Logsign

Next-Gen SIEM

Gain Comprehensive Oversight of Your Network with Logsign.

Logsign Next-Gen SIEM

Logsign Next-Gen SIEM provides comprehensive visibility and control of your data lake. It allows security analysts to collect and store unlimited data, and to investigate, detect and respond to threats automatically.

Why SIEM?

Security:
You may need a SIEM product for several reasons. A critical one is security. Reducing the security risks and keeping your business operations up and running are only available with a strong security posture. Your organization in any industry requires creating a data lake and storing high volumes of data on a cluster, highly available big-data infrastructure. It provides you with the right environment to 'see and secure'. Real-time monitoring, threat detection, investigation and automated responses empowers your team to ensure your business operations continue and your organization is safe and secure.

Compliance:
Being compliant with GDPR, PCI DSS or any other regulation requires a SIEM that has automated and scheduled reports and is continuously logging without loss. Besides that, detecting threats both inside and outside your organization has never been so crucial.

Why Logsign Next-Gen SIEM?

01

Infinitely Scalable, Cluster Big Data Infrastructure

Logsign SIEM's infrastructure enables you to keep your operations running at all times.

02

Security Analytics Oriented High Visualization

Hundreds of built-in widgets, alerts, dashboards and reports result in actionable insights.

03

TI Embedded Next-Gen SIEM

Embedded TI service with more than 40 global and well-trusted TI feeds to enrich your data and provide you with insights to detect threats and attacks.

04

Smart and Simple UI

Wizards, lucene search, drag-and-drop flexibility, and rapid respond to any query.

05

Simple Deployment & Onboarding Service

Available with more than 400 pre-defined integrations and free plugin services. Onboarding enables you to ensure your SIEM is up and running.

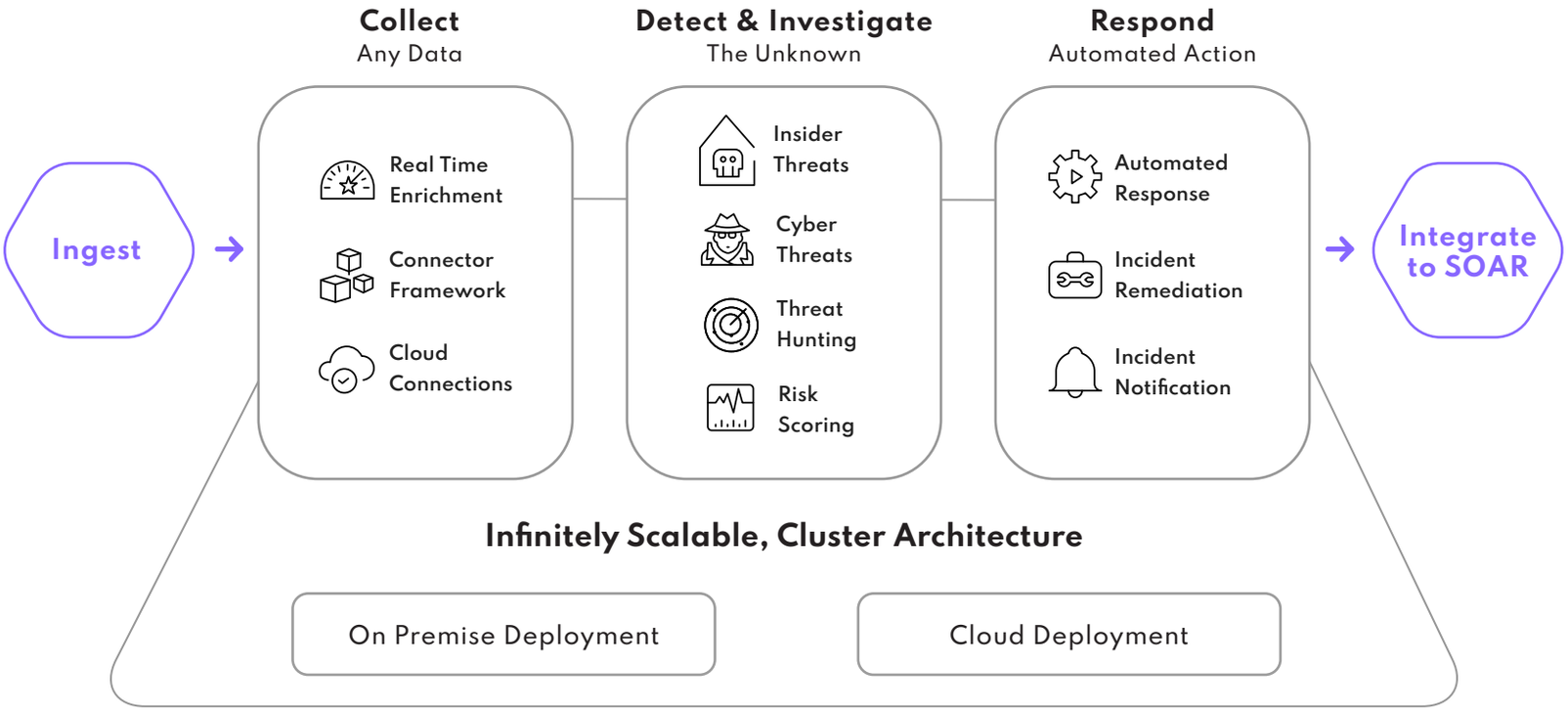
06

Flexible & Affordable Pricing Options

No matter how many log sources or how much volume of EPS you have, you will find a best fit among the multiple options.

How It Works?

Logsign Next-Gen SIEM collects logs and events data from any IT source at any time. Managing the volume of data is also available with the Data Policy Manager, eliminating the need to consider the storing volume. After normalization, it enriches the data with threat intelligence feeds, user identity and behavior data. It also indexes all data for security analytics and visualization. Logsign detects security incidents in real-time via built-in alerts, correlation rules and advanced investigation capabilities. Detecting internal and external threats, threat hunting and behavior analysis enable security teams to see what is hidden and provide understandable, actionable outcomes so comes the response.



Collect »»» Detect »»» Respond

Wide pre-defined integration and free plugin service starts data ingestion, followed by advanced parsing and indexing techniques. Logsign supports many log collection methods such as SYSLOG, SMB, WMI, FTP, SFTP, LEA, SQL, ORACLE, Flow. It classifies and normalizes data, and enriches it with embedded TI services in real time.

Find what you need in milliseconds. Logsign correlates the data, detects threats in real-time and lowers the number of false positives according to Mitre Att&ck framework. Detects any complex and modern threats and finds the hidden ones, anomalies and IOCs; and uses advanced behavior techniques to prioritize the insider threats.

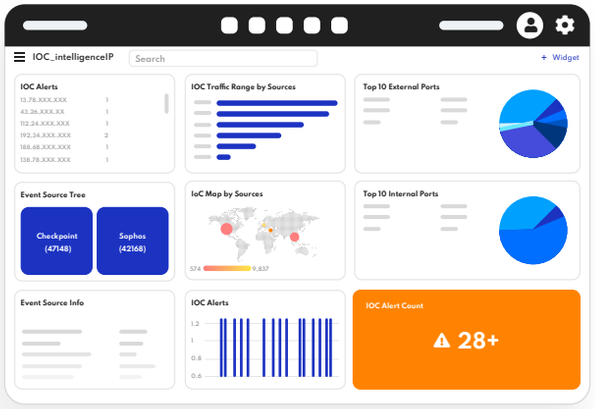
Eradicate threats and attack proactively on other integrated security tools such as firewalls, DLP and NAC when detected. You are always notified on time, every time with automated SMS and email notifications. Logsign mitigates threats and vulnerabilities, and automatically enables remediation actions on other integrated security tools such as AD, EDR and EPP.

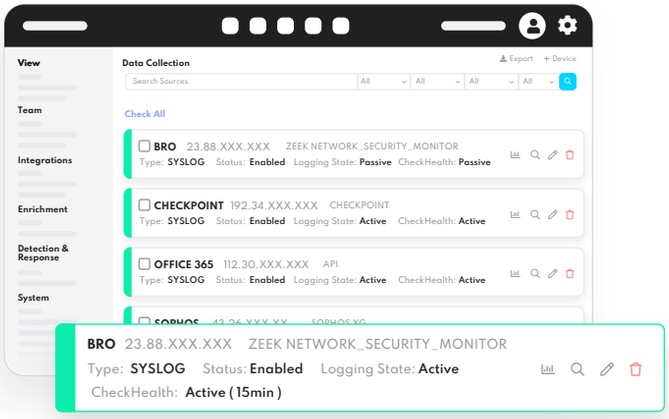
Highlighted Features

Logsign Next-Gen SIEM offers you a single-pane holistic view of your organization's information security. Whether you need a strong security posture or to be compliant, a smart SIEM leverages your security event management and makes your life easier. Deployment is always a big issue for the SIEM products unless you deploy Logsign SIEM. In addition to main SIEM functions, we excel at providing simple deployment in every environment, a welcoming onboarding service, and smart, simple usability.

Infrastructure

- Vertical and horizontal, unlimited scalability
- Cluster, high availability
- Unlimited log storage and long-term data retention
- Simple deployment both on-premise and cloud environments



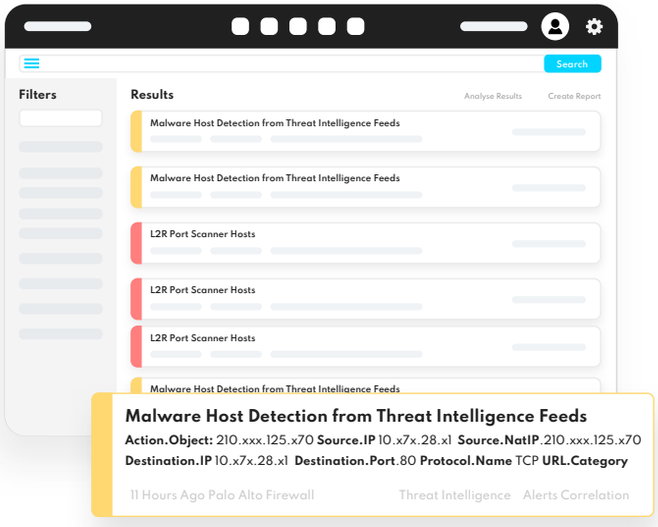


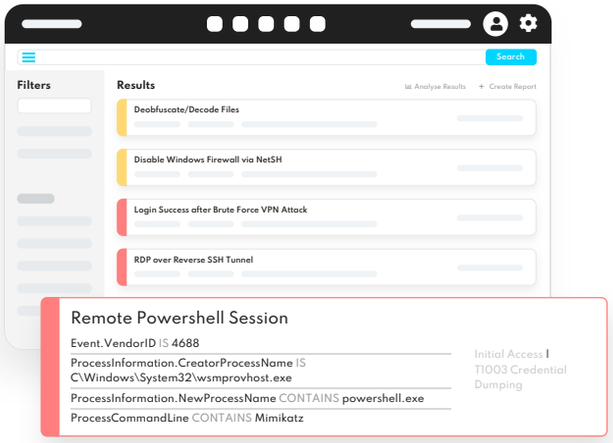
Limitless Log Collection & Storage

- 400+ built-in integrations and vendor-free integration capabilities
- Free plugin service
- Real-time enrichment with Threat Intelligence
- Controls your data volume with the Data Policy Manager

Search - Investigate - Hunt!

- Drill-down, full-text, lucene search
- Investigates on correlated and enriched data, and gets results in milliseconds.
- Threat Hunting for hidden threats, IOCs
- Validate threat levels and triage



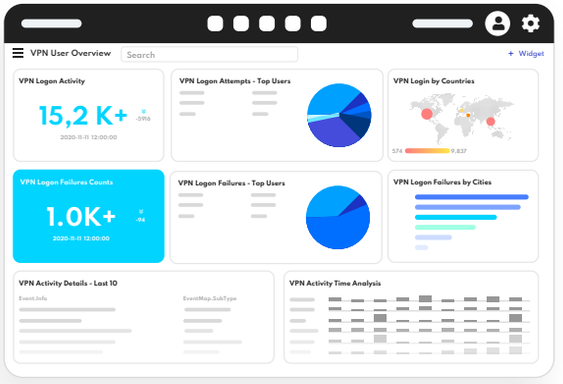


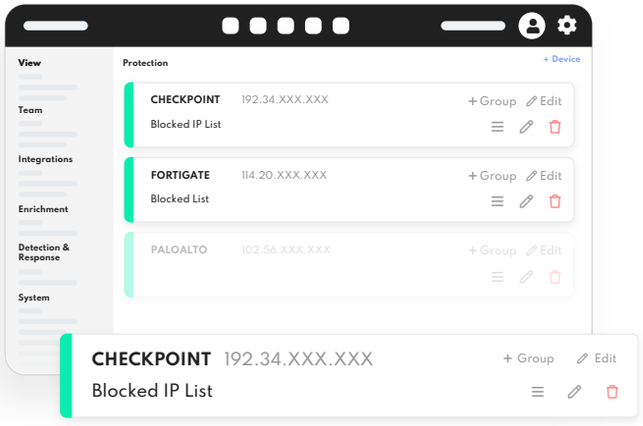
Detect Complicated Threats

- Comprehensive correlation techniques in Mitre Att&ck Framework
- Disrupt complex and modern threats
- Detect any vulnerabilities and threats
- Advanced behavior analytics capabilities

High Visualization

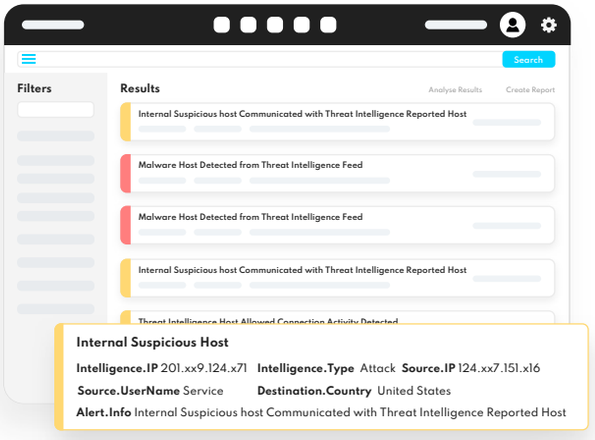
- Hundreds of built-in alerts, dashboards and reports
- Easy to create new dashboards and reports with wizards in seconds
- Role or location-based delegation of visualization tools





Protect Your IT

- Mitigate or eradicate cyber security incidents
- Automated response on firewalls, DLP or NACs
- Automated notifications
- Automated remediation actions



Threat Intelligence

- In memory real-time IOC Enrichment
- Combined user info, behaviors and threat Intelligence feed in a single view
- Built-in correlations for Threat Intelligence

Logsign

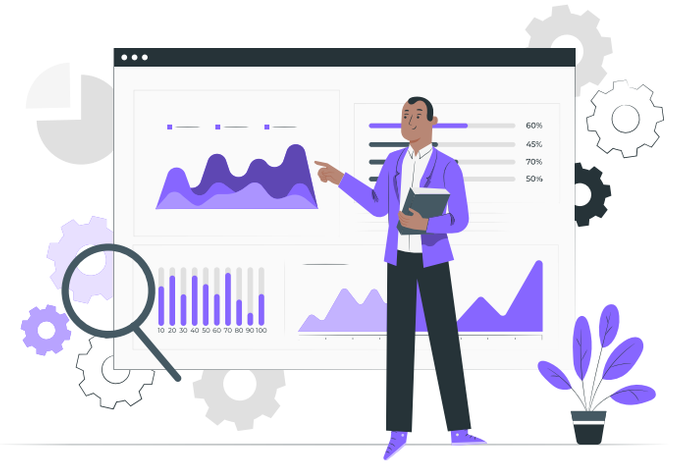
Use Cases by Security Challenges

Once implemented, a SIEM solution becomes a vital component of an enterprise security strategy. As a result, there are a large number of use cases that it caters to. A security team does not know what they will face next. With the increasing number of endpoint devices and growing reliance on cloud-based services, the potential attack surface area is expanding. Considering these factors, it becomes difficult for security teams to keep track of events happening across an enterprise network.

It is a fact that organizations install multiple security devices and software to detect unusual behavior and identify a security incident.

However, these devices and software work in isolation and their efficiency falls short when it comes to detecting advanced threats.

Without a doubt, attackers use an arsenal of tools to plan and execute an attack as well as advanced techniques to evade detection by an organization's security system.



"See and Secure"

- Data Exfiltration
- Zero-Day Attacks
- Remote Access From Suspicious Location
- Privilege Escalation
- Brute-Force Attacks
- PowerShell Attacks
- DDOS Attacks
- SQL Injection Attacks
- Lateral Movements
- Insider Threat Detection
- Malware Detection
- Unauthorized Access to Shared Folders
- GDPR Compliance
- PCI DSS Compliance
- Excessive Web Activities

Logsign

Solutions Areas

We equip enterprise security operations teams with smart SIEM and SOAR tools that improve workforce efficiency and provide better, accelerated investigations and responses. In addition to providing the latest technology products, we also offer a number of services that help users' cyber security operations management and add value.

Addressing problems during deployment and use; improving maintenance, monitoring and analysis; reducing false positives; or creating new playbooks and bots are all necessary for you to use the platforms efficiently. Our competent and trained support team is available 24/7 to support you at any time.

01 Advanced Threat Detection

Detection of internal and external threats in real time, mitigation and eradication of threats are extensively handled.

02 Threat Hunting

Logsign SIEM proactively detects insider threats or outside attackers and quickly responds to any suspicious behavior.

03 Security Analytics and Visualization

You cannot manage what you can't see. Logsign focuses on security big data analytics and visualizes the outcomes on dashboards and reports to provide understandable outcomes.

04 Threat Intelligence

Logsign SIEM rapidly investigates hidden threats and finds IOCs and suspicious attack vectors by combining global threat intelligence data with internal feeds to determine risk levels and triage.

05 SOC Management

SIEM products are located in the center of SOC operations and tools. They are strictly required for real-time detection of alerts, detailed investigation, analysis, threat hunting and response.

06 Compliance

Logsign SIEM makes compliance management easy and rapid with more than 1,200 comprehensive reports pre-prepared for global regulation and control frameworks.

07 Centralized Log Management

Logsign SIEM collects and stores data by integrating with all data sources, and it analyzes all data in one central platform.

Products

SIEM

SOAR

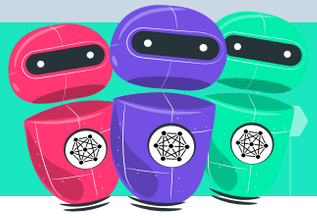
Threat Intelligence

Value-Added Services

SOC

Co-Managed SIEM

Support & Onboarding



Meet The Logsign SOAR!

Who We Are

We deliver automation-driven cyber security solutions and are committed to providing the smartest, easiest-to-use and most affordable cybersecurity detection and response solutions and value-added services.

Logsign was established in 2010 to enable cyber security practitioners to work more efficiently with smart, clutter-free and next-generation softwares. Securing the IT systems and managing cyber security operations should not be so complex, time consuming and over-priced. This is why we developed our smart and simple-to-use SIEM and SOAR softwares considering the market's current and future needs. Automation starts the new era in cybersecurity. We believe with this era, automation handles the manual workload of humans upto 98%. Thus, efficiency in cybersecurity operations is not a dream anymore. SOAR software is in the heart of operations enhancing security teams work in a smart, collaborative and effective environment. You can't protect before you see and detect. Collecting any data, visualizing and turning into actionable intelligence are possible via our infinitely scalable and cluster SIEM. With 10 years of experience, Logsign is a sincere team player for all internal & external parties, trusted by more than 500 enterprises, ministries and state agencies.

www.logsign.com

support.logsign.net

Info Security Products Guide 2020 Global Excellence Bronze

Cyber Security Excellence Awards Winner 2020

Cyber Security Excellence Awards Winner 2019

Info Security Products Guide 2019 Global Excellence Silver

Info Security Products Guide 2019 Global Excellence Gold

Cyber Defense Global Awards Cyber Defense Magazine 2018 Winner

Logsign