Logsign

Logsign Next-Gen SIEM Correlation Engine

Datasheet

How Logsign SIEM Correlation Engine Works

Correlation defines the dependent or independent relationships of all the incident data and the data collected for security analytics, and sends warnings when necessary. Correlations assist in rapidly detecting IT problems, conducting the root cause analyses, minimizing the losses during business continuity, and rapidly solving problems.

The Logsign SIEM correlation engine analyzes, in real-time, all normalized incident data and all data included in the taxonomy, automatically forms the relationships within the ongoing incident logs, and assists in creating notifications. In addition, it enables real-time threat visibility by simultaneously (in-memory) combining the cyber threat intelligence data with incident logs.

The alerts created with correlation output are re-indexed on the Logsign SIEM system and turned into incident logs so they can be used for various correlation types. Therefore, the result of a correlation may be used for another correlation relationship.

Correlation Categories

Logsign correlation engine automatically starts working at the first installation with 16 predefined categories. Similarly, there are more than 200 predefined behavioral sets of information for these categories.

Correlation Techniques

The Logsign correlation engine triggers alerts and actions to prevent threats and create awareness. It achieves this by investigating the relationship between past data and real-time data, and the correlation output it received from the integrated TI data created with the help of predefined rules. Logsign SIEM conducts active monitoring with real-time correlation and keeps the data at the memory level.

Its correlation engine, which correlates unlimited number of EPS with its scalable technology, also performs cross correlation and enables the correlation and interpretation of various incidents that look independent from one another.

Logsign SIEM enables and interprets the relationship and the interpretation of the relationship between the incidents and the operating system by using the inventory correlation. In short, it predicts possible threats with behavioral pattern analyses.

Correlation Models

Logsign SIEM takes part in perceiving the behavioral models listed with complex incidents and the correlation library and categories. Logical correlation is the correlation and interpretation of various incidents that appear independent. Cross Correlation is the correlation and interpretation of incidents with security gaps. Inventory Correlation is the relationship and interpretation of incidents with the operating system.

Event-Based Correlation

Event correlation is the correlation model whose result does not depend on statistical data.

Including the “Security Use Case” contents while defining the rule set enables you to determine more specific incidents.

Statistical Correlation

Statistical correlation uses special digital algorithms to calculate the threat level of security incidents on various IT entities.

When the accustomed data density reaches beyond the standard amount, the mechanism that creates the alerts is activated.

Rules-Based Correlation

Rules-based correlation uses the data from a realized or alert-creating incident. For instance, there may be situations where previous attacks need to be monitored for an attack to be detected.

This scenario is coded as “if that is, therefore, some actions need to be taken.” It makes relational evaluations based on statistical lists and standard data, and draws relational conclusions using rule-based correlation data.

Cross Correlation

Many related incidents need to be analyzed for the attacker or the suspicious activities to be detected. Logsign SIEM searches among the undetected secret cyber security problems by combining the data generated from various resources.

For instance, cross correlations are needed in case of suspicious behavior on the relevant system following a DDOS or XSS attack on a critical system, or for the inclusion of a correlation that is analyzed for the incident. Logsign checks whether the first alert is triggered at the right time and the right way.

Historical Correlation

Repeated attack models, as well as automatic and slow attacks that may be covered during millions of security incidents, can be detected.

Logsign rapidly detects the malicious incidents not recognized before. As a result, analysts are better positioned to discover future zero-day attacks in real-time.

Multi Correlation

When we want to specifically detect the attacker in real terms, we usually detect the real attacker when we create an alert from the incident.

This is the structure that is nourished from “Asset&Behaviors”, the equivalent of the collection of contexts that include many correlations in Logsign SIEM infrastructure.

Malware & Botnet Infection Correlation (TI supported)

Relational rules may be written with other context data by enabling the log to be enriched by TI services, forming relationship according to the data in the security data, and collecting data on possible external threats within our structure.

Threat-Based Correlation

The objects we call threats may be vulnerabilities and malware. Vulnerability applications, which are referred to as “endpoint” and “threat intelligence” systems, collect information about the objects.

While correlating the data, the relevant Logsign SIEM user does not need to know about each attack vector and vulnerability. They only need to know which context to use. Thanks to this information, collecting the threats from various systems under one or more “contexts” enables an effective use.

Product Based Correlation

We are allowed to obtain product-independent results with the product-independent evaluation of the advantages of taxonomy and normalization and similar events under the same category.

For instance, when we write a rule with a successful log-in, that enables a correlation that works together with other relational rules without considering which product it is.

How the Correlation Engine Works

Logsign SIEM's correlation engine correlates an unlimited number of EPS with its scalable technology and ability to detect threats with its predefined rules in real-time. It foresees the threats that may occur with the behavioral pattern analyses, and uses the incidents and information created as a result of the analysis of past data.

The features, behaviors and types of correlation rules can be classified under more than 30 categories and filtered. New ones can be formed as well.

TI Services Integrated with Correlation Engine

The platform makes it easy for relevant IT managers to act. Logsign correlation is integrated with the global threat data, which is shared by the Logsign SIEM TI service, and makes momentary threat detections.

IT managers interfere in the activation and spread of the threat vectors by collecting the produced analyses and information. Other than the TI services defined on Logsign SIEM, new TI services can be defined, and TI services can become more active. Logsign SIEM is compatible with more than 35 third-party TI service providers that collect information such as various analyses, scores, blocklists, malware, etc.

Alert Automatic Action

Through SMS and E-mail, Logsign SIEM enables IT managers to proactively react the cyberattacks and make rapid and correct decisions during intervention processes.

IT managers prevent the cyber threats by taking actions such as IP blocking, port blocking, limited blocking or cancellation, or adding objects on the rule group, Palo Alto, FortiGate, or Check Point firewall devices.

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