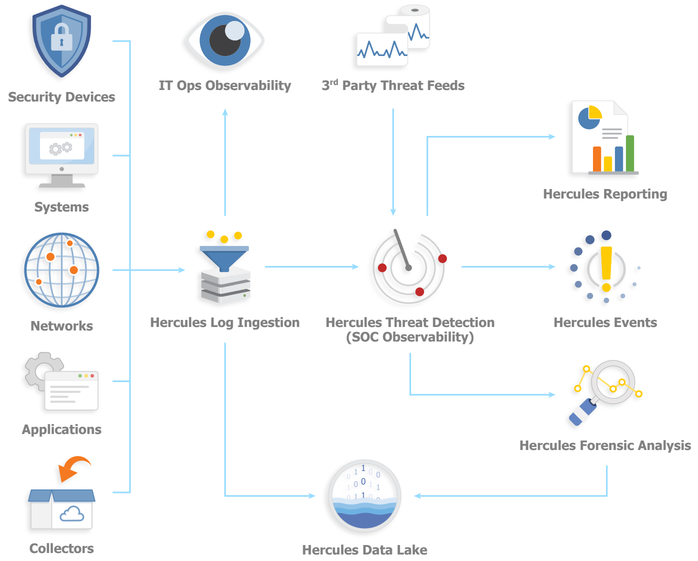
Hercules SIEM+

Turn your log entries and events from security systems into actionable information for your SOC and Customers

For organizations needing a centralized solution to automate security log information and threat detection

Product Overview

Delivered as a turnkey solution as a service, Hercules SIEM+ supports your security team, allowing visibility to relevant data to better detect threats in real time, manage incident response, perform forensic investigation on emerging and past security incidents, and prepare audits for compliance purposes.



Business Level Benefits

- Customer and system onboarding support
- Detection rules that are proven to address MITRE ATT&CK Framework best practices
- NIST aligned support approach
- Log agnostic ingestion without agents or heavy forwarders
- Cloud or on-premise hosting, adapted to your environment (e.g., to your service desk applications)
- Includes jurisdiction-specific compliance support
- Connects to other security areas (e.g., Policy, SOAR, Incident Response, etc.)

Features

Agnostic Log Ingestion

Accepting logs in native formats from log collectors, sources, and systems

Log Archive

Data lake adapted to your log retention schedules, no matter how long

Threat Detection

Out of the box inclusion of over 90% of all MITRE ATT&CK Framework threats and the ability to accept additional threat feeds

FARO Differentiators for Government

You can count on FARO's Solutions to support customer confidence in IT execution:

- Pre-Engineered Solutions – We removed the "some assembly required" issues with low risk, proven solutions, that reduce delays in implementation
- Customer Site or Cloud Friendly – FARO works with any FedRAMP Moderate Public Cloud
- Team Support – We are integrated, with named resources that align as an extension of your existing team
- Deployment Support – Fully managed or shared responsibility
- Compliance Support – Unlike other vendors, FARO is at your side with NIST, FIPS, HIPAA, and State-specific compliance and audit tasks
- 24x7 Support – Our team is providing "around the clock" support including night and weekend deployments with your teams or on behalf of your teams
- Engineering Support – Connecting and supporting defined solutions in a complicated ecosystem of your environment

Compatability Model

Hercules SIEM+ can be integrated with numerous popular products including:

- Splunk
- Microsoft
- AWS
- Salesforce (Mulesoft)
- Elastic
- DataDog
- Exabeam
- IBM