securonix

DATASHEET

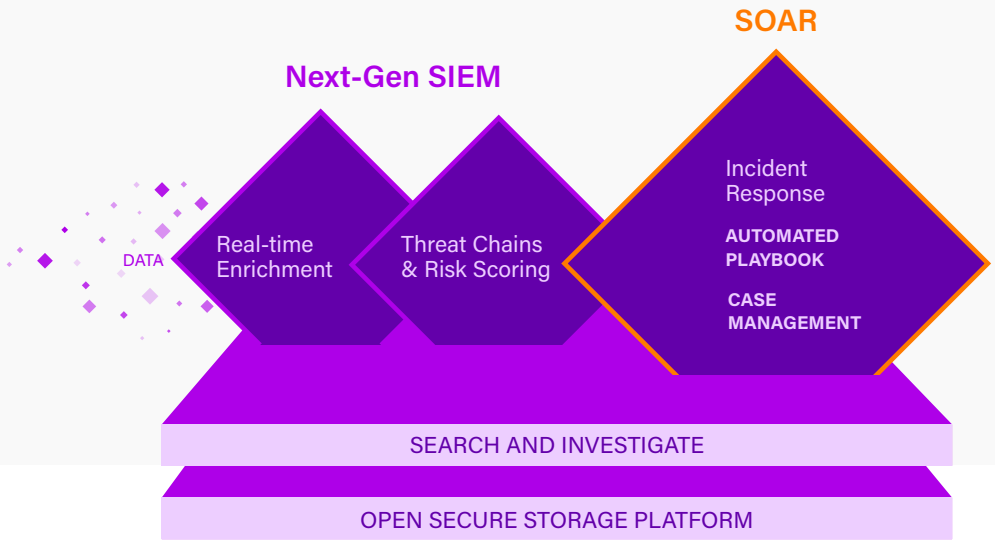
Security Orchestration, Automation, and Response

Mitigate Risk and Response to Complex Threats Faster

Why Securonix?

Rapid response is essential to mitigate the risks of cybersecurity threats. However, separate security tools for detection and response add unnecessary complexity for security teams.

Securonix SOAR helps SOCs accelerate incident response by bringing all of your details from your IT environment into a single pane of glass. By simplifying investigations with a converged view, we help security teams drive efficiency and reduce complexity for faster response.



Why Single Detection and Response Solution?

Simplify Investigations

Easily add SOAR to your SIEM to lower the time it takes to investigate and respond to threats. With Securonix SOAR, you remove complexity for your analysts with an integrated view of detection and response across your entire security environment.

Work Smarter

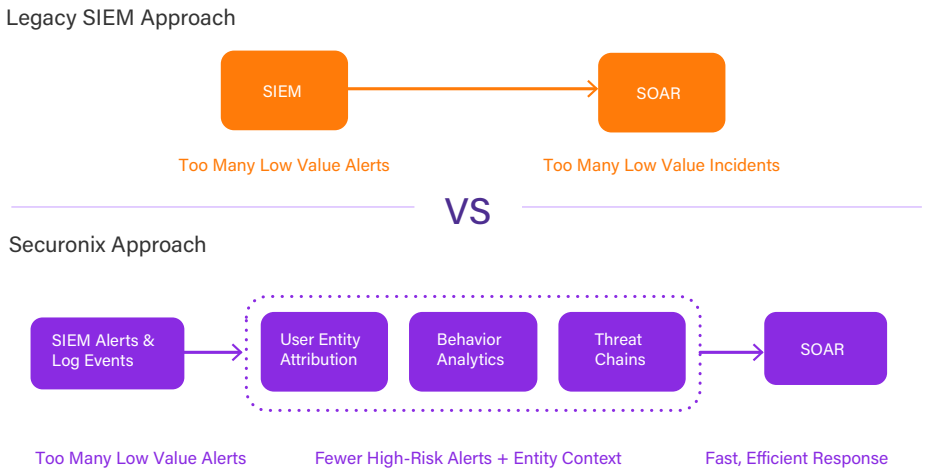
SOAR helps your team work smarter, not harder with repeatable, automated security orchestration. Our solution leverages advanced analytics to automate incident response workflows, allowing your team to focus their time where it matters the most.

Boost SOC Performance

Security leaders need to be able to track how incident response improves over time to justify their security investments. Securonix SOAR's robust reporting and response metrics helps you track KPI's and improve performance while increasing return on investments (ROI).

Take Your Next-Gen SIEM to the Next Level

Automated response capabilities help security teams reduce the level of risk in their organization while unburdening analysts.



Automated Workflows

Simplify response with orchestration and automation

Recommendation Engine: Enable autotuning and better threat triage with machine learning that analyzes the past remediation actions of your top analysts.

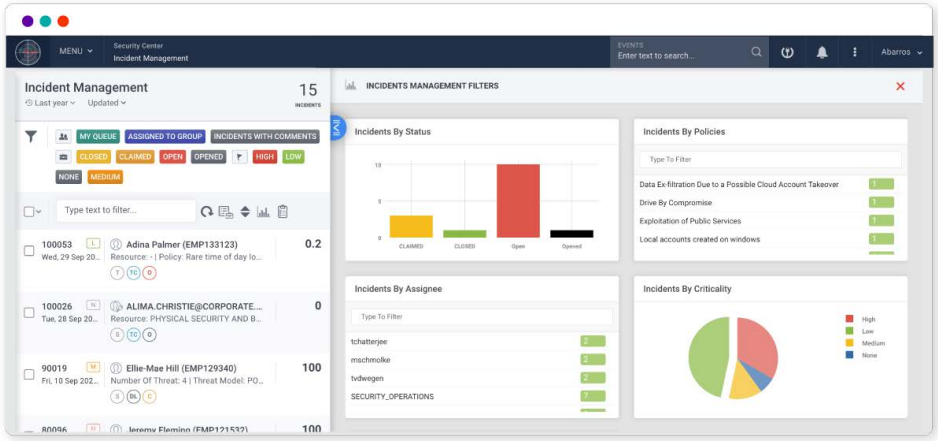
Playbooks: Remove complexity for analysts with over 3,000 out-of-the-box, fully customizable playbook actions that allow you to automate response actions for common use cases.

Robust Management and Reporting

Understand how your response is improving over time

Incident Management: Understand and track your KPI's using the built-in incident management tool. Our solution allows you to track workflows and investigation steps that are useful for compliance audits and tracking data breaches.

Performance Metrics: Optimize your SOC performance with metrics around resolved incidents, mean dwell times, and mean-time-to-respond.



Multi-Tenant Response

Securonix supports response actions in a multi-tenant environment, enabling your analysts to take actions across multiple tenants from a centralized console. This capability is beneficial for managed service providers using Securonix to support multiple diverse customers.

For more information about the Securonix SOAR, schedule a demo at: www.securonix.com/request-a-demo.