THE BRIDGE

CYBER SECURITY

SIEM

Macrodatos

- Los macrodatos, también llamados datos masivos, inteligencia de datos, datos a gran escala o **big data**.

- Los macrodatos se pueden describir por las siguientes características:
  - **Volumen**: la cantidad de datos generados y guardados.

  - **Variedad**: el tipo y naturaleza de los datos para ayudar a las personas a analizar los datos y usar los resultados de forma eficaz. Se usan textos, imágenes, audio y vídeo. También completan pedazos ¿Qué pedazos? pedidos a través de la fusión de datos.

  - **Velocidad**: en este contexto, la velocidad a la cual se generan y procesan los datos para cumplir las exigencias y desafíos de su análisis.

  - **Veracidad**: la calidad de los datos capturados puede variar mucho y así afectar a los resultados del análisis.

  - **Valor**: deben ser útiles, accionables y tener valor

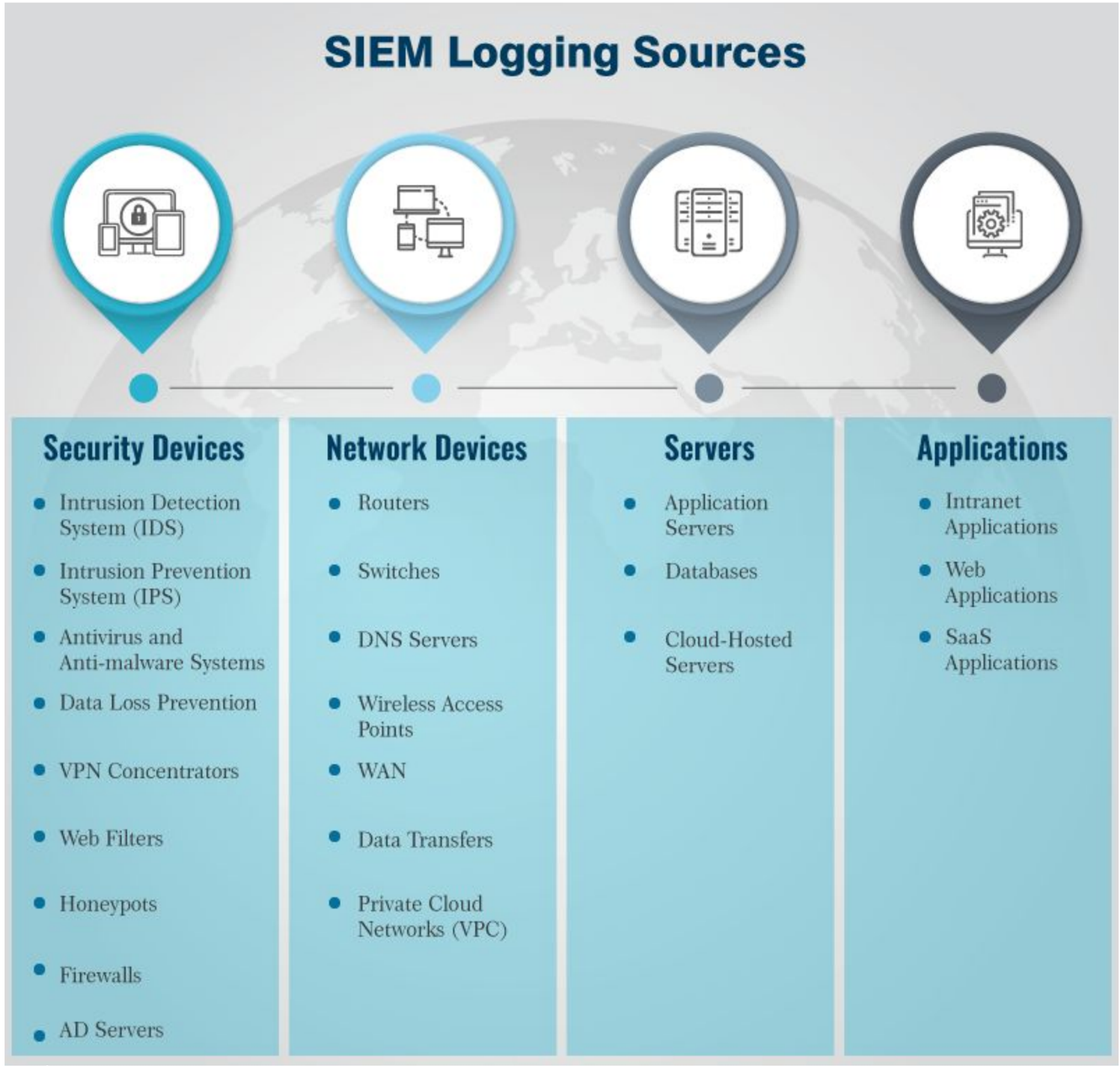
https://www.avante.es/cuanto-deberian-saber-las-empresas-de-big-data/

Correlación

- La correlación de eventos toma datos de diversas aplicaciones o de equipos, para luego analizar los datos e identificar las relaciones entre ellos.
- Las herramientas pueden realizar acciones, como enviar alertas por fallos, basándose en reglas definidas por el usuario.
- Puede determinar la causa subyacente de un problema y resolverlo rápidamente para minimizar cualquier impacto y pérdida de negocio.
- Un **ejemplo de correlación** de eventos puede ocurrir para detectar un ataque de fuerza bruta
  - **Recopilación de datos**: recibir logs de diferentes fuentes
    - **Firewall**: Detecta múltiples intentos fallidos de inicio de sesión desde una misma dirección IP.
    - **Servidor**: Registra intentos fallidos de inicio de sesión en un corto período de tiempo.
    - **IDS**: Detecta patrones de tráfico inusuales que coinciden con un ataque de fuerza bruta.
  - **Correlación de eventos**:
    - Por los eventos individuales se detecta que los intentos fallidos de inicio de sesión en el servidor y los patrones de tráfico inusuales detectados por el IDS provienen de la misma dirección IP.
    - Además, el firewall ha registrado múltiples intentos fallidos de inicio de sesión desde esa misma IP.
- Este proceso de correlación permite identificar amenazas que no serían evidentes si se analizaran los eventos de manera aislada.

Fuente de Datos

- Es el lugar donde se originan los datos utilizados o es un lugar donde se recoge la información.
- Puede ser el lugar donde se crearon los datos o donde se digitalizó la información física.
- Sin embargo, incluso los datos más elaborados pueden considerarse una fuente, siempre que otro proceso acceda a ellos y los utilice
- La fuente puede ser una base de datos, un archivo plano, un documento XML o cualquier otro formato que un sistema pueda leer.
- La entrada se captura como un conjunto de registros que contienen información utilizada en el flujo de trabajo.
- **Ejemplos de Fuentes de Datos en Ciberseguridad**



https://layots.com/security-information-and-event-management-siem-solution-its-importance/

SYSLOG

- El Protocolo de registro del sistema (**Syslog**) es una forma en que los dispositivos de red pueden usar un formato de mensaje estándar para comunicarse con un servidor de registro.

- Fue diseñado específicamente para facilitar el monitoreo de dispositivos de red.

- Los dispositivos pueden usar un **agente syslog** para enviar notificaciones mensajes bajo una amplia gama de condiciones específicas

- Los tres **servidores syslog** más utilizados son:
  - **Rsyslog**:
    - Se encarga de implementar el protocolo de syslog básico, lo extiende con filtrado basado en un contenido dado, con capacidades de filtrado enriquecido, opciones de configuración flexibles y agrega características como uso de TCP para el transporte.
    - Su diseño es de cliente / servidor, por lo tanto, puede configurarse tanto como cliente como como servidor.

  - **syslog-ng**:
    - Amplía el modelo syslogd original con filtrado basado en contenido, amplias capacidades de filtrado, opciones de configuración flexibles y agrega funciones importantes a syslog, como el uso de TCP para el transporte.
    - Por **syslog** se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

  - **Nxlog:**
    - Es una herramienta de centralización y recopilación de registros multiplataforma que ofrece funciones de procesamiento de registros, incluido el enriquecimiento de registros (análisis, filtrado y conversión) y el reenvío de registros.
    - Es compatible con todos los principales sistemas operativos, como Windows, macOS, IBM AIX, etc., y es compatible con muchos **SIEM**.
    - Puede manejar diferentes fuentes y formatos de registro, por lo que se puede utilizar para implementar un sistema de registro escalable

Conceptos

- **Archivo de logs**
  - Los Archivos de registro (o archivos de log) son archivos que contienen mensajes sobre el sistema, incluyendo el kernel, los servicios y las aplicaciones que se ejecutan en dicho sistema.

  - Existen diferentes tipos de archivos de log dependiendo de la información.
    - Por ejemplo, existe un archivo de log del sistema, un archivo de log para los mensajes de seguridad y un archivo de log para las tareas cron.

  - En general, la línea de un log contiene:
    - Evento recopilado (p. ej., inicio de programa)
    - Marca de tiempo, que le asigna fecha y hora
    - Por lo general, la marca de tiempo se genera primero, con el fin de reflejar la secuencia cronológica de los eventos.

  - La mayoría de los archivos de registro en **Linux** están localizados en el directorio **/var/log,** aunque algunas aplicaciones como por ejemplo httpd y samba tienen un directorio en **/var/log** para sus archivos de registro.

  - En todas las versiones de servidores **Windows** se encuentra la aplicación llamada Visor de Eventos (**Event Viewer**)

  - En la práctica, el Reglamento **GDPR** exige que se mantenga un registro de las operaciones realizadas con los datos.

    - Esto es así para que, en caso de control, se pueda demostrar que se han tomado todas las medidas de protección.

    - En este sentido, guardar los archivos de registro es muy útil.

SIEM

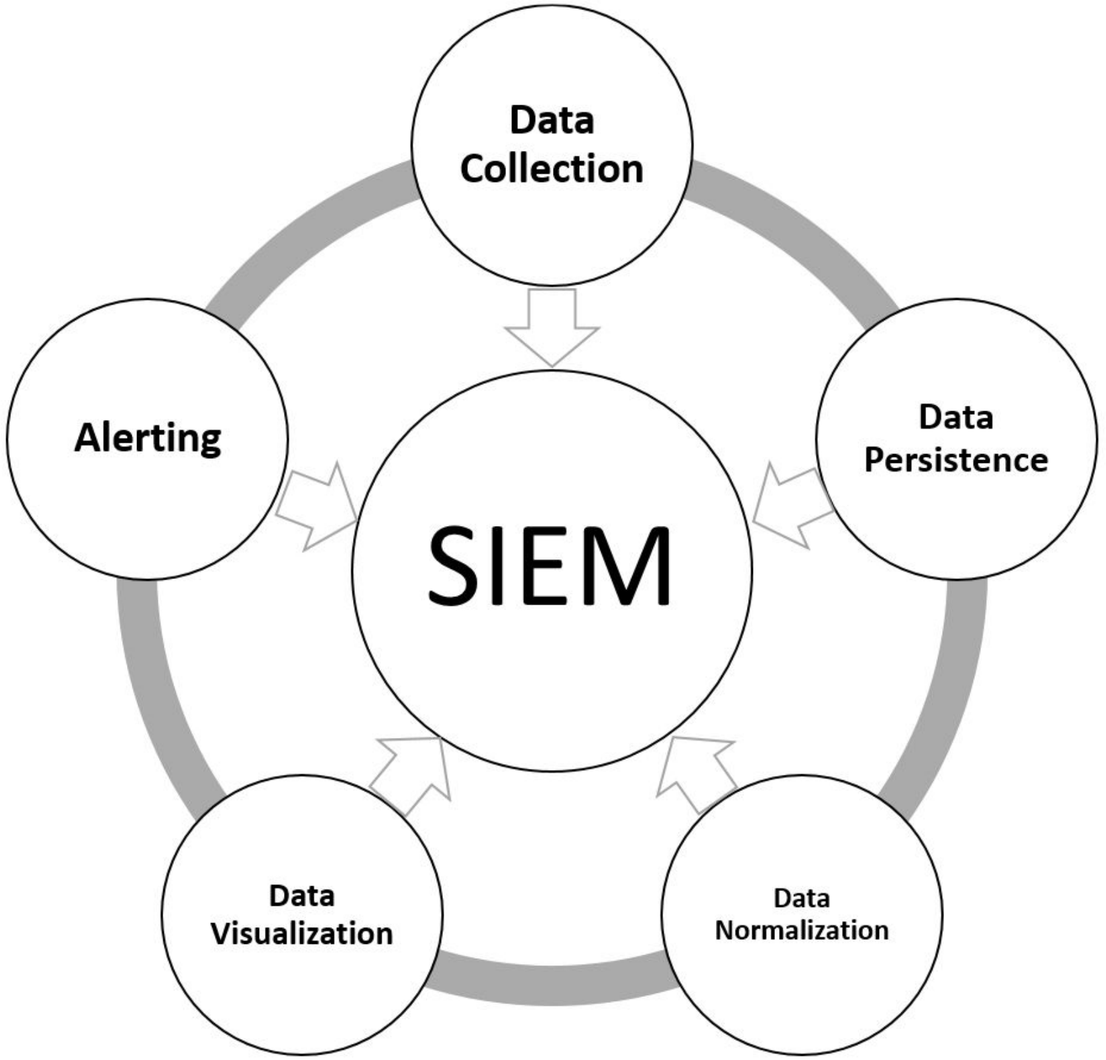
- **SIEM**, que significa **Security Information and Event Management** (**Gestión de Información y Eventos de Seguridad**), es una solución de seguridad que ayuda a las organizaciones a detectar, analizar y responder a amenazas de seguridad antes de que afecten sus operaciones.

- Los sistemas **SIEM** recopilan y analizan datos de eventos de seguridad de diversas fuentes dentro de una infraestructura de TI, como aplicaciones, dispositivos, servidores y usuarios.

- Utilizan reglas y análisis en tiempo real para identificar actividades anómalas y generar alertas.

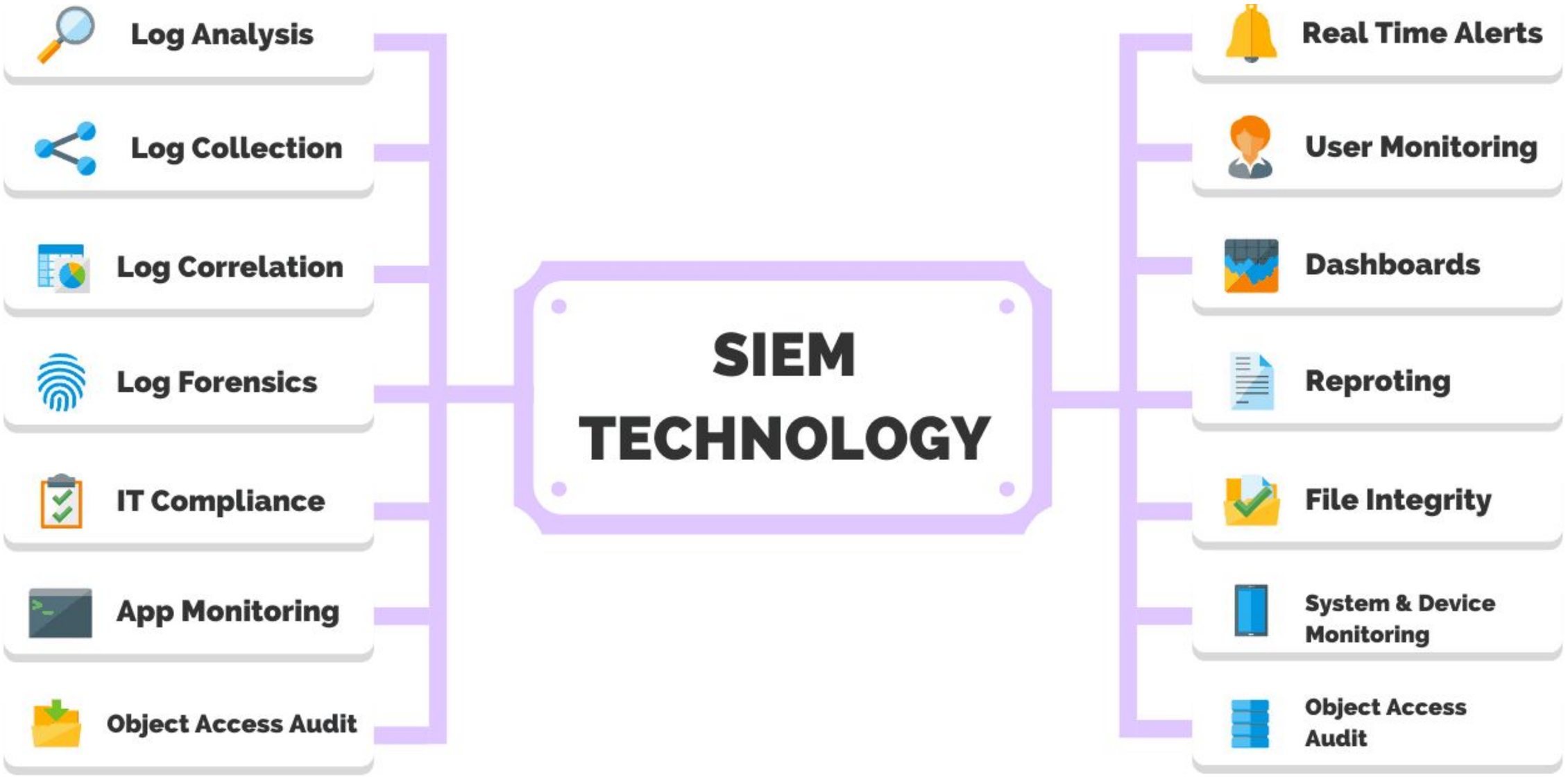
- Además, integran inteligencia artificial y aprendizaje automático para mejorar la detección de amenazas y la respuesta a incidentes.

- En resumen, **SIEM** proporciona una visión centralizada de la seguridad de una organización, permitiendo una respuesta rápida y eficaz a posibles ciberataques



https://subscription.packtpub.com/book/data/9781788472173/11/ch11lvl1sec85/understanding-siem

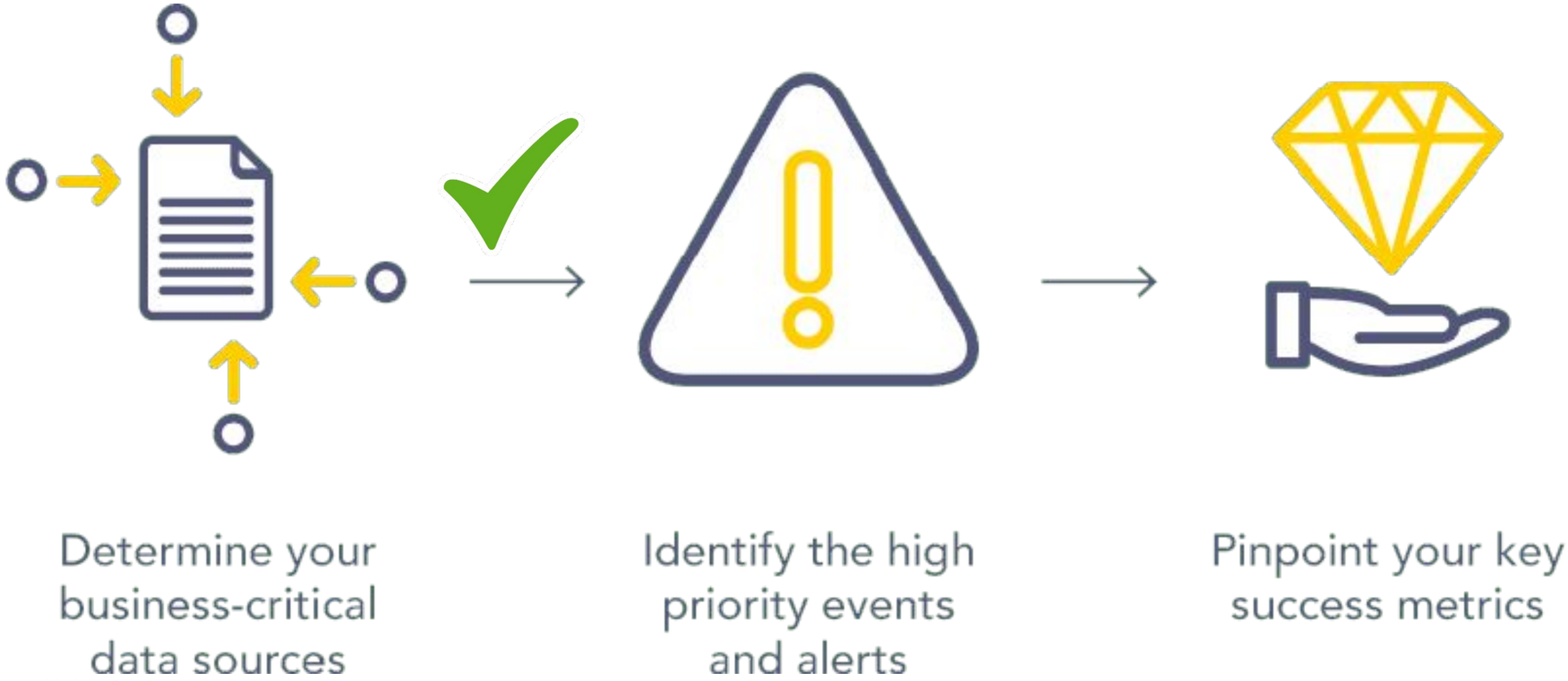
Componentes SIEM



https://purplesec.us/siem-solutions/

Pasos para implementar un SIEM

- **Determine las fuentes de datos críticas para su negocio**
  - Una vez que tenga una idea del alcance ideal del proyecto, puede identificar las fuentes de registro dentro del alcance para determinar cómo obtener los datos relevantes necesarios.
  - Por ejemplo, los firewalls, los sistemas de detección de intrusos y el software antivirus sirven como fuentes de datos principales para los casos de uso de seguridad SIEM. Pero hay muchos más, incluidos enrutadores, filtros web, controladores de dominio, servidores de aplicaciones, bases de datos y otros activos conectados digitalmente.
  - Debe priorizar las fuentes incluidas para garantizar que SIEM proporcione los datos deseados para respaldar los casos de uso seleccionados.



https://www.logpoint.com/en/understand/what-is-siem/

Pasos para implementar un SIEM

- **Identificar los eventos y alertas de alta prioridad**
  - Cuando se trata de proteger una organización contra amenazas internas y externas, los equipos de seguridad se enfrentan a una lista cada vez mayor de eventos de seguridad que deben analizarse y actuar en consecuencia.
  - Para superar el ruido, el software SIEM se puede usar para hacer que los eventos y los datos sean más reveladores.
  - Aun así, las empresas primero deben determinar sus eventos de alta prioridad y cómo derivarlos de las aplicaciones y dispositivos dentro de la infraestructura.
  - De esta manera, los equipos de seguridad pueden usar SIEM para dedicar más tiempo a incidentes y alertas que pueden ser críticos para el negocio y sus datos.

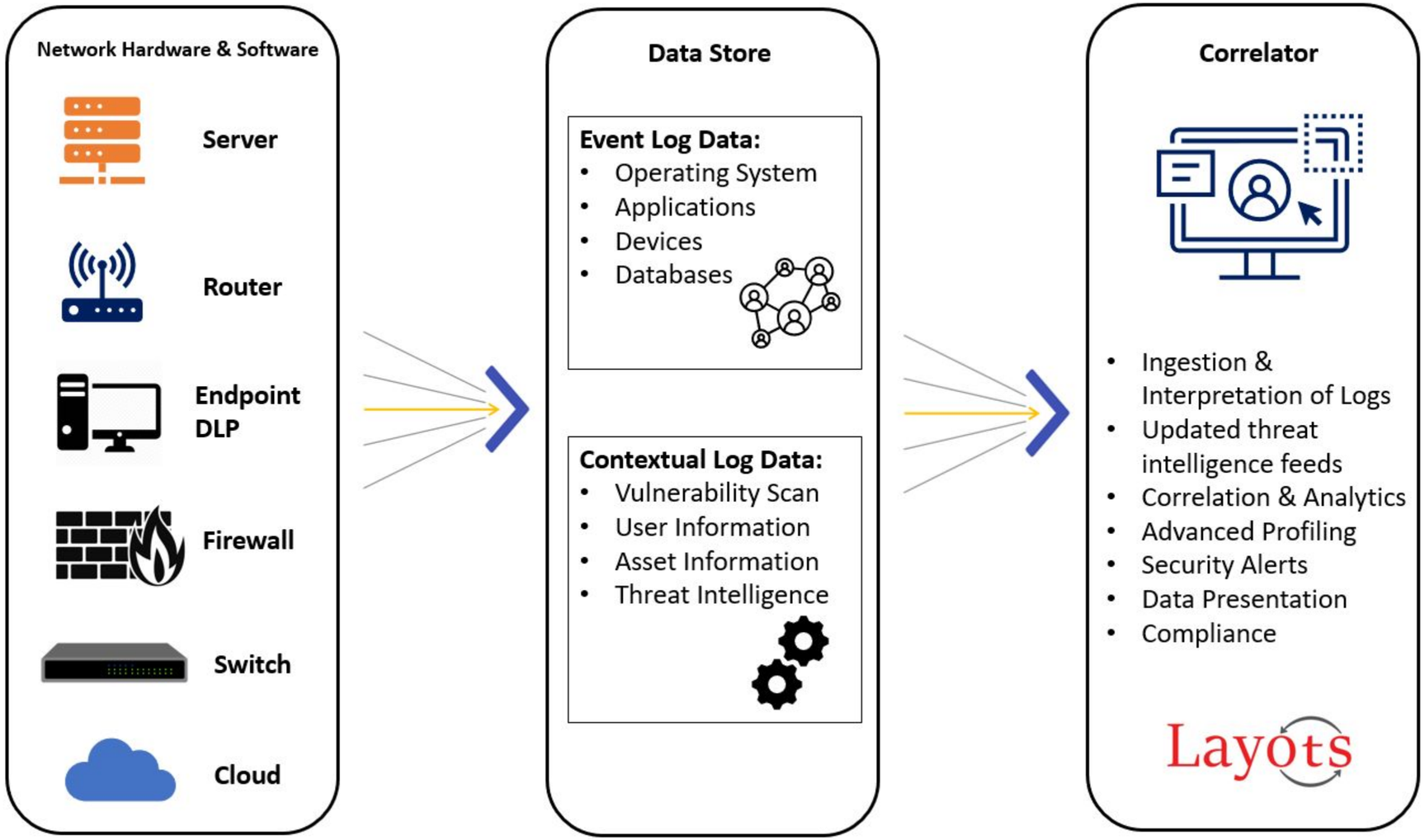
https://www.logpoint.com/en/understand/what-is-siem/

Pasos para implementar un SIEM

- **Identifique sus métricas clave de éxito**
  - Una implementación exitosa de SIEM se alinea con sus objetivos comerciales.
  - Las métricas clave de éxito deben determinarse antes de la implementación para garantizar el máximo retorno de la inversión.
  - Por ejemplo, reducir el robo de datos o mejorar la forma en que las empresas detectan posibles infracciones o amenazas internas pueden ser métricas a establecer.
  - Pero hay muchos otros. Las empresas deben determinar qué significa el éxito para ellas y cómo se pueden utilizar los casos de uso de seguridad SIEM para lograrlo.

https://www.logpoint.com/en/understand/what-is-siem/

Fases



https://layots.com/security-information-and-event-management-siem-solution-its-importance/

Capas

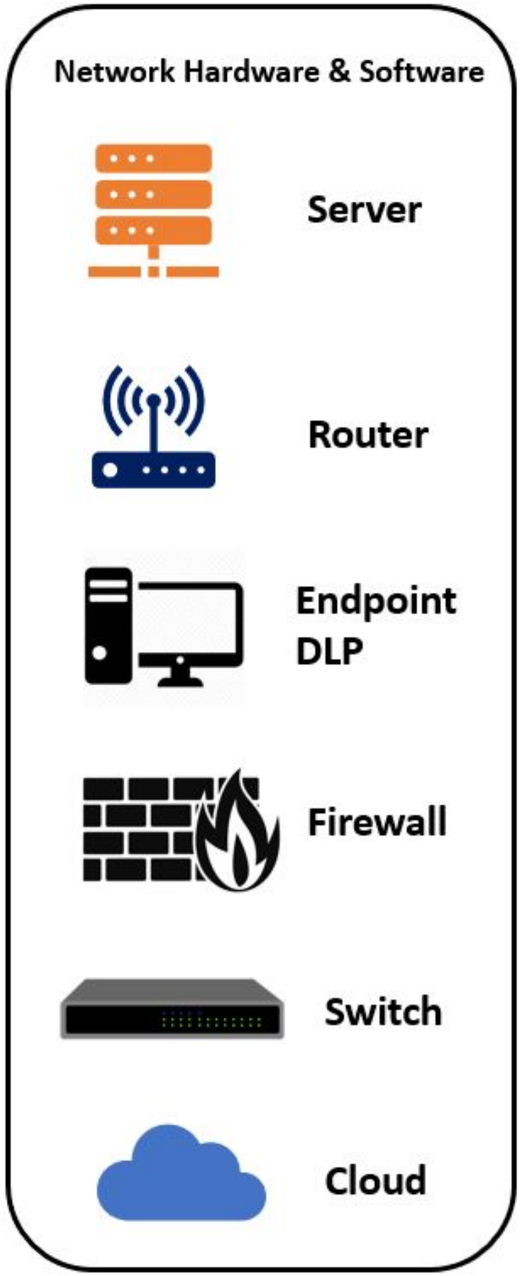
- **Recolección de datos**
  - Flow Tráfico de datos
    - Tráfico de router, switch, etc...

  - **Registros de eventos**
    - **Eventos**: Logs de firewall, syslog, proxys, servidores Windows, servidores WEB.
      - **syslog**
        - Estándar para envío de mensajes a una red.
        - Es un protocolo + una aplicación o biblioteca.
        - Implementación en Linux : rsyslogd
        - Implementación en Windows : nxlog

      - **wincollect**
        - Forwarder de eventos de Windows a un sistema centralizado.
        - Puede instalarse como agente en una maquina Windows o bien que una maquina Windows con WinCollect recoja del resto de equipos Windows sin instalarse.

    - **SNMP**

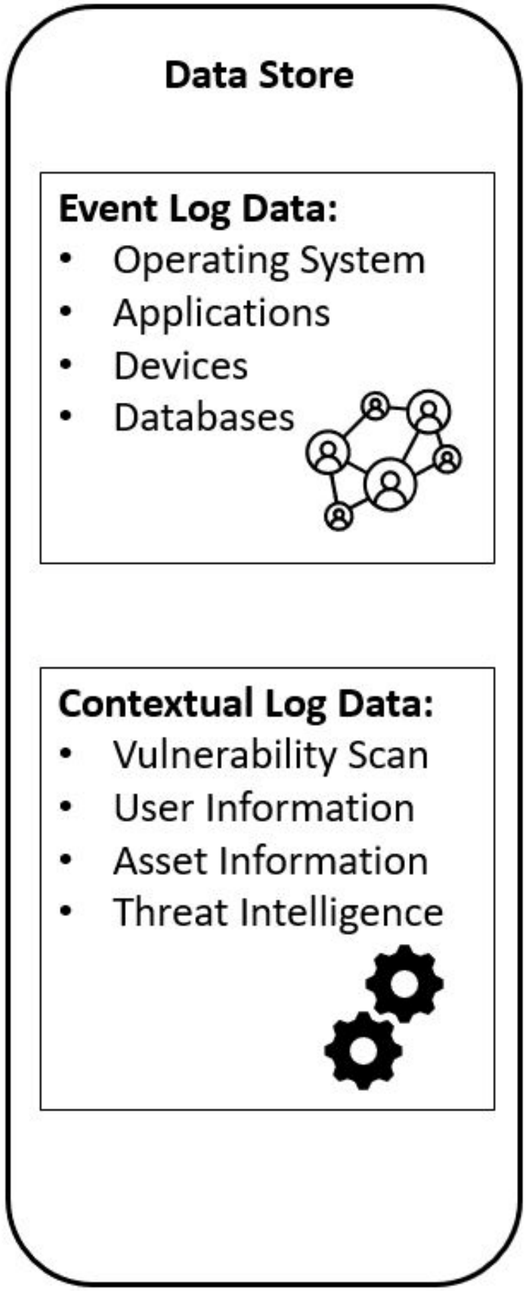
    - **Propietarios**



https://layots.com/security-information-and-event-management-siem-solution-its-importance/

Capas

- **Almacenamiento y procesamiento de datos**
  - **Almacenamiento**
    - SQL y NoSQL
    - Esquema de la base de datos
      - Importante tener un mapa del esquema de la base de datos para las consultas
      - Ejemplo : Elastic Common Schema
        - https://www.elastic.co/es/blog/introducing-the-elastic-common-schema
  - **Procesamiento**
    - Clasifica los datos en
      - Alertas
      - Ataques
      - Métricas de riesgo
      - Vulnerabilidades
      - Registros para forense
      - Cada software lo gestiona de una manera diferente y hay varios módulos para esto



https://layots.com/security-information-and-event-management-siem-solution-its-importance/

Capas

- **Búsqueda y correlación de datos**
  - Búsquedas mediante interfaz
  - Búsquedas avanzadas
    - **RegExp**
      - Secuencia de caracteres que forma un patrón de búsqueda.
      - Indica una manera de buscar basada en una cadena de caracteres.
      - Se puede usar en herramientas como grep, sed, sublime text...
        - https://regexr.com/
        - https://regex101.com/
      - **SQL**
        - Subconjunto de SQL para consultas en tablas de la base de datos del SIEM usando SELECTs.
        - AQL IBM QRadar
        - Elastic SQL
      - **DSL**
        - Domain Specific Language
        - Búsquedas basadas normalmente en JSON
        - Elastic DSL

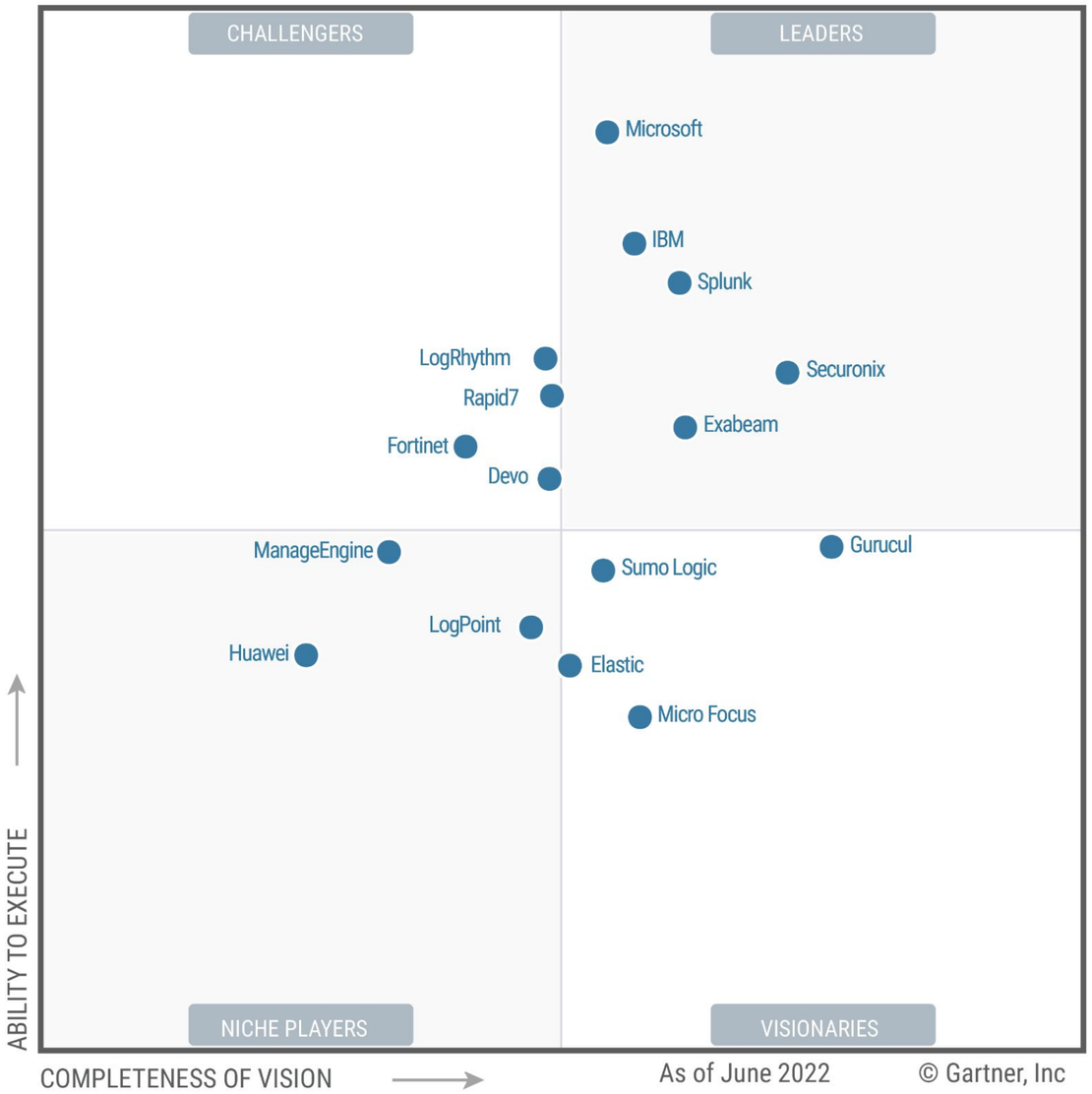
https://layots.com/security-information-and-event-management-siem-solution-its-importance/

Soluciones de mercado

Open Source

- AlienValue
- Wazzuh
- Elastic Search
- OSSEC
- SAGAN

Figure 1: Magic Quadrant for Security Information and Event Management



https://www.manageengine.com/latam/log-management/manageengine-reconocido-gartner-magic-quadrant-2022-siem.html


THE
BRIDGE