Logsign | bakotech®

Improving Cyber Resilience: How Logsign Unified SO Platform Outshines SIEM, SOAR, and XDR

What are the key differences between SIEM, SOAR, XDR & Logsign Unified SO Platform?

SIEM, SOAR, XDR and Logsign USO Platform are all cybersecurity technologies that help organizations detect, investigate, and respond to cyber threats. However, they differ in their scope, capabilities, and focus. Here are the key differences between them:

SIEM

Security Information and Event Management (SIEM) solutions collect and analyze security-related data from various sources, such as network devices, servers, and endpoints. SIEM tools correlate the data and generate alerts when suspicious activity is detected. SIEM is focused on identifying security incidents and providing visibility into security events across an organization's IT environment.

SOAR

Security Orchestration, Automation, and Response (SOAR) solutions automate and streamline incident response processes. SOAR tools integrate with other security technologies, such as SIEM and EDR, to help security teams manage alerts, automate incident response tasks, and investigate and resolve security incidents more efficiently.

XDR

Extended Detection and Response (XDR) is an advanced and more developed version of EDR and expands the scope of detection and response beyond endpoints to include other parts of the IT environment, such as cloud infrastructure and network devices. XDR solutions use analytics and machine learning to correlate security data across different security products and generate alerts when threats are detected.

Logsign Unified SO Platform:

The Logsign Unified SO Platform is an advanced security management platform enriched with features such as log management, event correlation, enrichment and detection, threat intelligence, incident management, automation-orchestration, and advanced reporting. It uses advanced analytics to analyze security data from multiple sources, including network devices, servers, applications, and endpoints. Logsign USO Platform integrates next-gen SIEM, threat intelligence, UEBA, and SOAR and empowers organizations to optimize and streamline their cybersecurity operations.

In addition to that, the platform offers seamless integration capabilities, allowing them to effortlessly integrate their existing security software and leverage our vast integration library, expanding the Logsign USO Platform's functionality and providing a comprehensive security management experience. With these extensive capabilities, it allows organizations to improve their security posture and ensure compliance with relevant regulations and standards.

Solutions Chart for SIEM, SOAR, XDR & Logsign Unified SO Platform

Solutions	Key Functionality	Main Feature	Use Cases
SIEM	Collects and aggregates security events from different sources, analyzes events to detect security threats, generates alerts for investigation	Centralized security event management	Identifying potential security incidents, providing a centralized view of security events, compliance monitoring
SOAR	Automates incident response through playbooks and workflows	Orchestration and automation of security operations	Automating investigation and remediation of security incidents, reducing response time, improving consistency of response
XDR	Provides comprehensive threat detection and response across multiple domains	Cross-domain threat detection and response	Correlating and analyzing security events from different sources, detecting advanced threats across endpoints, network, and cloud
Logsign Unified SO Platform	Provides a comprehensive, unified-whole platform for security management, threat detection, and incident response for enterprises of all sizes.	Security management on an integrated platform	Collecting, correlating and analyzing data from various sources, providing comprehensive visibility, investigating, identifying potential threats efficiently, respond promptly to incidents automatically to remediate and mitigate.

Note: Certain functions of the technologies mentioned may vary from vendor to vendor. Explained by considering general abilities.

Comparison Chart for SIEM, SOAR, XDR & Logsign Unified SO Platform

Solutions	SIEM	SOAR	XDR	Logsign Unified SO Platform
Log Management	✓	✕	✕	✓
Real-Time Monitoring	✓	✓	✓	✓
Detailed Investigation	✕	✓	✓	✓
Data Examination	✓	✕	✕	✓
Compliance Reporting	✓	✕	✕	✓
Incident-Case Management	✕	✓	✓	✓
Threat Detection and Response	✕	✓	✓	✓
Mitre ATT&CK Mapping Support	✕	✓	✓	✓
Anomaly Detection	✕	✓	✓	✓
Human Resources Requirement	✓	✕	✕	✕
Automated Response	✕	✓	✓	✓
Automation and Orchestration	✕	✓	✓	✓
Threat Intelligence	✕	✓	✓	✓
UEBA	✕	✕	✕	✓

Note: Certain functions and use cases of the technologies mentioned may vary from vendor to vendor. Explained by considering general abilities.

Conclusion

Logsign Unified SO Platform provides all of the features in the charts mentioned above on a single platform in an integrated manner to help organizations elevate their security posture and reduce the risk of cyber attacks by providing them with an integrated and efficient security management platform that includes all the abilities of SIEM, SOAR, XDR and so much more. With the Logsign USO Platform, organizations will be able to centralize their security operations, thus achieving advanced efficiency in terms of time and human resources in addition to drastically improved security.

Logsign

Logsign is a global vendor that specializes in providing comprehensive cybersecurity solutions that enable organizations to enhance their cyber resilience, reduce risk, and streamline security processes while decreasing HR and operational chaos. Logsign consistently offers an efficient, user-friendly, and seamless platform and employs the latest technologies to establish secure, resilient, and compliant environments while providing organizations with comprehensive visibility into their IT infrastructure, enhancing threat detection capabilities, and streamlining response efforts. In today's complex threat landscape, Logsign ensures that businesses have an excellent cybersecurity process in place, proactively safeguarding their systems, data, and digital assets. With a presence on four continents and a customer base of over 600 enterprises and governmental institutions, and mentioned by Gartner SIEM Magic Quadrant two years in a row, Logsign also has high ratings on Gartner Peer Insight and G2 sites.

bako tech®

BAKOTECH is an international Value Added IT Distributor that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor, BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers.

logsign.bakotech.com   logsign@bakotech.com