Logpoint Converged SIEM

Logpoint Converged SIEM helps SOC teams combine data sets from multiple sources. Instead of using multiple standalone products, they now have one single source of truth. Converged SIEM is the only unified, cloud-based platform that delivers SIEM+SOAR, UEBA, and BCAS capabilities as a service directly to enterprises and MSSPs – all from a single plane of glass.

For more information, contact Logpoint:
https://www.logpoint.com/en/contact/

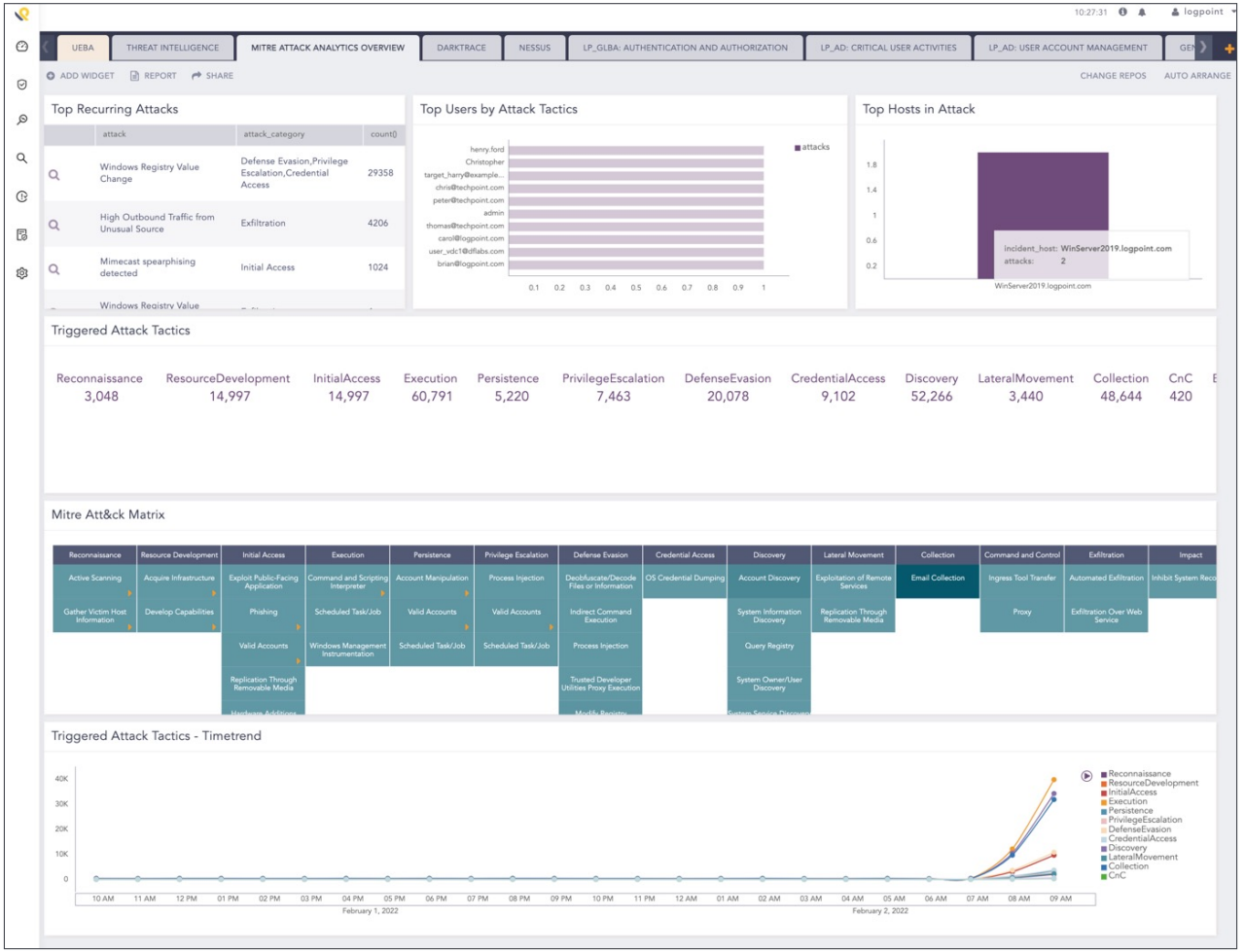
/logpoint

Increase efficiency with an all-in-one cybersecurity solution

Logpoint Converged SIEM enables you to

- Collect and centralize log data
- Meet the strictest compliance regulations with ease
- Detect the most advanced threats utilizing machine learning$
- Boost SOC productivity with automated alert triage
- Automate the whole detection, investigation, and response workflow with out-of-the-box playbooks targeting the most common security use cases

Converged SIEM collects log data from devices and applications across the entire IT infrastructure. Logs are then transformed into high-quality data through normalization and correlations. The solution automatically identifies and sends alerts about incidents and abnormalities using machine learning algorithms. In addition, Converged SIEM maps the alerts to the MITRE ATT&CK framework, brings in threat intelligence, and gathers contextual information to define the severity of the threats. Based on the information gathered, necessary response playbooks are automatically run mitigating the attacks quickly and safely in a matter of seconds.



In Converged SIEM the alerts are mapped to the MITRE ATT&CK framework

/logpoint

The most efficient and effective way to protect your business

Key benefits

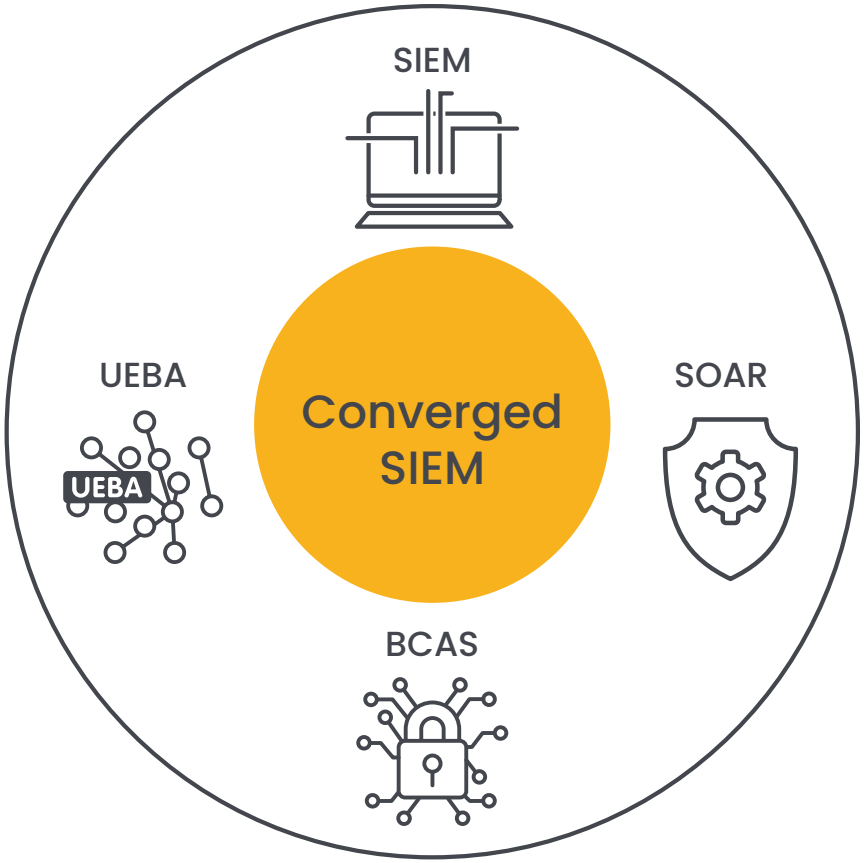
Easy to deploy: As a SaaS platform, onboarding and implementation is a simplified process, making Converged SIEM available with a minimal lead time.

Simple to operate: Cloud-based delivery removes the hassle of maintaining and updating systems, allowing you to focus on security.

Continuous product improvements: A dedicated team of security researchers regularly update the product's detection and response capabilities, increasing your agility to deal with the emerging threat landscape.

A single tool for all security aspects of your business: Converged SIEM unifies and automates incident detection, investigation, and response processes, drastically improving efficiency and minimizing risk.

Security teams are short-staffed. These staff shortages mean teams are struggling to investigate incidents and effectively respond to threats in a quick and effective manner. Logpoint Converged SIEM automates time-consuming and repetitive, yet critical, actions so your team can collaborate and manage incidents more effectively.



/logpoint

Amplify your team with automation

Key features

Cloud-based deployment: Cloud delivered Converged SIEM makes deployment and scaling hassle-free

Data privacy: Converged SIEM assures total isolation and protection of customer data in the cloud and is compliant with the strictest data privacy regulations, including Screms-II, General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA).

Support for 1.000+ data sources: Converged SIEM collects data from endpoints, cloud platforms, and business-critical applications, enabling covering the whole infrastructure with a single tool

Data normalization: Converged SIEM normalizes log data into a single common language, making it easy to correlate data across applications and identify patterns

80+ detectors using machine learning: Converged SIEM uses machine learning to analyze user behavior to identify the known unknowns, allowing you to react, investigate, and mitigate quickly

800+ integrations out of the box: Converged SIEM orchestrates disparate tools and automates actions

75+ ready to use playbooks: Converged SIEM automates the investigation and response processes, accelerating response time from hours to a matter of seconds.