Palo Alto Networks Cortex XSOAR

LogPoint Solution Brief: Automated Incident Detection and Response

Automated Threat Analysis and Response Increases SOC Productivity

Traditionally a manual process, alert triage is highly draining for security analysts. When faced with a high volume of alerts, limited time, and shrinking budgets, it is common for security analysts to make mistakes. Paired with the growing legal and regulatory pressures that SOCs face, many security teams struggle to keep their organizations secure with a growing number of disparate and siloed tools.

Benefits of the Integration

Together, LogPoint and Cortex XSOAR enable you to:

Leverage productivity: Take information from LogPoint to coordinate security responses from 700+ Cortex XSOAR third-party product integrations, enriching response actions and decreasing time to value.

Discover critical incidents: Automatically prioritize alerts with risk based context and accurately scale incident response in your security ecosystem.

Automate response: Improve your team's efficiency with a host of easy-to-use management features to automate your control over incidents, including assigning relevant analysts for further investigation and resolving incidents after playbook execution.

To combat these issues, Cortex XSOAR and LogPoint are releasing an integration to combine security monitoring and incident response for streamlined incident resolution. The LogPoint SIEM content pack was created to save time and increase analyst productivity, scaling to cover your entire organization and providing customizable and automated workflows. Applying this content pack is a powerful amplifier to your overall security program because it enables SOCs to increase productivity with playbooks based on LogPoint SIEM data, get comprehensive and fast incident response, and maintain complete control over incidents. Use the full potential of your security resources including the siloed enrichment data that you already have by integrating LogPoint SIEM with your top tools and automated orchestration playbooks within Cortex XSOAR.

About LogPoint

LogPoint is a security information and event management (SIEM) solution that detects, analyzes, and responds to threats within your data for faster security investigations. The LogPoint SIEM provides a complete view of the threat landscape by automatically identifying and sending alerts about any critical incidents or abnormalities in your system. Paired with Cortex XSOAR, the integration combines security monitoring and incident response with powerful automation to help security staff respond to and resolve incidents quickly.

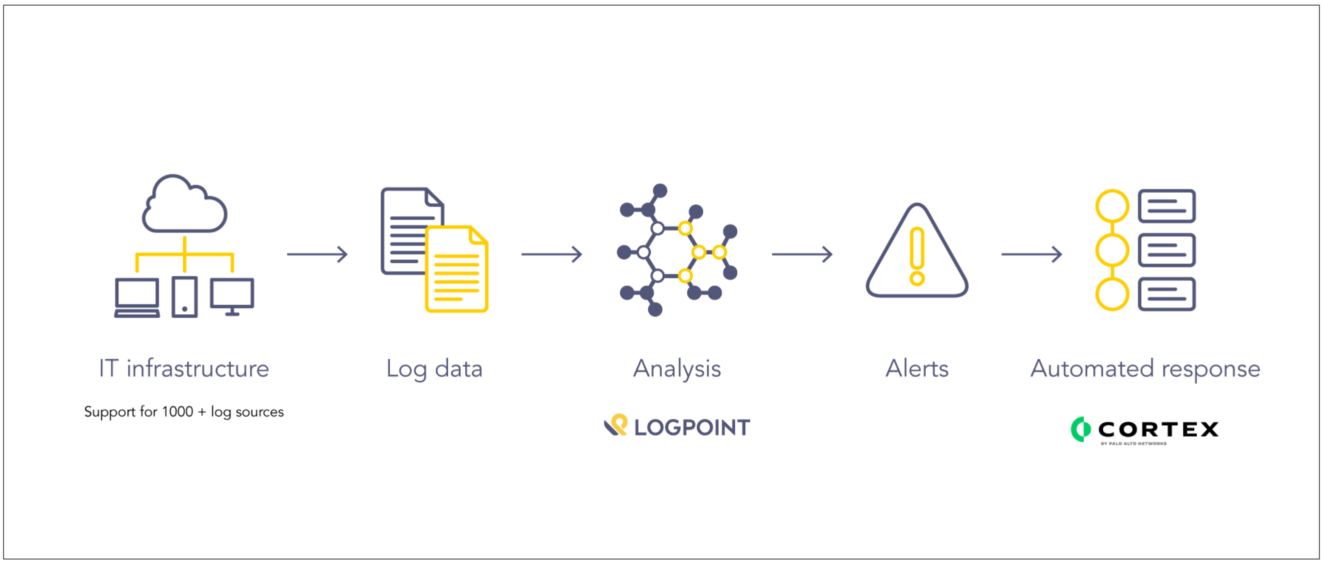

Figure 1: LogPoint acts as an intermediary between your IT infrastructure and Cortex XSOAR.

Cortex XSOAR unifies case management, automation, real-time collaboration, and threat intelligence management to transform every stage of the incident lifecycle, resulting in significantly faster responses that require less manual review.

The LogPoint SIEM content pack for Cortex XSOAR provides full coverage of incident detection and response capabilities, enabling your SOC to automate and standardize threat response. LogPoint collects and correlates data from devices across the organization, using this information to detect potential security incidents, automatically prioritize, and trigger alerts based on risk. Cortex XSOAR then ingests these alerts and executes automated playbooks to speed up incident response.

Leveraging both technologies, your security team will be able to seamlessly detect potential security risks and execute responses automatically. Utilize your hardware and software to reduce strain and work more effectively by handling incidents in the suggested order. Your SOC can use this powerful integration to:

- Bidirectional integration automatically contextualizes SOAR incident data and SIEM alerts with rich context in real time
- Flag and assign high-risk alerts for further investigation while automatically processing low-level incidents
- Diagnose potential issues or abnormalities in your system with real time data from the Cortex XSOAR War Room
- Threat hunt by easily searching and pivoting within the data during investigation

Through a powerful set of playbooks, analysts can correlate the discovered information with data provided from internal security systems (e.g., Cortex Data Lake, Cortex XDR™, Prisma® Cloud and Panorama™ network security management, Active Directory, SIEM) to help automate remediation for accelerated threat analysis and response.

Cortex XSOAR Marketplace

is a digital storefront for discovering turn-key security orchestration content packs centrally within Cortex™ XSOAR.

Content packs

are prebuilt bundles of integrations, playbooks, dashboards, fields, subscription services, and all the dependencies needed to support specific security orchestration use cases.

The LogPoint SIEM pack

allows the SOC to get a complete view of the threat landscape and automatically respond to incidents, leveraging comprehensive security monitoring to provide control over incidents.

The LogPoint SIEM content pack is easily deployed with a single click from the online Marketplace, giving you all the content needed to accelerate incident detection and response with Cortex XSOAR.

Core content pack includes:

- 1 classifiers
- 20 incident fields
- 1 incident types
- 1 integration
- 1 playbook

Bridge gaps and advance the maturity of your security program by tapping into the fastest-growing community of security experts.

To discover new SOAR content, visit **paloaltonetworks.com/cortex/xsoar/marketplace**

VISIT MARKETPLACE

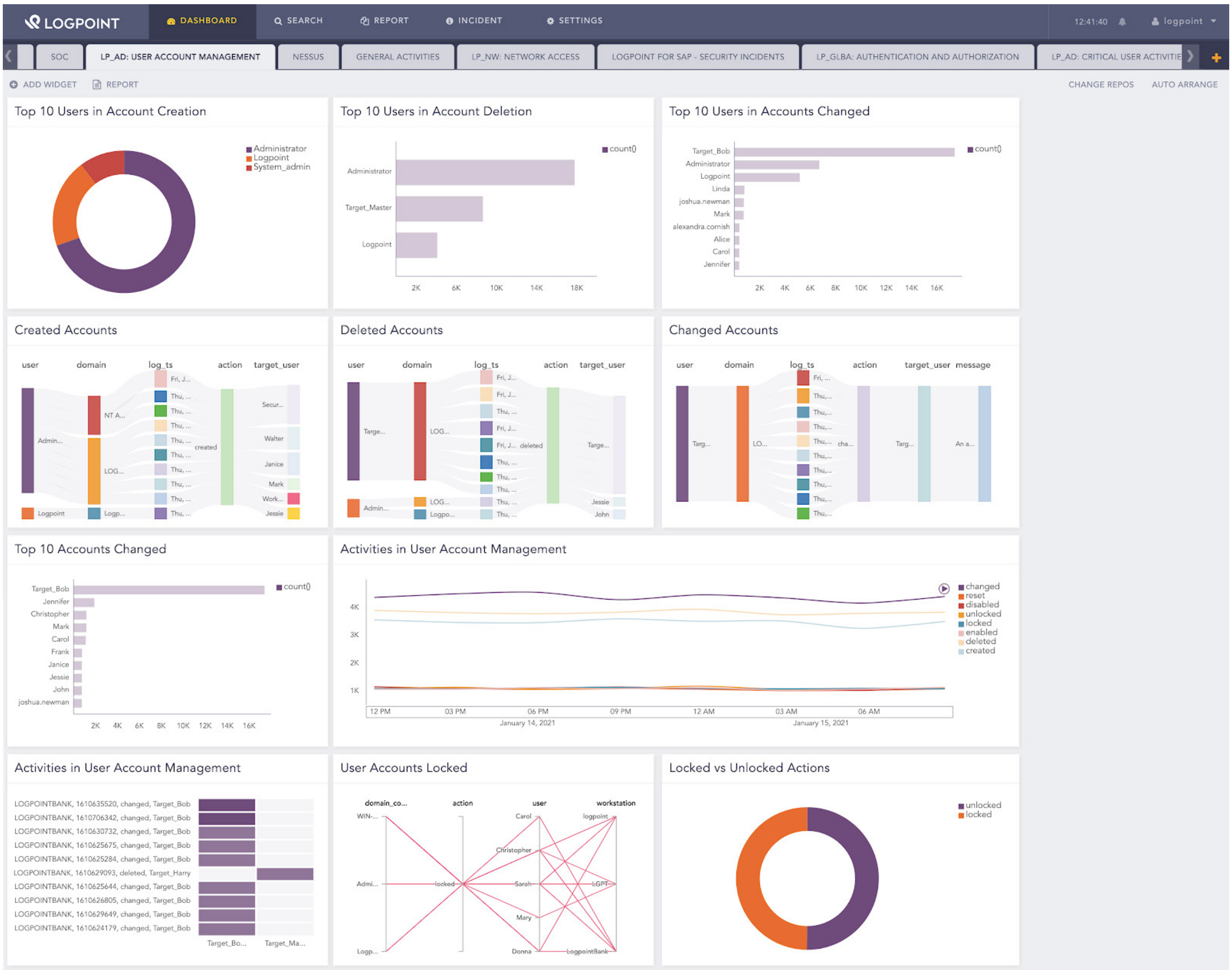

Figure 2: LogPoint Dashboard

Use Case 1: Investigating failed login attempts

Challenge: Data breaches are highly dangerous for an organization and often involves lost or stolen credentials. While multiple failed login attempts are a good indicator of a brute force attack, it can be difficult to see these alerts in the overwhelming amount of indicators SOCs face day to day.

Solution: LogPoint regularly checks for failed login attempts by Active Directory (AD) users, and triggers an alert at a failed attempt. When a predefined threshold of failed attempts is reached, LogPoint creates an incident and alerts Cortex XSOAR.

Benefit: When LogPoint sends an incident involving multiple failed login attempts, it triggers a playbook with Cortex XSOAR that automatically notifies the user and resets their password. Take automated steps to protect your organization.

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 with UEBA provides advanced analytics and ML-driven automation capabilities that enable our customers to securely build, manage, and effectively transform their businesses.
For more information, visit www.logpoint.com.

paloalto NETWORKS

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.
For more information, visit www.paloaltonetworks.com.

Contact LogPoint

If you have any questions or want to learn more about LogPoint and our next-gen SIEM solution, don't hesitate to contact us at www.logpoint.com/en/contact/