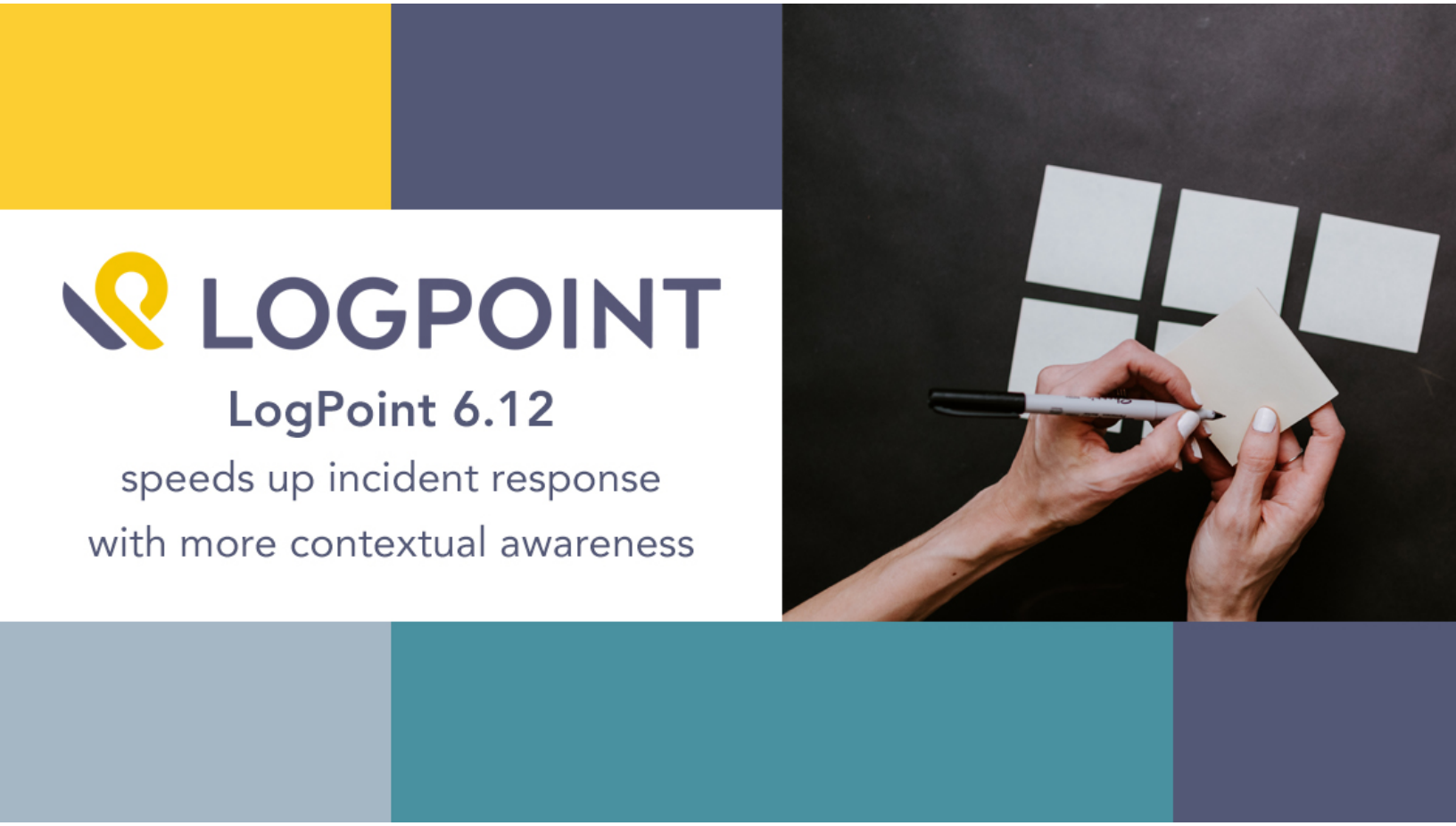
LOGPOINT



Oct 05, 2021 10:11 CEST

Launching LogPoint 6.12: Speeding up incident response with more contextual awareness

With LogPoint 6.12, it is now possible to categorize alerts and incidents to a single common taxonomy like the MITRE ATT&CK framework

COPENHAGEN – October 5, 2021 – LogPoint, the global cybersecurity innovator, has launched version 6.12 of its SIEM solution. In the new release, security analysts can categorize alerts and incidents to a single taxonomy like the Mitre ATT&CK framework. LogPoint 6.12 also enables role-based access to specific search and report templates.

Security analysts often face an overwhelming number of incidents, making it difficult to know what to prioritize for investigation. Introducing the MITRE ATT&CK framework in LogPoint 6.12 allows security analysts to react to and resolve threats quickly by knowing instantly which type of threat it is. To give the best possible overview for security analysts, classifying alert rules allows filtering all alert rules based on either log sources, attack category, or attack tag.

Collaborating and sharing knowledge across functions is crucial in security operations. In LogPoint 6.12, security analysts can share search and report templates as references to the same item to ensure that updates are applied to all users using the template. Role-based access to templates increases efficiency because it eliminates the need to create duplicates every time you make changes in your content.

In addition to providing an overview and minimizing the time to identify what type of alert or incident needs to be addressed, categorization helps analysts respond. Incident categorization ensures that third parties or their tools can use this downstream to resolve the incident. The result is that with this update, you are enabling orchestration with automated tools like SOAR.

To learn more about LogPoint 6.12, check our blog post and watch the short video with Nils Krumrey to get the release rundown.

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 SIEMand NDRtechnologies 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
+45 25 66 82 98