Herramientas SIM/SEM/SIEM

Splunk

Tipo: SIEM

Potente para análisis de grandes volúmenes de datos. Costoso pero muy versátil.

Descarga: https://www.splunk.com/en_us/download.html

Documentación: https://docs.splunk.com/

Elastic SIEM

Tipo: SIEM

Basado en ELK stack (Elasticsearch, Logstash, Kibana). Gratuito y escalable.

Descarga: https://www.elastic.co/downloads/

Documentación: https://www.elastic.co/guide/en/security/current/index.html

IBM QRadar

Tipo: SIEM

Usado en grandes corporaciones, con funciones avanzadas de análisis.

Descarga: https://www.ibm.com/products/qradar-siem

Documentación: https://www.ibm.com/docs/en/qradar-common?topic=SS42VS

AlienVault OSSIM

Tipo: SIEM (open source)

Muy completo, incluye IDS, escaneo de vulnerabilidades y SIEM.

Descarga: https://cybersecurity.att.com/products/ossim

Documentación: https://cybersecurity.att.com/documentation

LogRhythm

Tipo: SIEM

Fuerte en monitoreo en tiempo real y análisis de comportamiento.

Descarga: https://logrhythm.com/free-tools/

Documentación: https://docs.logrhythm.com/

Graylog

Tipo: SIM

Enfocado en gestión y análisis de logs. Interfaz moderna.

Descarga: https://www.graylog.org/downloads

Documentación: https://docs.graylog.org/

ArcSight (Micro Focus)

Tipo: SIEM

Antiguo líder en el sector, usado en entornos empresariales grandes.

Descarga: https://www.microfocus.com/en-us/products/arcsight-siem/overview

Documentación: https://www.microfocus.com/documentation/arcsight/