Logsign®

Logsign Next-Gen SIEM for Security Big Data Analytics

Datasheet

Security Big Data Analytics

What is Security Analytics?

Security analytics is the process of using data and a variety of tools to protect computer systems from cyber threats. It forms data analysis infrastructure suitable with the digital infrastructure and culture of companies and organizations to monitor, detect, predict, and investigate malicious risks (internal and external attacks, information security violations, violations about the protection of personal data, cyber sabotages, cyber bullying, etc.).

Security Analytics – Areas of Use

- Proactive security incident perception and response.
- Maintenance of compliance with legislation.
- Advanced digital forensics abilities.

Logsign SIEM Security Analytics Use Cases

- Analyzing user behaviors to detect potential suspicious activities
- Analyzing network traffic to detect trends that show the potential attacks
- Detecting data leakage
- Detecting internal threats
- Detecting compromised accounts
- Investigating cyber threat incidents

Threat hunting

- Analyzing data leakage
- Performing compliance and statutory audit requirements (ISO27001, HIPAA, SOX, GPDR etc.)
- Monitoring the compromised privileged and service accounts
- Monitoring the applications to detect suspicious behaviors
- Monitoring to detect suspicious log-in models
- Detecting fraud

Incident response and case management

Logsign SIEM Security Big Data Analytics Approach

Security departments collect and analyze security information to detect indicators of false positives or legitimate threats and investigate relevant correlations. However, this creates a serious load that wastes time and resources. Our Logsign SIEM security analytics approach solves this issue. It increases the correctness of threat perception by automatically conducting most of the security incident correlations and analyses.

Logsign Big Data infrastructure increases the need for data management and data discipline. Our Logsign Security Analytics approach provides strong security data modelling and management.

With the digitalization of work processes, businesses today create terabytes of security incident data. Even though machine learning and behavioral analytics will become more important, it is impossible for them to replace rules. A cSOC should detect both known and unknown threats.

Strengthened with elastic search, Logsign SIEM receives the data outputs in milliseconds for any type of data analysis (real-time or past) by using various search algorithms. It conducts anomaly and threat analysis with detailing or collecting methods. cSOC teams perform these analyses by using complicated search inquiries. Moreover, System and Network teams conduct real-time monitoring by using detailed indicator tables.

Logsign Security Analytics enables you to reveal and prioritize real threats, and discover known and new threats.

Using signatures and rules is both rapid and correct; they are the best methods to detect known threats. But what about the unknown ones? Detecting these types of threats increases the need for basic data processing steps such as recovery, managerial commentary and enrichening. Logsign SIEM security analytics technology will therefore be your most important player for security analytics solutions. In other words, Logsign SIEM security analytics will make it easier than ever for you to achieve real-time results among terabytes of corporate data.

The purpose of security analytics is to examine the data collected for security monitoring, threat perception, and detecting suspicious activities and threats. Security analytics is included in the algorithms to detect big and various data sets.

Logsign security analysis tools use different methods to analyze data, including traditional rule-based methods, as well as statistical analysis and machine learning. The application may also include other components to automatize and configure incidents.

Logsign Security Analytics enables you to reveal and prioritize real threats, and discover known and new threats.

Using signatures and rules is both rapid and correct; they are the best methods to detect known threats. But what about the unknown ones? Detecting these types of threats increases the need for basic data processing steps such as recovery, managerial commentary and enrichening. Logsign SIEM security analytics technology will therefore be your most important player for security analytics solutions. In other words, Logsign SIEM security analytics will make it easier than ever for you to achieve real-time results among terabytes of corporate data.

The purpose of security analytics is to examine the data collected for security monitoring, threat perception, and detecting suspicious activities and threats. Security analytics is included in the algorithms to detect big and various data sets.
Logsign security analysis tools use different methods to analyze data, including traditional rule-based methods, as well as statistical analysis and machine learning. The application may also include other components to automatize and configure incidents.

Benefits of Logsign SIEM Security Big Data Analytics

Proactive Cyber Threat Perception

Current SIEM approaches force you to approach security reactively and passively. On the contrary, Logsign SIEM Security Analytics provides a long-term approach to system and data security by focusing on the analysis of data in order to create proactive security measures.

This results in a flexible approach that can continuously be improved to confront new threats and vectors.

Effective Security Analytics and Threat Perception on One Platform

Logsign SIEM Security Analytics emphasizes the analysis of security data rather than their management. For an effective analysis, it collects data from various sources including security analytics interior and external network traffic, access and identity management systems, connected devices, and business software. These data are combined with external security threat intelligence and current collections of notified security incidents.

Collected data are processed and analyzed by traditional statistical analysis at an accelerated rate by artificial intelligence and machine learning. As a result, you can measure the potential threats according to what is going on both on your system and the world outside your corporate network.

Cloud-based Security Analysis and Deep Threat Analysis with Big Data Infrastructure

Logsign SIEM Security Analytics benefit from all the advantages of cloud-based infrastructure, which provides almost unlimited and uncertain data storage that is scalable based on your needs. This enables you to protect potentially beneficial data without being limited to corporate data storage policies.

In addition to defining known threats, Logsign SIEM Security Analytics also learns to detect undocumented problems by analyzing large amounts of data to reveal secret relations, anomalies, trends, and fraudulent behavior types. It proactively protects the vital data and infrastructure of your corporation.

As a result, Logsign Security Analytics provides better protection and more scalability at a reduced cost.

Advanced Threat Detection and Analysis with MITRE ATTACK

Logsign SIEM, using MITRE ATT&CK framework, allows you to define techniques, tactics, and procedures against cyber threats.

Its early warning system enables you to detect suspicious behavior and define the prevention actions with its early warning mechanism.

About Us

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

0 850 660 0 850

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