SIEM

"INTELLIGENT AND FAST" SECURITY INFORMATION AND EVENT MANAGEMENT SOLUTON

Logsign is a full feature, all-in-one SIEM solution that unifies Log Management, Security Intelligence and Compliance, delivering great value via clear visualization and better understanding to organisations.

Furthermore, it also ensures that you distinguish the threats much more easier and take precautions and strengthen your security stance by the help of its developed threat analysis approach and advanced level of correlation skills. It has strengthened security and perfect delegation skills for the purpose of ensuring high level of customer satisfaction and it works in accordance with your teams.

Benefits and Features of Logsign SIEM

Real-Time Monitoring and Dashboards

You may achieve visibility at your desired levels via security based, pre-defined and customizable analyses. Besides, you may execute real time and easy reporting by preparing dashboards and widgets which are appropriate for your new and adhoc necessities.

Greater Team Effectiveness
Flexible and Easy Dashboards, Delegation

Advanced Delegation Capability

By virtue of delegation skills, you may execute authorizations in accordance with the duties and responsibilities of your IT teams. Thus, all teams may prepare their own dashboards / reports and you may establish source-responsible relationship within your team.

Fast and Flexible Search

Via the HDFS-based NoSQL architecture you may reach millions of data within seconds. The file integrity presented in the same solution ensures that you detect advanced attacks such as zero day / zero second attacks by virtue of user and behaviour monitoring. You may make in depth analyses in all prepared reports and visuals. You may narrow the results by filtering and achieve outputs aimed at action.

Automated Reports for Compliance and Internal Auditing

You may fulfill the legal compliance regarding 5651, PCI DSS, ISO 27001, HIPAA, SOX and generate reports by single click or automatically. By the help of analytic based multiple reporting feature you may have some separate reports in the form of a single report. You may schedule all reports for specified periods.

HIGHLIGHTS

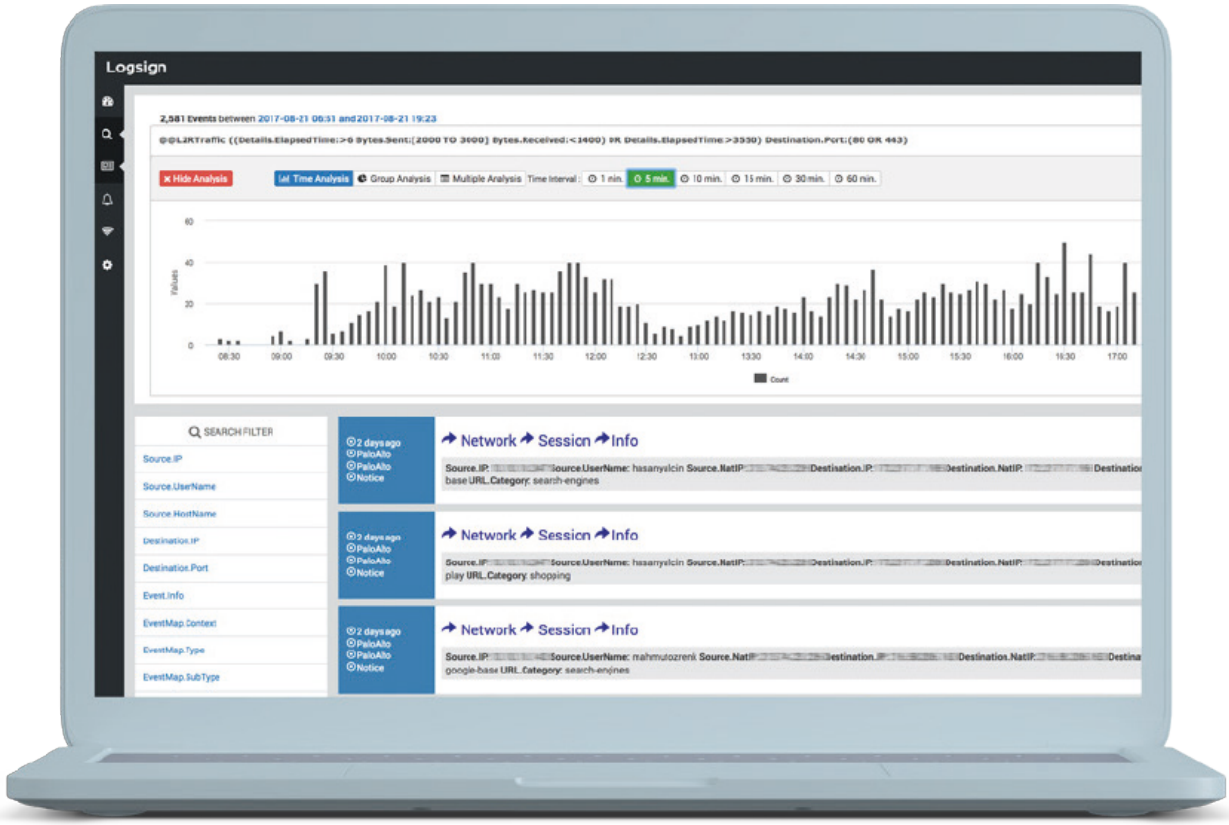
- With its flexible&scalable architecture, it provides high availability and redundancy.
- Discovers next-gen threats and take precautions.
- Detects internal and external threats.
- High capacity log classification.
- Multi-machine correlation architecture.
- Threat Intelligence embedded correlation.
- Hundreds of pre-defined dashboard and reports.
- Optimizes compliance and information security processes.
- Lowers the total cost of ownership.

Comprehensive Log Collection

It collects security data such as Firewall, IPS, OS data and logs generated from data bases, network devices and applications. It supports many log collection methods such as SYSLOG, SMB, WMI, FTP, SFTP, LEA, SQL, ORACLE, Flow. It easily collects logs from central and dispersed structures.

200+ Pre-Defined Integration

Logsign can be installed in physical, virtual and cloud systems easily and in a very short time. Easy and flexible installation is possible with more than 200 predefined, ready integrations. Besides, it provides free plugin services for your integration requirements.



Log Normalization, Classification and Enrichment

It collects, normalizes and classifies for analysis the security walls, IDS/IPS devices, APT devices, WAF solutions, routers, keying, servers, operating system journal and application journal events. Thus, it makes it easier for you to determine, monitor and report same type events occurring in difference sources.

200+ Pre-Defined Integrations
Fast and Flexible Deployment

Efficient Data Management with Logsign Data Policy Manager

Logsign has a powerful data management system for the purpose of optimizing system power with respect to entry, data processing and storage levels of the system.

Alerts and Security Automation

By the help of its developed correlation skills, it warns your teams and enables them to take action concerning determined security flaws, violations and attacks. With its low false-positive numbers, it avoids time and labor loss. In addition to hundreds of pre-defined alarms, it enables definition of new alarms easily. It has security automation procurement skills by being integrated into security devices with API connections. It provides real-time security by ensuring action-taking for the devices it is connected automatically.

Multi-machine Correlation Architecture

High Capacity Correlation

Early Threat Detection and Response with Logsign Threat Intelligence Service.

It combines data obtained from local sources with global intelligence data on real-time and thus it enables you to detect probable threats prior to their occurrences and take precautions accordingly. While executing the mentioned operation, it processes all open source and commercial lists together, determines the lists in accordance with the required priorities and is being fed.

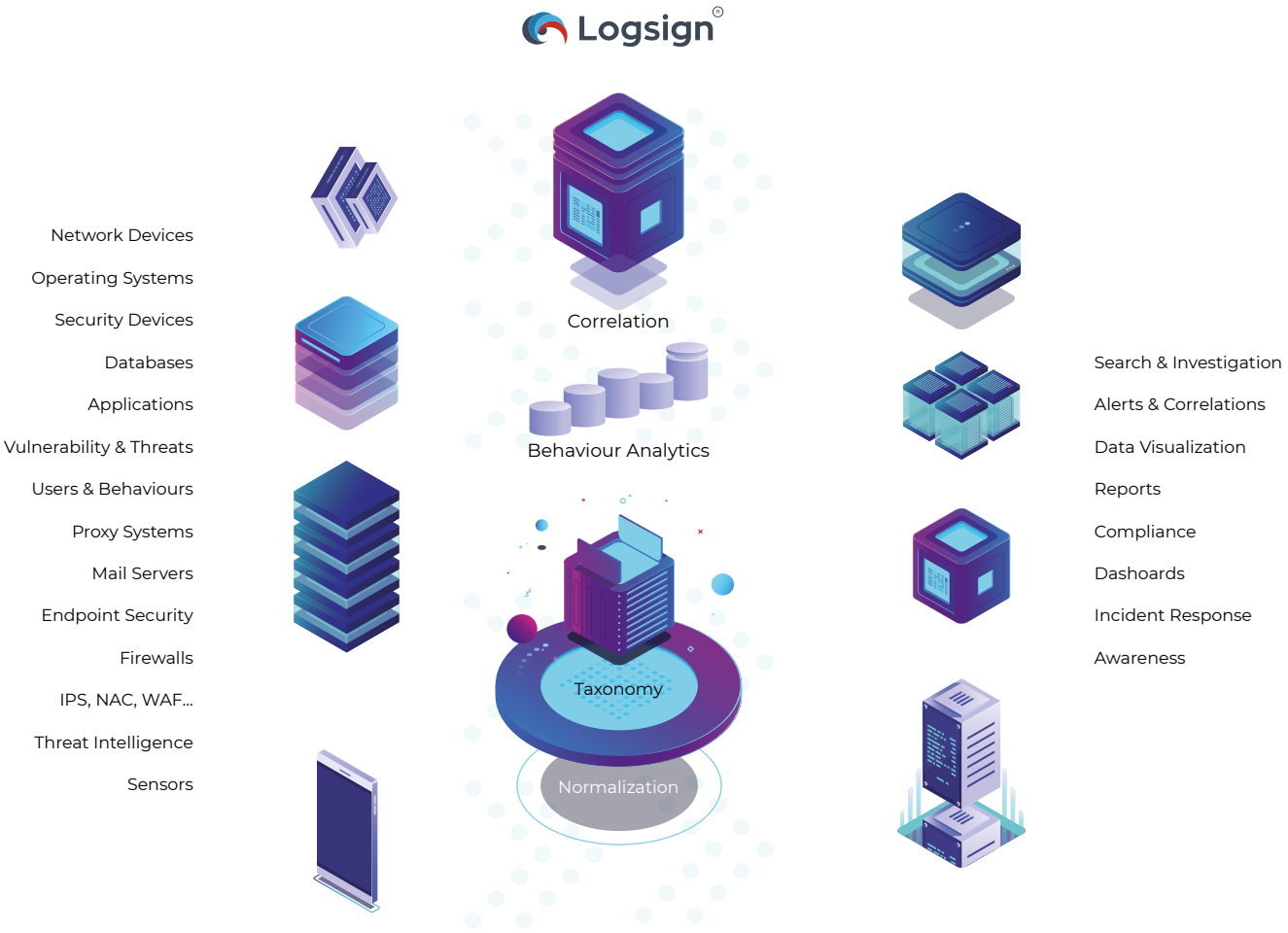
Thereby, you have the opportunity to transform threat flows incoming from prioritized lists to action in proper ways. It focuses on vicious IPs and URLs such as botnet, phishing ip, malware, offensive IPs, phishing and zero day attacks. It makes real-time determinations and transforms strategic decisions into action.

Correlation Architecture

By virtue of its multi-machine correlation architecture, it provides comprehensive solutions for the necessities of large scale institutions. It is equipped with high level scalability skills with respect to the fields of increase in the capacity of the correlation system, ensuring redundancy of the correlation system and load distribution. It has a wide correlation library. It executes real-time enrichment of all security journals and events incoming from different sources by combining them with global cyber intelligence data and it generates quick, correct results and results which can be subject to action easily. It correlates millions of data in seconds.

Detect, Response

Correlation, Alerts, Incident Response



Scalability Matters
Cluster Architecture, Redundancy

Availability and Redundancy

Logsign has multilayered data and service back up capacity. You may store and back up live and offline data at the petabyte level. It ensures redundancy in all layers, it stores your data in distributed or central form. It protects your data safely and makes them all time accessible by the help of its automatic activation, service increase, load transfer and self improvement skills in potential disaster scenarios. This feature provides you flexibility, mobility and the opportunity to take action in instantaneous states.

High Scalability

Logsign can easily be scaled horizontally and vertically as your necessities increase. You may add more users, admins or locations. You may work with tens of server groups having similar roles and you may assign different roles for different servers. Logsign scalable architecture is appropriate for usage as SOC infrastructure.

“Customer Satisfaction Index”

%94*

*According to ZenDesk 01.01.2019-28.02.2019

TOP 25 CYBER SECURITY COMPANIES – 2018 APPLICATIONS

CYBER SECURITY EXELLECENCE AWARDS ★ WINNER ★ 2019

500 Technology Fast 500 2017 EMEA WINNER Deloitte.

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD ★★★★★

CIO Review 10 MOST PROMISING CYBER SECURITY SOLUTION PROVIDERS - 2018

Logsign is a Security Information and Event Management (SIEM) solution which provides security analyses and compliance to regulations in one platform. Founded in 2010, Logsign believes that cyber security is a teamwork and that security products have to be much smarter. With this conviction, it focused its endeavors on Security Intelligence and SOC solutions. It actively provides services for more than 500 medium and large scale firms and governmental agencies. It is working to be an irreplaceable team-mate for all of its stakeholders in the field of cyber security, to raise its customers' security awareness to the maximum and to reinforce their position concerning security. It also proved its competence in the field of technology as a cyber security software producer, landing among Deloitte Technology EMEA Fast 500 in 2017 for the second time.