

Improve Cyber Resilience. Reduce Risks. Avoid Chaos.

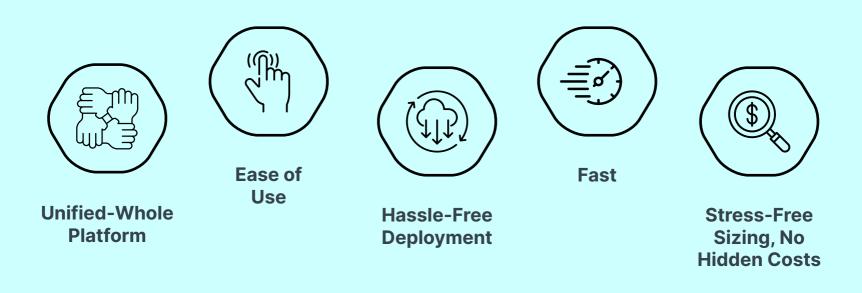
Unified Security Operations Platform

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?



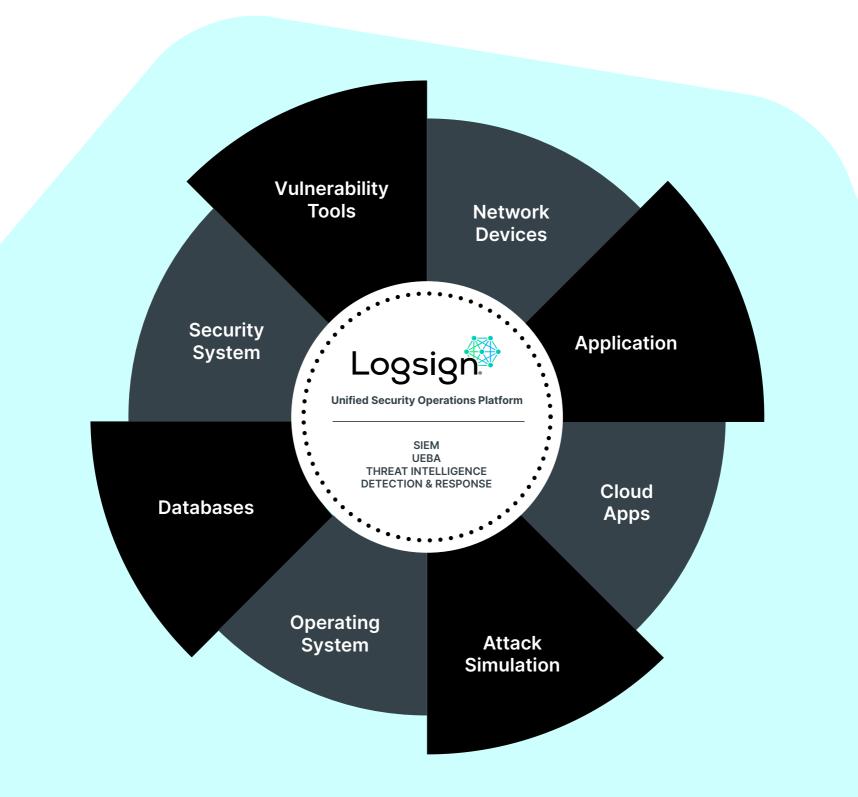


66

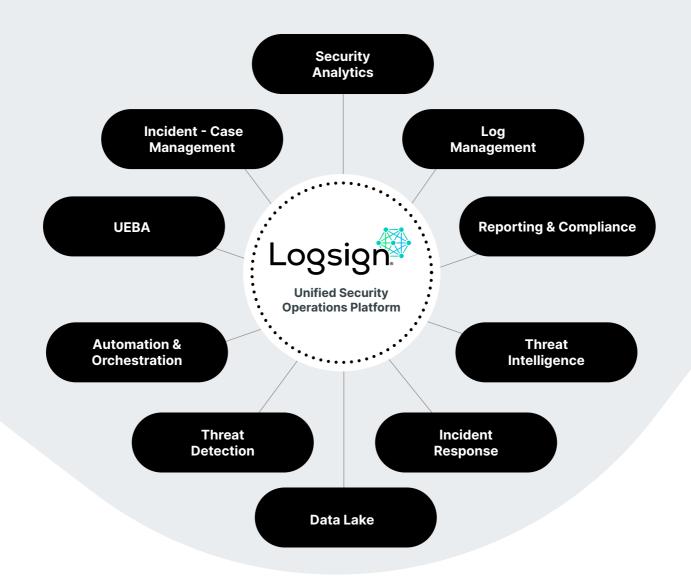
How Does the Logsign Unified SO Platform Work?

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.

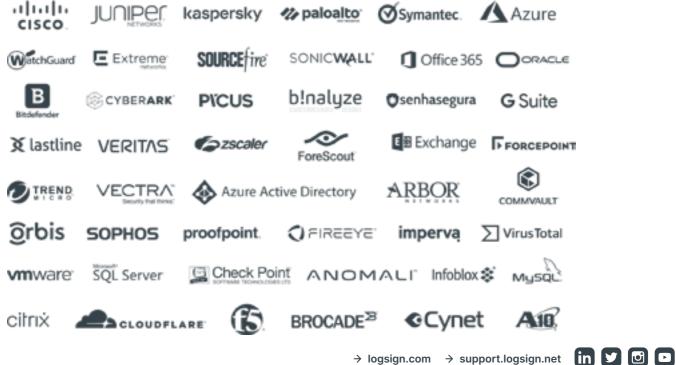






The Logsign Unified SO Platform integrates seamlessly with all other SOC tools to enable the best security management and team experience. Logsign is at the heart of the process. It has an extensive integration library with more than 500 pre-defined integrations, free plugin services, and custom parsing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

400+ Log Collection & 100+ Response Integrations



Logsign

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
- \rightarrow Long-term data storage
- \rightarrow 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.

•••						
■ ✓ Device Type 🗘 🗉	Device Name	≎ ∓ Device IP ≎ ∓	Ven/Product 0 T	Logging State ≎ ₹ 5	Status 🗘 🐨	Total Devices 9
SYS LOG	Win1	192.XXX.2X.X1	SYS LOG	NXLOG VWINDOWS_AGENT	Enabled Stats Search	Edit Delete
SYS LOG	Win1	192.XXX.2X.X1	SYS LOG	NXLOG VWINDOWS_AGENT	Enabled Stats Search	Edit Delete
avigation Item	^	192.XXX.2X.X1	SYS LOG	NXLOG VWINDOWS_AGENT	Enabled Stats Search	Edit Delete
Data Collection		192.XXX.2X.X1	SYS LOG	NXLOG VWINDOWS_AGENT	Enabled Stats Search	Edit Delete
Data Policies						
Responses		🔿 Sho	ow Loggin	g State	⊥ Export	+ Devic
Custom Plugin						
Credentials						
Demo Mode						

- \rightarrow 400+ pre-defined data collection integrations
- \rightarrow 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
- ightarrow Easy to work with normalised, classified data
- → Data manipulation & modification
- → Multiple data collection techniques: API, NetFlow, WMI, Syslog, Oracle, SFTP, FTP, SQL, SMB, JDBC

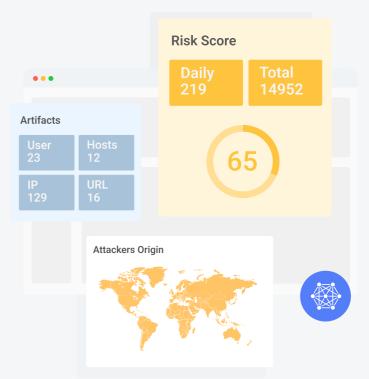
0

in У

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
- \rightarrow 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.

Malware Found	Security Event			
Destination.IP: 10.0.222 a few seconds ago Microsoft				
	Source			
Suspicious Malware Activity				
Source.IP: 10.10.1 Source 3 minutes ago PaloAlto - Fire	↓ IP: 192.XXX.2X.X1			
	UserName: John Parker			
Network Connection Deny Source IP: 10.10.2 So	HostName:John's Macbook Pro			
4 minutes ago PaloAlto - Fire	City: New York			
	Country: USA			
	Position: in			
	ADUserName:John F. Parker			
	Department: Directors			
	Behaviours: "Brute Force Attack", "Port Scan"			
	Context: Suspicious Insiders			

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.

8 Total I	Users	4 📀 U:	ser Urgency		🕂 Risk Trend	
C Activit	ty Trend ~7 3.2K	+59	12 Medium High	Critical 128 189		Ilth
76	Sergio Rupert					Total Score 1589
	dentity: Srupert Email: rupert@mails.com Created: 10.10.2022 14.45 Modified: 10.10		ce Memberot: Admins Man	ager: Manager1 Incidents: 12		1309
65	John Doe					Total Score
	dentity: JohnDo Email: joe234@mailx.com	Department: Marke	ting Member of: Admins M	anager: Manager2 Incidents: 24		12447

- → 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

- \rightarrow Monitors user access to critical data
- → Prevents botnet infections

itity: Srupert Email: rupertg/mails.com Departm ated: 10.10.2022.14.45 Modified: 10.10.2022.14.50

- → 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.

			•				•
	Analysis	Conta	ainment	Eradication	Reco	overy Po	ost Incident
Action.Object	t: 19.68.1.1			🖉 Respon	ses	4 💮 Inci	dent Count
Risk Score				Artifacts			
uily Total 19 14952		(65		User Host 32 68	1P URL File 129 14 4	ныл 211
15-2021 10:02	Activities						Last 24 Hours V
-15-2021 10:02	Activities	Applications	Byte Sent	Byte Received	Uniq Ports	Srcs	Last 24 Hours V
-15-2021 10:02	Events	Applications SSL	Byte Sent 1024315	Byte Received 45031	Uniq Ports	Srcs	
-15-2021 10:02						Srcs 19230X-2X-X1	
-15-2021 10:02	Events	SSL		45031	1		Data
-15-2021 10:02	Events	SSL sychost.exe	1024315	45031 45031	1 5	192.XXX.2X.X1	Data 192.XXX.2X.X1
-16-2021 10:02	Events	SSL svchost.exe SSL	1024315	45031 45031 45031	1 5 62	192.0XX.2X.X1 192.0XX.2X.X1	Data 192.XXX.2X.X1 192.XXX.2X.X1
18-2021 10:02	Events Network Process File	SSL svchost.exe SSL svchost.exe	1024315	45031 45031 45031 45031	1 5 62 4	192.00X.2X.X1 192.00X.2X.X1 192.00X.2X.X1 192.00X.2X.X1	Dets 192,X0X,2X,X1 192,X0X,2X,X1 192,X0X,2X,X1
15-2021 10:02	Events Network Process	SSL svohost.exe SSL svohost.exe SSL	1024315	45031 45031 45031 45031 45031	1 5 62 4 1	192.00X.2X.X1 192.00X.2X.X1 192.00X.2X.X1 192.00X.2X.X1 192.00X.2X.X1	Dats 192,X0X,2X,X1 192,X0X,2X,X1 192,X0X,2X,X1 192,X0X,2X,X1 192,X0X,2X,X1

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

in У

0

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.

•••		
	VENDOR	
\frown	VirusTotal	
		ACTION Check IP Reputation
		Check URL Reputation
Inves	tigate Result for 8.x.90.11	VirusTotal
Hash: 2	7881f3249a5c3769/6b43a058c6f521b Detection: Avast Malware	
Link: vir	ustotal.com/qui/ip-address/8.x.9.11	

Reporting & Compliance

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

•••	
01-04 February SQL Databas Query: EventSource.IP:"10.x	
Status: Completed	New Record Schedule
	Schedule Name: Report: Stelect Report: V 🖉 Graph 🔲 Table (+ Add)
All Network Activity Events 8 Reports	Time Range: Time v Export Type: © Exect HTML Repeat Select v
	Schedule Time: Select time: (B) 12:02:23 (C) Receipents: Select User Expire Time: 7 Days
	Carcel Saw

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



0 🕨

in