# Security Information & Event Management

- Security Information Management (SIM)
  - Seguimiento de eventos en tiempo real
  - Envío y generación de alertas e informes
  - Respuesta automática a las incidencias
  - Correlación de datos de múltiples fuentes para mejorar la calidad de la información presentada
  - Traducción de registros de eventos de diferentes recursos a través de archivos XML
- Security Event Management (SEM)
  - Monitorización de eventos en tiempo real
  - Obtención de eventos de seguridad en dispositivos y aplicaciones dentro del sistema
  - Correlación de eventos para proporcionar una imagen clara del sistema de información
  - Analizar los registros según su nivel de importancia
  - Respuesta a incidentes en tiempo real
- SIEM
  - Advanced Threat Detection: capaces de supervisar y correlacionar de forma continua y en tiempo real la totalidad de la empresa, por lo que pueden ayudar a detectar, mitigar y prevenir amenazas avanzadas
  - Forensics and Incident Response: pueden ayudar a las organizaciones en una investigación forense almacenando y protegiendo los registros históricos y proporcionando herramientas para navegar rápidamente y correlacionar los datos. Los SIEM pueden ayudar a los analistas de seguridad a darse cuenta de que se está produciendo un incidente de seguridad y a establecer medidas inmediatas para solucionarlo
  - Compliance Reporting and Auditing: pueden ayudar a las organizaciones a demostrar a los auditores y reguladores que se cumplen ciertos requisitos. El SIEM agrega los datos de registro de toda la organización y los presenta en un formato listo para la auditoría
  - Otras razones por las que las empresas necesitan SIEM son: el almacenamiento de datos, la obtención y el mantenimiento de certificaciones (ISOs), la gestión y retención de registros, la gestión de casos o los sistemas de tickets, y la validación de la aplicación de políticas y las violaciones de las mismas.
- Plataformas
  - Splunk
  - Graylog
  - Arcsight
  - QRadar
  - LogRhythm
- Logging and Aggregation
  - Syslog — Syslog Messages
    - Priority Value (PRI) — El valor de la prioridad se deriva tanto del código de la instalación como del nivel de gravedad
    - Header — Contiene información de identificación, como por ejemplo: marca de tiempo, nombre del host, nombre de la aplicación, ID del mensaje. Esto es útil para entender de dónde proviene el mensaje del sistema
    - Message — texto simple y legible o sólo legible por la máquina. El contenido del mensaje no está definido por el protocolo, sólo el formato
  - Windows Event Logs
    - Ruta
      - `Windows 2000 to WinXP/Windows Server 2003: %WinDir%\system32\Config*.evt`
      - `Windows Server 2008 to 2019, and Windows Vista to Win10: %WinDir%\system32\WinEVT\Logs*.evtx`
    - Categorias
      - Aplicación: Eventos registrados por una aplicación (ejecución, error de despliegue, etc.)
      - Sistema: Eventos registrados por el sistema operativo (carga de dispositivos, errores de inicio, etc.)
      - Seguridad: Eventos relevantes para la seguridad del sistema (inicios y cierres de sesión, eliminación de archivos, concesión de permisos de administración, etc.)
        - Account logon events (valid and invalid sign-ons and sign-offs)
        - Account management (creation, modification, interaction and deletion of user accounts)
        - Privilege use
        - Resource usage (file creation, modification, interaction and deletion)
      - Servicio de directorio: Es un registro disponible sólo para los Controladores de Dominio, almacena los eventos de Active Directory (AD).
      - Servidor DNS: Es un registro disponible sólo para los servidores DNS, se almacenan los registros del servicio DNS.
      - Servicio de Replicación de Archivos: Es un registro disponible sólo para los Controladores de Dominio, almacena los eventos de Replicación de Controladores de Dominio.
    - Event Viewer — Vistas personalizada — Login Monitoring
      - `User Logon Successful - 4624`
      - `Special Logon - 4672`
      - `User Initiated Logoff - 4647`
      - `User Logoff - 4634`
  - Sysmon
    - Registra la creación de procesos con la línea de comandos completa tanto para el proceso actual como para el proceso padre
    - Incluye un GUID de sesión en cada evento para permitir la correlación de eventos en la misma sesión de inicio de sesión
    - Registra la carga de drivers o DLLs con sus firmas y hashes
    - Registra opcionalmente las conexiones de red, incluyendo el proceso de origen de cada conexión, las direcciones IP, los números de puerto, los nombres de host y los nombres de puerto
    - Detecta los cambios en la hora de creación de los archivos para saber cuándo se creó realmente un archivo. La modificación de las marcas de tiempo de creación de archivos es una técnica comúnmente utilizada por el malware para cubrir sus huellas
    - Filtrado de reglas para incluir o excluir determinados eventos de forma dinámica
  - Otros
    - `Microsoft Azure`
    - `Amazon Web Services`
    - `OSQuery`
    - `Moloch`
- Log Aggregation
  - Proceso de recopilación de registros de múltiples sistemas informáticos, su análisis, la extracción de datos estructurados y su agrupación en un formato que sea fácil de buscar y explorar con las herramientas de datos modernas.

    Hay cuatro formas habituales de agregar registros, y muchos sistemas de agregación de registros combinan varios métodos. Estos incluyen:
    - Syslog — Un protocolo de registro estándar. Los adminis de red pueden configurar un servidor Syslog que reciba los registros de varios sistemas y los almacene en un formato eficiente y condensado que sea fácilmente consultable
    - Event Streaming — SNMP, Netflow e IPFIX permiten a los dispositivos de red proporcionar información estándar sobre sus operaciones, que puede ser interceptada por el agregador de registros, analizada y añadida al almacenamiento central de registros
    - Log Collectors — Agentes de software que se ejecutan en los dispositivos de red, capturan la información de los registros, la analizan y la envían a un componente agregador centralizado para su almacenamiento y análisis
    - Direct Access — Los agregadores de registros pueden acceder directamente a los dispositivos de red o a los sistemas informáticos, utilizando una API o un protocolo de red para recibir directamente los registros. Este enfoque requiere una integración personalizada para cada fuente de datos
- Correlation
  - Normalization and Processing
    - Log Enrichment — adición de información importante que puede hacer que los datos generales sean más beneficiosos para los analistas de seguridad cuando investigan las alertas o la actividad inusual
    - Log Indexing — La indexación puede agilizar la búsqueda de atributos específicos en grandes datos, en comparación con la necesidad de escanear cada uno de los datos del almacenamiento SIEM para obtener las respuestas que se necesitan
    - Log Storage
    - Normalization — proceso de cambiar los formatos de los registros a un formato que sea lo más similar posible en todos los dispositivos y fuentes de registros, lo que da un respiro al SIEM y permite una búsqueda y un desglose de la información más coherentes
  - `Sigma`

Presented with xmind