



Detect Faster, Respond Easier

Streamline Security Operations with Best-in-class SIEM

Logsign Security Information, Event Management, and Response Platform

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.



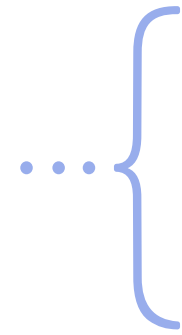
Our products are recognized and followed by all security authorities and independent research companies. We build solid and long-term relationships with our end-users and channel partners.

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.



Why & How Logsign SIEM Helps You?

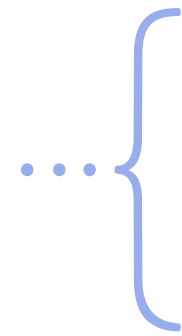
Secures organizations with increased visibility, real-time detection, and response



For strong cyber security needs

- 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

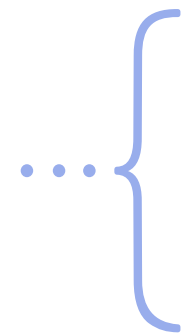
Provides compliance



For compliance requirements

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

Worths to invest in Logsign SIEM

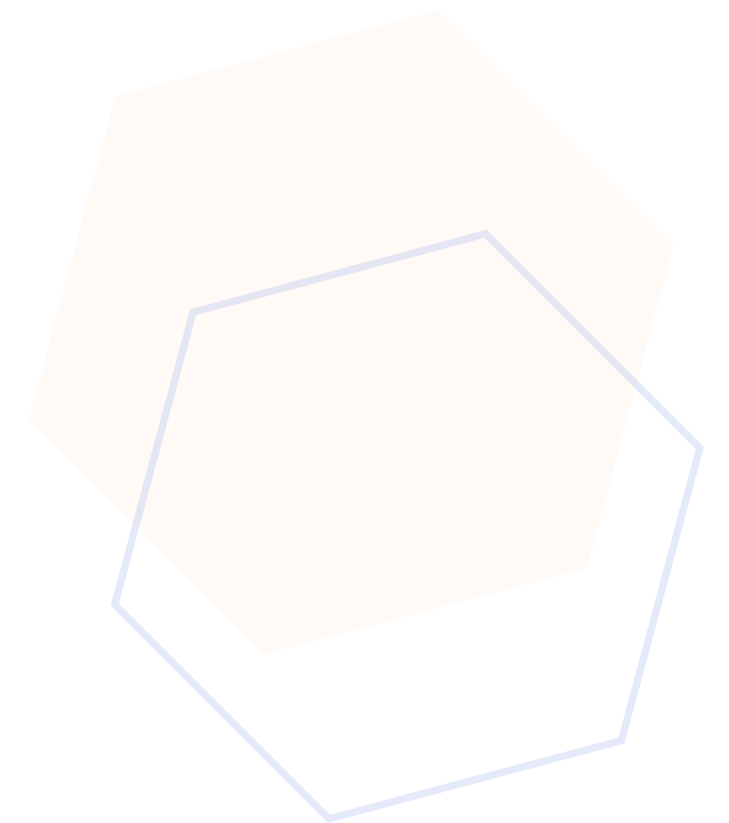
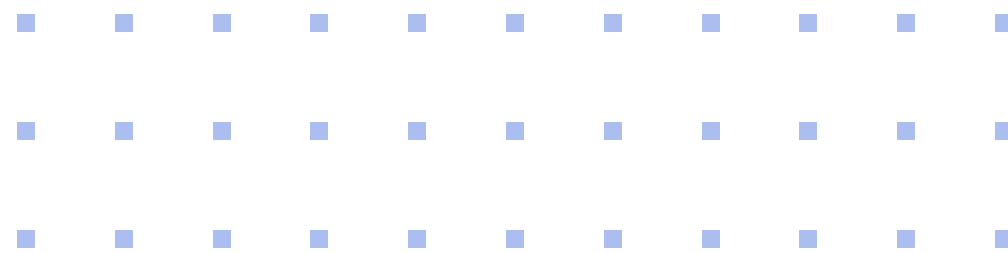


For overcoming investment and operational challenges

- 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

Let's Take a Look!

What Logsign SIEM Does & How Differentiates?



Logsign In a Nutshell



**Search & Investigate
in Milliseconds**



**Visualize the
Actionable Results**



**Act on
One Click**



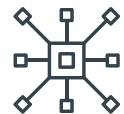
**Detect Real-time with
In-memory Threat Intel**



**Create Superpower
Data Lake**



**Integrate Easy,
Collect More**



**Rapid and Painless
Deployment**



**Be Compliant,
Feel Safe**



**Value Added
Services**

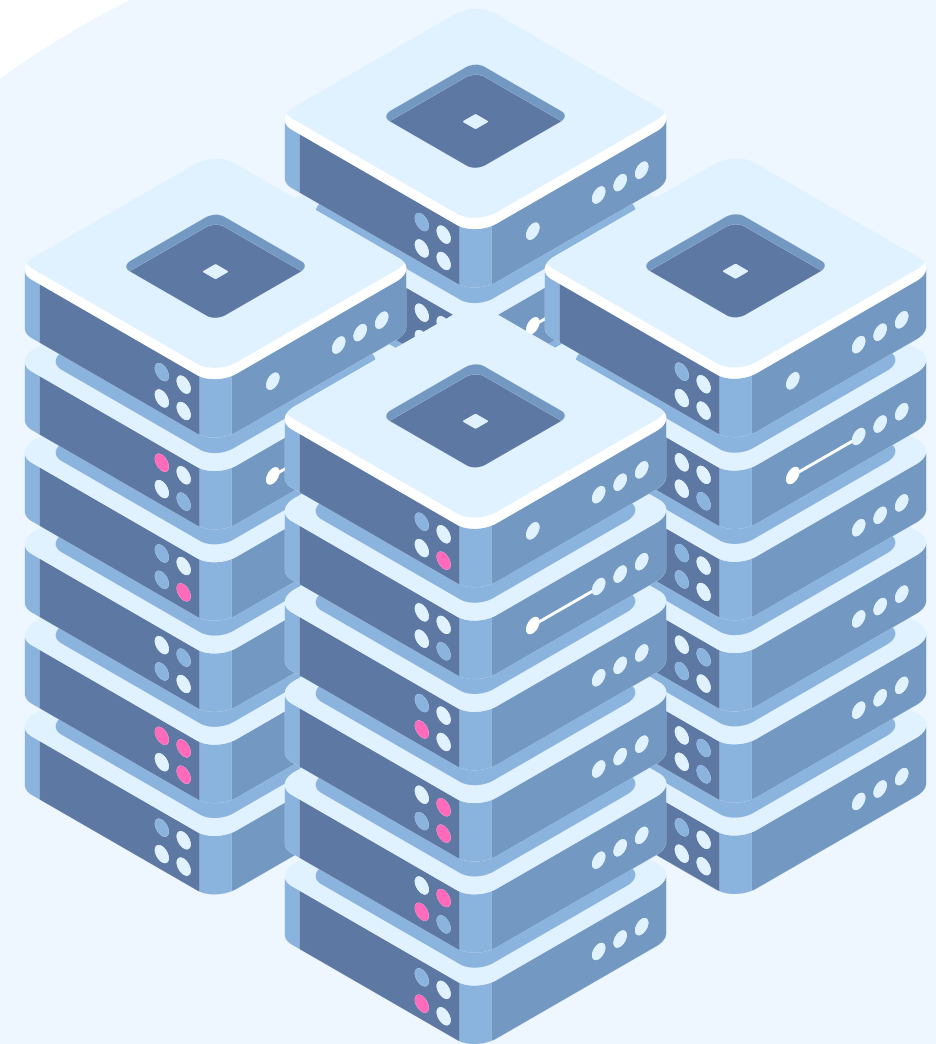


Out-of-the-Box Incident Management & Response

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.

Super Power Data Lake

- Vertical and horizontal, enterprise-grade scalability
- Cluster architecture, high availability
- Fast, simple deployment for hybrid environments
- Long-term data storage and retention
- High capacity data collector for distributed environments



Extensive Integration Framework

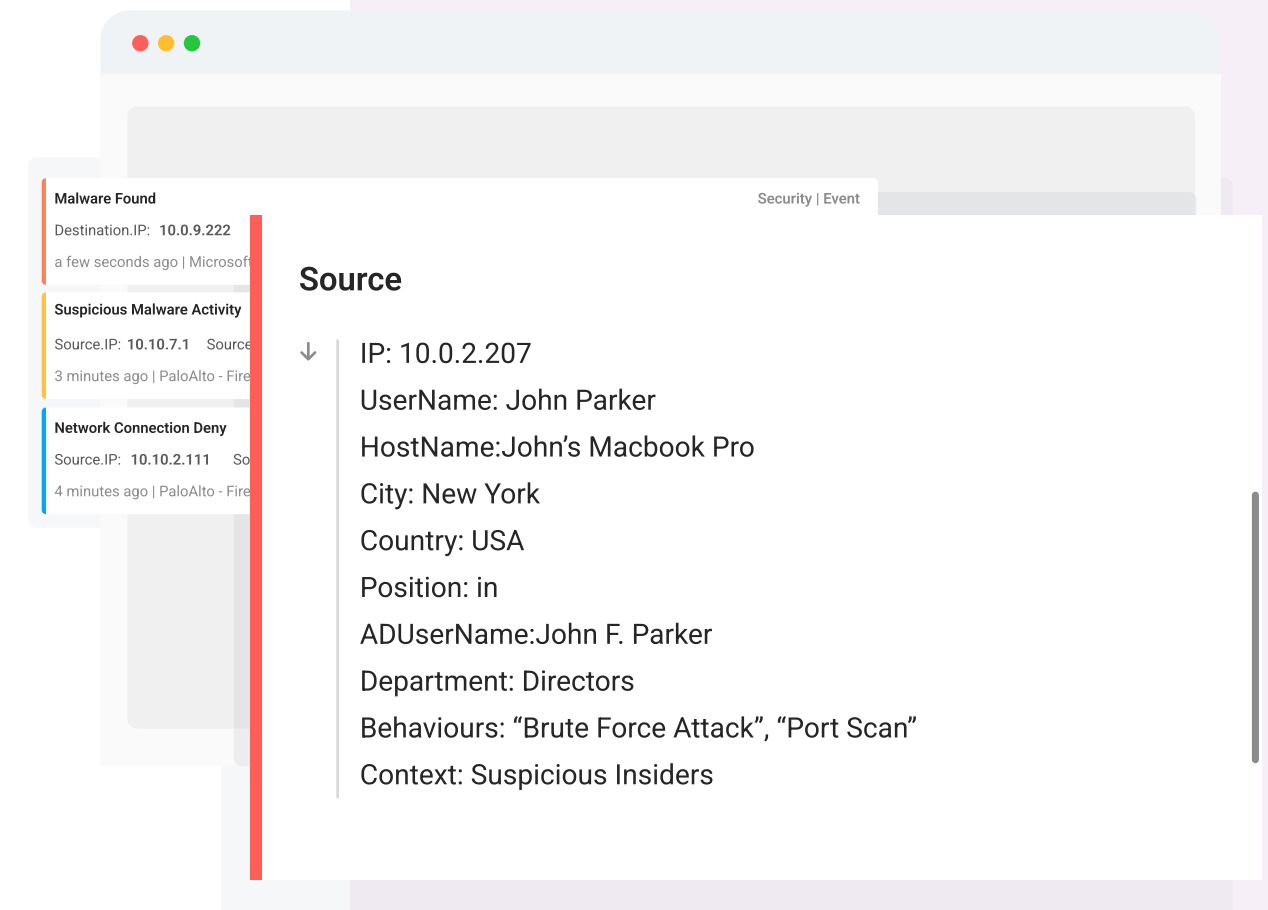
- 400+ built-in data collection integrations
- 100+ built-in detection & response integrations
- Custom parser & free plugin service
- Reduce the data noise with the data policy manager
- Classification and normalization
- Data manipulation and modification
- Data collection techniques: API, NetFlow,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

500+ Integrations



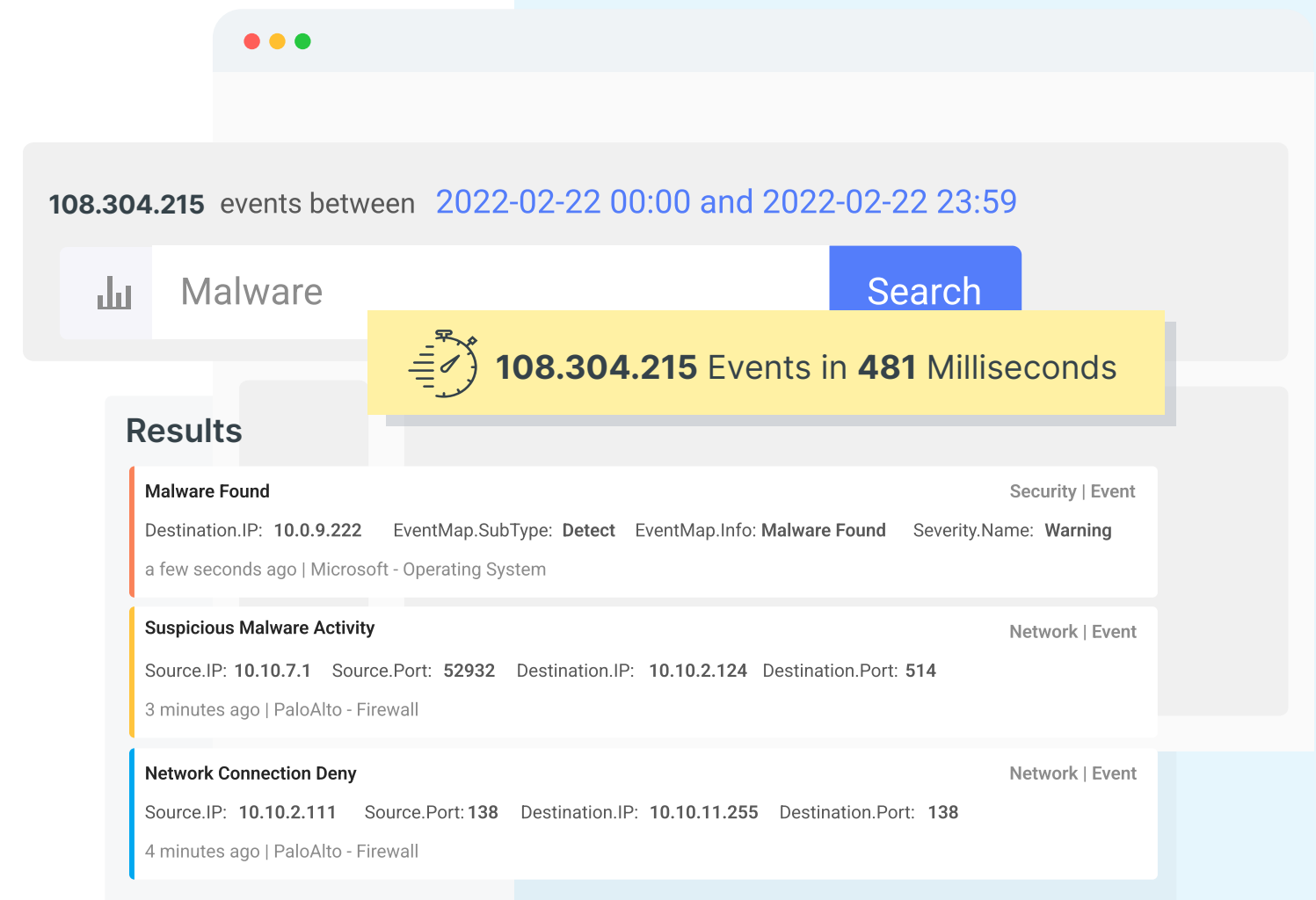
Data Enrichment

- Asset and identity enrichment
- In-memory, real-time threat intelligence enrichment
- GeoLocation enrichment
- Network position, branch, etc. enrichment
- Behaviour enrichment
- Context enrichment
- Custom enrichment
- Instant data processing




Investigation in Milliseconds

- Drill-down, full-text, advanced, and Lucene search
- Investigates correlated and enriched data, and finds results in milliseconds
- Threat hunting for hidden threats, IOCs, and IOAs
- Validation of threat levels, and incident triage
- Forensic investigation



108.304.215 events between 2022-02-22 00:00 and 2022-02-22 23:59

Malware Search

 108.304.215 Events in 481 Milliseconds

Results

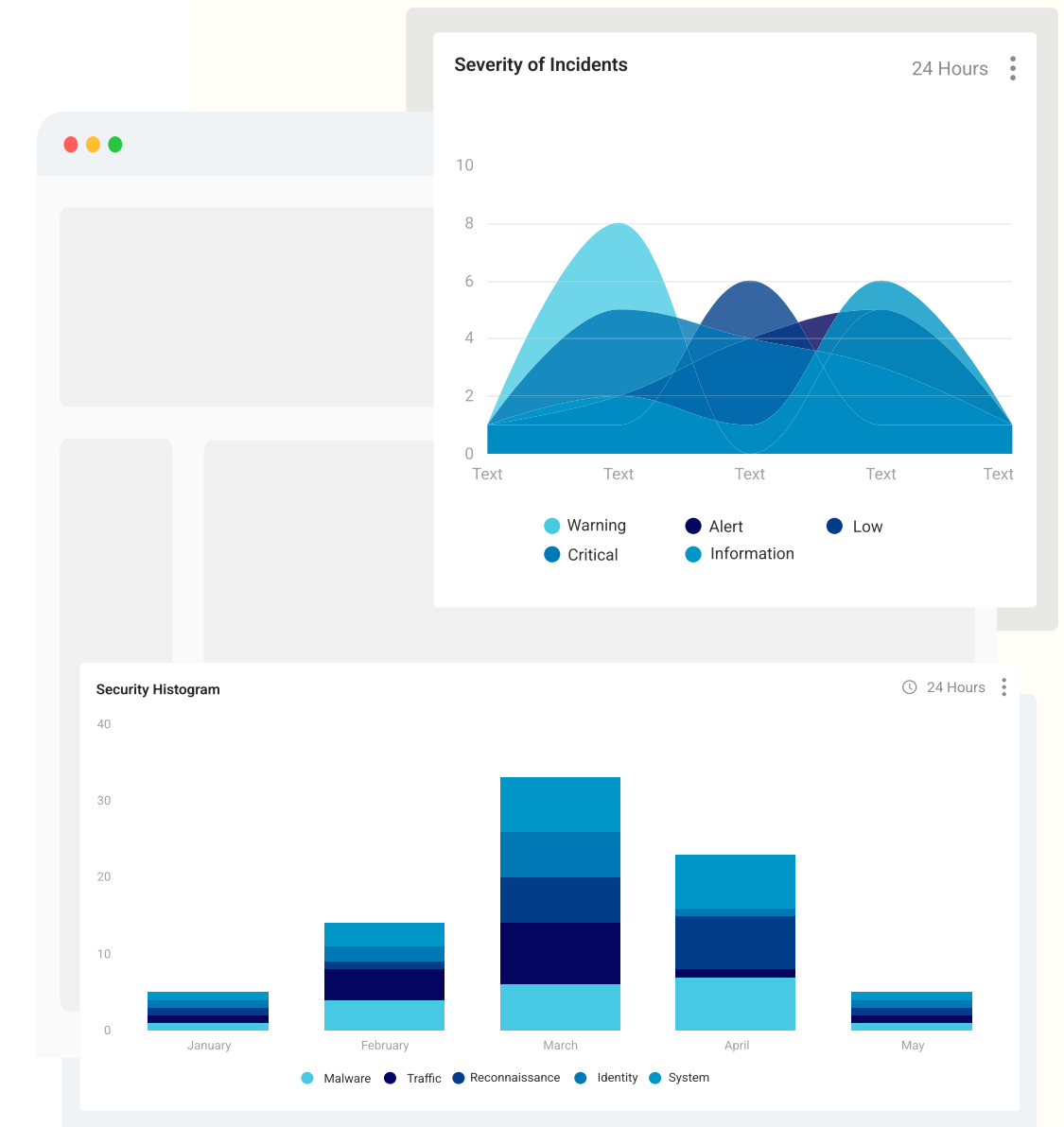
Malware Found	Security Event
Destination.IP: 10.0.9.222 EventMap.SubType: Detect EventMap.Info: Malware Found Severity.Name: Warning	
a few seconds ago Microsoft - Operating System	

Suspicious Malware Activity	Network Event
Source.IP: 10.10.7.1 Source.Port: 52932 Destination.IP: 10.10.2.124 Destination.Port: 514	
3 minutes ago PaloAlto - Firewall	

Network Connection Deny	Network Event
Source.IP: 10.10.2.111 Source.Port: 138 Destination.IP: 10.10.11.255 Destination.Port: 138	
4 minutes ago PaloAlto - Firewall	

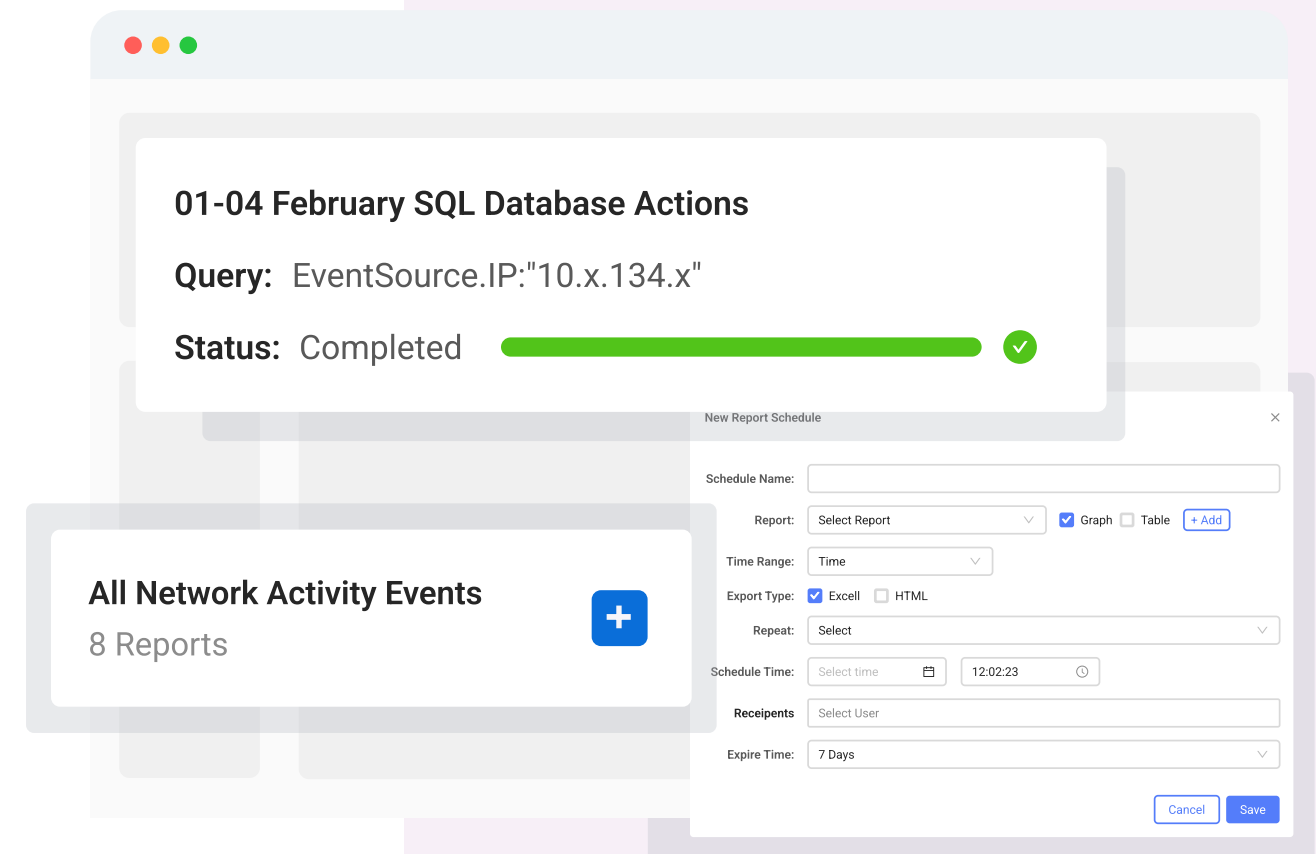
Security Analytics

- Hundreds of out-of-the-box dashboards
 - Security, database, file, user activities, behaviours, cloud security, threat intel monitoring etc.
- Easy to customize, 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 customizable time frame



Security & Compliance Reporting

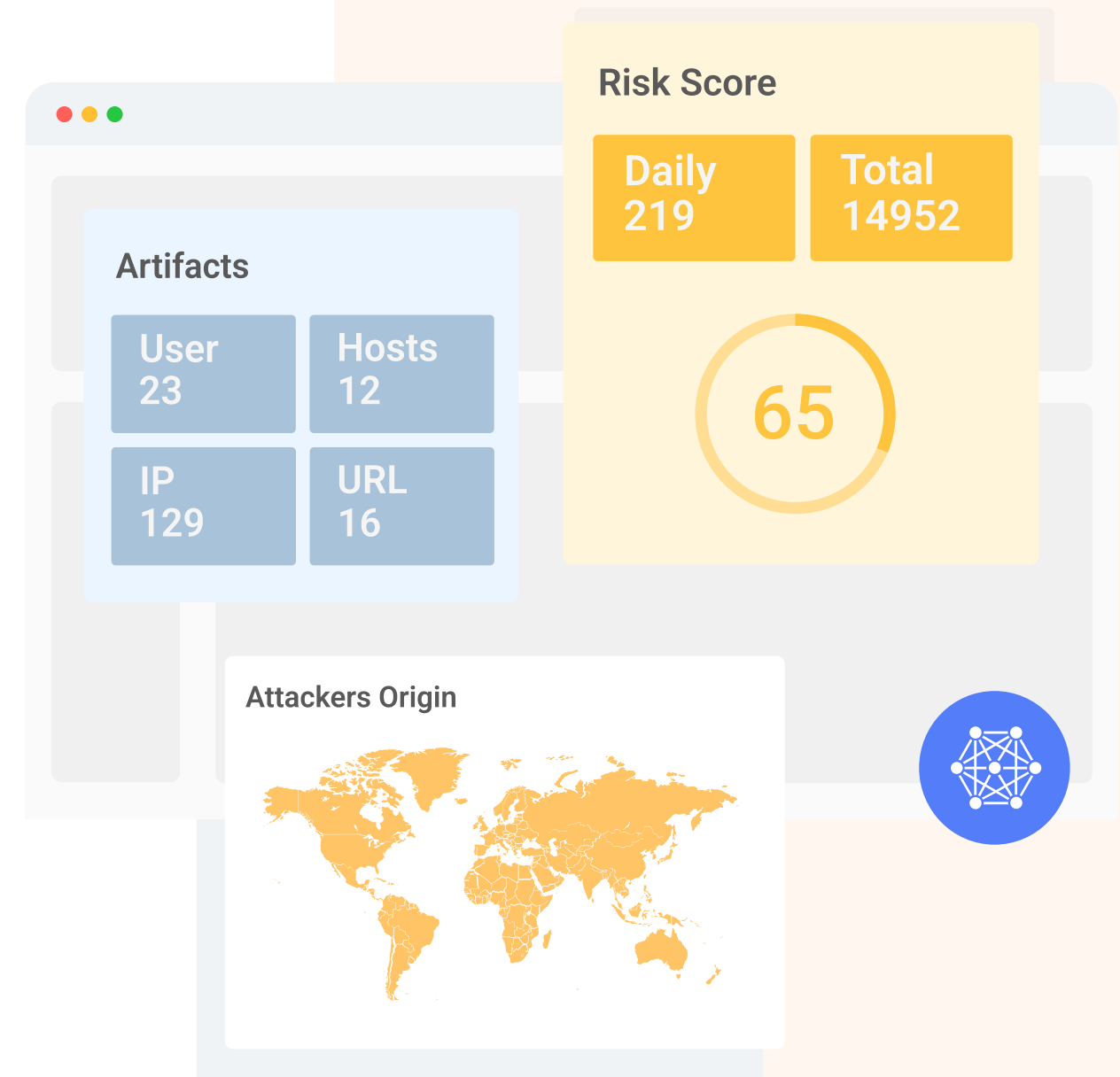
- Hundreds of built-in reports
- Easy to create, and configure new ones
- Creating and exporting in seconds
- Built-in compliance reports
- Automated & scheduled reports
- Ad hoc reporting, executive reporting
- Delegation: Role-based access control



Detection of Complicated Threats

“ Detects attackers on their first attempt. ”

- Comprehensive correlation techniques
 - Risk based, rule based, behavior based, threat based correlations, historical correlation, vulnerability based correlation, cross-correlation
 - 500+ built-in correlation rules
- MITRE ATT&CK® and Cyber Kill Chain frameworks
- Advanced behavior analytics
- Threat intelligence

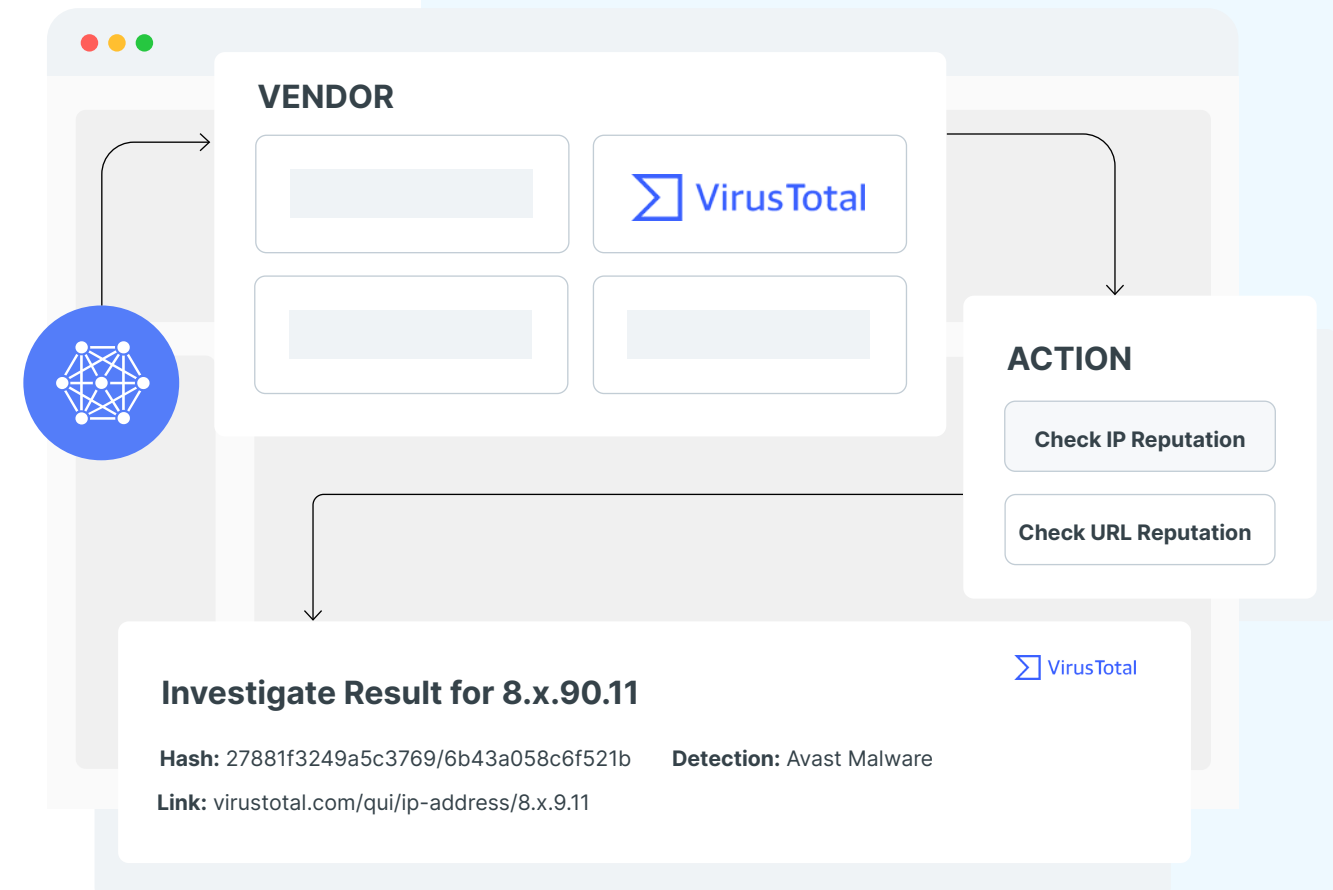


Threat and Anomaly Detection, Zero-Day Attacks, Phishing, Brute Force, Malware, DOS/DDOS, IOC, etc.

Incident Management and Response

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

- Automated or semi-automated response
- Action button for one-click response
- NIST incident life cycle
- Visual cards for investigation, detection, and response
- Artifacts, assets, and identity management
- Incident timeline
- Incident summary and detailed views



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.



SIEM Guide

Instructions related to SIEM installation and usage



Submit a request

Contact us through a specially prepared form



Logsign Academy

Get started with Logsign.



Community

Join discussions with other users



Thank
YOU!