Logsign
Your teammate in cyber security

DATASHEET

LOGSIGN THREAT CHECK SERVICE

COMBINE THE INTERNAL SECURITY SOURCES WITH THE GLOBAL THREAT INTELLIGENCE IN REAL TIME!

What Is Threat Intelligence?

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

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

As a result of this, threat intelligence enables you to identify and contextualize your adversaries.

HIGHLIGHTS

- Provides adaptable and automatic protection.
- Offers processable global and local threat intelligence.
- Offers real-time detections and strategic reactions (responses).
- Focuses on malicious ips and urls such as botnet, hostile ips, malware and phishing.

The Threat Intelligence Cycle

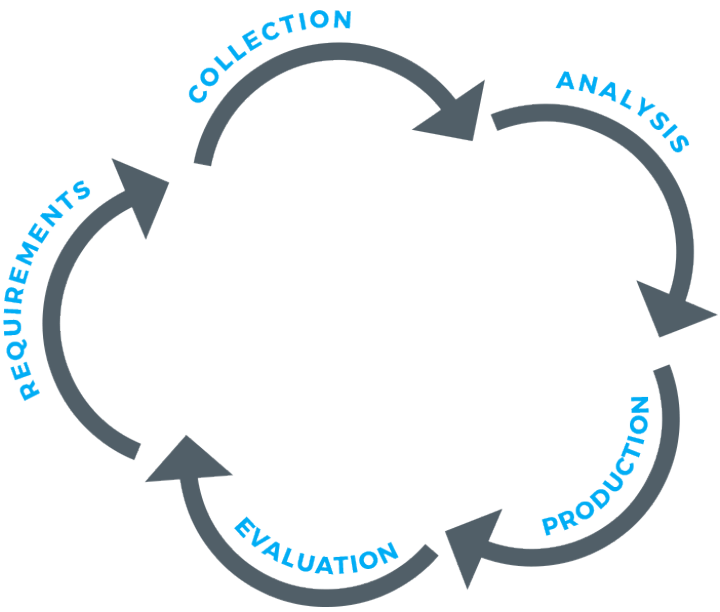
Briefly, the Threat Intelligence Cycle is a continuous process with five stages. Intelligence teams are working to provide timely intelligence and leadership to reduce risks and uncertainties.

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.

Advantages of Logsign Threat Check Service

- Better Integration: Logsign Threat Intelligence combine internal threat intelligence ,open source intelligence and commercial threat feeds. Threat intelligence data enriched with internal logs and quickly identify risk.
- Identifying Threats: Logsign Threat intelligence feeds from lists according to a certain priority. So you can assign incoming threat feeds and prioritize your response appropriately.
- Detecting Advance Attacks: Logsign Threat Intelligence feeds provide rich context such as malicious URLs , botnets,froud,C2 IPs, phishing and suspicious.All the feed context automatically added to a blacklists.
- Automatically Prevention: Logsign Threat Intelligence blacklists can integrate Alarms and automatic action with PaloAlto Firewall.So you can dynamically block usernames, URLs, internal or external sources,etc.
- Correlation Enterprise Security Sources: Logsign Threat Intelligence correlation near real-time other security sources. So you can analyze and used response rapid and precise event recognition and prioritization.

V

How Logsign Threat Check Service Works?

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

Threat Center Feeds

IP Adress
- 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

File
- File Names
- File Hashes

Phishing
- Email Addresses
- Email Subjects

User Agents
- Known Attack User Agents
- Malware User Agents

Malware Processes

20 MOST PROMISING CYBER SECURITY SOLUTION PROVIDERS 2016 — CIO Review

TOP 25 CYBER SECURITY COMPANIES - 2017 — CIO APPLICATIONS

500 Technology Fast 500 2016 EMEA WINNER Deloitte.

Solutions Review

10 fastest growing security companies SR 2017

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 2016.

For more information visit www.logsign.com

Help Center support.logsign.net / 0 850 660 0 850

Please contact us at info@logsign.com

İstanbul HQ ● Ankara ● San Francisco