Logsign

Improve Cyber Resilience. Reduce Risks. Avoid Chaos.

Logsign Unified Security Operations Platform

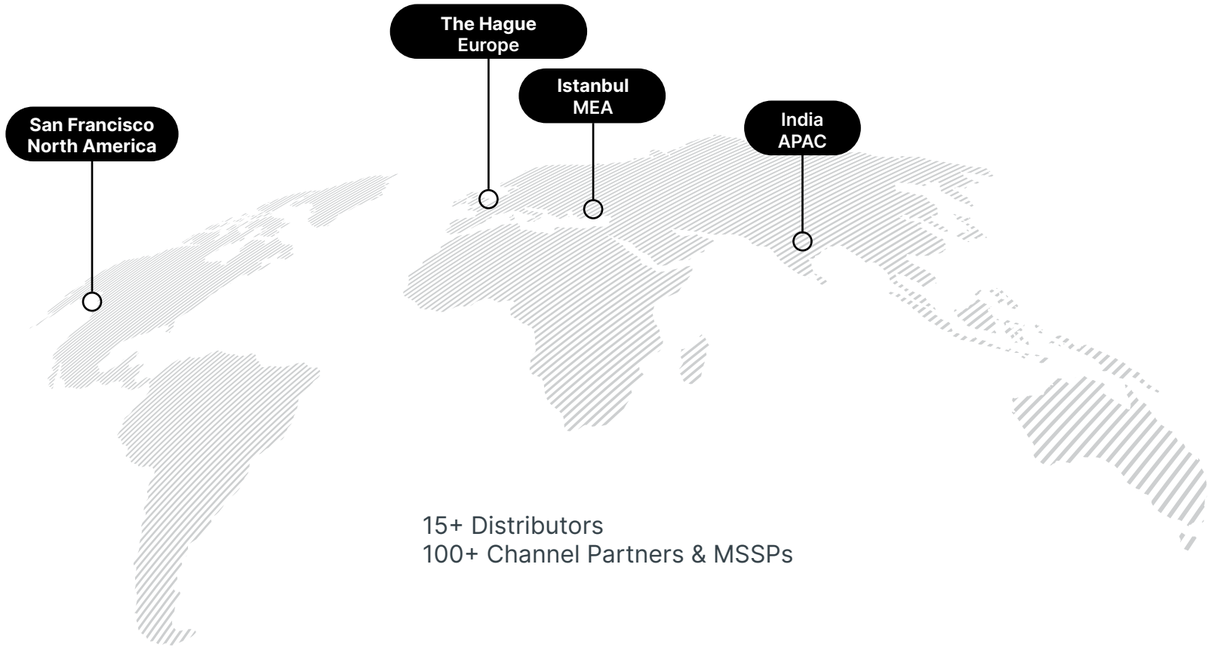
Single. Fast. Unified Whole. Scalable.

About Logsign

Our vision is always to enable cybersecurity practitioners to work more efficiently with smart, clutter-free and next-generation software. And finally, we created a consolidated, intelligently integrated, easily implemented, and user-friendly platform with the help and inspiration of the expertise from our customers and market experience.

The Logsign Unified SO platform embodies this vision, saving organisations time and resources by eliminating the need to bring different products together.

Logsign always provides fast and hassle-free platforms by using latest technologies for mature, robust security environments & compliance.



15+ Distributors
100+ Channel Partners & MSSPs

2010 — Founded

2013 — Log Management Tool

2015 — Big Data Technologies, NoSQL Database, Hadoop integrated in SIEM.

2017 — Threat Intellligence Launch

2018 — Logsign SOAR Launch; SOC Lab & Co-Managed Service Launch

2021 — Next-Gen SIEM; EMEA & APAC Expansion

2022 — UEBA Launch

2023 — Unified SO Platform Launch

2024 — Multitenancy & Cloud Technologies

About Logsign | Recognitions

Logsign

Gartner®

2 YEARS IN A ROW

Logsign mentioned in the 2022
Gartner® Magic QuadrantTM Report

Gartner, Magic Quadrant for Security Information and Event Management, October 2022.

Logsign

Logsign Reviews

in Security Information and Event Management

4.4 ★★★★½

Products: Logsign Next-Gen SIEM

5.0 ★★★★★ Mar 9, 2023

Not just a SIEM solution, it's easy and straightforward

Reviewer Function: IT Services | Company Size: 50M - 250M USD | Industry: IT Services Industry

The product is very easy to install and use.In general, the implementation of siem products takes so long time, but Logsign is implemented very quickly. The resources you add to the system are easily tracked with dashboards specific to your company. It is very successful in the application ...

5.0 ★★★★★ Aug 2, 2022

Next-Generation SIEM build according the best practices of the industry

Reviewer Function: IT Security and Risk Management | Company Size: 500M - 1B USD | Industry: IT Services Industry

LogSign is a next-generation solution, with user-friendly and intuitive interface, smart-search options and multi-vendor integrations support.

G2 Easiest To Use SPRING 2023

G2 High Performer SPRING 2023

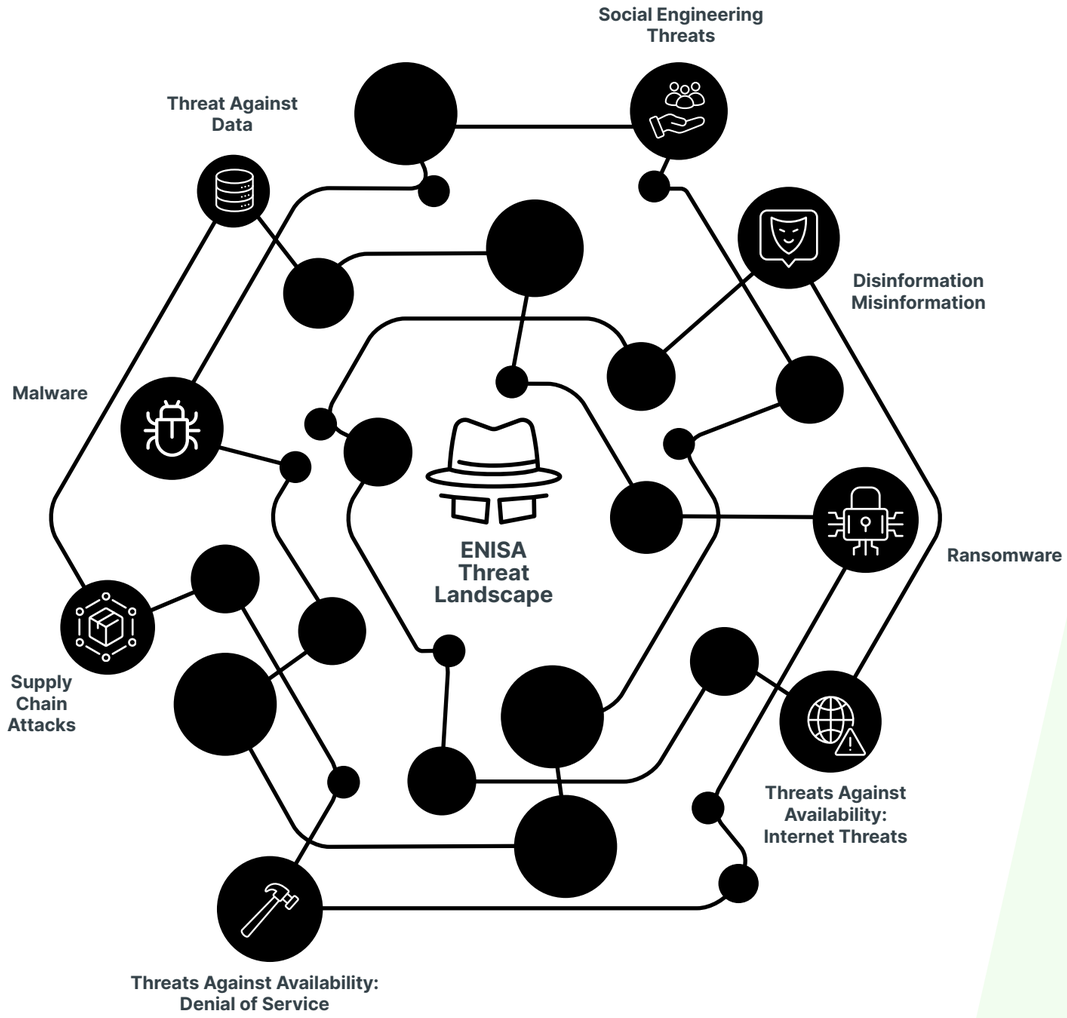
G2 Easiest Setup SPRING 2023

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

GLOBEE AWARDS 2021 GLOBEE AWARDS SILVER WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2021

Organizations Struggle With...



Resource: Enisa Threat Landscape Report 2022

Who benefits and how?

Example Business Stakeholders	Basis/Potential Requirement
Chief Executive Officer (or delegate)	General business risks: hignest-level vlew of risk pertaining to te overall business.
CIO	All 180 functions and the protective monitoring thereof.
Chief Financial Officer	Financial loss due to cybercrime such as ransomware and extortion, as well as general business disruption from cyber attacks, resulting in financial loss due to lack of availability of regulatory fines.
Chief Legal Counsel	Requlatory, legal or compliance violations due to cyberatacks data breach/data leakage). Potential contractual violations sto to data breach.
Human Resources Officer	Insider threats.
Head of Marketing	Brand protection

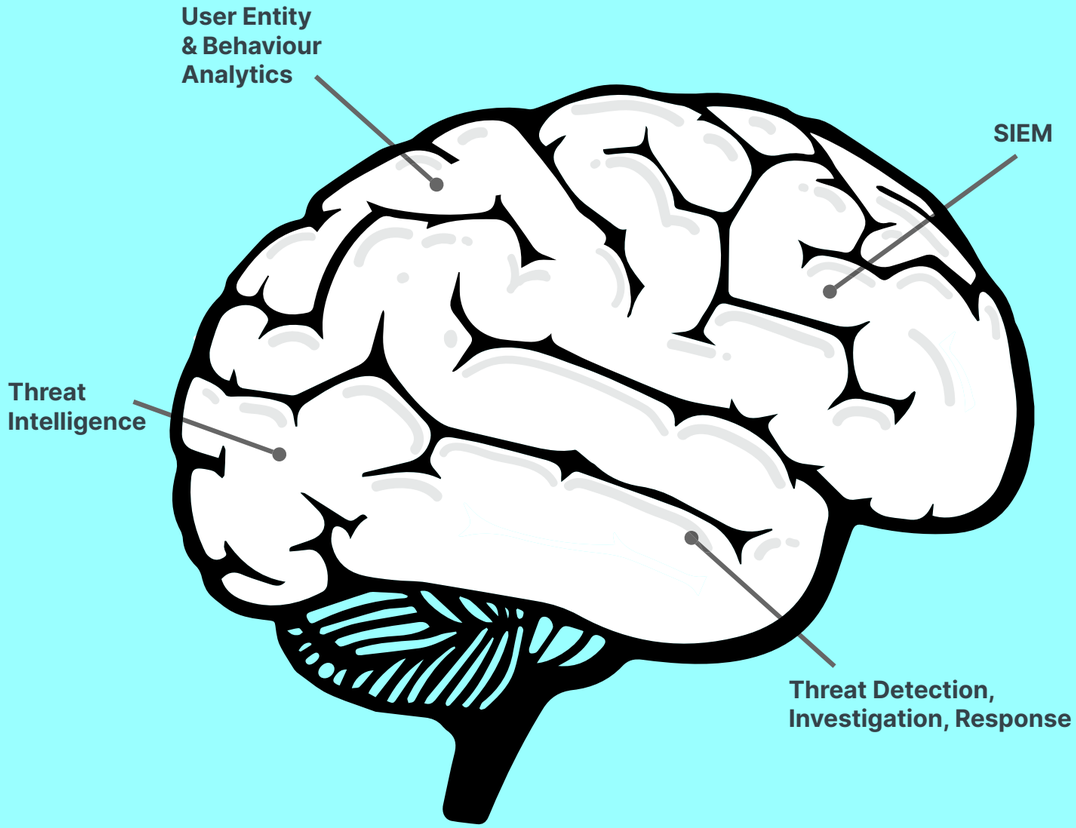
Resource: Gartner_3 Ways to Apply a Risk-Based Approach to Threat Detection, Investigation and Response

Logsign Unified SO Platform

Logsign helps organizations to improve their cyber resilience through avoiding risks and chaos, besides ensures 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 Entity Behaviour Analytics (UEBA), Threat Detection, Investigation, Response (TDIR).

- **Next-Gen SIEM**
- **Threat Intelligence**
- **UEBA**
- **Threat Detection, Investigation, Response**



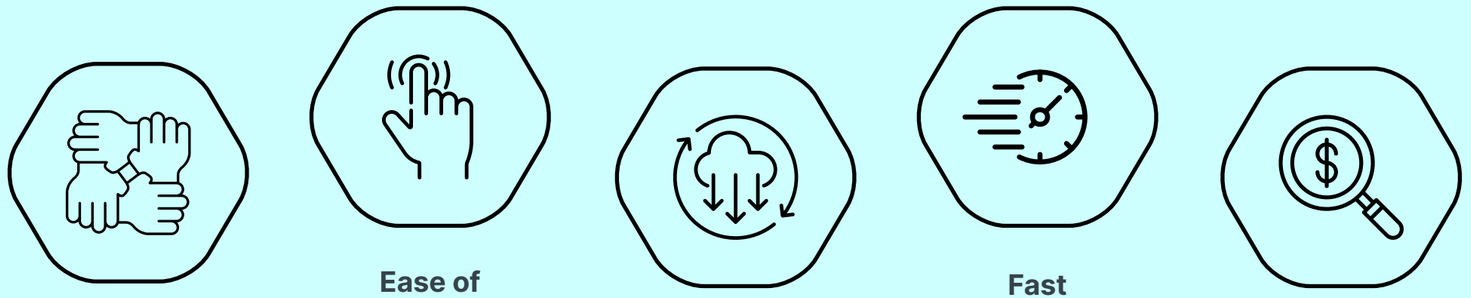
Just as the nervous system integrates and processes information from various parts of the body to coordinate a response, this platform integrates and processes information from various security tools to identify and respond to threats in a timely and effective manner.

How Logsign Unified SO Platform Differentiates?

Logsign

Holistic Approach to Strong Security Strategy

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



Unified Whole Platform

Ease of Use

Hassle-Free Deployment

Fast

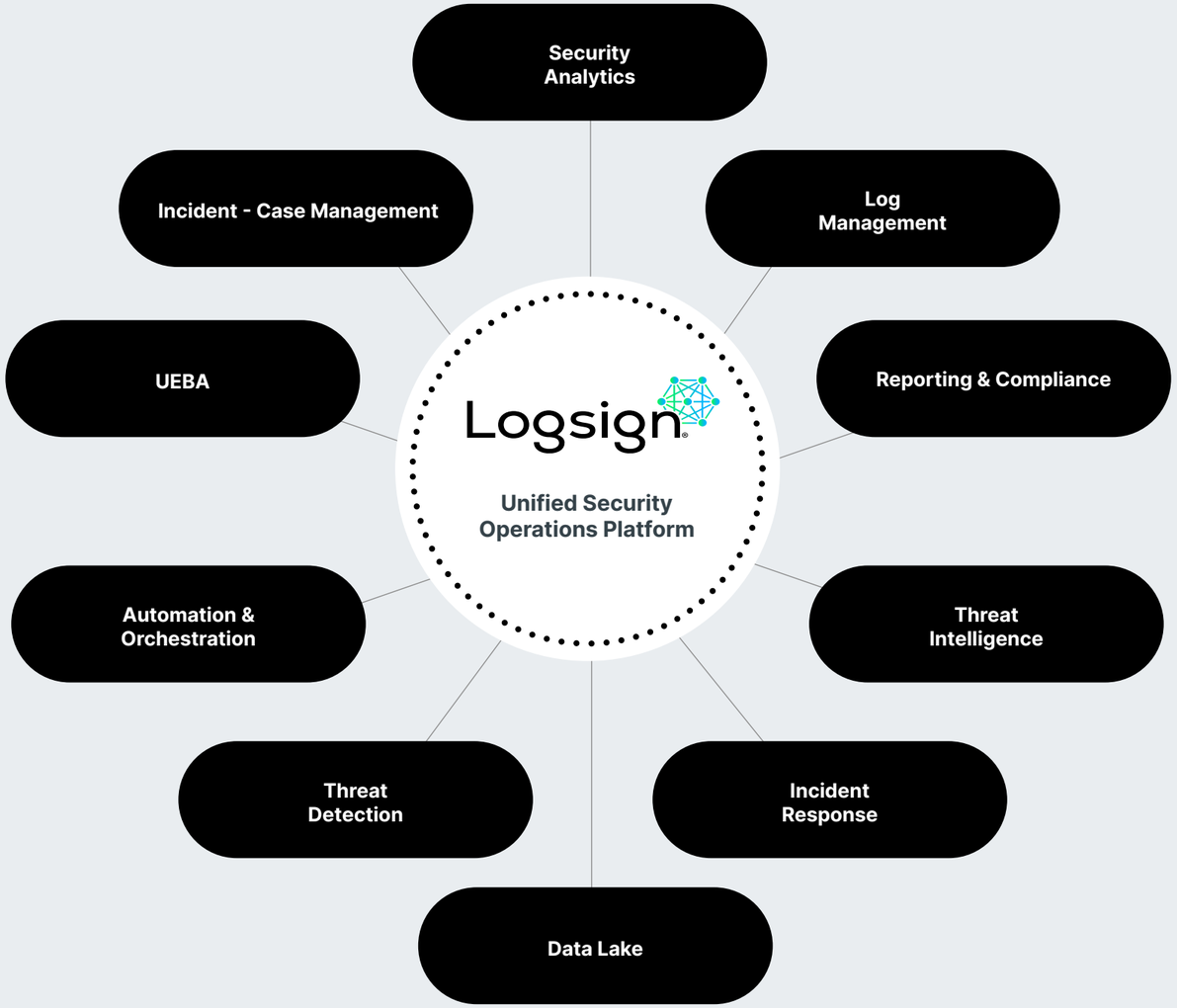
Stress-Free Sizing, No Hidden Costs

Logsign Unified SO Platform Functions at a Glance

Holistic Approach to Strong Security Strategy

Logsign Unified SO Platform is a comprehensive security tool that, enables you to create a data lake, investigate threats and vulnerabilities, analyze 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.



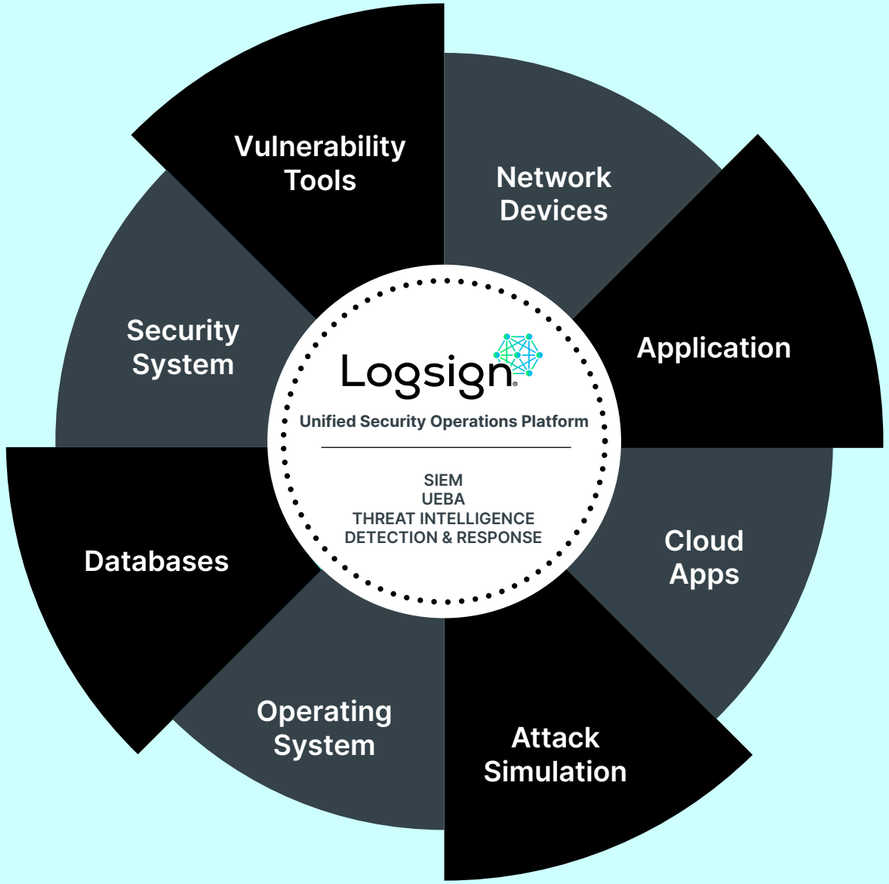
Logsign Unified SO Platform Functions at a Glance

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 an Unified Security Operations Platform, it works seamlessly with other components of a Security Operations Center.

400+ Log Collection & 100+ Response Integrations



Let’s take a deeper look

Create Your Superpower Data Lake

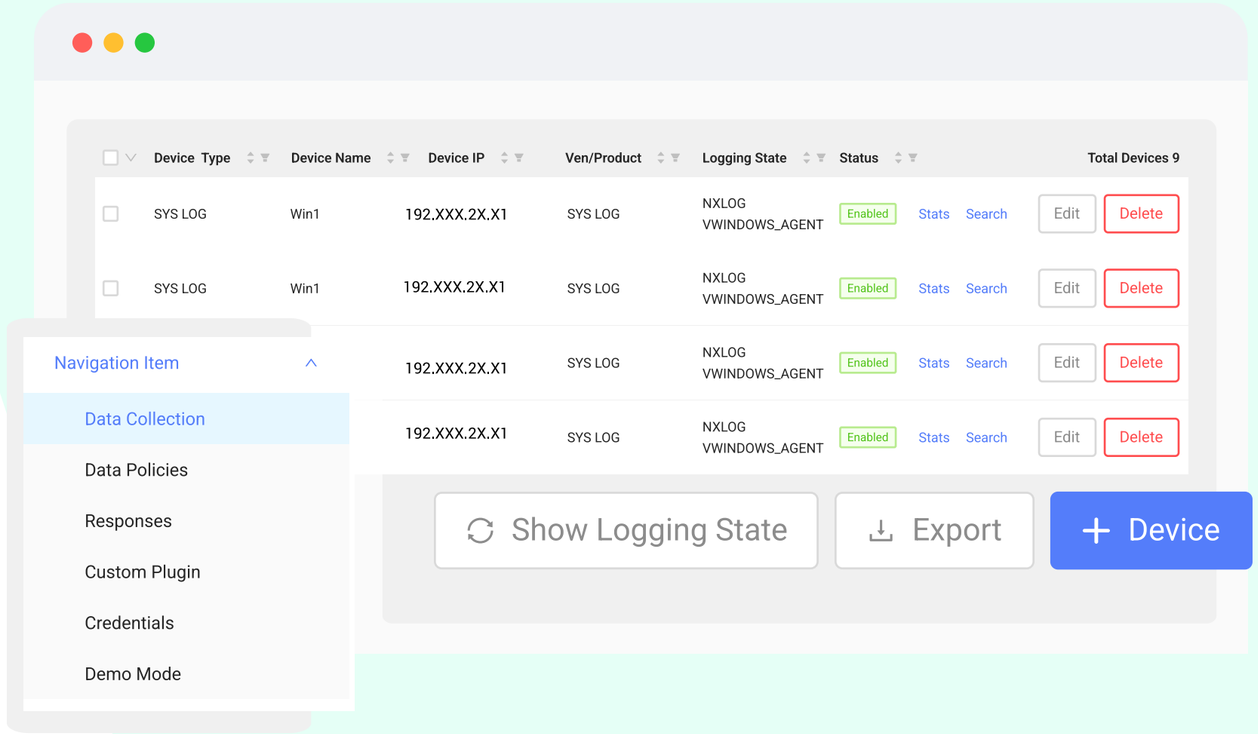
Logsign collects the data from all sources to create a superpower data lake and works on it. The key success factor is the architecture which enables:

- → 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 the data and management easily (high capacity data collector)
- → Filtering the data & reducing the 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 predefined integrations.

- → 400+ pre-defined data collection integrations
- → 100+ pre-defined detection & response integrations
- → Free plugin service for an unlimited time
- → Custom parser for whom wants to do on their own
- → Advanced parsing and 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

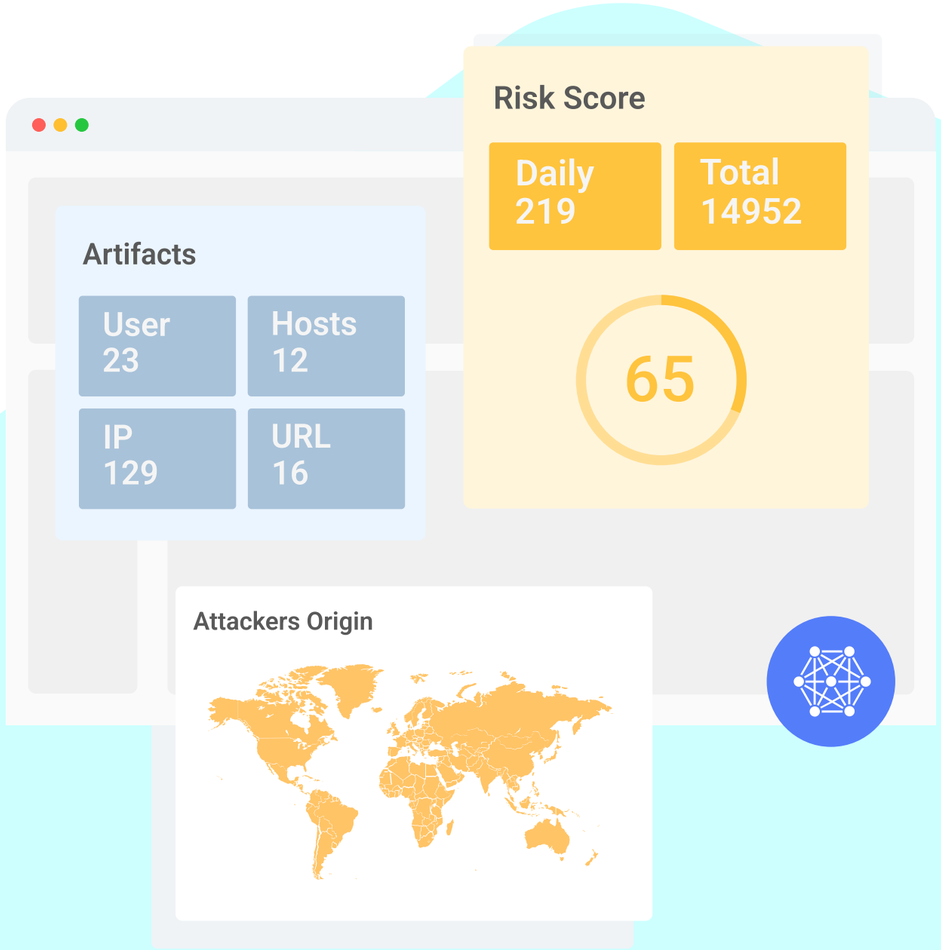


Threat Detection & Investigation

Logsign

Easy & simple to create any query to reach fast and understandable, 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



Threat and Anomaly Detection, Zero-Day Attacks, Phishing, Brute Force, Malware, DOS/DDOS, IOC, etc.

Real-Time Enrichment & Advanced Correlation

Logsign

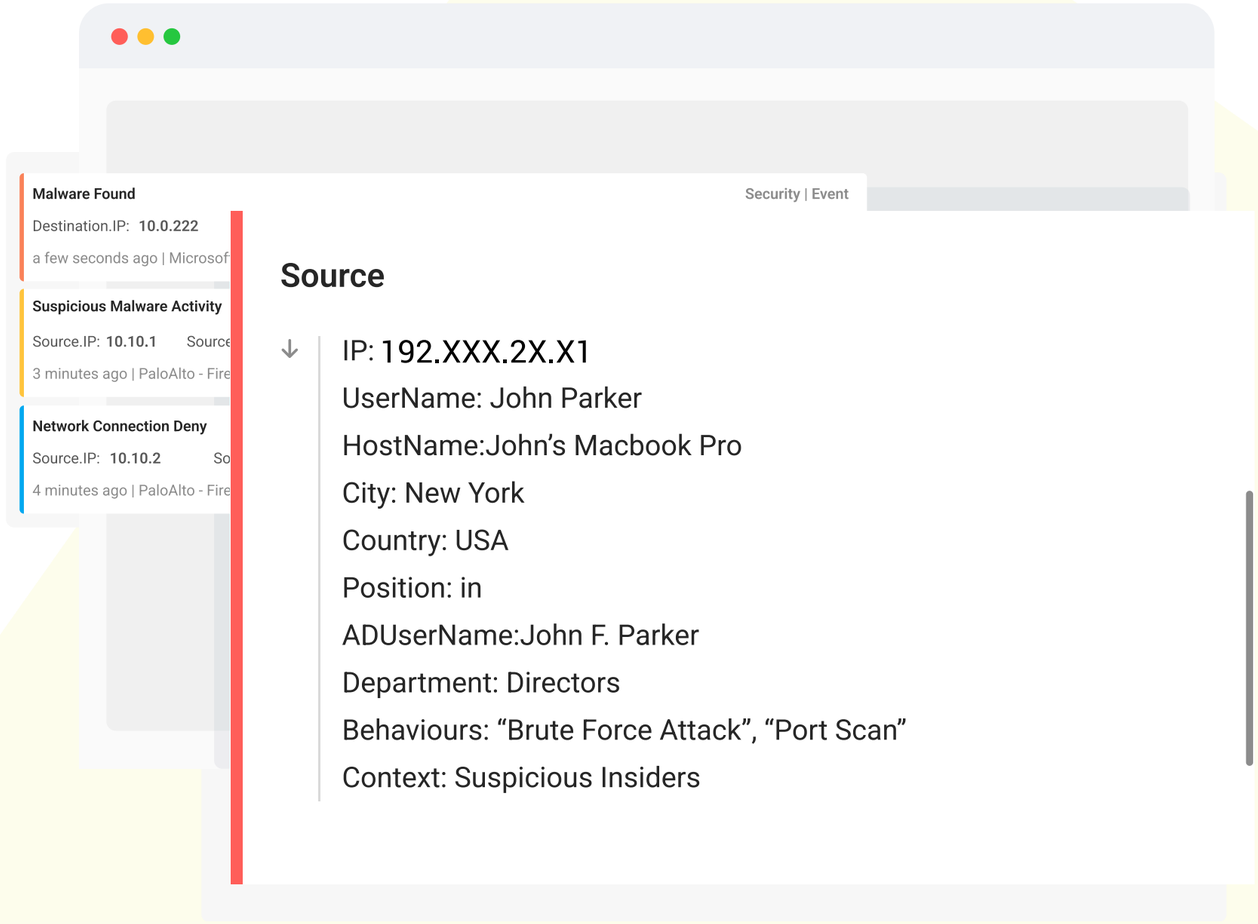
Logsign enriches the data and correlates in multiple ways to reach to detect & disrupt any hidden, complex and modern threats using Mitre Att@ck Framework.

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 techniques:**
  Cross-correlation, historical, rule based, behavior based, vulnerability based, threat based correlation methods
- → 500+ predefined correlation rules
- → Built-in correlations for threat intelligence



Threat Intelligence

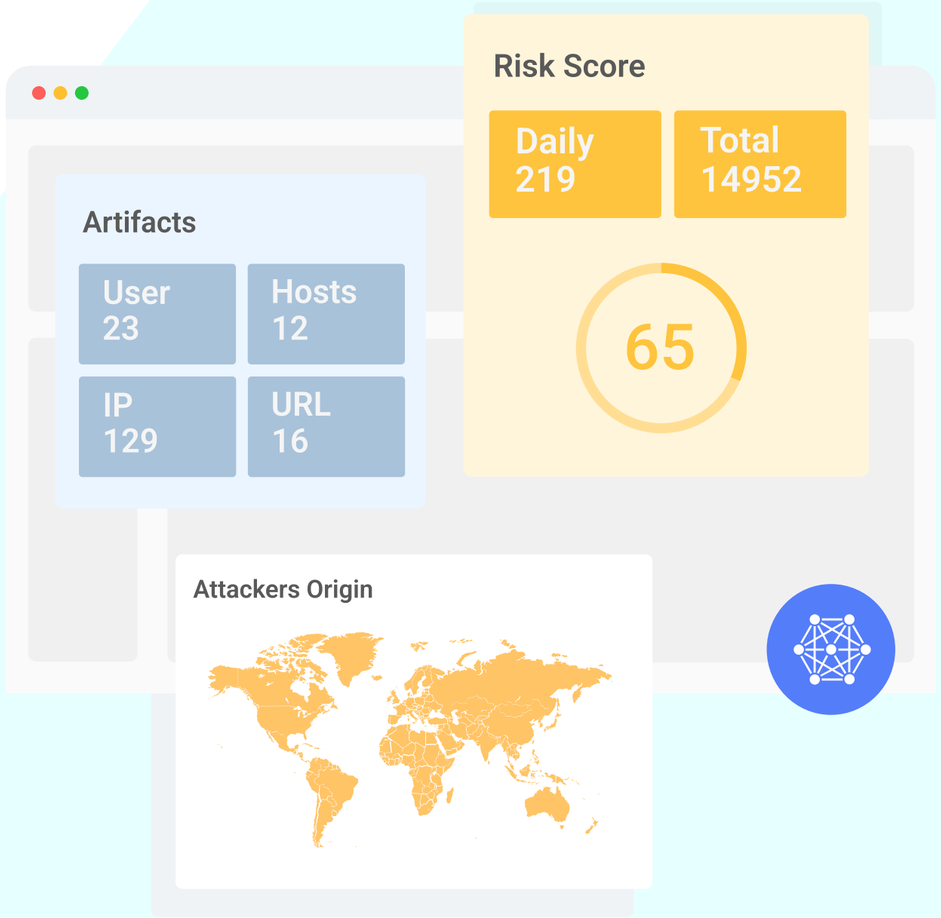
Logsign collects all data, enriches, and compares it with the streaming threat intel in real-time. It detects attackers on their first attempt.

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.

40+

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

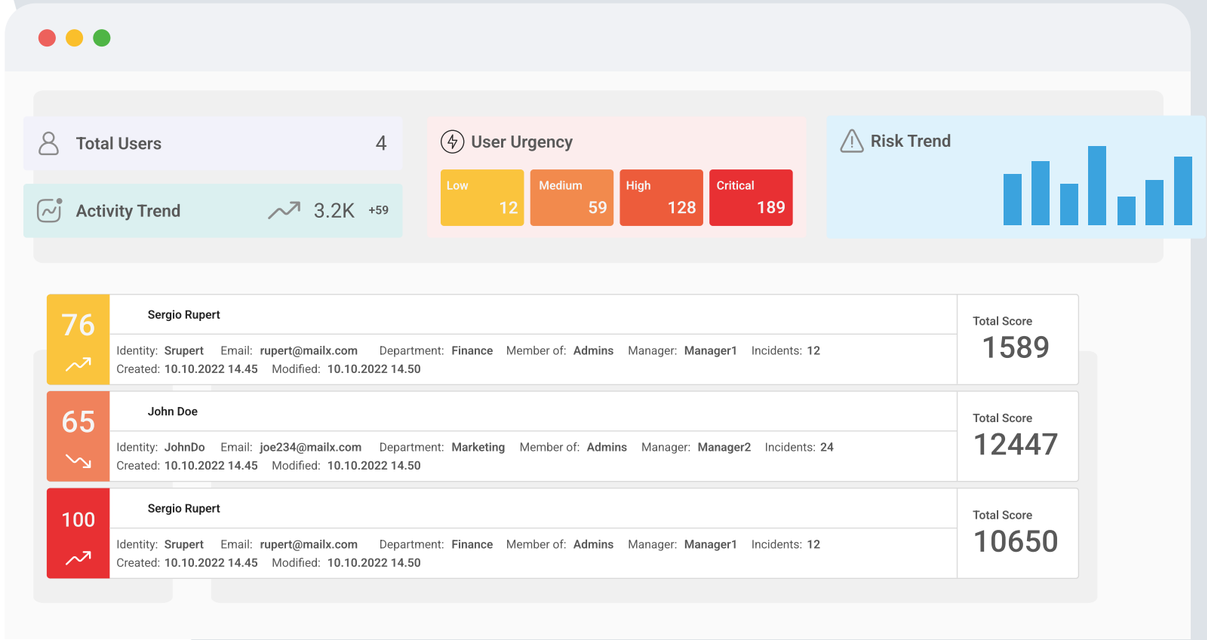


Threat and Anomaly Detection, Zero-Day Attacks, Phishing, Brute Force, Malware, DOS/DDOS, IOC, etc.

User Entity and Behaviour 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 behaviour represent a cybersecurity threat. In simpler terms, Logsign UEBA helps detect and prevent cyber threats by analyzing user behaviour and alerting users to potential risks.

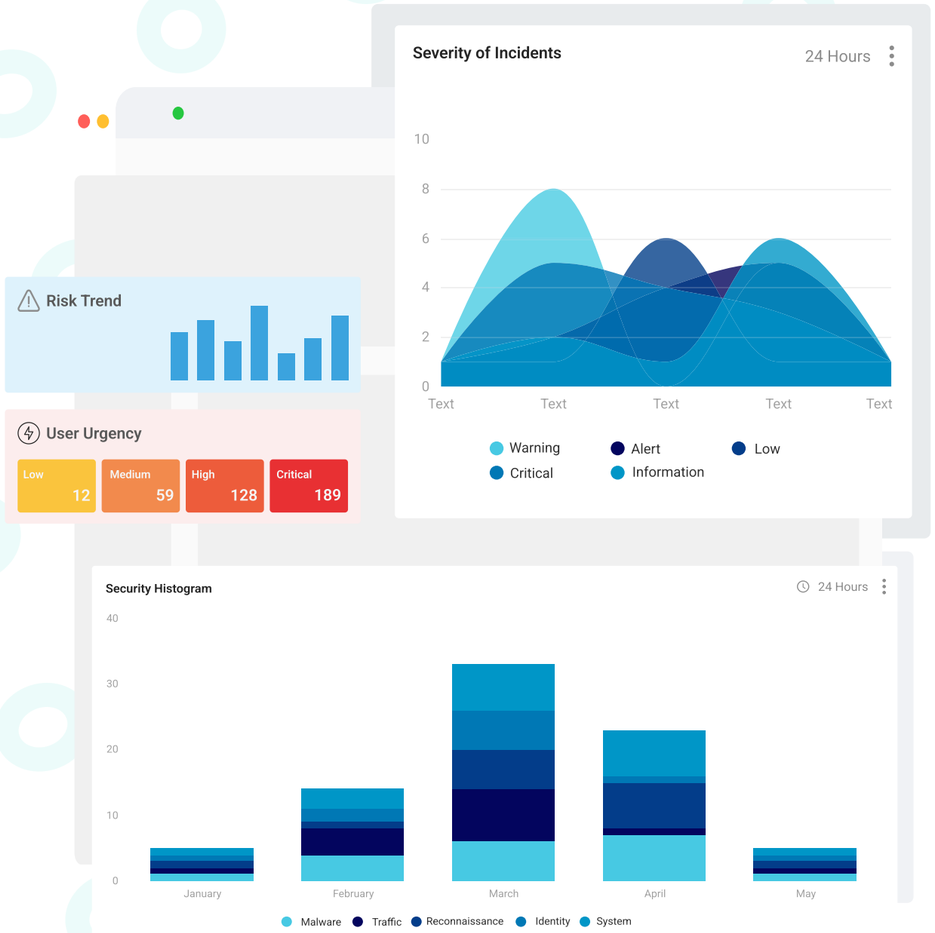
- → Monitors user access to critical data
- → Prevents botnet infections
- → Detects risky user and watchlist user behaviour
- → Realtime entity context
- → Stop data exfiltration



Security Analytics

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

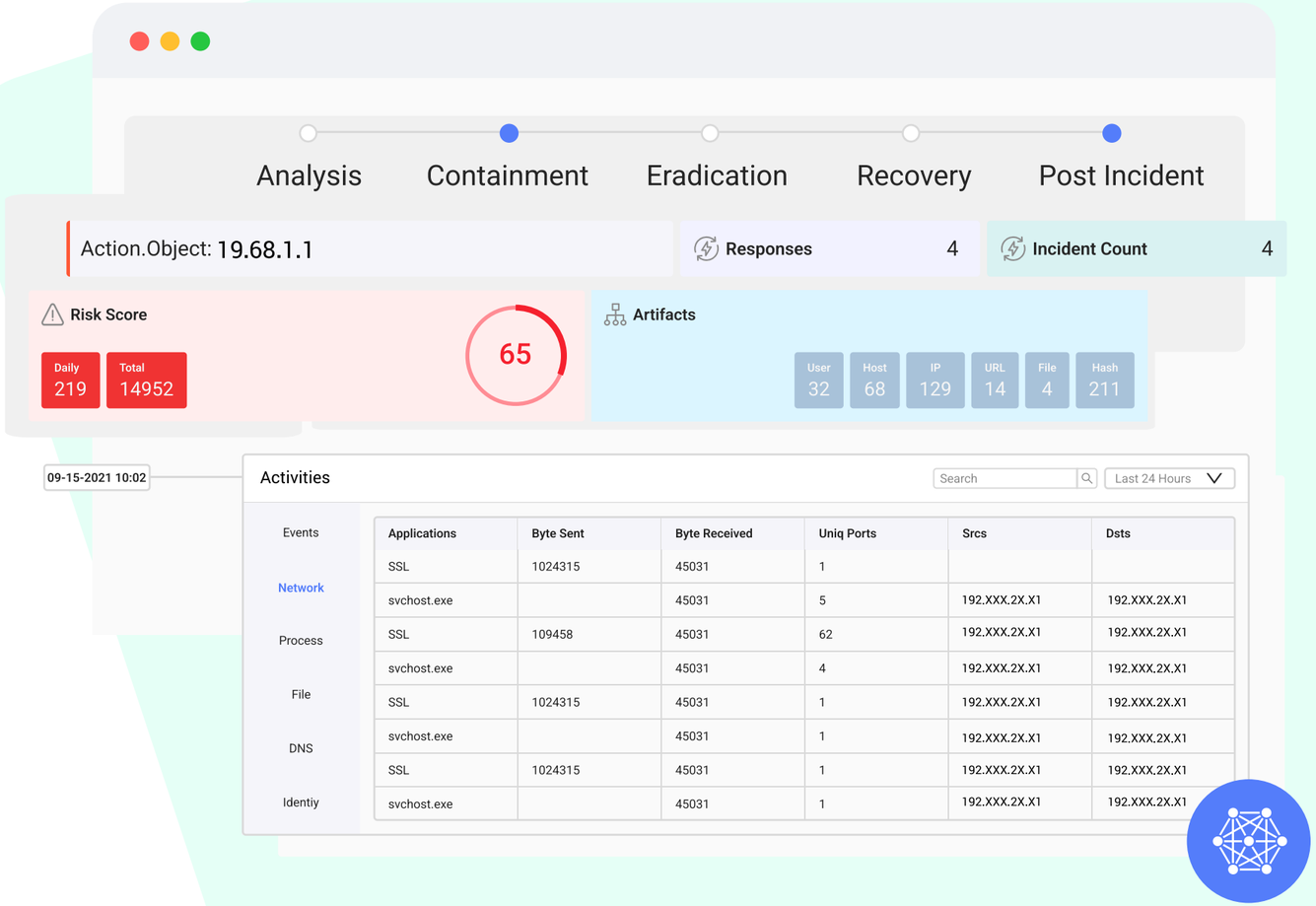
- → Hundreds of built-in widgets, alerts, dashboards & reports result in actionable insights with the help of wizards.
- → Easy to customize & configure new dashboards & widgets
- → Powerful wizards
- → Delegation: Role-based access control
- → Dynamic search filters, drill-down search on dashboards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



Incident – Case Management

Logsign provides a response lifecycle that references the NIST Incident Response Framework. This lifecycle 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

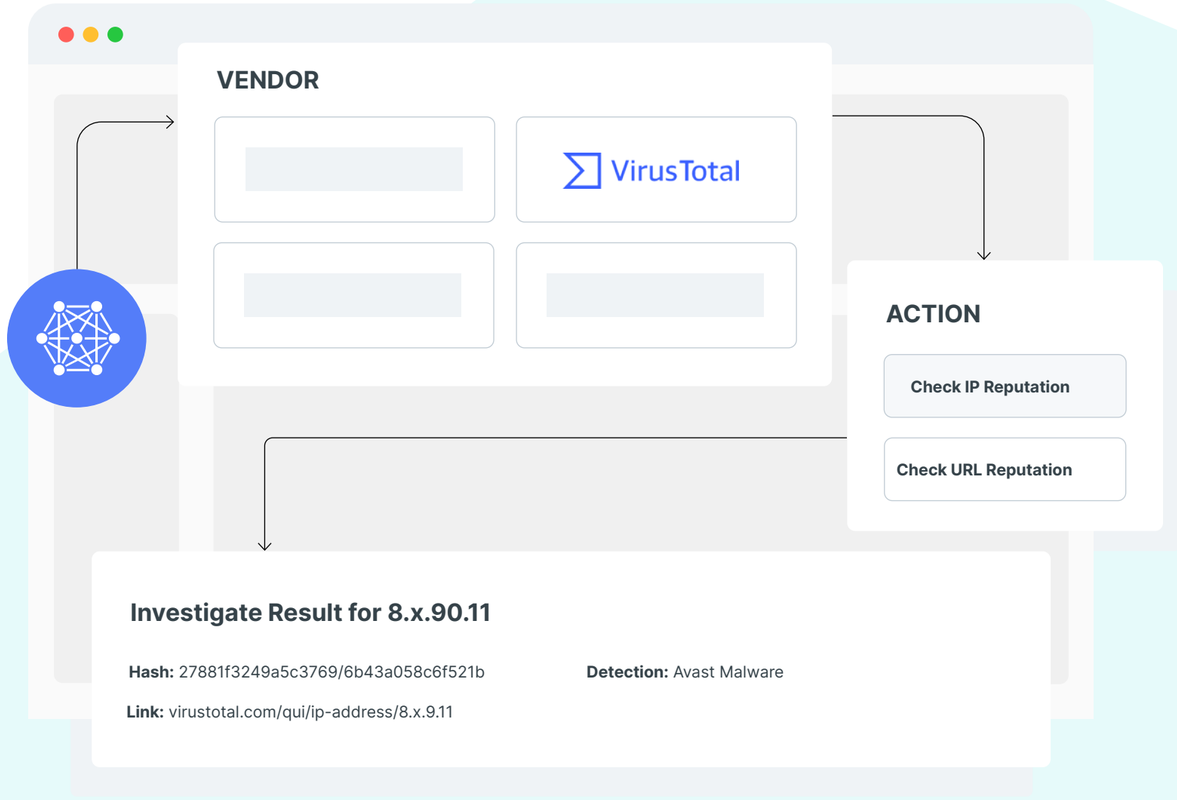
Logsign

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 as “Quick Actions”.

Semi-Automated Response: Some incidents still require manual actions to be taken even after automatic interventions.

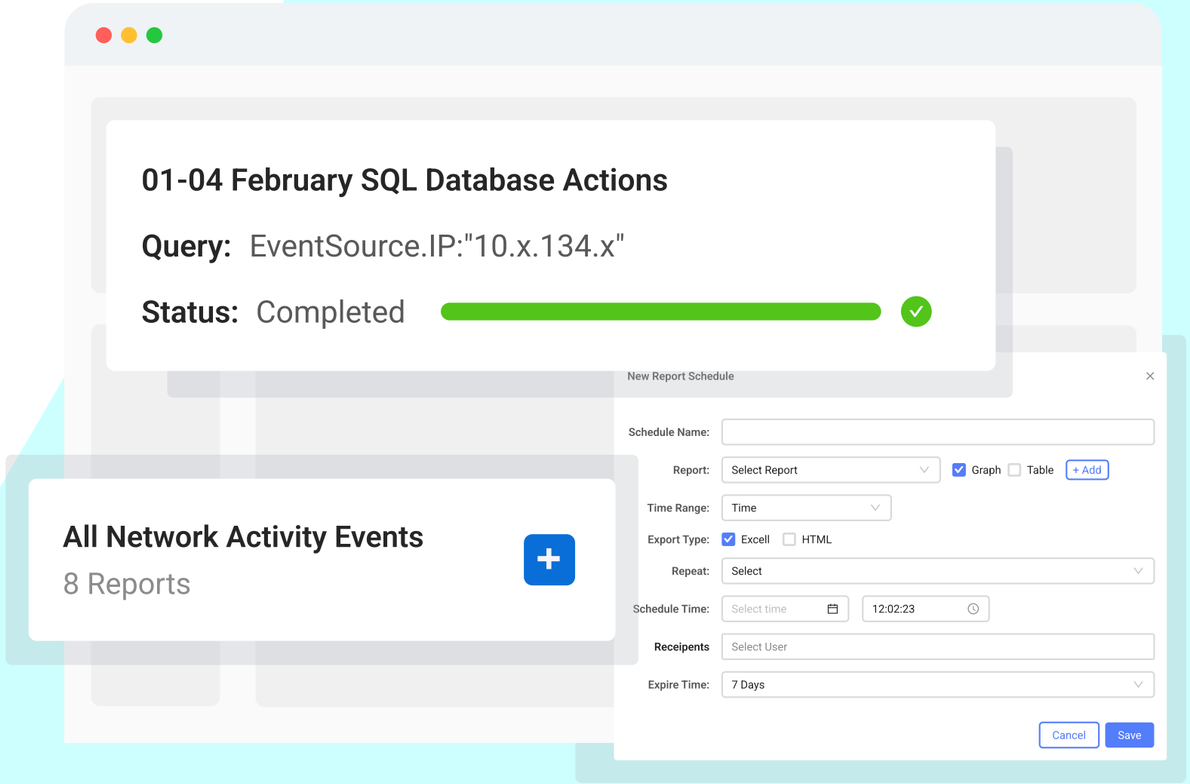
This is possible with “Action Button”, one-click action. provides a single point of investigation, intelligence and response while managing an incident on a single page.



Reporting & Compliance

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

- → 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



Licencing | Unified Security Operations Platform Plans

Logsign

	Essential	Business	Guard	Advanced	Premium	Platinium
Capacity - Log Sources	10/25 Log Sources	No Limit	No Limit	No Limit	No Limit	No Limit
Capacity - EPS	No Limit	No Limit	No Limit	No Limit	No Limit	No Limit
# of Users	2	2	5	10	15	Unlimited
Search	✓	✓	✓	✓	✓	✓
Reporting and Compliance	✓	✓	✓	✓	✓	✓
Dashboard	✓	✓	✓	✓	✓	✓
Delegation	✓	✓	✓	✓	✓	✓
Alerts Management	✗	✓	✓	✓	✓	✓
Data Collection Framework	✗	✓	✓	✓	✓	✓
Asset and Identity Management	✗	✓	✓	✓	✓	✓
Response Integration Framework	✗	✗	✓	✓	✓	✓
Incident Response Module	✗	✗	✓	✓	✓	✓
Risk Scoring	✗	✗	✓	✓	✓	✓
Threat Intelligence	✗	✗	✓	✓	✓	✓
UEBA	✗	✗	✗	✓	✓	✓
Custom Parser	✗	✗	✗	✓	✓	✓
LEAF Collectors	✗	✗	✗	✗	✓	✓
Leaf (# of nodes)	✗	✗	✗	✗	5	Unlimited
Cluster - (# of nodes)	✗	✗	✗	✗	✗	5 / Unlimited

Stress-Free Project Sizing, No hidden costs, No limit for EPS or volume, log source (exc. Essential), Feature-based

→ logsign.com → support.logsign.net /logsign

Trusted Customers

Logsign

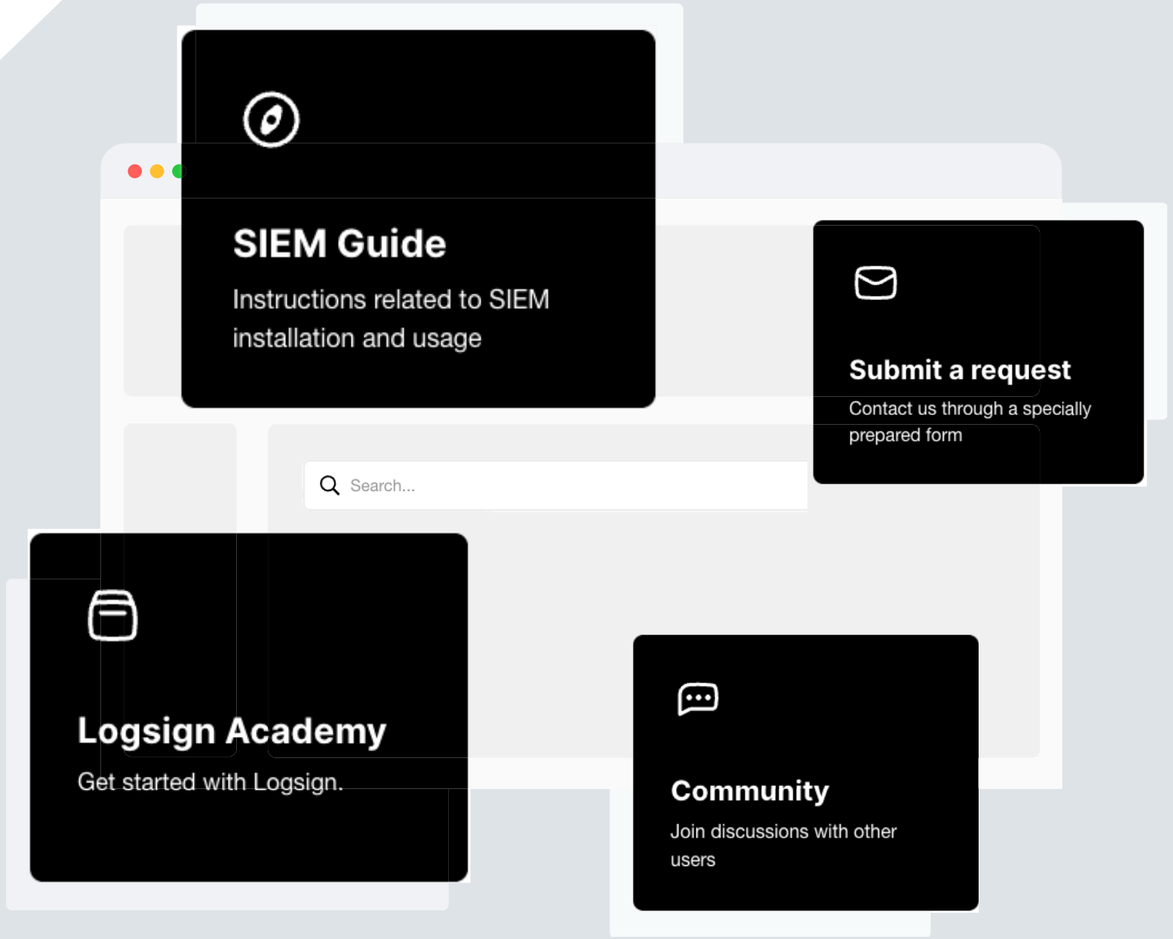
Stay with Us

support.logsign.net

Logsign cares about you. According to your needs and requests, it’s easy to reach support, product, and sales teams on the platform.

academy.logsign.com

Join Logsign academy to become a certified Logsign user or administrator. Free training and certifications for all.



Logsign

Thank YOU!

→ logsign.com → support.logsign.net /logsign