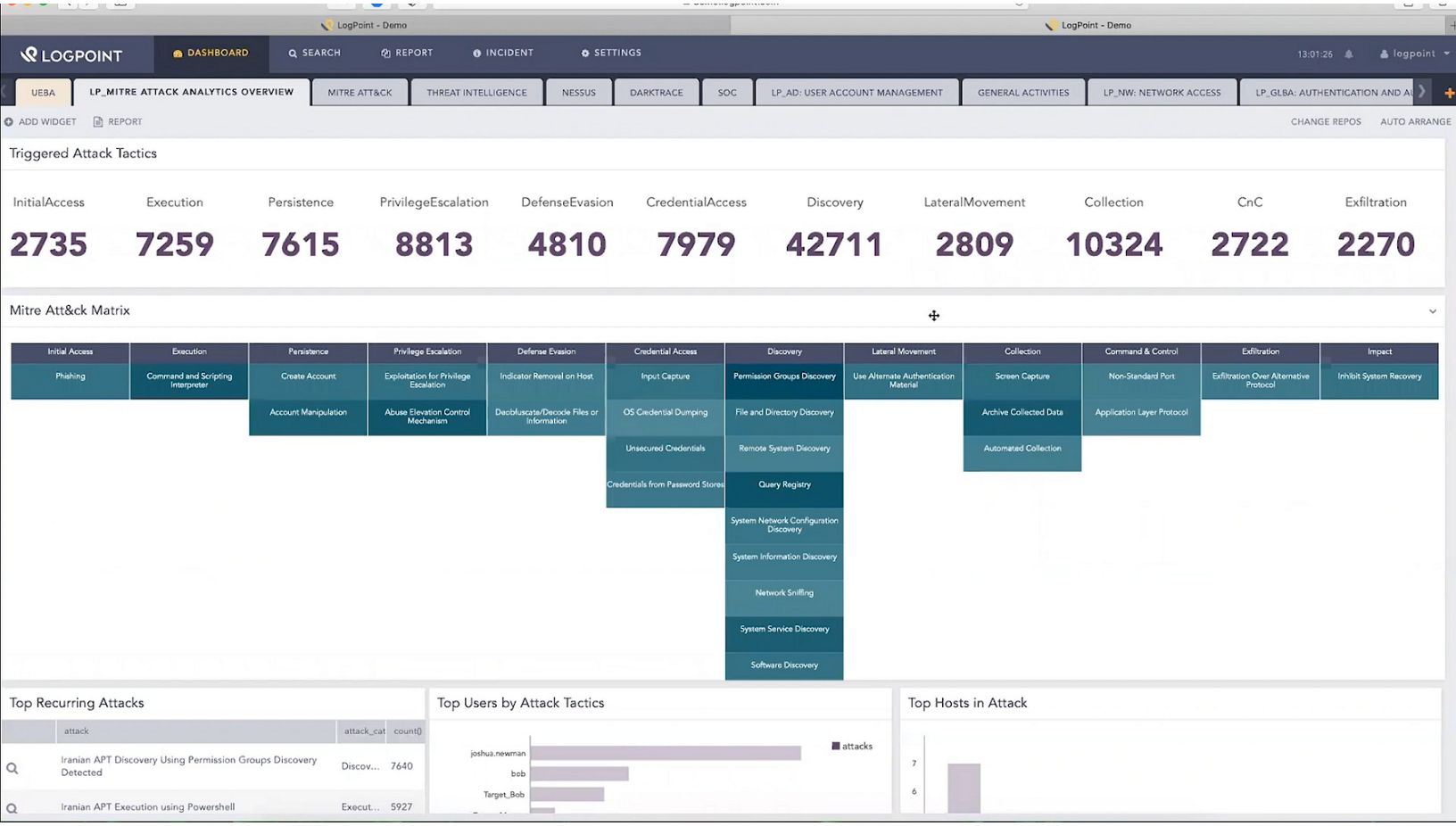

The MITRE ATT&CK visualization application in LogPoint 6.9 helps analysts track the stages of an attack and see ATT&CK observations in the network.

Nov 02, 2020 17:56 CET

Launching LogPoint 6.9: Speeding up investigation of cybersecurity incidents, introducing MITRE ATT&CK heat maps

LogPoint 6.9 helps analysts better understand what is critical to investigate and reduces the number of manual steps in the investigation process

COPENHAGEN and BOSTON – November 3, 2020 – LogPoint, the Modern SIEM and UEBA company, has launched version 6.9 of it's SIEM solution. The latest LogPoint release introduces a number of new efficient tools to speed up the investigation of cybersecurity incidents in the LogPoint SIEM solution.

“With LogPoint 6.9 you can connect the dots of cyberattacks with new MITRE ATT&CK visualizations. Drill-down more effectively during an investigation and simplify incident creation based on anomalies found by UEBA. It’s a release intended to improve the lives of the cybersecurity analysts working every day to keep companies and organizations safe,” says Alec Orlov LogPoint Head of Product Management.

The MITRE ATT&CK visualization application in LogPoint 6.9 helps analysts track the stages of an attack and see ATT&CK observations in the network. When an incident is triggered, it’s highlighted in a heat map, helping the analyst piece together different incidents and know what to investigate. Additionally, users can choose any tactic and see all associated alerts, helping to assess security coverage.

“A simple, yet effective feature in the new release is the ability to carry key-value pairs from search as input parameters to search templates. When analysts want to drill forward from logs to search templates, they can select relevant points, and the system will forward the user to the relevant search template. This is useful in incident investigation and helps analysts pivot from something in search to find out what else is going on,” says Orlov.

In LogPoint UEBA, analysts can save time by simply clicking on an anomaly to create an incident. The anomaly is saved in LogPoint and analysts can assign it to another user for further investigation. Manually creating an incident complements the existing automatic incident creation in UEBA where users can tune the alert based on inclusion, exclusion and risk threshold.

To learn more about LogPoint 6.9 read our blog post or take a few minutes to get the release rundown in the video with LogPoint Presales Manager @Guy Grieve.

Media and analysts can schedule a live, one-on-one demonstration of LogPoint 6.9 by contacting LogPoint media relations. The attached photo can be used freely by the media. For more information, visit www.logpoint.com/press

---

About LogPoint
LogPoint is committed to creating the best SIEM in the world. We enable

organizations to convert data into actionable intelligence: supporting cybersecurity, compliance, IT operations, and business analytics. LogPoint's Modern SIEM withUEBA provides advanced analytics and AI-driven automation capabilities that enable our customers to securely build-, manage, and transform their businesses. Our flat licensing model, based on nodes rather than data volume, drastically reduces the cost of deploying a SIEM solution on-premise, in the cloud or as an MSSP. LogPoint is easy to implement and offers unparalleled time-to-value. And don't just take our word for it. 1.000+ customers agree, our service is consistently receiving a 96% customer satisfaction rating. For more information, visit www.logpoint.com.

Contacts

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