LOGPOINT

LOGPOINT'S CONVERGED SIEM – AN ALL-IN-ONE SIEM+SOAR & UEBA SOLUTION WITH EDR CAPABILITIES

Logpoint gives analysts an out-of-the-box tool for the entire detection, investigation, and response process. With no integration or maintenance required, Logpoint offers a scalable solution that consolidates SIEM, SOAR, UEBA and EDR capabilities in just one platform to automate and help prioritize your analysts' work while ensuring higher security across your organization.

AUTOMATED THREAT DETECTION, INVESTIGATION AND RESPONSE

Key Benefits

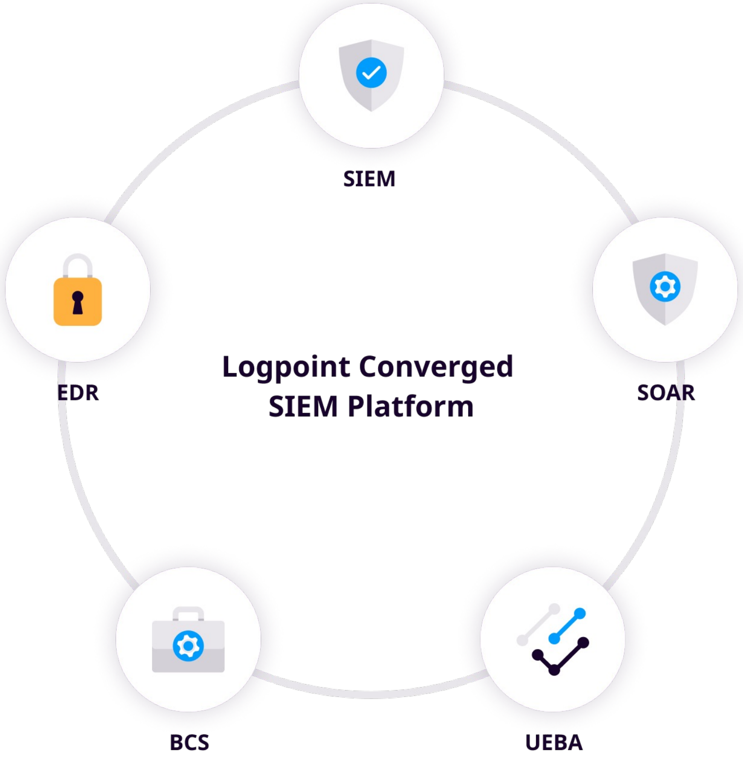
- Work faster and speed up the investigation process by connecting disparate technologies and threat intelligence in one central platform
- Total isolation and protection of the organization’s data to ensure compliance with data privacy regulations
- Prioritize and orchestrate across the entire infrastructure with automated alert triage and incident response
- Stay on top of the latest threats thanks to ready-to-use security content and automatically updated playbooks.
- Detect and remediate incidents in endpoints combining AgentX, our native endpoint agent, with SIEM, SOAR and UEBA.

Accelerate threat detection, investigation, and response with Logpoint, no matter your organization’s size or industry. Our product offering covers SIEM, SOAR, UEBA, EDR capabilities, and security for business-critical systems, such as SAP.

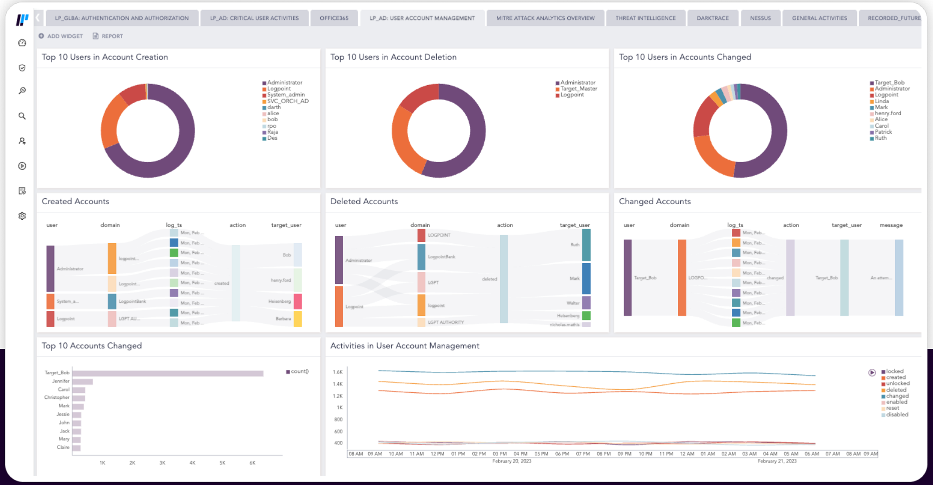
By combining multiple tools into just one platform, you will not only consolidate your tech stack but also eliminate the complexity and maintenance your security teams deal with. With no more siloed products, you can turn data sets into meaningful alerts and action plans..

At the same time, a converged security operations platform guarantees that data from different endpoints is fully integrated. This adds an extra layer of protection to the entire infrastructure against threats, whether they are internal or external.

Logpoint products make sure your organization stays compliant and your data secured. Whether or not you use SAP applications, our converged solution helps you prevent costly downtime and uncover compliance issues.



SIEM FOR EFFECTIVE THREAT DETECTION AND INVESTIGATION



Centralize data monitoring

Logpoint’s SIEM collects event data within your organization, visualizes it with easy-to-use dashboards, and puts it into context for better and quicker decision making. This way, security analysts gain full visibility of the network and IT infrastructure.

Our SIEM solution is all about enriching data to reduce cyber risk. By normalizing log files into a single language and mapping alerts to the MITRE ATT&CK framework, analysts can easily make sense of the threats and prioritize them based on their severity.

With out-of-the-box compliance support, you can rest assured that your organization follows all major regulations, such as GDPR, Schrems II and HIPAA. Logpoint also saves you time by automating compliance reporting.

Key Features

- Central collection and analysis of all security data
- Early detection of cyber breaches
- Central storage of current and historical data
- End-to-end event reporting
- EDR capabilities
- Available on SaaS, cloud and on-prem

AUTOMATIC INCIDENT DETECTION AND RESPONSE WITH SOAR

Security Operations Centers experience increased staff shortages, hindering the threat investigation and response. Logpoint's SOAR automates those critical actions that are time-consuming and repetitive, so your analysts can collaborate and manage incidents more effectively. The alerts raised by SIEM empower SOAR to act independently using playbooks that help investigate, contain and remove threats. These out-of-the-box playbooks remove the manual work and accelerate the incident remediation from hours to minutes.

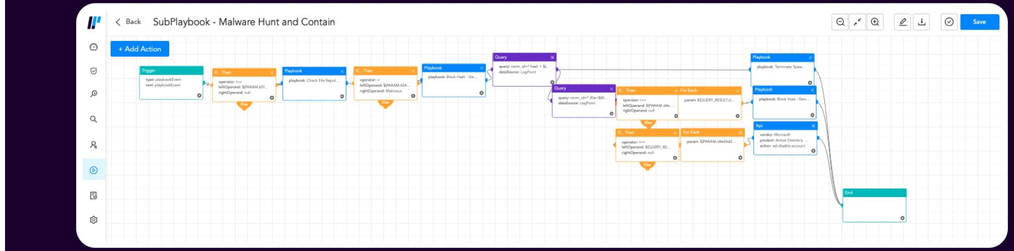
Amplify your team with automation

SOAR comes with 75+ ready-to-use playbooks targeting the most common security scenarios without limitations. Collect and centralize Threat Intelligence data to understand how various alerts from different systems are connected. Tailor playbooks to your needs in no time and without effort with a drag-and-drop interface. Bring contextual information to your investigation with incident grouping in case management.

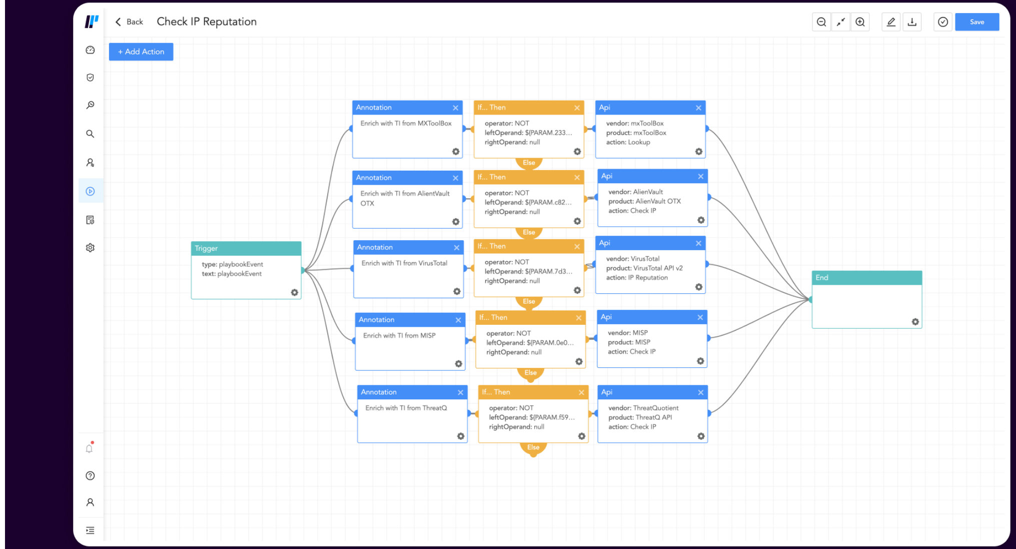
Use case of endpoint malware mitigation

Reducing alert overload and increasing SOC productivity is critical, especially for organizations, which typically have hundreds or thousands of endpoints as the main targets of attacks. And consequently, these endpoints generate tons of malware alerts every day – many of them are either low severity or false positives. Their manual investigation and response become time-consuming and result in greater risk.

Logpoint orchestrates and automates actions to easily investigate and respond to malware alerts, enabling the security team to prioritize the most critical attacks and drastically minimize risk.



Malware hunt and contain playbook



Trigger
type: playbookEvent
text: playbookEvent

Annotation: Enrich with TI from MXToolBox
If... Then: operator: NOT, leftOperand: $(PARAM.233…, rightOperand: null
Api: vendor: mxToolBox, product: mxToolBox, action: Lookup

Annotation: Enrich with TI from AlientVault OTX
If... Then: operator: NOT, leftOperand: $(PARAM.c82…, rightOperand: null
Api: vendor: AlienVault, product: AlienVault OTX, action: Check IP

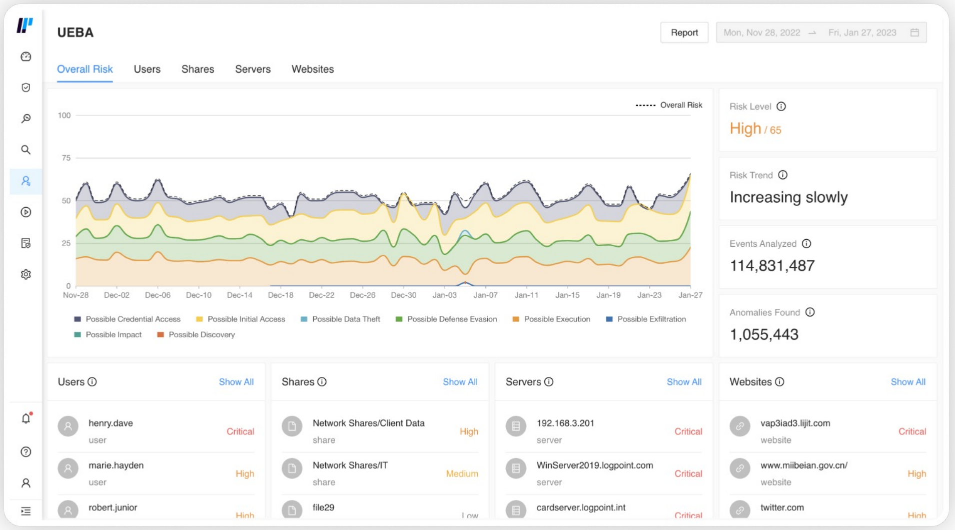
Annotation: Enrich with TI from VirusTotal
If... Then: operator: NOT, leftOperand: $(PARAM.7d3…, rightOperand: null
Api: vendor: VirusTotal, product: VirusTotal API v2, action: IP Reputation

Annotation: Enrich with TI from MISP
If... Then: operator: NOT, leftOperand: $(PARAM.0e0…, rightOperand: null
Api: vendor: MISP, product: MISP, action: Check IP

Annotation: Enrich with TI from ThreatQ
If... Then: operator: NOT, leftOperand: $(PARAM.f59…, rightOperand: null
Api: vendor: ThreatQuotient, product: ThreatQ API, action: Check IP

Phishing investigation and response playbook

UEBA HELPS YOU DETECT UNKNOWN THREATS



Risk Level: High / 65

Risk Trend: Increasing slowly

Events Analyzed: 114,831,487

Anomalies Found: 1,055,443

Users
- henry.dave (user) – Critical
- marie.hayden (user) – High
- robert.junior – High

Shares
- Network Shares/Client Data (share) – High
- Network Shares/IT (share) – Medium
- file29 – Low

Servers
- 192.168.3.201 (server) – Critical
- WinServer2019.logpoint.com (server) – Critical
- cardserver.logpoint.int – Critical

Websites
- vap3iad3.lijit.com (website) – Critical
- www.miibeian.gov.cn/ (website) – High
- twitter.com – High

Imagine you could make your SIEM and SOAR smarter. That is exactly what you get with Logpoint UEBA (User Entity Behavior Analytics), our solution to immediately spot threats coming from inside or outside of your organization.

By applying machine learning to its algorithm, it analyzes all activities across the organization to create a pattern of normal user and entity behavior. This way, Logpoint will automatically send you an alert as soon as it detects anything out of the ordinary.

Logpoint UEBA detects abnormal behaviors and creates risk scores, reducing false positives and making it easier for analysts to prioritize alerts. These risk scores facilitate threat detection and decrease the time in incident response.

When you combine UEBA with SIEM events, these will get more insightful. And in combination with SOAR, you can fully automate response processes. Here are three examples of what UEBA can help you detect:

Authentication abnormalities

If an account is compromised, UEBA can detect many login attempts, failed or successful. Your analyst can use this as a trigger to run SOAR playbooks that check this account.

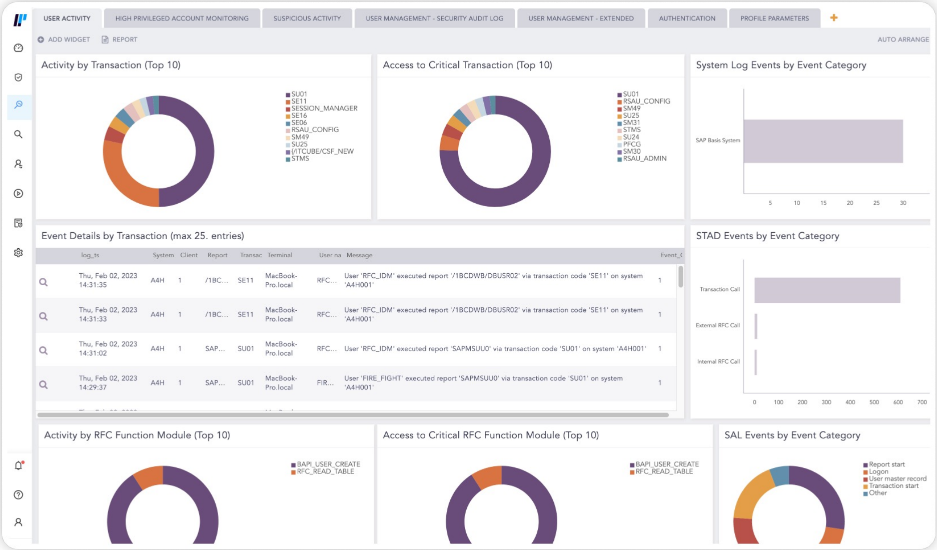
Suspicious data transfer activities

Using machine learning to create a baseline on the amount of data sent over the network, UEBA will detect the possibility of data theft. But rather than looking into it in contrast with the overall organization, there is the option of comparing the use with their peers to get a more precise picture.

Activity-based inconsistencies

Grouping users by peers allows UEBA to focus on patterns instead of pre-set limits to detect e.g., unusual working hours. It will compare behavioral patterns with the ones from the user’s peers instead of with the whole organization.

GET FULL ERP VISIBILITY WITH BCS FOR SAP



Event Details by Transaction (max 25. entries)

log_ts	System	Client	Report	Transac	Terminal	User na	Message	Event_(
Thu, Feb 02, 2023 14:31:35	A4H	1	/1BC...	SE11	MacBook-Pro.local	RFC...	User 'RFC_IDM' executed report '/1BCDWB/DBUSR02' via transaction code 'SE11' on system 'A4H001'	1
Thu, Feb 02, 2023 14:31:33	A4H	1	/1BC...	SE11	MacBook-Pro.local	RFC...	User 'RFC_IDM' executed report '/1BCDWB/DBUSR02' via transaction code 'SE11' on system 'A4H001'	1
Thu, Feb 02, 2023 14:31:02	A4H	1	SAP...	SU01	MacBook-Pro.local	RFC...	User 'RFC_IDM' executed report 'SAPMSUU0' via transaction code 'SU01' on system 'A4H001'	1
Thu, Feb 02, 2023 14:29:37	A4H	1	SAP...	SU01	MacBook-Pro.local	FIR...	User 'FIRE_FIGHT' executed report 'SAPMSUU0' via transaction code 'SU01' on system 'A4H001'	1

Search Template for User Activity in BCS for SAP

According to Bloomberg, 64% of all ERP systems have been breached in the last two years. As SAP systems are interconnected, their vulnerability becomes a target for cyber-attacks and a priority for you. We got you covered with Logpoint's BCS for SAP.

By onboarding your SAP data into a SIEM solution, you can secure your business-critical systems against threats coming from both inside and outside of your organization.

Need more reassurance? You can always combine it with UEBA to strengthen the investigation of user behavior in events occurring within SAP systems. You will discover and respond to threats in no time.

BCS for SAP adapts to your organizational needs

Security and audit compliance monitoring: Extract logs and data from SAP into the SIEM to automate the threat detection, investigation, and response process.

Business integrity monitoring: Detect flaws and deviations in the business process standards to prevent fraud, financial, and reputational losses.

PII (Personal Identifiable Information) access monitoring: Control who has access to several types of personal information to prevent compliance failure.

IT service intelligence: Identify operations problems in the SAP landscape, as well as detect issues and respond to threats that can jeopardize it.

ABOUT LOGPOINT

Trusted by more than 1,000 enterprises

KONICA MINOLTA
CAPTIVATE
BOEING
GoSecure
RÉMY COINTREAU

Awards and honors

Gartner Peer Insights. Customer First
Gartner
Gartner Magic Quadrant
Leader SPRING 2023
Software Reviews GOLD MEDAL 2022

For more information, visit www.logpoint.com

Logpoint is backed by a market-leading support organization available 24×7 to assist our customers and partners around the world.

In offices throughout Europe, North America and Asia, more than 300 passionate Logpoint employees work in concert with 60+ certified partners to create business value for our customers.

Don’t just take our word for it. 1.000+ customers agree. Logpoint service consistently receives a 98% customer satisfaction rating, and we are recognized by leading independent industry analysts.