LOGSIGN THREAT CHECK SERVICE

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

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.

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.

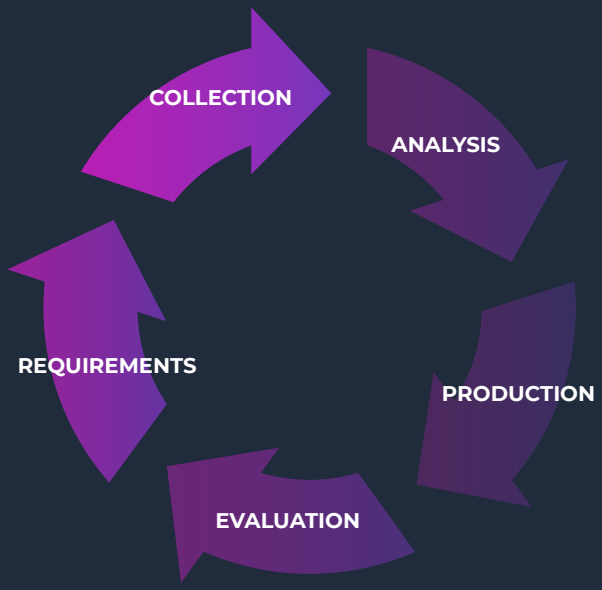
The Threat Intelligence Cycle

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

- 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.

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

CIO TOP 25 CYBER SECURITY APPLICATIONS COMPANIES - 2018

CYBER SECURITY EXCELLENCE 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.