



Detect Faster, Respond Easier

Streamline Security Operations with Best-in-class SIEM

Logsign Security Information, Event Management, and Response Platform

*How a SIEM helps your Organization
coping with Cyber Threats?*

About Logsign

We enable robust and clutter-free cybersecurity by providing automation-driven detection and response products and value-added services. With over ten years of experience, we provide services to more than 600 enterprises and government institutions and continue our operations in four continents. We commit ourselves to providing these products and services in the smartest, and simplest-to-use way in the market.

Our key product, Logsign SIEM is one of the fastest SIEM tools: simple to deploy, easy to use, and comprehensive. Differentiates with innovative capabilities and visionary approach to incident management, and response.



Our products are recognized and followed by all security authorities and independent research companies. We build solid and long-term relationships with our end-users and channel partners.

Gartner SIEM Magic Quadrant 2021 - Honorable Mentions, Kuppingercole Leadership Compass Reports, Forrester Now Tech: Security Orchestration, Automation and Response, Cyber Excellence, Globee, Global Infosec Security awards, G2 and Gartner Peer Insight

Why & How Logsign SIEM Helps You?

Secures organizations with increased visibility, real-time detection, and response

...

For strong cyber security posture

- 360-degree network visibility, monitoring real time, and have actionable results
- Real-time detection of any threats, and vulnerabilities
- Real-time, automated response to decrease MTTR
- Incident Management Lifecycle management

Provides compliance

...

For compliance requirements, regulations

- Protecting sensitive data, and collecting evidence
- Report generation which required promptly
- Protecting the organization from high fines

It worths to invest in Logsign Next-Gen SIEM

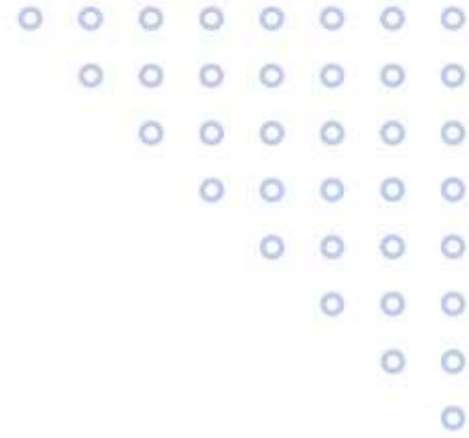
...

For overcoming investment and operational challenges

- When you make a SIEM investment, the product needs to be installed easily and quickly
- The installed SIEM product should also be easy-to-use and should not be left aside
- High performing product and after-sales team

What to Expect from a SIEM?

How to cope with cyber threats?



Logsign In a Nutshell



**Search & Investigate
in Milliseconds**



**Visualize the
Actionable Results**



**Act on
One Click**



**Detect Real-time with
In-memory Threat Intel**



**Create Superpower
Data Lake**



**Integrate Easy,
Collect More**



**Rapid and Painless
Deployment**



**Be Compliant,
Feel Safe**



**Value Added
Services**



Out-of-the-Box Incident Management & Response

Logsign Incident Life Cycle Management: Detection with multi-correlations and risk scoring via MITRE ATT&CK® & Cyber Kill Chain frameworks. Provides visual investigations, mitigates, and remediates in real-time. Visual Cards for response stages, artifact, and risk analysis. More than 50 out-of-box visual cards improve threat detection and accelerate incident response, reducing containment and remediation times.

Extensive Integration Framework

- 400+ built-in data collection integrations
- 100+ built-in detection & response integrations
- Custom parser & free plugin service
- Reduce the data noise with the data policy manager
- Classification and normalization
- Data manipulation and modification
- Data collection techniques: API, NetFlow, WMI, Syslog, Oracle, SFTP, FTP, SQL, SMB, JDBC

500+ Integrations



Detection of Complicated Threats

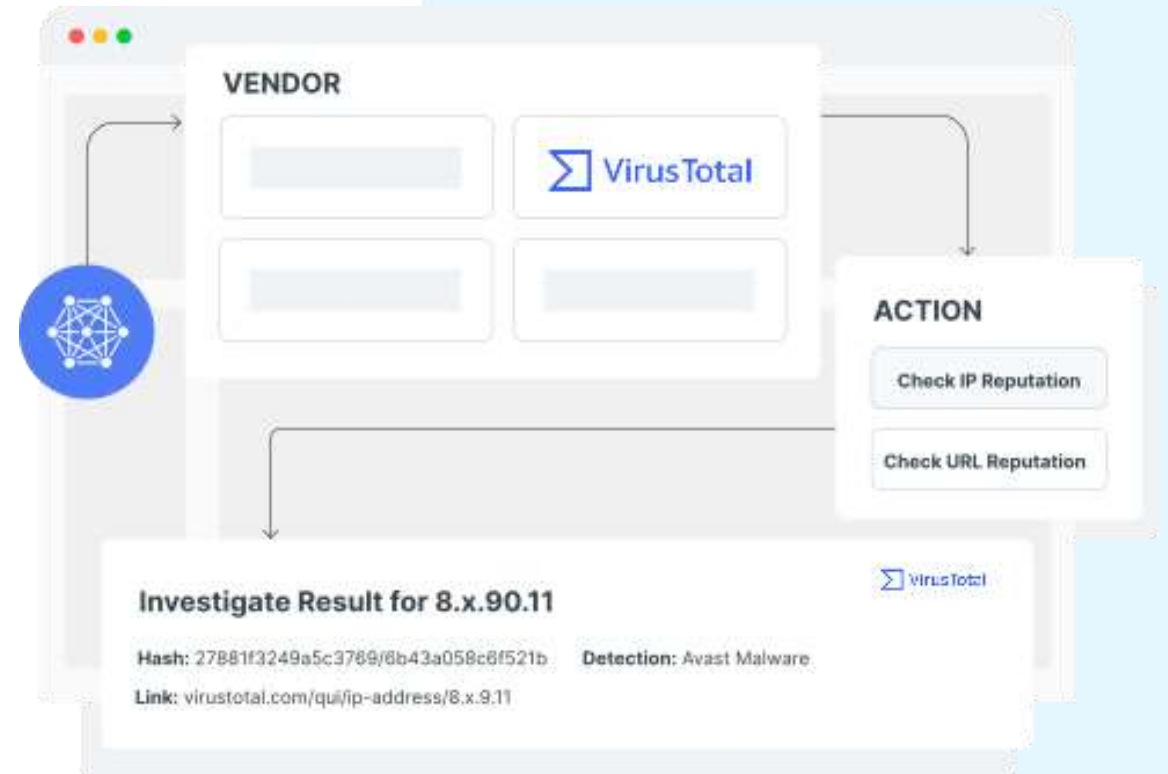
“ *Detects attackers on their first attempt.* ”



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

Incident Life-cycle Management

*Proactive approach to Incident Response:
Detailed views of incidents, mitigation,
eradication and remediation in real-time.*





**THANK
YOU**

Visit us at the **SOFTPROM Booth in Hall 7!**