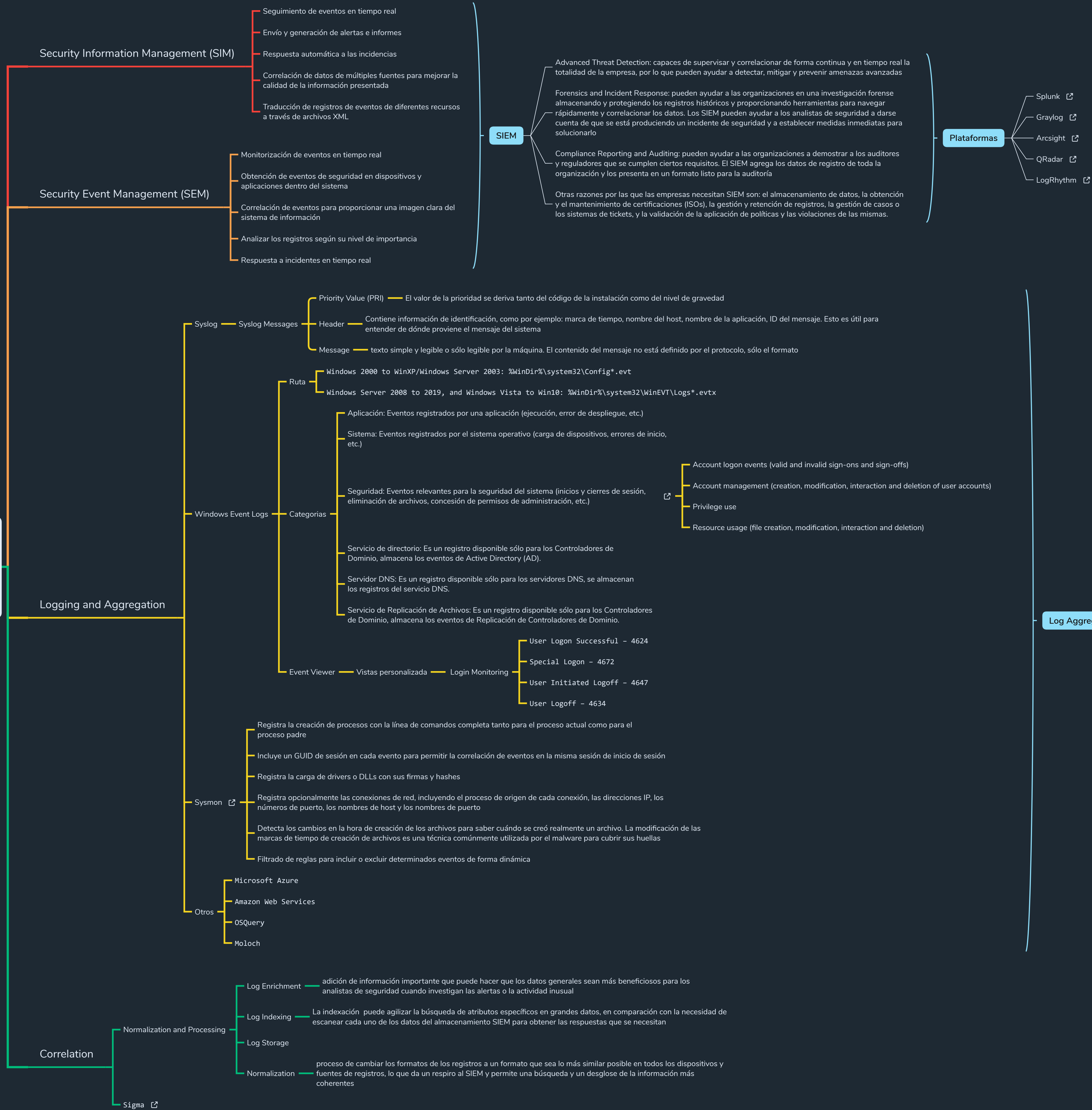


Security Information & Event Management



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