

# Logpoint releases enhanced automation, investigation, and incident response capabilities

Sep 12, 2023 09:00 CEST

## Logpoint releases enhanced automation, investigation, and incident response capabilities

Logpoint releases various updates to its Converged SIEM platform to help SOC teams operate with practical SOC-centered functions and improved end-to-end functionality. The new release enables organizations to increase automation, investigation, and the ability to react to security events.

**COPENHAGEN & LONDON, September 12, 2023** – [Logpoint](#) is announcing the release of new capabilities to its Converged SIEM platform, built on SIEM, SOAR, UEBA, and Business-Critical Security (BCS) technologies. The new practical SOC-centered functions connect detection with investigation, automation, response, and orchestration to provide enhanced visibility,

automation, and response and improve the end-to-end functionality for end customers and MSSP partners.

“Cyberattacks have become a daily nuisance for organizations today, and improving the security posture is a top priority,” says Edy Almer, Logpoint Director of Product. “We’re now enhancing endpoint capabilities and strengthening our case management tool to help analysts better understand what’s happening. Gaining that complete insight makes it easier to identify security breaches, simplifies investigation, and accelerates response, allowing small organizations to handle attacks and leverage MSSP capabilities to save time and resources. The SOC team can also share information more easily with the rest of the organization, helping CISOs justify their cybersecurity approach or build a case to modify it.”

The new release improves investigation, the cornerstone of the incident response process, by introducing more contextual information in Logpoint SOAR. Security analysts will have all the information they need in the case management tool, with incidents mapped to the MITRE ATT&CK framework and a new graphical overview of connections between artifacts.

Logpoint also introduces case summaries, providing analysts with a comprehensive PDF report on ongoing and finalized cases to easily share with stakeholders, and the playbooks are enhanced with improved documentation and increased flexibility to create more precise and less time-consuming workflows.

The capabilities in AgentX, Logpoint’s native endpoint agent, have also been expanded, with the opportunity to select installation directory and manage the TLS authentication directly from the user interface. In addition, SOAR now automatically authenticates AgentX, saving time and preventing mistakes happening from manual authentications.

“While cyberattacks do pose a problem and concern CISOs worldwide, we aim to provide the necessary tools and information to let them rest assured that they get the information they need about activities in the IT infrastructure,” says Edy Almer. “We strive to provide value beyond the security function, and with the new release, we close the loop between the alerts, investigation, and response, enabling our customers to increase operational speed, optimize business processes, and expose weaknesses faster.”

Logpoint Converged SIEM is an end-to-end cybersecurity platform that covers the entire threat detection and incident response (TDIR) process. The platform automatically adds threat intelligence, business context, and entity risk to observations to transform weak signals into meaningful investigations and enables analysts to respond faster with automation and orchestration.

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

---

## About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's [SIEM](#) and [NDR](#) technologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit <http://logpoint.com>.

## Contacts



### **Maimouna Corr Fonsbøl**

Press Contact

Head of PR

PR & Communications

[mcf@logpoint.com](mailto:mcf@logpoint.com)

+45 25 66 82 98