Logsign®

Improve Cyber Resilience. Reduce Risks. Avoid Chaos.

Unified Security Operations Platform

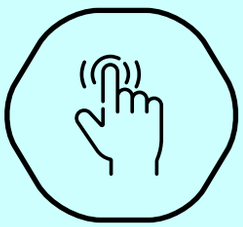
Single. Fast. Unified-Whole. Scalable.

Logsign helps organisations improve their cyber resilience by avoiding risks and chaos, in addition to ensuring compliance with relevant regulations by bringing together all data, threat detection, investigation, and incident response capabilities on a single, unified whole platform. This is achieved through the integration of various native Logsign tools, such as Security Information and Event Management (SIEM), Threat Intelligence, User and Entity Behavior Analytics (UEBA), and Threat Detection, Investigation, and Response (TDIR).

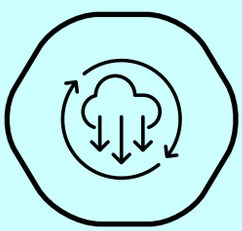
> **Bringing separate tools together doesn't cut it.**
> **They're considered unified but don't create a whole solution.**

How Logsign Unified SO Platform Differentiates?

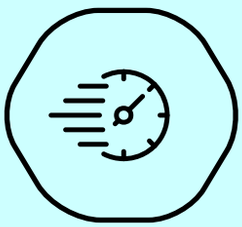
Unified-Whole Platform



Ease of Use



Hassle-Free Deployment



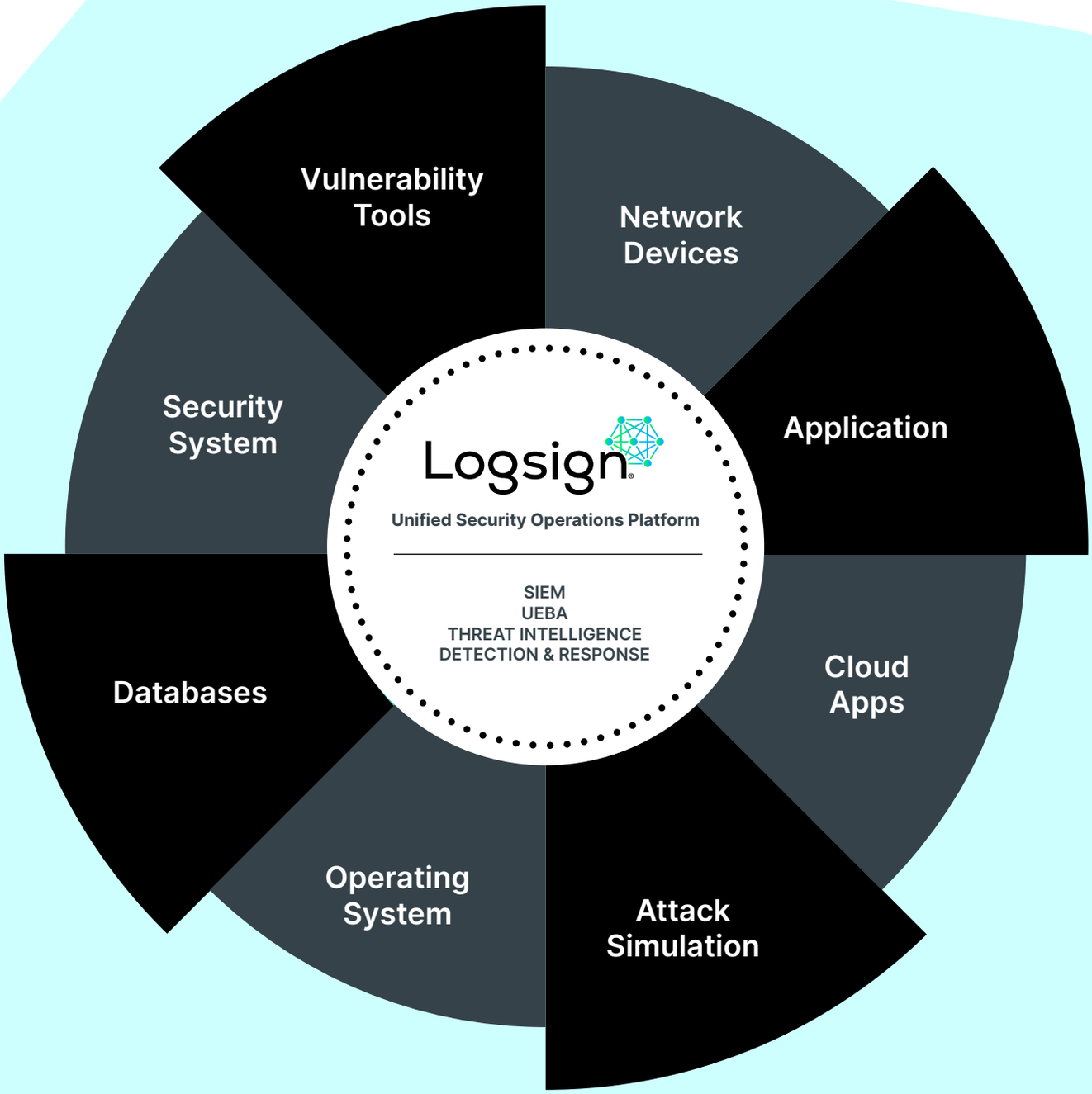
Fast

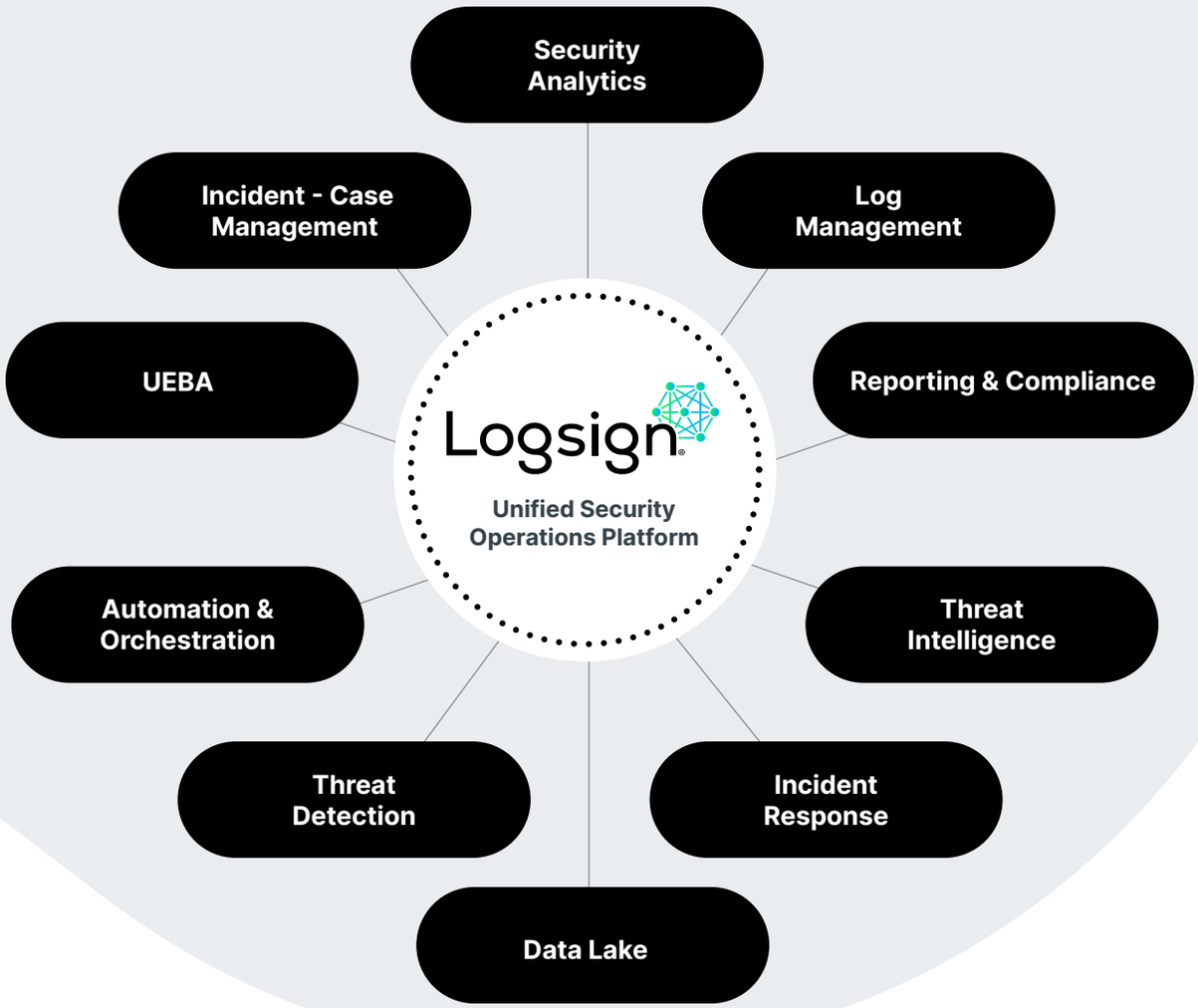
Stress-Free Sizing, No Hidden Costs

How Does the Logsign Unified SO Platform Work?

The Logsign Unified SO Platform is a comprehensive security tool that enables you to create a data lake, investigate threats and vulnerabilities, analyse risks, and respond to threats automatically.

The platform's automation and orchestration capabilities come from SOAR experience and are involved in every stage of the detection, investigation, and response processes. This enables the eradication and mitigation of threats and vulnerabilities in seconds, reducing MTTD and MTTR.





The Logsign Unified SO Platform integrates seamlessly with all other SOC tools to enable the best security management and team experience. Logsign is at the heart of the process. It has an extensive integration library with more than 500 pre-defined integrations, free plugin services, and custom parsing capabilities. As a Unified Security Operations Platform, it works seamlessly with other components of a Security Operations Center.

400+ Log Collection & 100+ Response Integrations

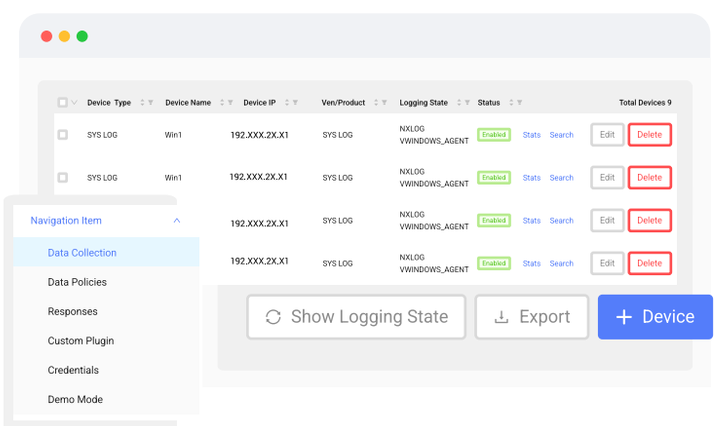
Create Superpower Data Lake

Logsign collects data from all sources to create a superpower data lake and works on it. The key success factor is the architecture, which enables:

- → Vertical & horizontal, enterprise-grade scalability
- → Cluster deployments & high availability
- → Long-term data storage
- → Advanced data retention for hot & cold data
- → Fast, simple deployment for hybrid environments
- → Leaf node for distributed networks to centralise data & management easily (high capacity data collector)
- → Filtering data & reducing noise with Data Policy Manager
- → Demo Mode: Log generation simulation for a new source.

Log Management

Logsign can collect data from hundreds of different types of products from various manufacturers that is related to security and regulatory compliance. It can currently collect and respond via more than 500 pre-defined integrations.

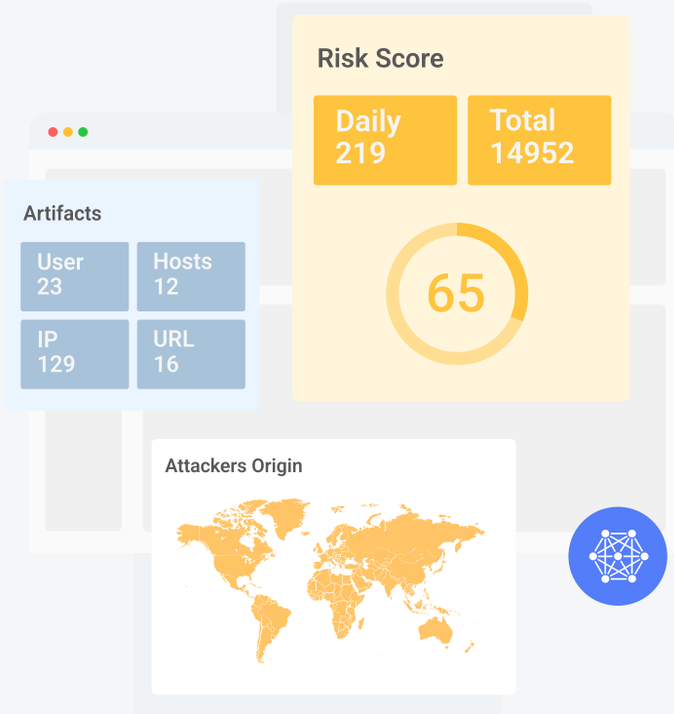


- → 400+ pre-defined data collection integrations
- → 100+ pre-defined detection & response integrations
- → Free plugin service for an unlimited time
- → Custom parser for those who want to do it on their own
- → Advanced parsing & indexing techniques
- → Easy to work with normalised, classified data
- → Data manipulation & modification
- → Multiple data collection techniques: API, NetFlow, WMI, Syslog, Oracle, SFTP, FTP, SQL, SMB, JDBC

Threat Detection & Investigation

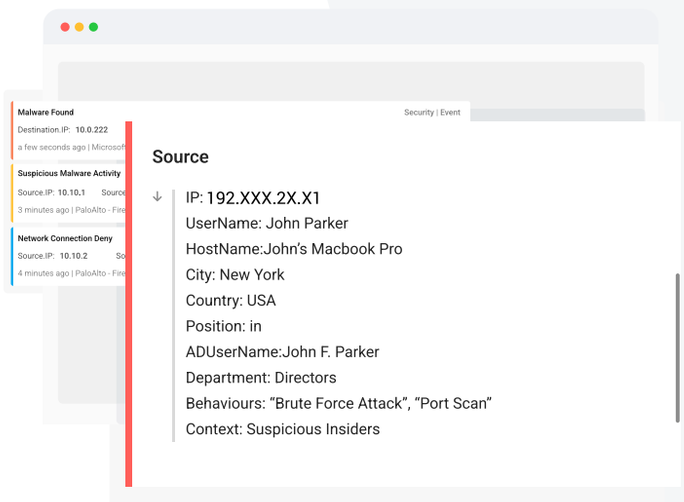
Easy and simple to create any query to reach fast, understandable, and actionable results.

- → Drill-down, full-text, advanced, Lucene search
- → Respond to queries in milliseconds
- → Investigates correlated and enriched data
- → Threat hunting for hidden threats, IOCs and IOAs
- → Threat level validation
- → Incident triage
- → Forensic investigation
- → MITRE ATT&CK and Cyber Kill Chain Frameworks
- → Risk scoring



Real-Time Enrichment & Advanced Correlation

Logsign enriches the data and correlates in multiple ways to detect, and disrupt any hidden, complex, or modern threats using MITRE ATT&CK framework.



For Enrichment:

- → Asset & identity enrichment
- → Geo IP, position, location, LDAP/AD
- → Context, custom enrichment
- → Behavior enrichment
- → Threat intelligence feeds
- → Network position, branch, etc.
- → Instant data processing

For Correlation:

- → Multiple correlation methods:
  Cross-correlation, historical, rule based, behavior based, vulnerability based, threat based correlation methods
- → 500+ pre-defined correlation rules
- → Built-in correlations for threat intelligence

Threat Intelligence

Logsign collects all data, enriches, and compares it with the streaming threat intel in real-time. It detects attackers on their first attempt.

Logsign Unified SO Platform rapidly investigates hidden threats, IOCs, and suspicious attack vectors by combining global threat intelligence data. It also uses internal threat source feeds to risk prioritization.

Over 40 threat intelligence feed lists support Logsign threat intelligence and visualize with predefined dashboards, alerts, and reports to track threat intelligence incidents.

Well-trusted TI feeds to enrich your data and provide you with insights to detect threats and attacks.

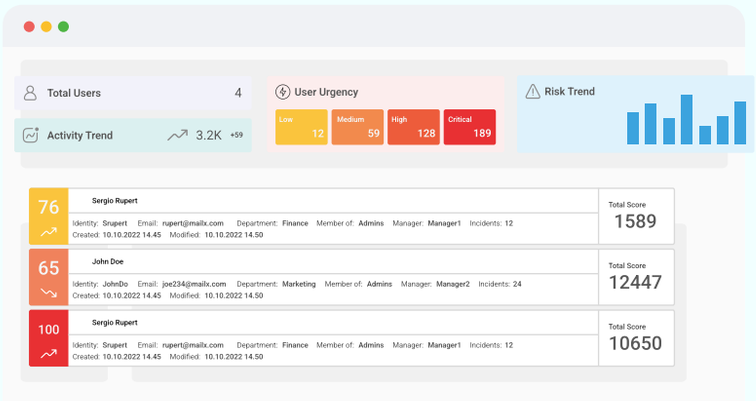
40+

Well-trusted TI feeds to enrich your data and provide you with insights to detect threats and attacks.

User and Entity Behavior Analytics

Logsign UEBA uses advanced analytics to collect and analyse data related to assets and identity.

It analyzes specific threat data to determine whether certain types of behavior represent a cybersecurity threat. In simpler terms, Logsign UEBA helps detect and prevent cyber threats by analyzing user behavior and alerting users to potential risks.



- → Accurately detects advanced & insider threats
- → Surfaces highest risk alerts and prioritize low & slow threats
- → Prioritizes high-risk threats with identity-centric behavior analytics that maps to the MITRE ATT&CK framework
- → Prevents and stops malicious insider attacks with advanced behavior analytics from Logsign
- → Monitors user access to critical data
- → Prevents botnet infections
- → Detects risky user and watchlist user behaviors
- → Realtime entity context
- → Stops data exfiltration

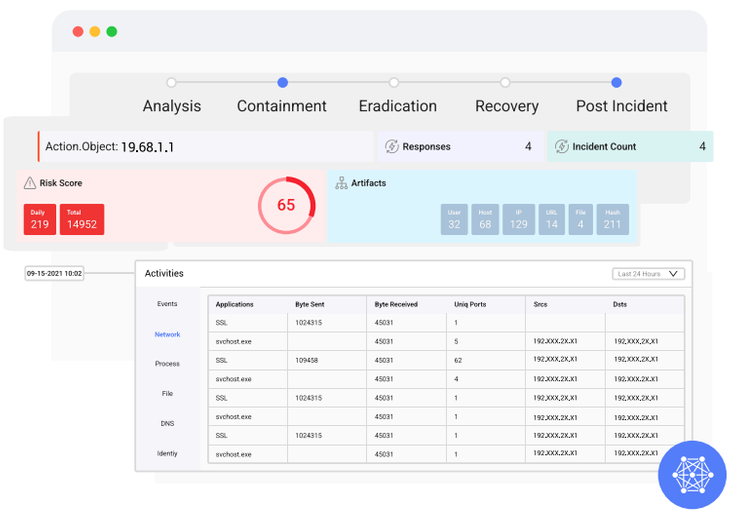
Security Analytics

Logsign offers security analytics-oriented high visualization via hundreds of pre-defined visualization tools.

- → Hundreds of built-in widgets, alerts, dashboards and reports result in actionable insights with the help of wizards.
- → Easy to customise, and configure new dashboards and widgets
- → Powerful wizards
- → Delegation: Role based access control
- → Dynamic search filters, drill-down search on dashboards
- → Filtering in dashboards with customisable time frame

Incident – Case Management

Logsign provides a response life cycle that references the NIST Incident Response Framework. This life cycle is associated with the actions offered by Logsign. Every time you take action, it automatically shows you which stages of the life cycle you have completed.

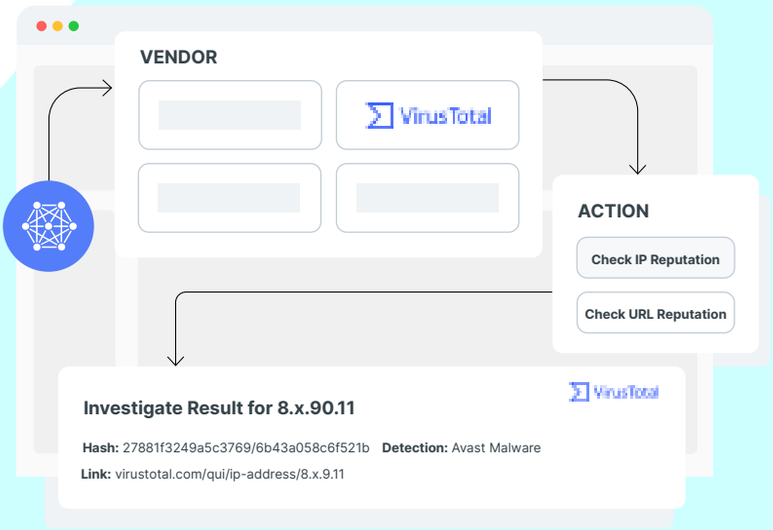


- → Artifacts, assets, and identity management
- → Incident timeline
- → NIST incident life cycle
- → Incident summary and detailed views
- → Visual cards for investigation, detection, and response

Incident Response

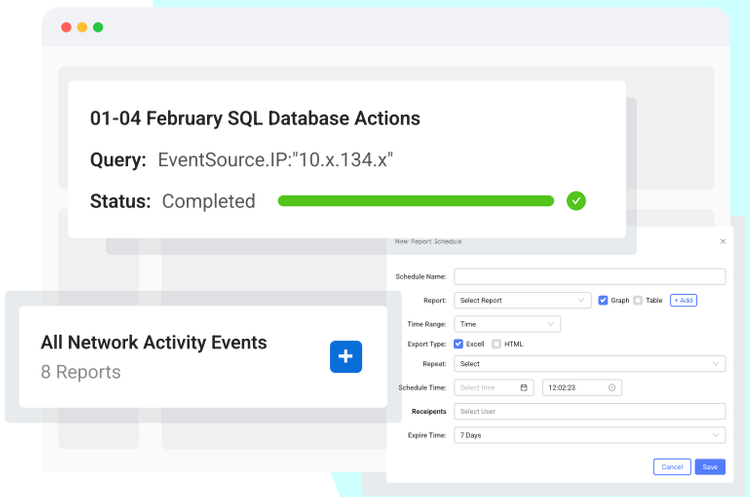
Proactive approach to incident response: Detailed views of incidents, mitigation, eradication and remediation in real-time.

- **Automated Response:** Logsign USO Platform can take automatic actions. This is what we call “Quick Actions.”
- **Semi-Automated Response:** Some incidents still require manual actions to be taken even after automatic interventions. This is possible with the “Action Button”, a one-click action. It provides a single point of investigation, intelligence, and response while managing an incident on a single page.



Reporting & Compliance

Being ready for audits & executive reports. GDPR, PCI DSS, ISO/IEC 27001, HIPAA, etc.



- Hundreds of built-in reports
- Easy to create, and configure new ones
- Creating and exporting in seconds
- Built-in compliance reports
- Automated & scheduled reports
- Ad-hoc reporting, executive reporting
- Delegation: Role based access

High Performer FALL 2023 · Best Usability FALL 2023 · Easiest Setup Mid-Market 2023

2021 GLOBEE AWARDS SILVER WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2021

Logsign Reviews
in Security Information and Event Management
4.6
Products: Logsign Next-Gen SIEM