LOGPOINT

Jan 30, 2024 10:00 CET

Logpoint releases new capabilities to optimize cybersecurity performance

- **Logpoint enhances its Converged SIEM platform to help organizations and MSSPs improve cybersecurity performance and free up time and resources in security operations.**
- **The new release reduces the workload on operational tasks, empowering SOC teams to gain efficiency in threat detection, investigation, and response.**

COPENHAGEN & LONDON, January 30, 2023 – Logpoint is announcing the release of new capabilities to its Converged SIEM platform, enhancing threat detection and security operations and streamlining case management. Organizations can focus on essential security matters with the new

capabilities by reducing workload, simplifying automation, and freeing up resources.

The new release delivers increased system stability and reliability and more efficient use of resources by introducing adaptive memory management, which optimizes memory usage automatically. This allows users to prevent service disruptions and eliminate time spent on manual memory tuning. They can also add more nodes and increase visibility due to the release of extra memory.

Logpoint enhances the experience of configuring alerts with one single window and fewer clicks. Additionally, the way users populate and update lists has been simplified. Now, they can upload a list of, e.g., IoCs, malicious domains, IPs, etc., in a .CSV or .TXT file. This provides users with a flexible way to add lists from different sources, facilitates their jobs, and helps keep threat detection up to date.

Logpoint now allows complete collection chain configuration with a single click from LogSource Templates and enables distribution at scale for MSSPs from Logpoint Director, a platform to manage large deployments. This enhancement makes the initial configuration of Logpoint a breeze with pre-configured templates for all major Log Sources.

“Visibility, time to respond, and confidence in the investigation are important factors in fending off cyberattacks successfully, and we’re excited to help organizations improve on that with the new Logpoint release,” says Edy Almer, Director of Products at Logpoint. “We’re essentially helping organizations get more resources for focusing on what matters for their security, which is essential as the pressure on cybersecurity professionals increases from expanding data and cybersecurity regulations and the threat actors’ ever-changing and innovative methods.”

With the new update, Logpoint is streamlining security orchestration, automation and response (SOAR), and case management. For example, incident artifacts are automatically extracted into cases, adding context, reducing analyst workload, and improving detection and response. Playbooks can automatically read incidents and add all extractable data as artifacts to the case. Additionally, security teams can search logs directly from the case management tool with a single click and feed the result back into the case, simplifying investigations.

The new update allows MSSPs and those working with different tenants to save time and reduce errors when distributing playbooks to customers. Logpoint is releasing generic playbooks related to typical security use cases that can be updated once and distributed to the tenants. These playbooks are integration-agnostic, so tenants with different integrations can benefit from them. Additionally, MSSPs will save crucial time in the process of distributing them.

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 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