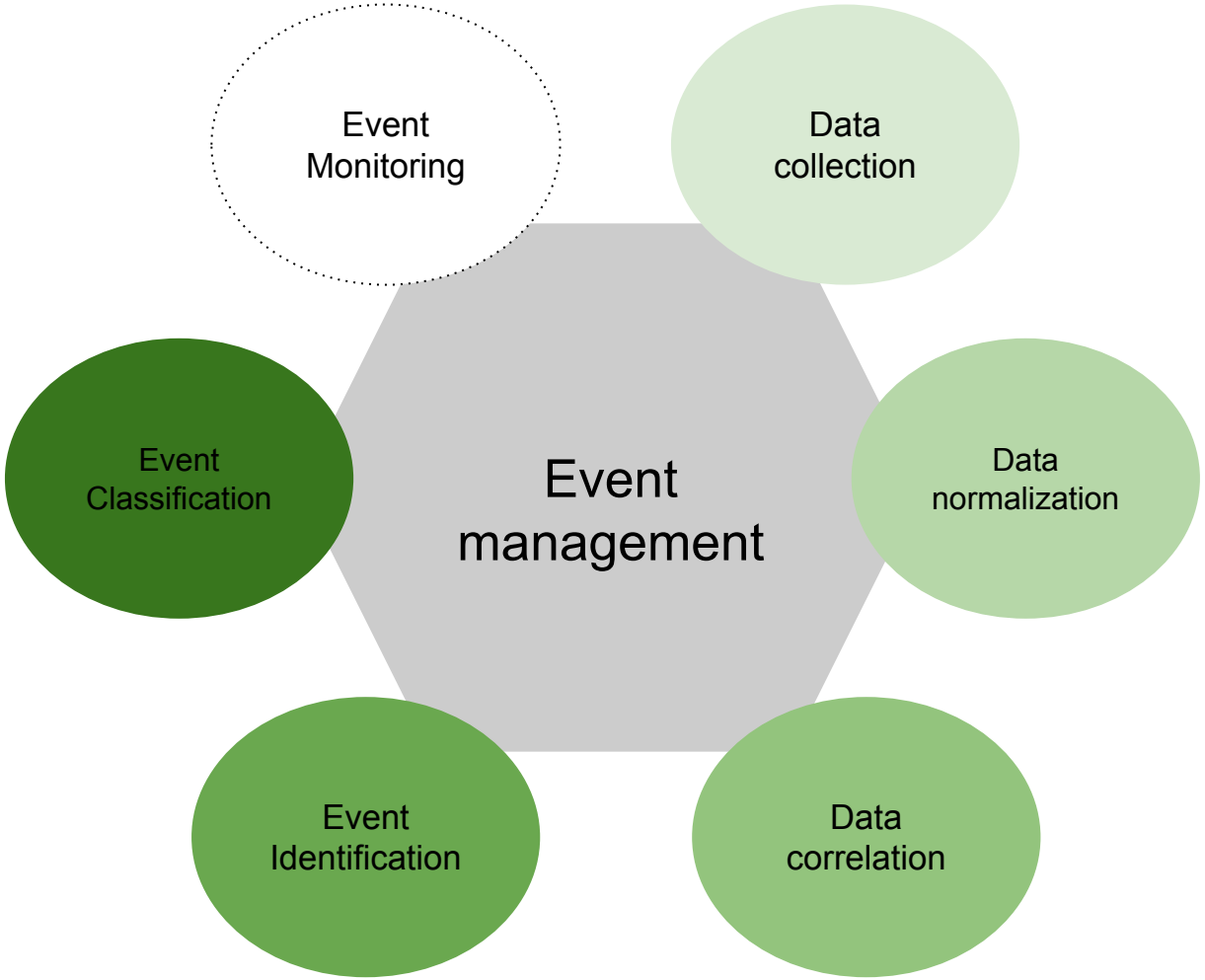
- SOC data collection describes the systematic approach used by the organization to gather **timely and relevant** information about the enterprise.
- The CISO must develop a strategy to ensure **adequate** information is collected to support analysis and identification of issues.



Event Management Model

Data Normalization

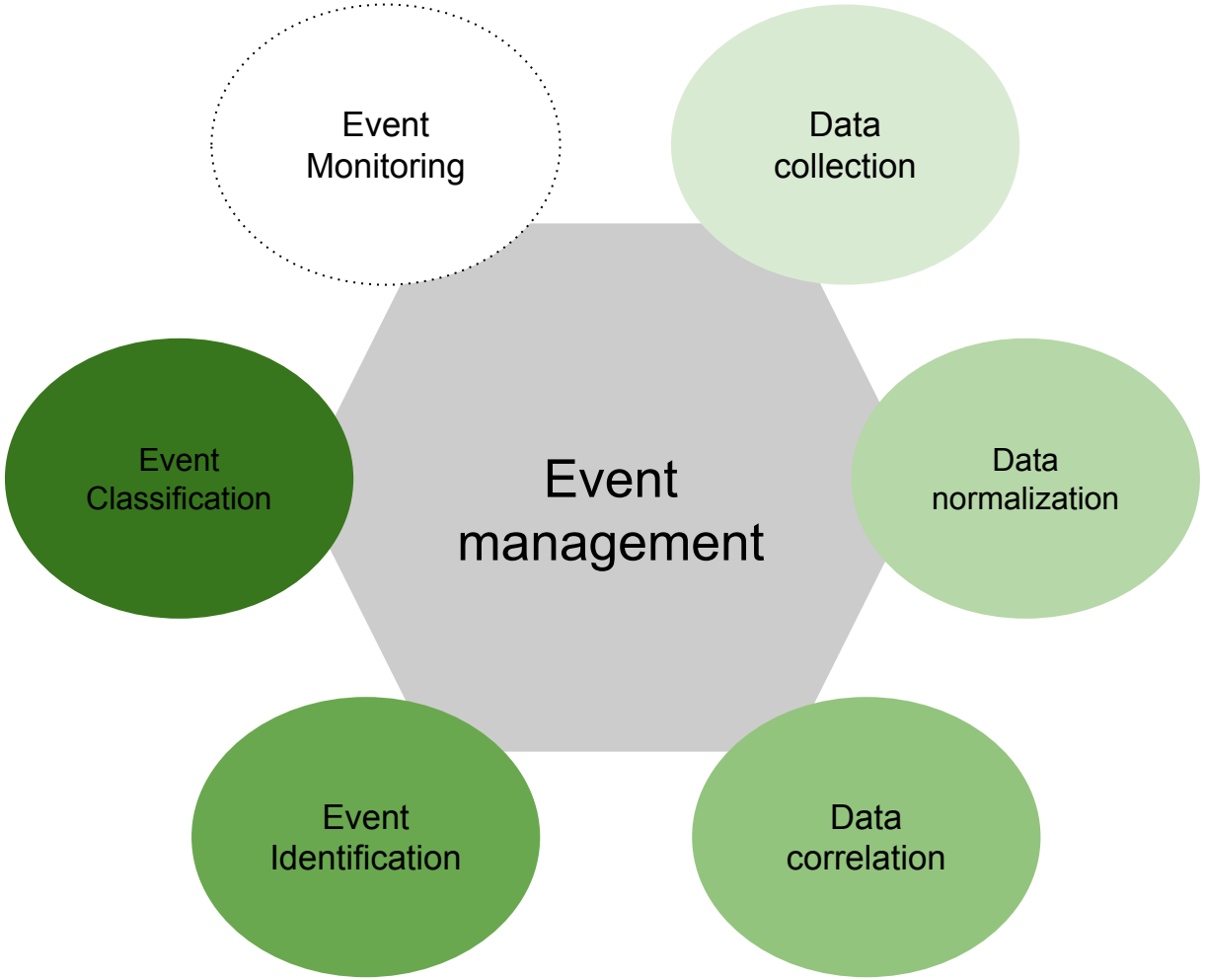
- Normalization allows analysis and identification tools to use standardized queries and data structure input to evaluate data from multiple sources and **isolate signs of anomalous or malicious** activity.
- Because normalization transforms data, the CISO should develop a strategy to obtain original data if additional investigation and forensic analysis is necessary.



Event Management Model

Event Identification

- Identifying the **type of event and assigning a category** that supports/define the subsequent steps in the event management and incident response processes.
- The CISO must define the criteria that distinguish an incident from an event.



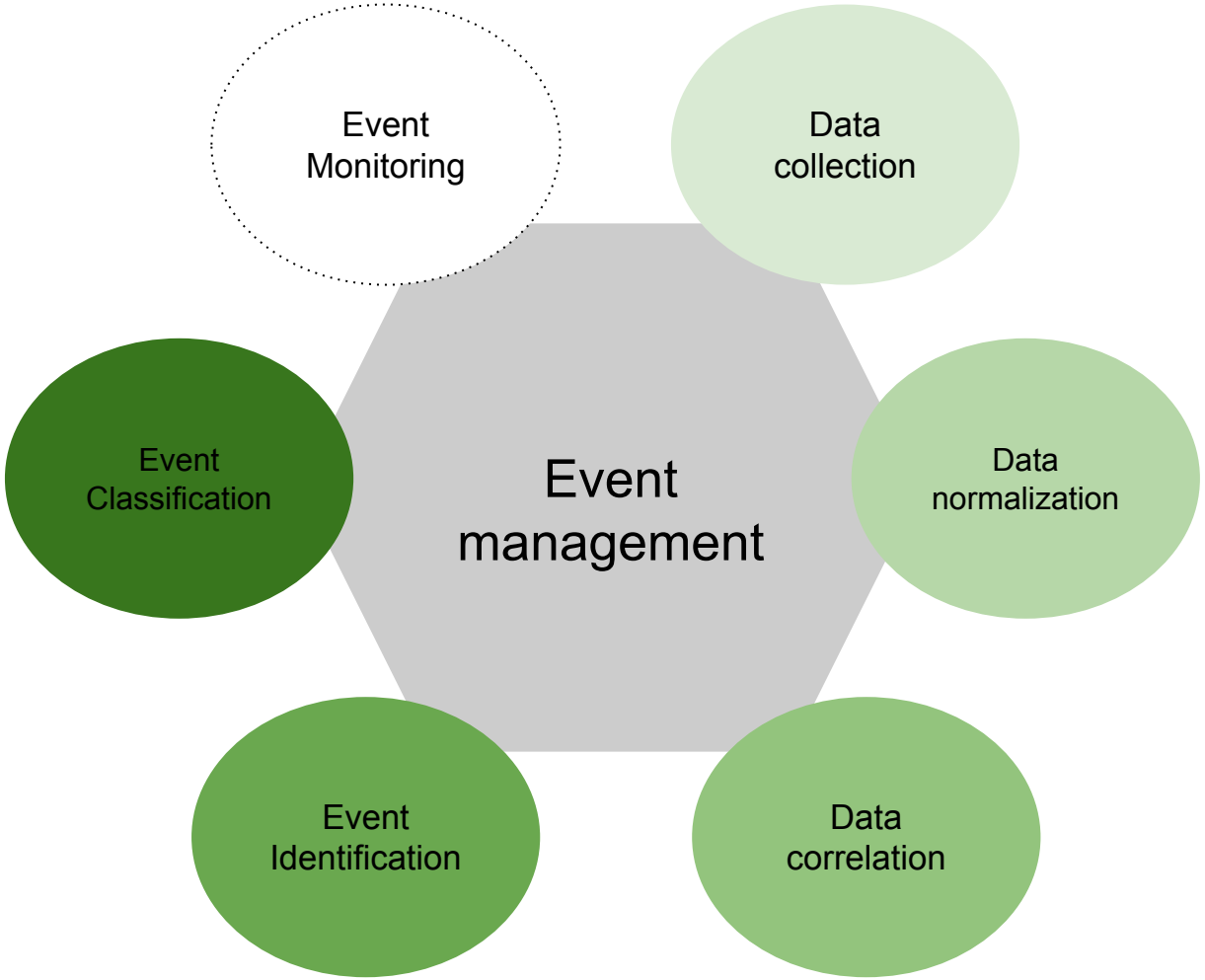
Event Management Model

Event Classification:

- This is often based on the type and impact of the threat.
- With proper context, events can be categorized based on **criticality, impact, and the relationship** to other events being managed by the security operations team.

Reportable Event Categories	
Category	**Description**
0	Training and Exercises
1	Root-Level Intrusion
2	User-Level Intrusion
3	Unsuccessful Activity Attempt
4	Denial of Service
5	Noncompliance Activity
6	Reconnaissance
7	Malicious Logic
8	Investigating
9	Explained Anomaly

Event categorization



Registro de eventos

Las soluciones **SIEM (Security Information and Event Management System**) resuelven varios de los requerimientos de la gestión de eventos de seguridad pero también traen consigo algunos retos:

i. Grandes volúmenes de eventos de seguridad (miles, millones)
ii. Eventos de seguridad con diferentes propiedades y atributos (fuente, destino, puerto, username, path, method, IPs, País, recurso solicitado, alarma, riesgo, etc.)
iii. Diversidad de eventos de seguridad (Brute froce, ssh authentication, DoS, etc)
iv. Tráfico muy heterogéneo (eventos maliciosos combinados con eventos normales de la operación)
v. Algunos eventos de seguridad tienen conexión-relación entre ellos (otros no)
vi. Algunos eventos de seguridad son precisos y útiles (otros no)

¿Cómo revisar manualmente millones de eventos?

¿Cómo inspeccionar manualmente las propiedades y atributos de millones de eventos?

¿Debo tratar cada tipo de evento por aparte?

¿Cómo identificar y excluir el tráfico normal de operación?

¿Cómo encontrar relación entre eventos de seguridad?

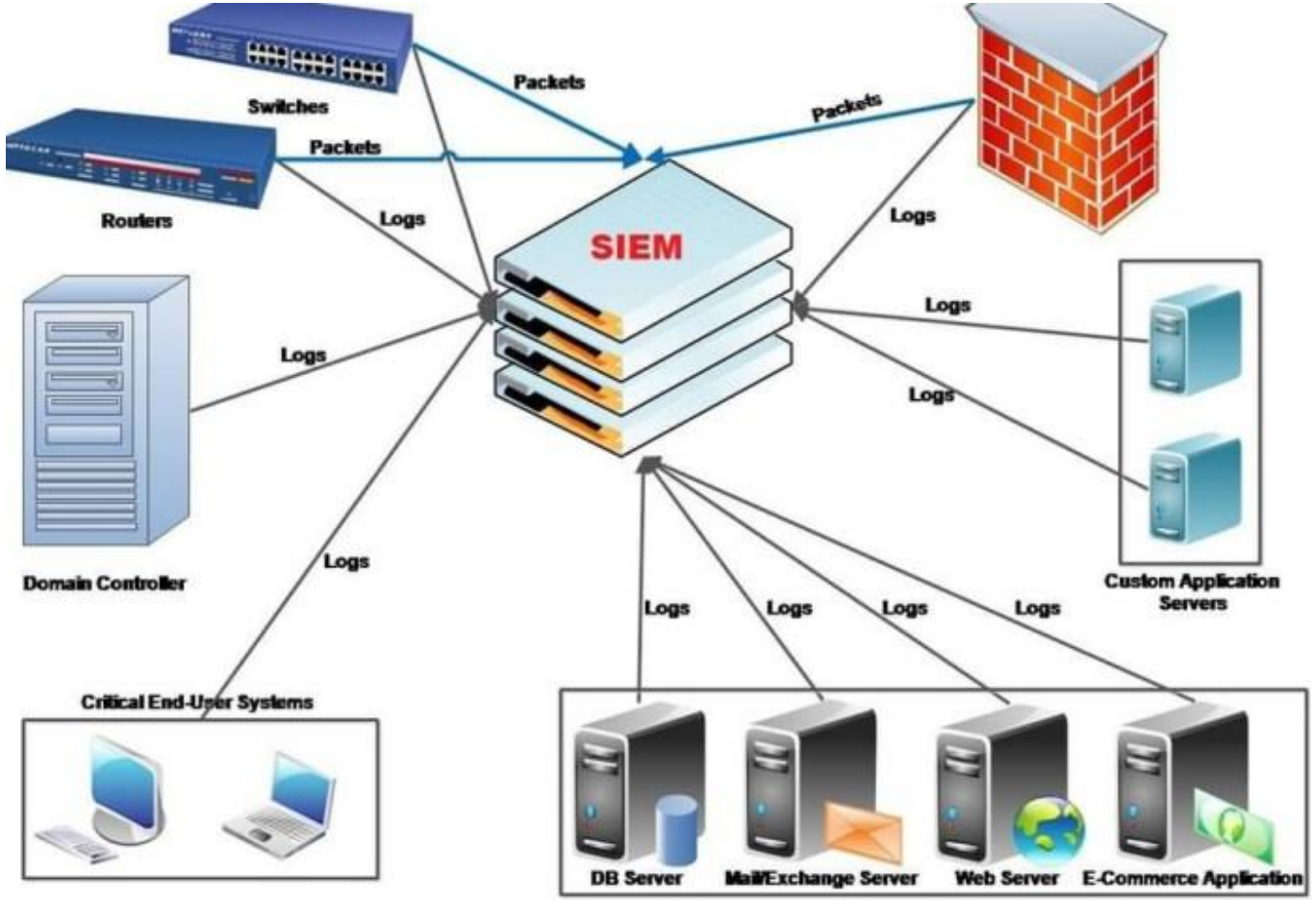
¿Cómo descartar eventos inútiles?

Una solución **SIEM (Security Information and Event Management System**) resuelven varios de los requerimientos de la gestión de eventos de seguridad

Un SIEM combina un SIM (security information management) y un SEM (security event management) en un único sistema.

Una solución SIEM (Security Information and Event Management) permite:

- Descubrir activos
- Evaluar vulnerabilidades (VA)
- Realizar detección de intrusos
- Monitoreo de integridad de archivos
- Correlación de eventos
- Realizar intercambio de información de amenazas



Security Information and Event Management (SIEM)

SIEM functionalities:

- SIM - Security Information Management: Management of logs, analysis and compliance reports.
- SEM - Security Event Management: Real-time monitoring and incident management for security events in networks, security devices, systems and applications.

A SIEM deployment provides a mix of threat management and standards compliance.

- Threat management: Real-time monitoring and reporting of user activities, data access, application activity, in combination with query capabilities.
- Compliance: Management of logs and compliance reports

Security Information and Event Management (SIEM)

- SIEM is the primary tool used to support the **Security Operations Center (SOC)**
- The SOC typically manages the SIEM as an activity within the security operations program
- Because of CapEx and OpEx concerns, some organizations leverage ***Managed Security Service Providers (MSSPs)*** to provide SOC operational support, to include SIEM use and management
- An MSSP rents the SIEM equipment and is also in charge of its administration, while the client company supervises

- The underlying principle of an SIEM:
  - **Collect** relevant data about an enterprise's security.
  - **Aggregate** information from multiple locations.
  - **Correlation** information for analysis.
  - **Analyze** information into a single point of view, making it easier to spot potential security incidents or adverse trends.

In a SIEM, several use cases can be defined to detect anomalies.

Defining the **use cases** requires:

1. Define the **requirements** for the use case and identify the **expected outcome**
2. Define the **scope** of the requirement
3. Validate **event sources** that support the expected use case function
4. Define the alert logic and **associated attack vector**
5. Perform **implementation and testing** to confirm that SIEM produces the desired result
6. Define **use case response procedures**
7. Carry out maintenance to support continuous improvement and adjustment

Magic Quadrant for Security Information and Event Management (SIEM)

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	High

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Not Rated
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Magic Quadrant for Security Information and Event Management (SIEM)

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (February 2020)

Líderes: Productos con componentes funcionales fuertes para satisfacer Mercado SIEM, y tienen la mayor base instalada y mayores ingresos.

Visionarios: Productos con componentes funcionales fuertes para satisfacer el mercado SIEM, pero con menor presencia en el mercado.

Magic Quadrant for Security Information and Event Management (SIEM)

Retadores (Challengers): Múltiples productos y líneas de servicio, al menos una base de clientes de tamaño modesta y productos que cumplen sólo un subconjunto de los requerimientos generales del mercado.

Jugadores de nicho (Niche Players): Productos que satisfacen un caso de uso SIEM específico o un subconjunto de requerimientos funcionales. Se enfocan en un segmento particular de clientes (pymes, proveedores de servicio, una región específica).

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (February 2020)

La solución SIEM AT&T Cybersecurity (Antes AlienVault Unified Security Management (USM)) provee:

- SIEM
- Evaluación de vulnerabilidades (VA)
- Descubrimiento de activos
- Detección de intrusiones basada en Host y Red (NIDS/HIDS)
- Monitoreo de integridad de archivos (FIM)

AlienVault USM utiliza los siguientes componentes open source:

- OpenVAS (VA)
- Snort
- Suricata (IDS)
- OSSEC (HIDS/FIM)
- OSSIM (SIEM)

AlienVault utiliza OTE (Open Threat Exchange) que es una comunidad para compartir información reputacional de URL’s y direcciones IP.

Registro de eventos

- Los laboratorios AlienVault proveen una suscripción a un servicio de inteligencia de amenazas integrada (integrated threat intelligence) que incluye actualizaciones de firmas, vulnerabilidades , reglas de correlación, reportes, y contenido de respuesta a incidentes.

- AlienVault USM está disponible como appliance, software o imagen virtual, igualmente por medio de Amazon Elastic Compute Cloud (EC2).

- Los sensores, generadores de logs y los componentes de servidor de USM pueden ser desplegados combinados en un Sistema (arquitectura todo en uno), o como servidores separados en capas horizontales y verticales para diferentes necesidades de escalamiento.

- El Mercado objetivo de Alienvault son empresas con un reducido personal de seguridad y programas de seguridad limitados que requieren múltiples tecnologías de seguridad integradas a un costo más bajo y con mayor simplicidad. Es mucho menos costosa que los competidores del cuadrante.

Registro de eventos

Componentes:

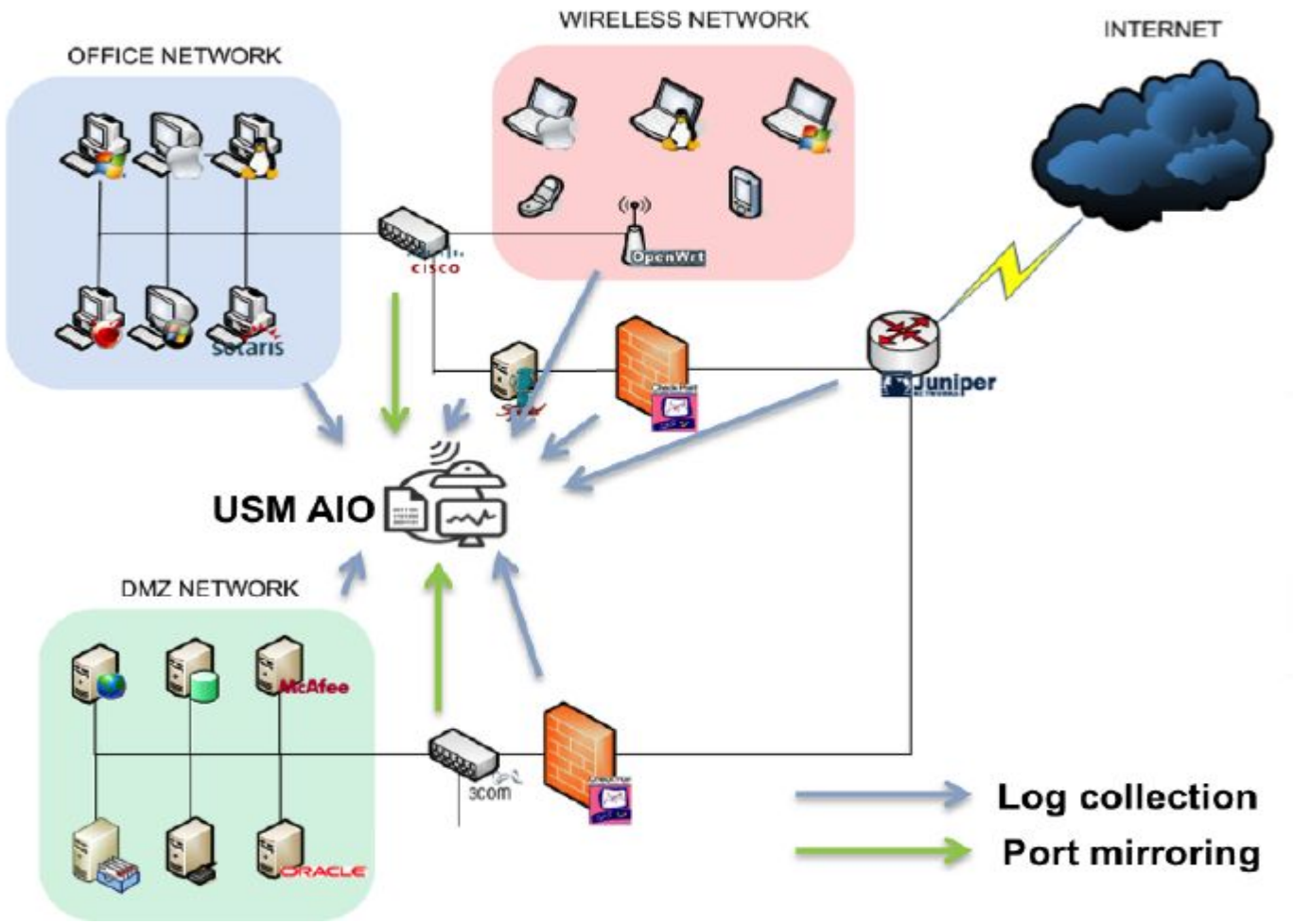
- **Sensor:** Recolecta logs y monitorea tráfico de red. Capacidades: Monitoreo de comportamiento, SIEM, detección de intrusiones, descubrimiento de activos y análisis de vulnerabilidades (1 o más instancias)

- **Server**: Agrega y correlaciona la información recolectada por el sensor. Gestión centralizada, reporte y administración (1 instancia)

- **Logger:** Almacena de forma segura los logs y eventos para investigación forense y cumplimiento de regulación (1 instancia)

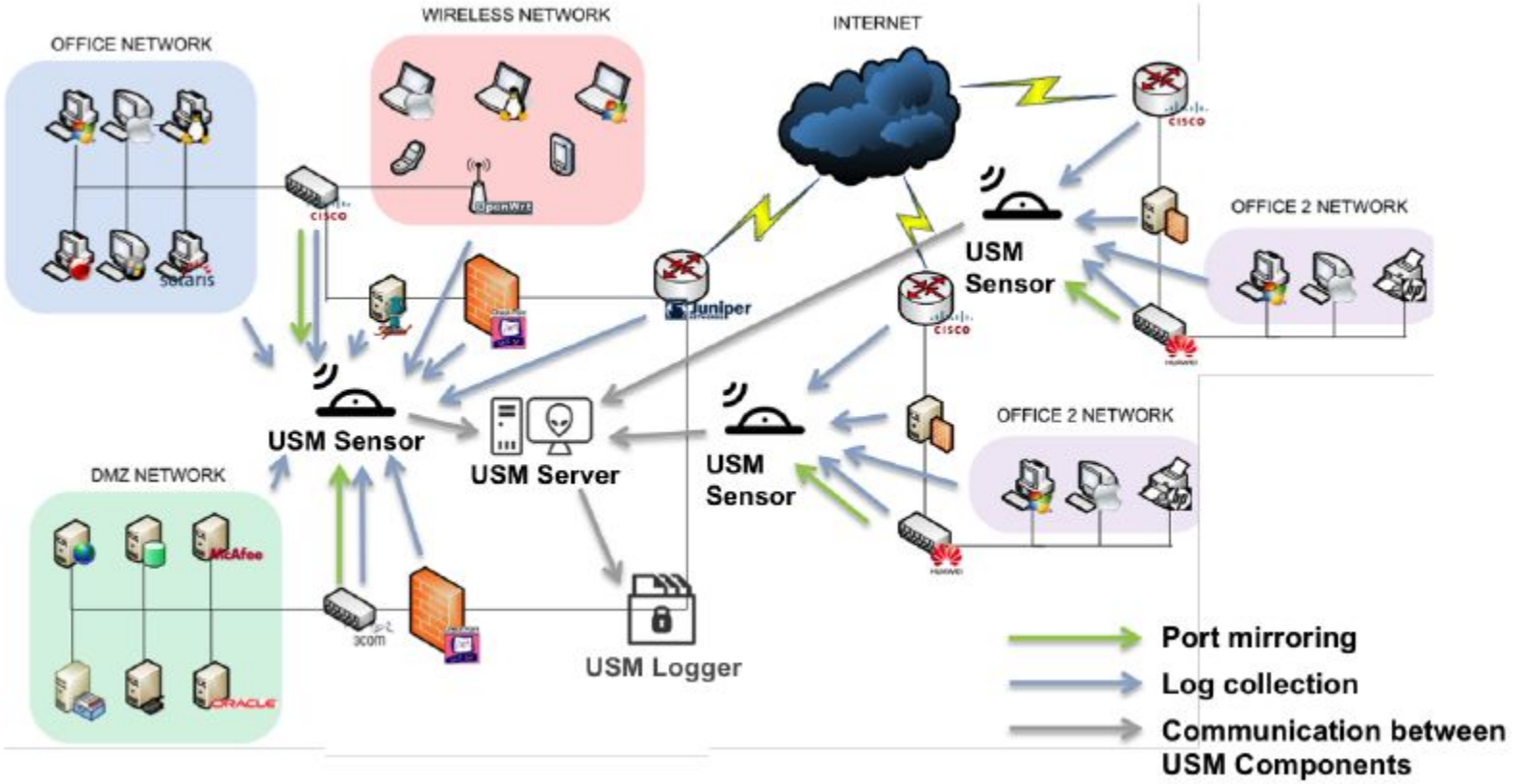
Registro de eventos

- Despliegue All-In-One



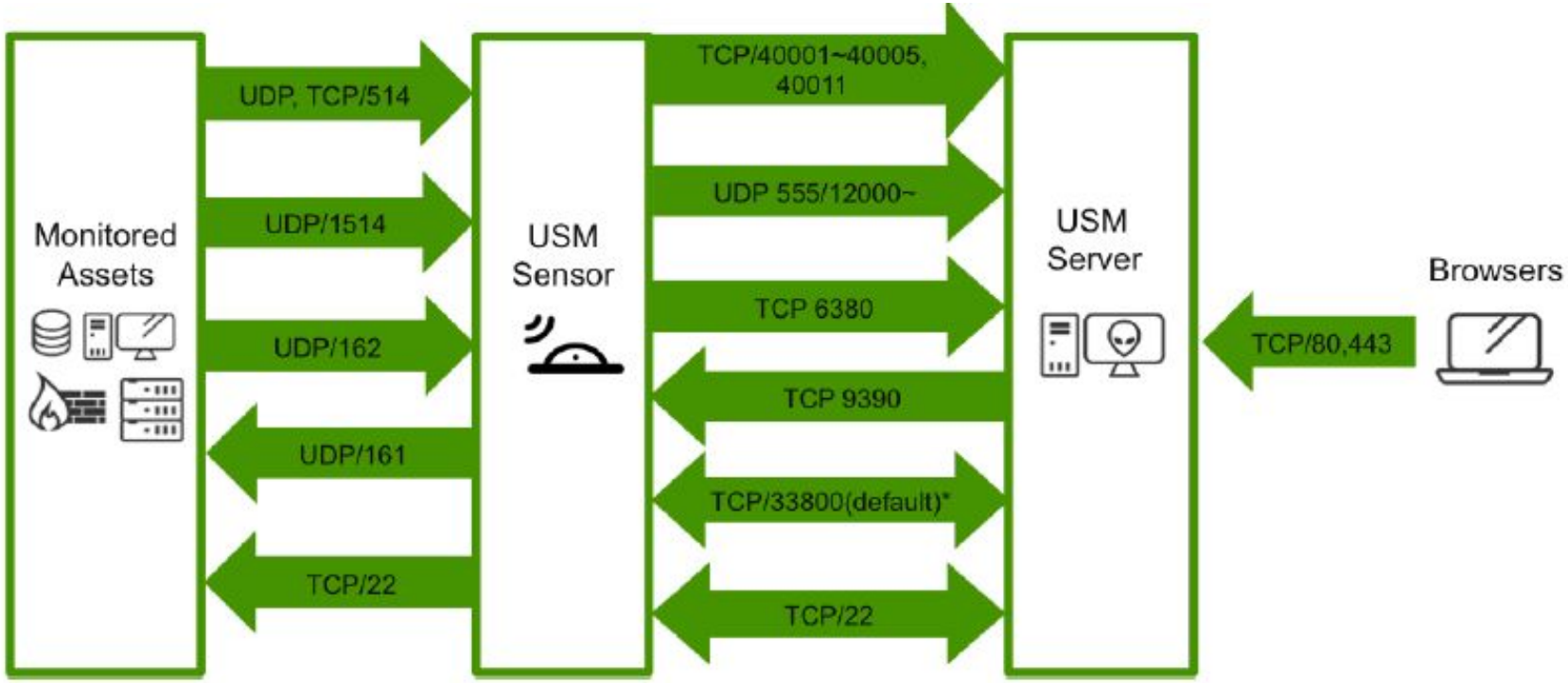
Registro de eventos

- Componentes USM Individuales: Un sensor en cada red



Registro de eventos

- Puertos usados entre componentes AlienVault



Registro de eventos

- Requerimientos para albergar un virtual appliance de OSSIM 5.1:

	USM All-in-One		Remote Sensor		USM Standard		
	1TB	500GB	1TB	250GB	Server	Logger	Sensor
Virtual Cores	8[1]		4		8		
RAM (GB)	16		8		24		
Storage (TB)	1.0	0.5	1.0	0.25	1.2	1.8	1.2
Virtualization Environment	VMware ESXi 4.x, 5.x, and 6.x						

Name	Value
CPU Type	Intel® Xeon E5620
RAM Type	DDR3 1333 MHz
Disk Type	SAS 10000 RPM (204 MB/s)
Memory Performance (MEMCPY)	3310.32 MiB/s
Disk Performance (random read/write)	15.97 Mb/s

Registro de eventos

- URL externas requeridas

Server URL	Port Number	AlienVault Features in Use	Applicable v5 Release
data.alienvault.com	80	AlienVault product and feed update	All v5 releases.
maps-api-ssl.google.com	443	Asset Location	" "
messages.alienvault.com	443	Message Center	" "
support.alienvault.com	20, 21	AlienVault Doctor	" "
telemetry.alienvault.com	443	Telemetry Data Collection	" "
tractorbeam.alienvault.com	22, 443	Remote Support	" "
www.google.com[1]	80	AlienVault API	" "
otx.alienvault.com	443	Open Threat Exchange	5.1+

Universidad del Rosario | Escuela de Ingeniería, Ciencia y Tecnología | MACC Matemáticas Aplicadas y Ciencias de la Computación | HINNT Hub de INNovación y Transferencia

GRACIAS

Daniel Díaz-López

Líder de Ciberseguridad - MACC
Profesor principal de carrera

danielo.diaz@urosario.edu.co

@MACC_URosario @MACC.URosario macc_ur