KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert
June 01, 2021

Logsign SOAR

Security Orchestration, Automation, and Response (SOAR) platforms are becoming essential components of security architectures in many organizations around the world. SOAR platforms are designed to provide a centralized analyst and management interface for security teams. They consolidate security event information and allow for faster and more efficient investigations and responses. Logsign offers integrated but flexible Security Incident and Event Management (SIEM) and SOAR products that interoperate with a variety of security infrastructure tools.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

As the number and sophistication of cyberattacks have continued to increase over the years, some vendors realized that the traditional approaches and tools of cybersecurity likewise have failed to keep up. Many security-conscious organizations can find themselves administering over 50 different and disjointed security tools. Security Information and Event Management (SIEM) products were once hailed as the ultimate solution for managing security operations. In many organizations, they still form the foundation of modern Security Operations Centers (SOCs).

Parallel to SIEM solutions, a class of incident investigation and response platforms has emerged focusing on creating more streamlined and automated workflows for dealing with security incidents. SOAR products are the latest iteration of this evolution. Driven by the growing demand to implement centralized, automated control over incident analysis and response workflows across disparate security solutions, vendors are expanding their existing security intelligence, security orchestration, or incident response platforms to combine the key capabilities across all three of these market segments. Complementing or directly integrating with SIEMs, SOAR platforms aim to become the foundation of contemporary SOCs.

SOAR solutions can help organizations reduce the Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR) security incidents. Research from multiple sources indicates that MTTD can be in the neighborhood of six months or more, a fact borne out by the recent SolarWinds incident. Likewise, MTTR can take two months or more, depending on the severity of a given incident. Orchestration and automation of responses is key to reducing these KPIs and damage resulting from security incidents.

SOAR systems generally have OOTB connectors (software configurations and code in the form of packaged API calls) to facilitate data layer integration from SIEMs and other upstream sources. These connectors, sometimes called "integrations" by vendors, also allow SOAR console users to operate and/or administer the other security tools in the architecture, to the degree permitted by exposed APIs.

The orchestration aspect of SOAR involves not only the collection of telemetry from these different sources, but also initiating a workflow, opening cases and tickets where appropriate, and correlation and enrichment of event information. Enrichment of event data can be facilitated by SOAR systems by the automatic collection of additional forensic evidence on-site, such as outputs of EPP scans, obtaining non-standard log files, memory dumps, etc. Some vendor solutions can kick off automated threat hunts (looking for IOCs across multiple nodes in an environment) and add the results to a preliminary investigation. SOAR solutions should also be able to generate queries to Cyber Threat Intelligence (CTI) sources based on suspicious items and patterns observed from upstream telemetry. Some vendors have extensive threat intelligence capabilities that are utilized by their SOAR solutions. Examples of threat intelligence content include IOCs, compromised credential intelligence, device intelligence, and domain/file/IP/URL reputation information. Some SOARs incorporate Machine Learning (ML) detection models as a means to reduce false positives and provide more actionable intelligence to analysts and admins. Ideally, SOAR solutions will accomplish many of these listed actions automatically prior to or while alerting a human analyst.

When an analyst is alerted and assigned a case, all pertinent information related to the event should be constructed and presented by the SOAR platform to the analysts for their investigation. The SOAR platform should package information coherently, with descriptions and recommendations for actions.

Most SOAR vendors adhere to the paradigm of a playbook. Playbooks typically address common security scenarios and can be triggered either by manual analyst action or automatically if allowed by policy and supported by the vendor. Examples of security events that may trigger playbooks are phishing, malware, ransomware, failed login attempts, excessive or abnormal use of privileged credentials, prohibited communication attempts, attempts to access unauthorized resources, file copying or moving, attempts to transfer data using unauthorized webmail providers, attempts to transfer data to blocked IPs or URLs, unusual process launches, unusual application to network port activities, unusual network communication patterns, and so on. SOAR platforms often support dozens to hundreds of playbook scenarios and offer hundreds to thousands of possible incident investigation and response actions.

2 Product Description

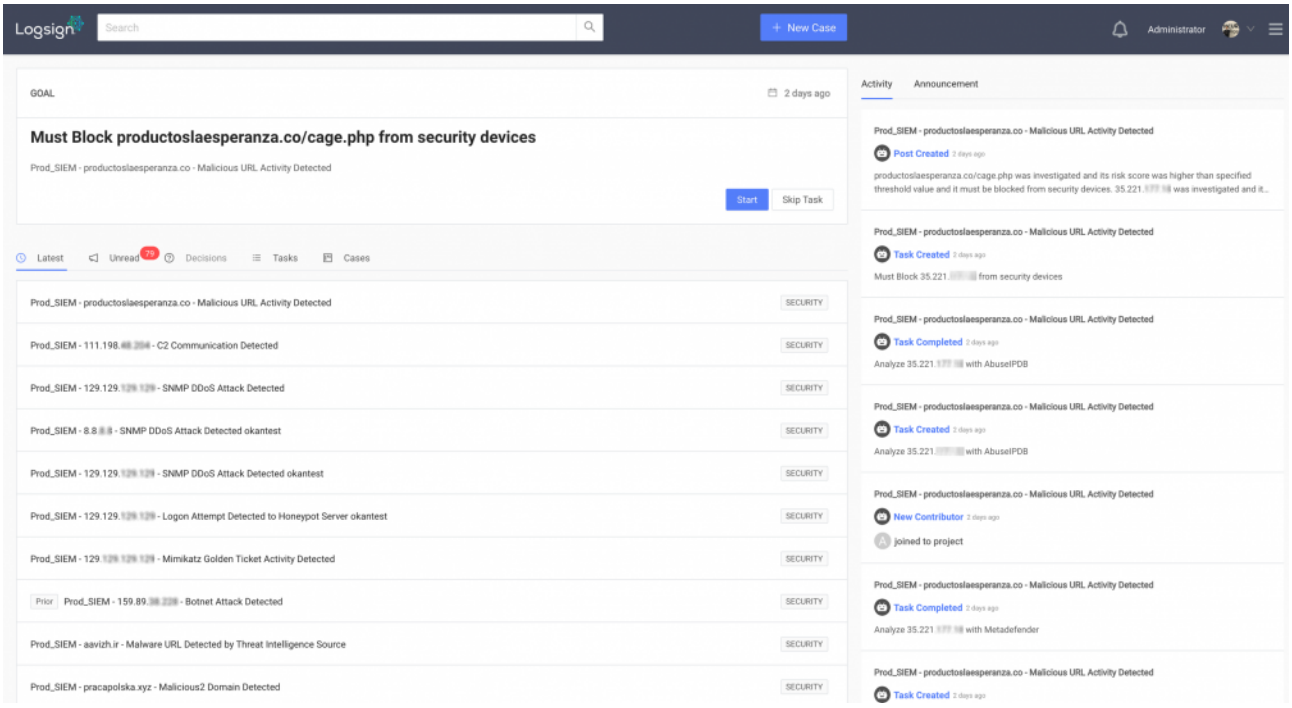
Logsign was founded in 2010. Logsign has offices in the Netherlands, Turkey, and US. Logsign specializes in security data collection, intelligence, and management. Logsign SOAR is primarily an on-premises product, running on Ubuntu Linux. Containerized, cloud-ready versions are in development for GCP. Later in 2021 the company plans to launch SOAR as SaaS and will run in GCP at launch.

Logsign's SIEM product was launched in 2015. Logsign SOAR debuted in 2021. The solution is licensed by the number of incidents tracked per day and the number of utilized integrations, combined into monthly or annual packages.

Integrations are the key to success with SOAR. Logsign has roughly 300 integrations for IT management and security products and services available, with more in work. Subsets of available integrations per functional area will be described below.

Security Incident and Event Management (SIEM) systems are security architectural components that need to be in place before SOAR. SIEMs are centralized repositories of enterprise-wide event and security logs. Logsign offers a SIEM solution which can work with their SOAR product. However, customers are not required to use the Logsign SIEM. Logsign has connectors for Elasticsearch SIEM, IBM QRadar, McAfee, Micro Focus ArcSight, Microsoft Azure Sentinel, Splunk, and SumoLogic.

Logsign considers their Personal Workbench analyst console to be their prime differentiator in the SOAR market. Whereas other SOAR products have main interfaces that are high level dashboards for SOC management, Personal Workbench is designed with typical security analyst and incident investigator workflows in mind. Personal Workbench opens with team goals and prioritized task lists for each analyst. Analysts can drill down from the task list into incident and event details. Logsign's case management facilitates collaboration and allows analysts to invite others to work on tickets together, or to hit the emergency button to get an entire team focused on a major incident. The lower section of Personal Workbench shows playbook actions available and execution status.



Must Block productoslaesperanza.co/cage.php from security devices

Prod_SIEM - productoslaesperanza.co - Malicious URL Activity Detected

Prod_SIEM - productoslaesperanza.co - Malicious URL Activity Detected	SECURITY
Prod_SIEM - 111.198.[redacted] - C2 Communication Detected	SECURITY
Prod_SIEM - 129.129.[redacted] - SNMP DDoS Attack Detected	SECURITY
Prod_SIEM - 8.8.[redacted] - SNMP DDoS Attack Detected okantest	SECURITY
Prod_SIEM - 129.129.[redacted] - SNMP DDoS Attack Detected okantest	SECURITY
Prod_SIEM - 129.129.[redacted] - Logon Attempt Detected to Honeypot Server okantest	SECURITY
Prod_SIEM - 129.[redacted] - Mimikatz Golden Ticket Activity Detected	SECURITY
Prior Prod_SIEM - 159.89.[redacted] - Botnet Attack Detected	SECURITY
Prod_SIEM - aavizh.ir - Malware URL Detected by Threat Intelligence Source	SECURITY
Prod_SIEM - pracapolska.xyz - Malicious2 Domain Detected	SECURITY

Prod_SIEM - productoslaesperanza.co - Malicious URL Activity Detected
Post Created 2 days ago
productoslaesperanza.co/cage.php was investigated and its risk score was higher than specified threshold value and it must be blocked from security devices. 35.221.[redacted] was investigated and it...

Prod_SIEM - productoslaesperanza.co - Malicious URL Activity Detected
Task Created 2 days ago
Must Block 35.221.[redacted] from security devices

Prod_SIEM - productoslaesperanza.co - Malicious URL Activity Detected
Task Completed 2 days ago
Analyze 35.221.[redacted] with AbuseIPDB

Prod_SIEM - productoslaesperanza.co - Malicious URL Activity Detected
Task Created 2 days ago
Analyze 35.221.[redacted] with AbuseIPDB

Prod_SIEM - productoslaesperanza.co - Malicious URL Activity Detected
New Contributor 2 days ago
A joined to project

Prod_SIEM - productoslaesperanza.co - Malicious URL Activity Detected
Task Completed 2 days ago
Analyze 35.221.[redacted] with Metadefender

Prod_SIEM - productoslaesperanza.co - Malicious URL Activity Detected
Task Created 2 days ago

Figure 1: Logsign SOAR Personal Workbench (used with permission)

For Logsign SOAR, playbooks are enacted by "bots", including separate bots for investigations, analysis tasks, response, and remediation actions. This allows Logsign playbooks to process multiple activity streams in parallel rather than only sequentially.

Security tickets can be managed completely within Logsign SOAR, from creation to disposition. It can interoperate with ITSM and ticketing systems, such as Atlassian Jira, ManageEngine Service Desk, ServiceNow, and ZenDesk. Integrations may allow Logsign to be authoritative over security events, or customers may choose to use an external ITSM as authoritative.

Logsign offers a curated CTI service separately. Logsign SOAR can also ingest feeds from Abuse IPDB, Alienware, Anomali, Cisco Talos, Domain Tools, IBM X-Force, MISP, Metadefender, Palo Alto AutoFocus, Shodan, and Virus Total. Suspicious code samples can be dispatched to malware analysis sandbox services such as Cisco AMP/ThreatGrid, Cuckoo, Hybrid Analysis, Intezer, Joe Sandbox, Lastline, and Palo Alto Wildfire.

Logsign SOAR comes with more than 300 playbook actions available. Many are designed to increase efficiency in the early phases of investigations: triage, collecting event information, executing queries and gathering fresh threat intelligence. Pertinent case information and relevant threat intelligence are delivered to analysts. Analysts can follow up with directed queries against other connected systems, most often SIEMs and security data repositories. Complex actions can be performed by Logsign bots and carried out in connected downstream systems such as EDR/NDR/XDR, firewalls, web/email gateways, IAM infrastructure, and VPNs. The exact capabilities that can be initiated by Logsign SOAR are determined by which integrations are available and what is exposed and permitted via the downstream products' APIs. Examples for each category are listed below.

Logsign features a visual playbook editor with an intuitive flow chart style format with some drag-and-drop components.

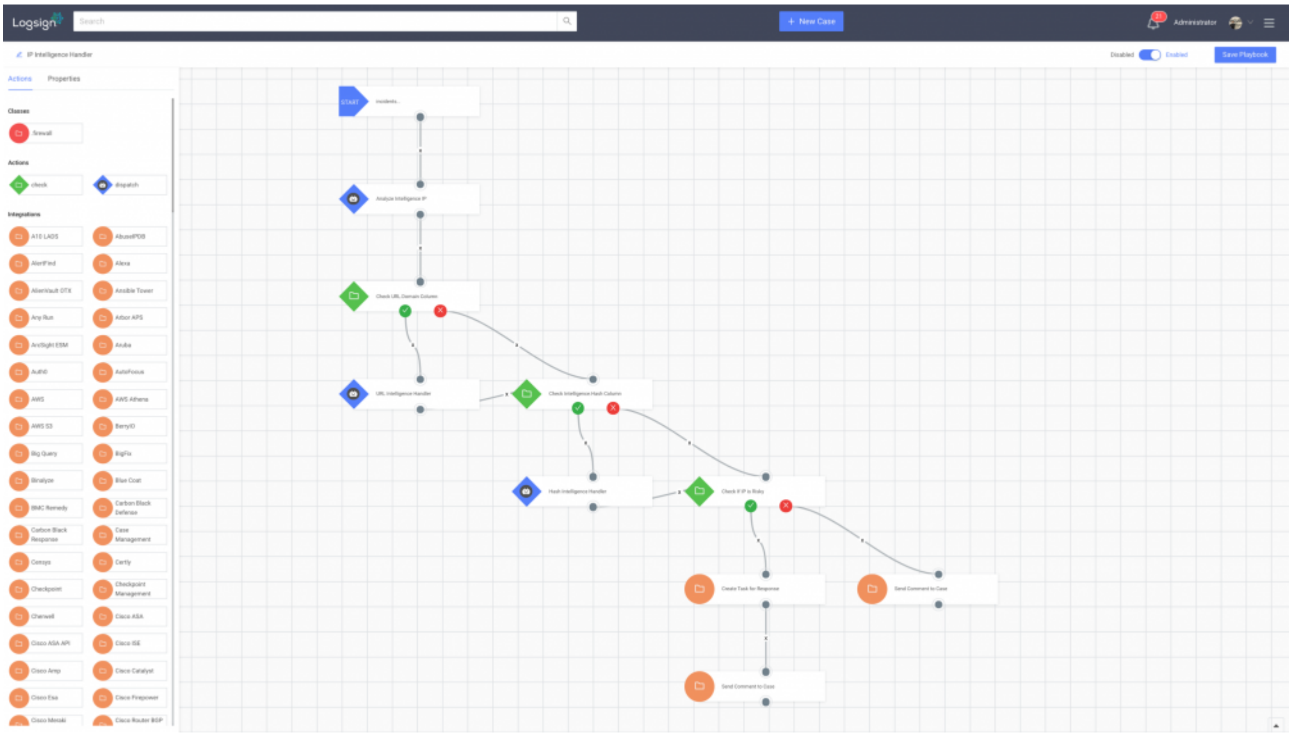


Figure 2: Logsign SOAR Visual Playbook Editor (used with permission)

For EPDR, Logsign has connectors for Blackberry Cylance, Cynet 360, FireEye, Kaspersky, Malwarebytes, McAfee, Palo Alto Traps, Sophos, Symantec, and TrendMicro. Logsign SOAR also integrates with DLP products by CA Technologies DataMinder, Code Green (Digital Guardian), Forcepoint, GTB Technologies, Ivanti, McAfee, Symantec, and TrendMicro. Response actions may include start scan, quarantine file, send file to sandbox, terminate process, and others, depending on what the individual integrations allow.

At the network layer, Logsign SOAR can work with Barracuda, Checkpoint, Cisco, Fortinet, Palo Alto, and WatchGuard firewalls; Cisco, Corero, and Extreme Networks IDS/IPS; Cisco, Extreme Networks, F5 BigIP, Fluke Networks, Gigamon, HP, and Juniper network traffic devices. Examples of actions include terminate network sessions and block IP addresses or ranges, depending on what each integration permits.

Logsign SOAR has integrations with web proxy and gateway systems, including Symantec (former Bluecoat), Cisco IronPort web security appliance, Citrix, EdgeWave, F5 BigIP, ForcePoint, McAfee, Sophos, Squid, and TrendMicro. Similar to network security products, example actions may include terminating web sessions and blocking IPs or URLs on the web proxy or gateway, depending on what is available in the downstream systems.

For vulnerability management, Logsign SOAR has connectors for Qualys, Rapid7, and Tenable. API integration enables regular information exchange and queries during investigations.

The final major category for integration is Identity and Access Management (IAM). Logsign offers some connectivity to Microsoft Azure AD, Cisco's Duo authentication platform, and Okta. For IAM to SOAR use cases, typical actions may include get user info, suspend potentially compromised user accounts, and force step-up authentication.

Two primary analyst duties are running investigations and threat hunts. Investigations can be aided by bots for parallel execution. Threat hunts can involve queries of attached SIEMs and other security tools. Both activities can begin within Logsign's Personal Workbench, which has starting points for incidents and case management. Logsign's case management capabilities encourage analysts to annotate tickets, collaborate more within their teams, and delegate tasks when necessary. The Logsign SOAR console features standard incident tracking dashboards and reports detailing MTTD and MTTR, as well as other metrics. Logsign also presents analysts with a built-in knowledge base that can be updated and extended by customers as needed. The Knowledge Base can help new team members ramp up and become more effective quickly.

3 Strengths and Challenges

SOAR solutions are growing in popularity among not only large enterprises but also at the upper end of the SMB market. Moreover, Managed Security Service Providers and SOC-as-a-Service providers are realizing the value that SOAR solutions have for handling security operations on behalf of many customers. The single console for incident management and analyst investigations is the way forward in the modern SOC, whether managed in-house or by service providers. Given that attackers are orchestrating and automating their malicious activities, the only way for businesses, non-profits, and government agencies to have success in security is by using automation as well.

Logsign is a new product in the SOAR space, built with the influence of Logsign's SIEM customers to handle the orchestration and automation needs in their SOCs. Logsign's Personal Workbench focuses on improving efficiency of security analysts by presenting the most important items for their daily consideration in priority order. Multiple workflows can be initiated directly from the well-designed interface.

Logsign SOAR does not require and is not limited to working with their own SIEM, a number of SIEM connectors for 3rd-party products are available as well.

Integrations are the foundation for SOAR platforms. In order to be effective in a given environment, SOAR tools must integrate at the API level with SIEMs, EPDR, NDR, XDR, web and email gateways, vulnerability management, and other security systems. More support for IaaS, PaaS, and SaaS is needed. Logsign has a good mix of common security integrations available at launch and will be adding more to their marketplace. The more integrations with other security tools that are possible, the more likely it is that a vendor will grow.

Security professionals prefer orchestration, automation, and policy creation tools that have flow chart style interfaces over other methods. Flow charts are generally intuitive to follow and modify, resulting in fewer errors and better coverage in the case of SOAR. Logsign's visual playbook editor is easy to follow and tweak as needed.

Logsign SOAR is a new entrant in the market by a smaller company, but they are planning for expansion, especially in the EMEA region. Strong authentication and/or multi-factor authentication to the console by admins and analysts is not yet available but is on the roadmap.

Strengths

- Personal workbench approach focuses on facilitating analyst productivity
- Logsign platform promotes collaboration among analysts across shifts and SOCs
- Visual playbook editor in flow chart style
- Automation achieved via bot paradigm to enable investigation and response actions in parallel
- Can work in conjunction with Logsign SIEM as well as other SIEM solutions
- Logsign dashboard shows MTTD and MTTR metrics for business value
- Logsign offers CTI service and can pull in other sources at customer request

Challenges

- Needs additional integrations for other security and IAM systems
- Needs integrations for IaaS and PaaS instances
- Smaller vendor with relatively new product in the field
- Security certifications will be beneficial when SaaS is launched
- Strong authentication and federation not present but planned

4 Related Research

SOAR Buyer's Compass
Leadership Compass on Security Orchestration Automation and Response

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.