Logsign®

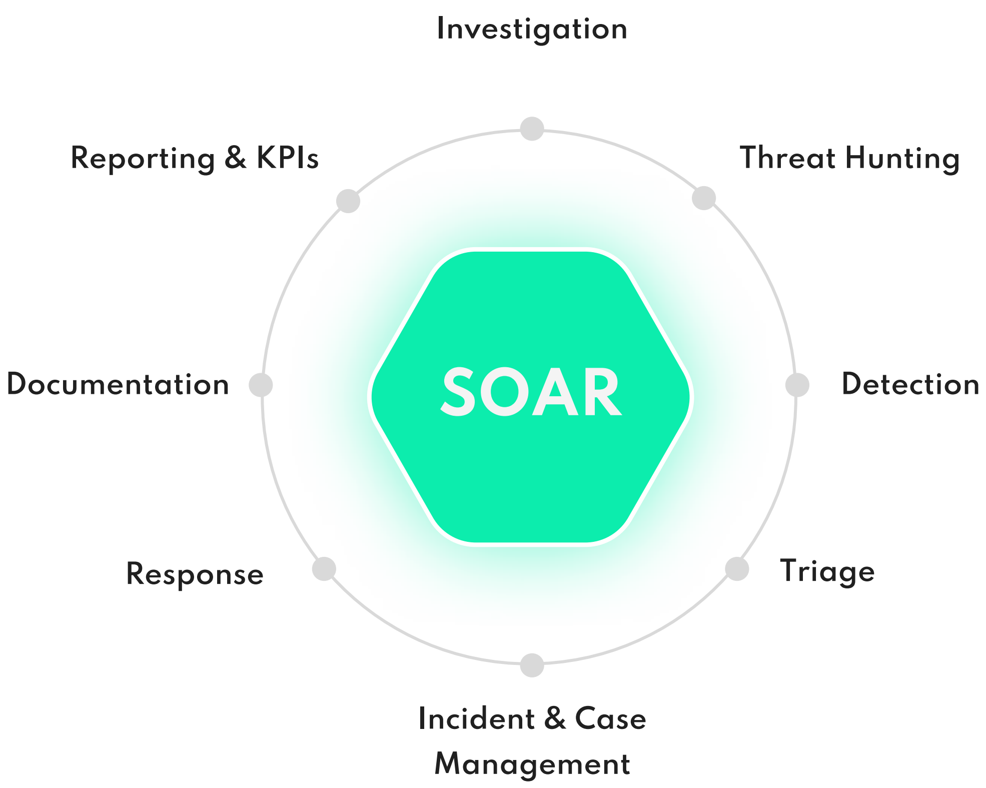
Security Orchestration, Automation and Response (SOAR)

Streamline Your Security Operations on a Centralized and Comprehensive Platform.

Automate your workflows, orchestrate your tools and people, reduce response times.

The Logsign Security Orchestration, Automation and Response Platform

Security automation is vital for creating an agile and efficient security environment. Once repetitive and time-consuming tasks are automated, analysts won't be exhausted and will have time to focus on incidents that are critical and require a decision process. In this way, automation and increased attention to and contribution of analysts on the critical tasks will significantly improves an organization's incident response capacity. Better and faster investigations, and reduced detection and response times are on the table with a well-designed, broad-based SOAR.



Automation

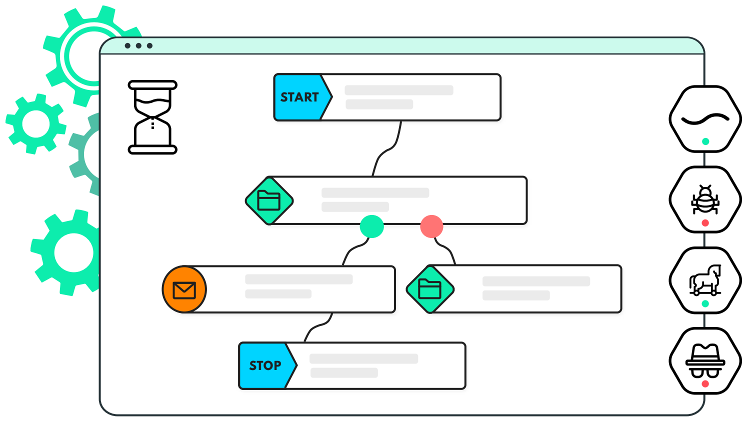
Security automation refers to automated processes of prevention, detection, investigation, triage and response without any human intervention. You can easily automate the workflows with the help of bots and playbooks, and out-of-the box integrations of security and non-security devices in the network. These automations shorten mean time to detect and respond, improving the organization's IR capacity.

Incident Response

Security teams spend most of their days investigating incidents and responding to them. This does not allow for the standardization of the incident response processes or increase incident response quality. Logsign SOAR comes with full lifecycle incident response playbooks based on the SANS incident handling methodologies. Incident Response enables you to manage the lifecycle of your security incidents from analysis to containment, eradication, and recovery.

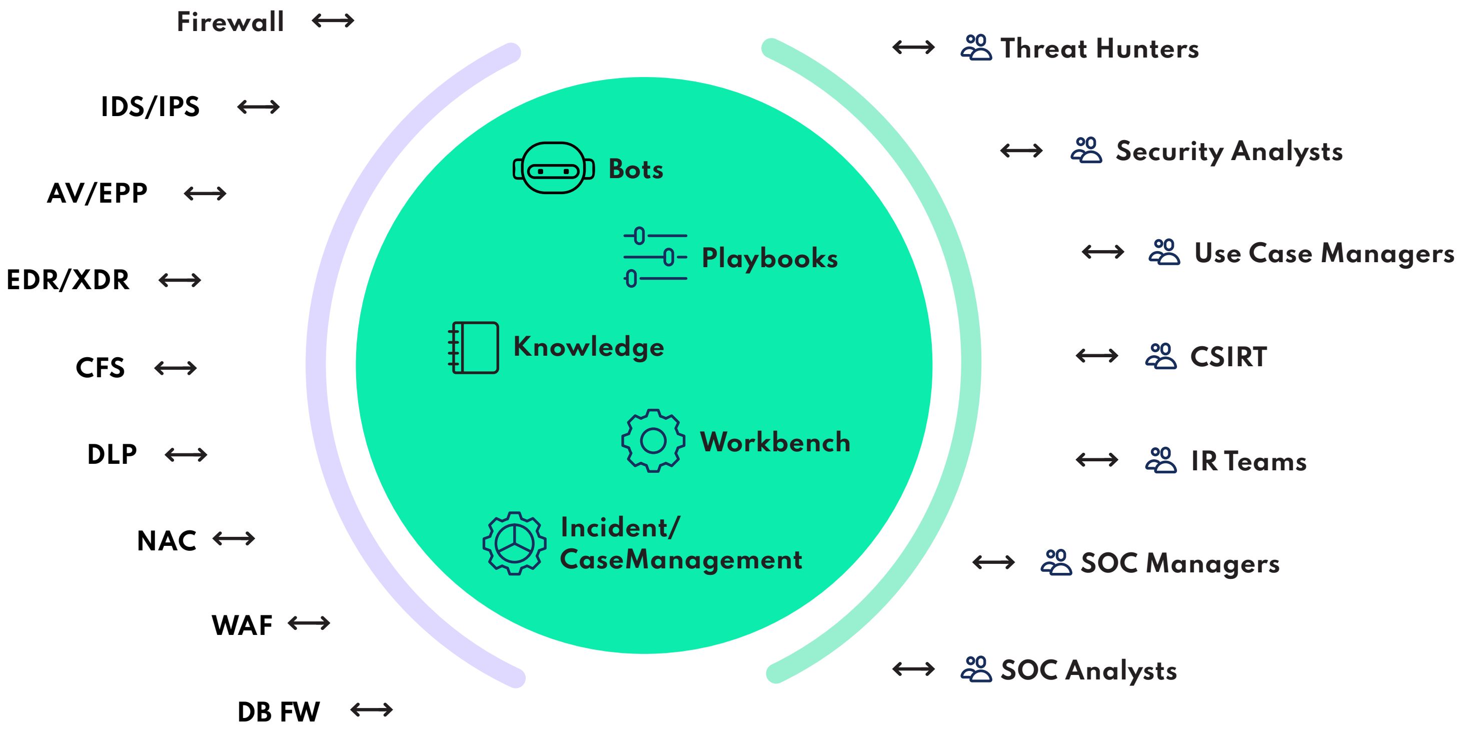
Orchestration

Security Orchestration is the method of connecting all tools, teams and processes, whether they are security-focused or not, for efficient and strong cyber security operations and faultless intervention in cyber incidents. Security orchestration is the harmonious work of people, process, and technology.



How It Works?

Logsign SOAR is 100% vendor free and seamlessly integrates all your security technologies and starts soaring. In addition to hundreds of built-in integrations, API-first approach enables Logsign SOAR to be deployed quickly without any vendor concern. With the execution of pre-defined bots and playbooks you can easily automate your workflows. SOAR automatically investigates, detects and triages the incidents, allowing security analysts to start working on assigned tasks, goals or contribute to any case which their knowhow is needed. Security Case management improves response processes, workbench focuses the analysts to the right task at the right time, and knowhow is documented and transferred to newcomers. As a result, the IR capacity of the organization is improved.



Why Logsign SOAR?

Case Management

Empowers Analyst Contribution & Collaboration

Every analyst can contribute to the case, and the owner and contributors communicate easily to resolve, respond or escalate to one another.

Bots & Playbooks

Force Multiplier Effect

We created Bots to enhance the power of analysts. Include the Logsign bots into your team. Let them work simultaneously with the analysts and run the playbooks.

Workbench

Designed For The Right GOAL

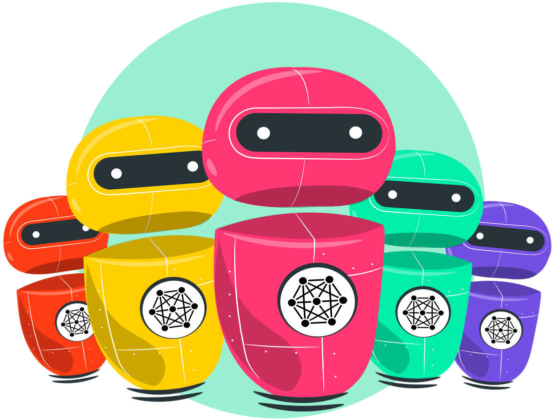
Logsign SOAR welcomes the analysts with a personal workbench screen to direct them to the right GOAL at the right time.

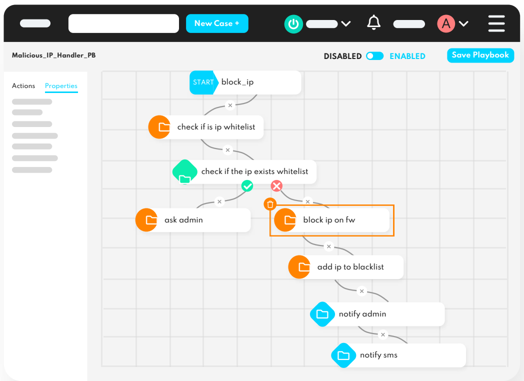
Highlighted Features

Humanoid Bots

Add Logsign humanoid bots to your team

Basic SOAR products are only playbook and workflow focused. They require playbook configurations each time when there is a change. This is extremely hard and complex to maintain the workflows and handle your organization's security strategy. Logsign Bots are designed to change and simplify this process in a modern way. Bots involve and run playbooks, dispatch the actions and changes so the playbook configurations are done simultaneously and workflows keep running. Their advanced capabilities strengthen security analysts' performance. There are many built-in bots and it is easy to create new ones for new actions or workflows. They interact with analysts, other bots or the playbooks inside them, and all automated actions keep working.





Visual Playbooks

Easily automate workflows

There are many built-in playbooks. In addition, Logsign enables users to create any **codeless** playbooks. The playbooks are simple to customize or to create new ones with drag-and-drop, the **visual playbook editor or DSL** support.

300+ Built-In Playbooks

Ready for automation, according to SANS PICERL incident response model.

Simulation Tool

Ensures you that the PBs are running and simulates if they are working.

Easy Configuration

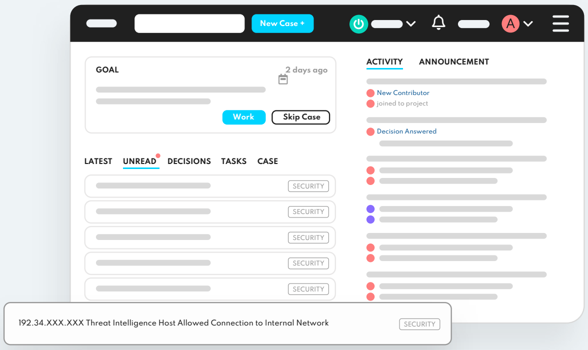
PBs are ready to be configured for any vendor or action change.

Personal Workbench

Designed for the right GOAL

Logsign workbench welcomes security analysts with goals and tasks they should focus on. It lists emergency cases, priority cases or tasks that need their contribution as well as requests and unread messages.

It's designed with a modern and high usability approach to maintain agility and collaboration and **increase analysts' efficiency.**



192.34.XXX.XXX Threat Intelligence Host Allowed Connection to Internal Network

Logsign

Incident & Case Management

Communication and collaboration always win

Logsign case management capabilities enable rapid collaboration and incident response to secure the environment by keeping security analysts together on the same page. Automated or manual investigation, detection and response on a single screen shortens your analysts' learning curve and response time.

Investigation & Prioritization

Either manual or automated investigation, and triage is available. Prioritized cases and tasks are shown to the analysts to focus them on highly critical ones first.

Case & Task Creation

Creates cases automatically or enables manual case and task creation.

Case Assignment

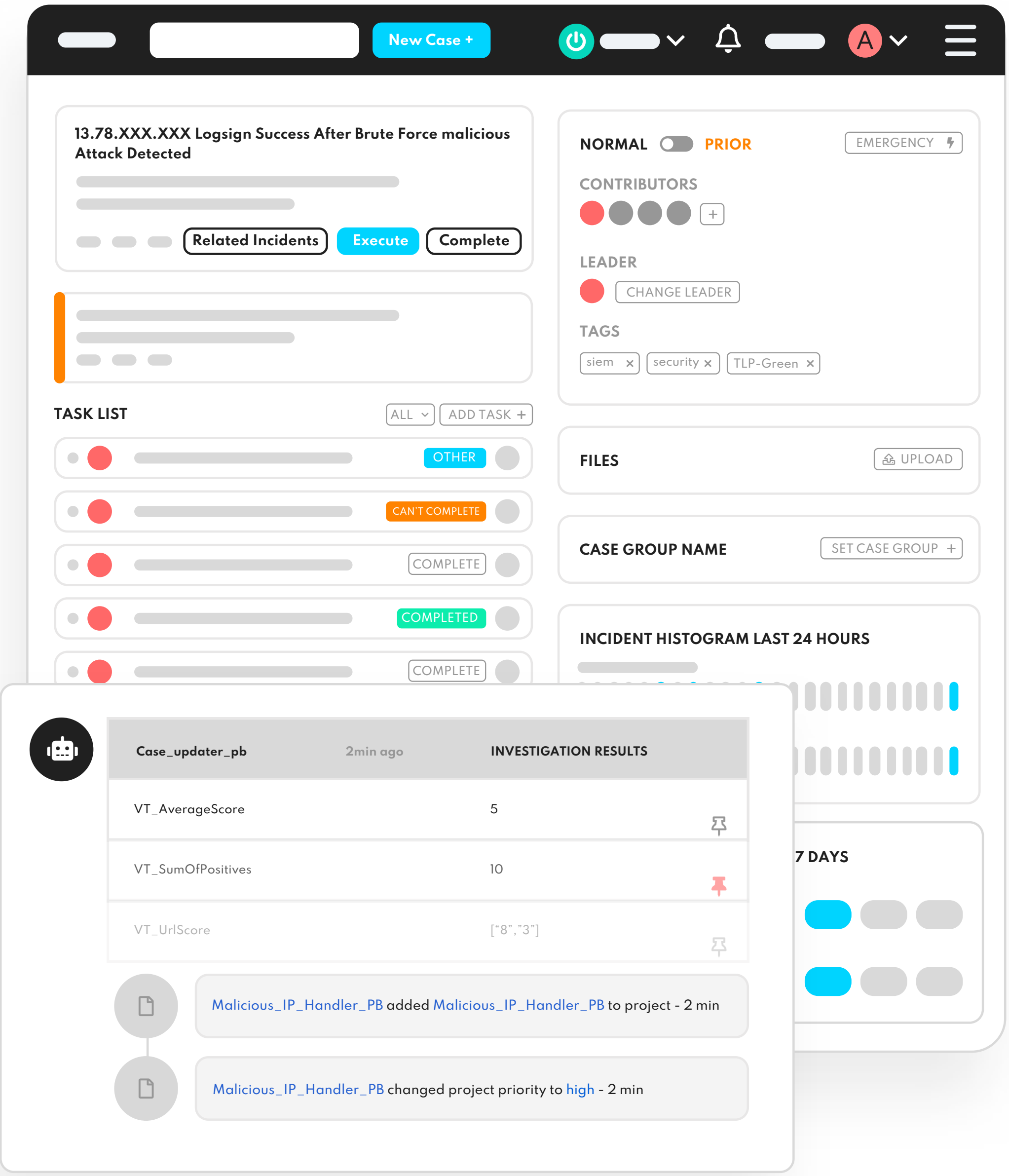
Manual or automated case and task creation is easy as assigning the right person. The owner can make the adjustments and create SLAs for the cases.

Case Grouping

Related alerts and cases can be grouped into one to respond faster.

Single Click Response

Enables analysts to respond manually on the case page.



13.78.XXX.XXX Logsign Success After Brute Force malicious Attack Detected

Case_updater_pb	2min ago	INVESTIGATION RESULTS
VT_AverageScore		5
VT_SumOfPositives		10
VT_UrlScore		["8","3"]

Malicious_IP_Handler_PB added Malicious_IP_Handler_PB to project - 2 min

Malicious_IP_Handler_PB changed project priority to high - 2 min

Contribution & Information Sharing

Logsign's case management approach facilitates communication among analysts to resolve cases and respond faster. It provides a fast learning curve for your team.

Hundreds of Integrations

Feel free to work with any vendor

Take advantage of hundreds of ready integrations, a free integration service, and a vendor-agnostic, broad-based SOAR. Logsign SOAR has an API-first approach to automate and orchestrate security and IT tools in a bidirectional way. It also integrates easily with the tools that they don't have an API.

Threat Intelligence

- ANOMALI
- ALIEN VAULT
- VIRUSTOTAL
- COFENSE
- CYMON.io
- DOMAINTOOLS
- FARSIGHT SECURITY
- OpenPhish
- Recorded Future
- paloalto NETWORKS

SIEM

- exabeam
- DEVO
- elastic
- LogRhythm
- MICRO FOCUS
- JASK
- Radar
- McAfee
- FORTINET
- sumo logic
- splunk>
- McAfee

Messaging

- Exchange
- PagerDuty
- slack
- twilio
- zoom

Network Security

- Check Point SOFTWARE TECHNOLOGIES LTD.
- paloalto NETWORKS
- f5
- PROTECTWISE
- Signal Sciences
- zscaler

Endpoint

- Carbon Black.
- CROWDSTRIKE
- CounterTack
- SentinelOne
- cybereason
- CYLANCE
- Symantec
- TANIUM
- CORTEX

Malware Analysis

- CISCO
- CUCKOO
- FIREEYE
- INTEZER
- JOESecurity
- paloalto NETWORKS
- lastline

Ticketing

- cherwell
- easyVISTA
- freshdesk
- Jira Software
- salesforce
- zendesk

Free Integration Service
Free integration for both security and non-security tools.

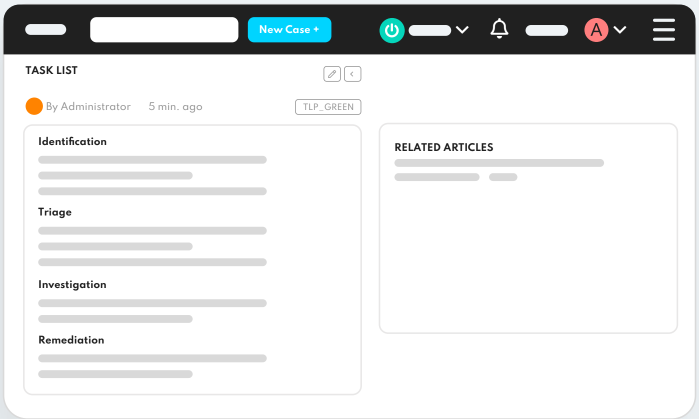
Wide Range of Integrations
Never-ending story. Number and variety of integrations are increasing every day.

Vendor-Agnostic
Vendor-free bidirectional integrations.

Knowledgebase

Knowledge is power

Knowledgebase is a kind of library. It is your organization's cyber knowhow documentation that allows security analysts to get the knowledge or share their information and experience easily. This knowledge base also empowers the orientation of the newcomers.



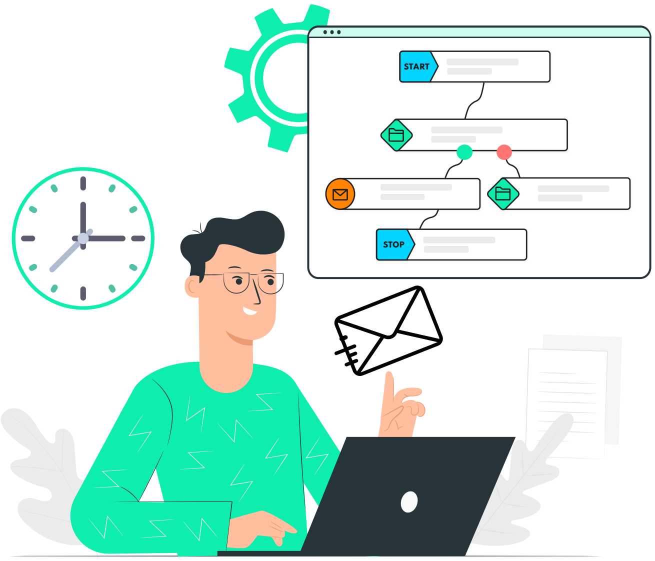
Solutions Areas

We equip enterprise security operations teams with smart SOAR and SIEM tools that improve workforce efficiency and provide better, accelerated investigations and responses. In addition to the latest technology products, we provide a number of services that help users' cyber security operations management and add value. Addressing problems during deployment and use; improving response capacity, investigation and analysis; incident triage; or creating new playbooks and bots are all necessary for you to use the platforms efficiently. Our competent and trained support team is available 24/7 to support you at any time.

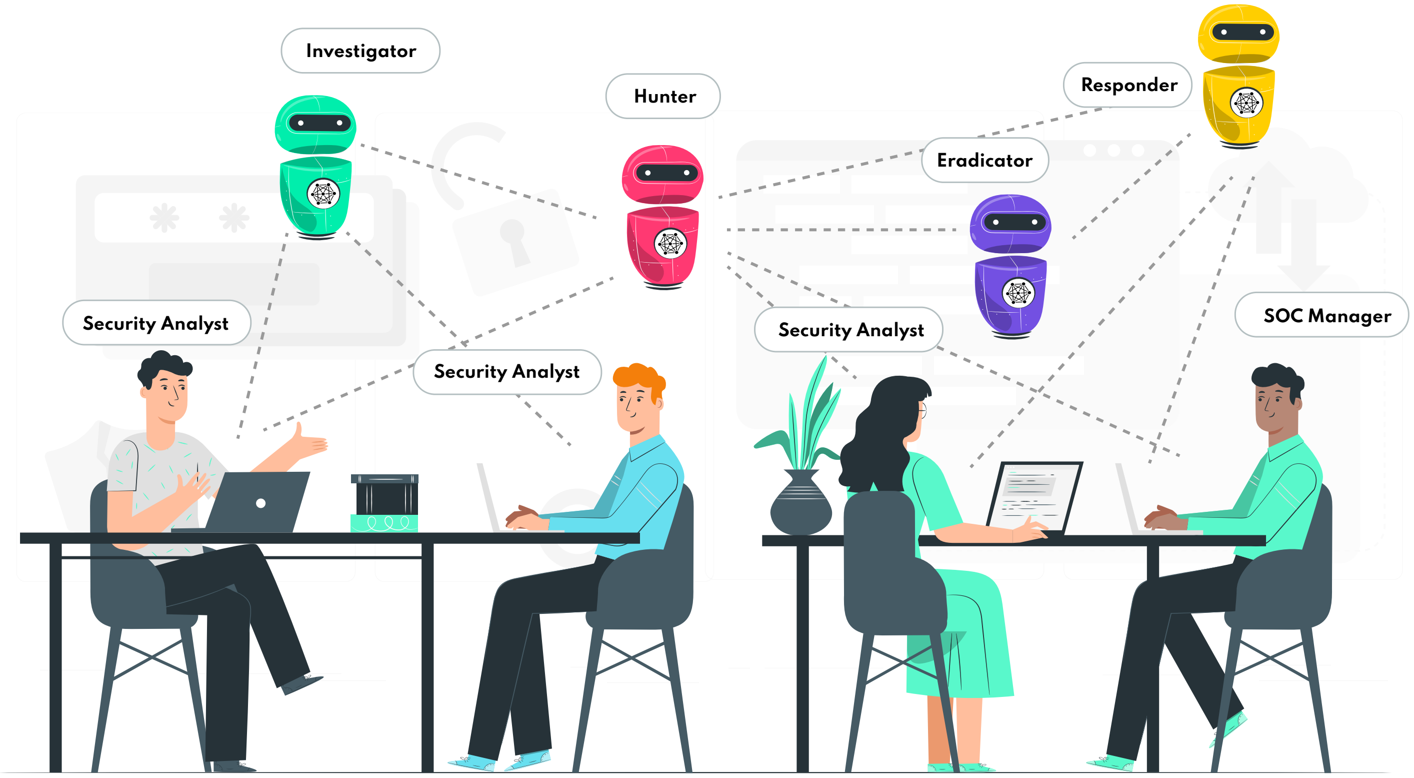
Streamlines Your Security Operations on a centralized, comprehensive platform.

Logsign SOAR streamlines your SecOps with its advanced capabilities. Automating not only repetitive tasks, but all the workflows that can be automated will decrease security analysts' workload. Investigations, threat hunting, alert triage or incident handling all can be automated with a well-designed SOAR. In addition to that, automation ensures there is no gap between the other tools.

Orchestration improves analyst contribution and collaboration so the response times are reduced and proactive precautions are taken. Comprehensive incident handling capability is achieved with Logsign SOAR, so the SecOps are streamlined. The organization strengthens its cyber security posture.



- Full & semi-automated workflows with bots & playbooks
- Improve analyst contribution & communication
- Comprehensive incident & case handling
- Task management automation
- Efficient workforce with personnel workbench



Logsign

Increases Maturity of IT Security Stack

Every tool or software added to the cyber security or IT stack can cause a huge vulnerability to the organization or misleading operations if they are not automated or integrated with other tools. Working with multi variety of vendors, maintaining the security of multi-located is hard to achieve without a centralized solution in the organization.

Attack patterns change, new technologies arrive, and the digitalization and modernization of organizations evolve every day. SOAR solves this struggle.

- Organizing and handling both the security and non-security tools
- Automate policy enforcement across disparate solutions
- Flexible and vendor-agnostic integration capability
- Improve security policies & protocols
- Multitenancy for multi-located or multi-organizational enterprises

Improves Team Efficiency & Solves Security HR Issues

In the cyber security industry, it's always hard to find, train or orient relevant personnel and newcomers to an organization. The solution is decreasing the workload and turnover rate of security analysts. Increasing analyst efficiency is achieved by stopping them from spending time on manual, simple or repetitive tasks and directing them to decision-critic cases. They feel much more professional without being overwhelmed and being able to focus on the right goals and tasks. SOAR increases team collaboration which enables analysts to respond to cases and reduce response times.

- Personal workbench improves analyst efficiency
- Bots strengthen analysts' hands to solve cases, work beside them
- Interactive communication improves
- Orientation is not a problem anymore with knowledgebase
- Less turnover, less HR problems and cost

Products

SIEM

SOAR

Threat Intelligence

Value-Added Services

SOC

Co-Managed SIEM

Support & Onboarding

Meet The Logsign SIEM!

Who We Are

We deliver automation-driven cyber security solutions and are committed to providing the smartest, easiest-to-use and most affordable cybersecurity detection and response solutions and value-added services.

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

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