LOGPOINT


Logpoint releases comprehensive new capabilities to its converged cybersecurity operations platform, helping security analysts to work more efficiently and decrease the time to respond to threat

Mar 30, 2023 11:11 CEST

# Logpoint launches enhanced observability capabilities to speed up response

- **Logpoint releases comprehensive new capabilities to its converged cybersecurity operations platform, helping security analysts to work more efficiently and decrease the time to respond to threats.**
- **A new case management interface provides a quick overview for security analysts to make managing cases and resolving incidents easier.**

**COPENHAGEN, Denmark, March 30, 2023 –** Logpoint today announced the

new release of capabilities to its cybersecurity operations platform, converging SIEM, SOAR, UEBA, endpoint security, and Business-Critical Security (BCS) technologies. The new capabilities enable security analysts to protect the organization against threats by increasing observability and decreasing the time to respond to threats.

According to a Forrester Study, SOC teams receive over 11,000 security alerts daily and struggle to get an overview of the alerts and then address them. The release comes with a new overview of incidents, cases, and system resources, which provides security analysts with easy access to the most relevant information. In addition, the new case management interface provides a quick outline and groups related incidents into the same case allowing analysts to run playbooks within a case to solve incidents faster.

“Gaining situational awareness is key for security teams. In the new case management system, our technology collates incidents that relate to specific attacks and provides a capability for the analyst to run suggested playbooks that fit the data, the TTP and the adversary at hand. Not only does the system greatly accelerate the detection, triage and response, but it increases the precision and efficacy as well,” says Christian Have, Logpoint CTO. “We always strive to speed up threat detection, investigation, and response for our customers. Our platform’s new capabilities improve observability and make it easier for our customers to take action on incidents threatening the organization and its digital assets.”

The release includes updates to the core SIEM, SOAR, UEBA, and Director technologies, offering better overview, new security content and improved playbooks, more precise detection of anomalies, better observability across tenants from a central location for MSSPs, and much more.

“With the new release, we’re taking further steps to simplify and improve security operations,” says Christian Have. “Our source management capabilities now support dynamic workloads such as cloud containers, remote workers and ephemeral systems. With this enhancement, our new endpoint agent has greater reach, more capabilities and ultimately provides a larger suite of tools to the fingertips of the analyst. ”

The release is the first since Logpoint launched its endpoint solution AgentX. It gives security analysts more precise detection of malicious malware and the ability to respond to endpoint threats. Logpoint’s security operations

platform protects the entire business by providing comprehensive threat detection, investigation, and response across clients, servers, network systems, cloud workloads, endpoints, and business-critical applications. The platform is available on-prem, in private cloud, and as SaaS.

To learn more about all the upgrades and improvements in Logpoint's cybersecurity operations platform, visit Logpoint's blog post here.

---

**About LogPoint**
Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, LogPoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, SOAR and SAP security technologies converged into a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit http://www.logpoint.com

## Contacts

**Maimouna Corr Fonsbøl**
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98