LOGPOINT

Is your business equipped to navigate treacherous cyber waters?

Every business faces a perilous sea of cyber threats

- Stealthy, multi-vector attacks that continuously evolve
- Numerous cybersecurity point solutions and not enough integration
- Difficult to prioritize alerts
- Not enough cybersecurity analysts and skills on board
- Threat volume and complexity have eclipsed manual solutions

Not all enterprises are well equipped for the voyage

- Tight cybersecurity budget
- Lacking security personnel and skillsets
- No SOAR –SOC team thinks it's too complex
- Little or no formal threat response process
- Manual SOC methods leave no time

You need SIEM + SOAR to navigate treacherous cyber waters

Businesses need both SIEM and SOAR to respond effectively and efficiently to the increasing volume and velocity of complex cyber threats. If your SOC is short on cybersecurity expertise and budget LogPoint SIEM-SOAR solutions can help.

SIEM
Security Information and Event Management

- Real-time data analysis
- Early detection of security breaches
- Central data collection and storage
- Event reporting

+

SOAR
Security Orchestration, Automation and Response

- Correlate and prioritize alerts
- Automate playbooks to accelerate investigation and response
- Guide analysts to the best response

=

- Less cyber risk
- Increased SOC efficiency
- Better cyber intelligence

Affordable SIEM-SOAR innovation for mid-size business

LogPoint SIEM-SOAR solutions deliver immediate and long-term value for reducing cybersecurity risk and improving SOC efficiency.

You get:

- Integrated collection, analysis, and prioritization of event logs from all cyber systems
- Built-in detection, investigation, and response playbooks automate critical processes right away
- Guided decisions increase SOC productivity and assure consistent response
- Out-of-the-box integrations and open APIs that accelerate time to value
- Coupled SIEM-SOAR solution is easy to deploy, learn and use
- Predictable cost structure

Fast Analysis

Normalize all event logs into a common structure to enable fast alert analysis, correlation and prioritization

Automation

Apply supporting and contextual information to accelerate investigation and provide and accurate threat picture

Orchestration

Put all relevant information at analyst fingertips and use automated playbooks to guide SOC response

Analytics

Full mapping to MITRE ATT&CK framework plus LogPoint's simple query language lets you analyze security data across all sources

LOGPOINT