Logsign Threat Intelligence Service

Enrich Your Data with Logsign Threat Intelligence Service in Real Time

Logsign Threat Intelligence Service

What Is Threat Intelligence?

Threat intelligence provides evidence-based information, indications, effects and applicable suggestions regarding an existing or emerging threat or danger for assets.

Essentially, threat intelligence means having information about the infrastructure, sources, targets and actions (impulses) of the threat.

Consequently, threat intelligence allows you to identify and contextualize your adversaries.

The Threat Intelligence Cycle

Briefly, the Threat Intelligence Cycle is a continuous process with five stages. Intelligence teams are working to provide timely intelligence and leadership to reduce risks and uncertainties.

Requirements: This is the first step and there must be requirements and priorities set. Decision-makers need to identify what they specifically want to know and what the TI process should be telling them.

Collection: The second step includes all the different activities, mainly research, that involves the collection of data to satisfy the requirements defined. The step that can dominate much of a Threat Intelligence budget is to collect the information or data that is expected, once analyzed, to fulfil the requirements.

Analysis: It is necessary to analyze and manipulate threat data with different intelligence. Whereas simple analysis studies are enough in some cases, detailed analysis studies are also required in different incidences.

Production: At this stage, the threat intelligence product is created and distributed to customers. The product will accommodate changes in intelligence and inferiority of the client, and will meet detailed requirements.

Assessment: Another challenge of threat intelligence is to assess whether it meets the requirements of the intelligence product. As needs evolve, it will help to prepare the infrastructure for development that meets new and deeper requirements through the intelligence product.

Highlights

Provides adaptable and automatic protection.

Offers processable global and local threat intelligence.

Offers real-time detections and strategic responses.

Focuses on malicious IPs and urls including botnet, hostile IPs, malware and phishing.

Collect → Analysis → Production → Evaluation → Requirements → Collect

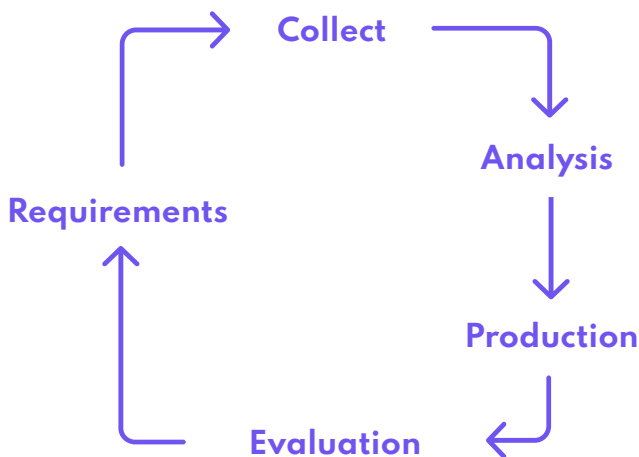## Advantages of Logsign Threat Intelligence Service

Perfect Integration: Logsign Threat Intelligence offers internal threat intelligence, open source intelligence and commercial threat intelligence all together. Threat Intelligence data are enriched with the data on the internal network and permit rapid detection of the risk.

Identifying the Risk: Logsign Threat Intelligence is supplied from lists (flows) based on certain priorities. This allows you to turn threat flows coming from prioritized lists into actions in the most appropriate way possible.

Advanced Attack Detection: Logsign Threat Intelligence flows provide rich content for malicious URLs, botnets, Froud, C2 IPs, phishing IPs and suspicious IPs. A summary of all these contents can be instantly converted to a blacklist.

Automatic Prevention: Blacklists created on the Logsign Threat Intelligence side can be used for alarms. Moreover, they provide integration for PA Firewall for instant action. Thisallows you to dynamically block usernames, URLs, internal or external IPs.

Correlation with Business Security Sources: Logsign Threat Intelligence provides real-time correlation with business security devices, allowing you to swiftly and instantly identify events and take action according to you prioritization.

Logsign

How Logsign Threat Intelligence Service Works?

Logsign Threat-Check Service Platform offers contents enriched by dynamic analyses.

Internal Feeds → Logsign ← **External Feeds**
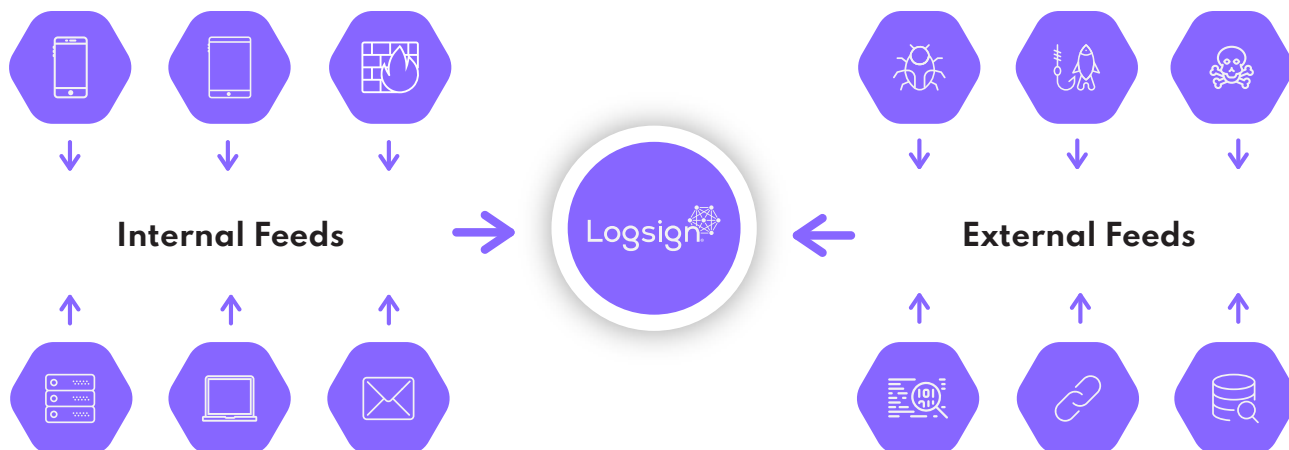
Threat Center Feeds

IP Adresss

Suspicious IP Adresses

Phishing IP Addresses

Malware IP Addresses

Botnet IP Addresses

Known Attack IP Addresses

URLs

Suspicious URLs

Phishing URLs

Malware URLs

Botnet URLs

Files

File Names

File Hashes

Phishing

Email Addresses

Email Subjects

User Agents

Known Attack User Agents

Malware User Agents

Malware Processes

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

Logsign