VARONIS

VARONIS + SPLUNK SOAR

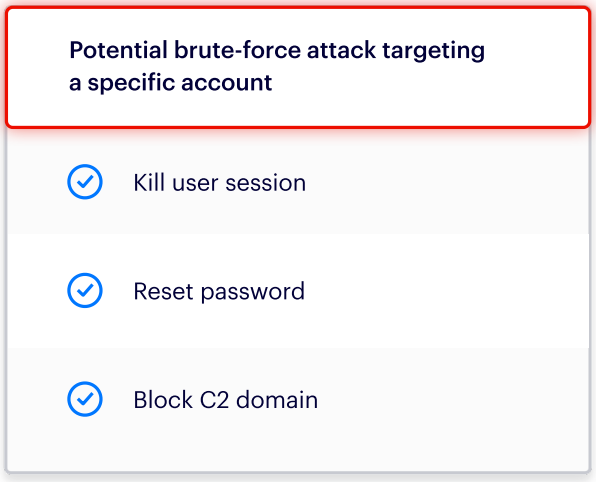
Gain a unified picture of data risk, enhance investigations, and improve incident response times.

CHALLENGE

Sophisticated attacks such as ransomware and insider threats can cause significant damage within minutes, necessitating rapid detection and response. However, the sheer volume of threats and the speed at which they evolve their techniques present a formidable challenge for security teams to handle manually. To quickly respond to attacks, security teams must integrate, automate, and orchestrate as many security tasks as possible with direct insight into the attacker's target: the data.

SOLUTION

Varonis offers comprehensive visibility into sensitive data risk and activity. It uses advanced AI-powered, behavior-based threat detection to proactively identify sophisticated cyber threats, including ransomware, insider threats, and APTs. Integrating Varonis with Splunk SOAR enables security teams to incorporate Varonis' context-rich and actionable alerts into their security playbooks to accelerate investigations and reduce response times. Security teams can leverage Splunk's orchestration and automation capabilities to act on Varonis' data-centric alerts, enabling them to respond quickly to cyber threats and prevent data breaches.



KEY BENEFITS

- Accelerate investigations with meaningful and actionable insights.
- Reduce time to detection and catch more threats.
- Centralize incident management and automate threat response.

"With Varonis, we're not getting overloaded with alerts and not spending time chasing after false positives. That's been a huge time-saver and a stress reliever."

KEN CHRISTMAN
Director of IT,
Mackenzie

Read the full case study here:
varonis.com/case-study

Reduce time to detect and catch more threats.

Varonis monitors data activity, authentication activity, directory service activity, and perimeter telemetry and uses behavior-based threat models to detect active threats in real time. From billions of events, Varonis surfaces only the most meaningful alerts and easily integrates into Splunk SOAR, allowing security teams to focus on true threats.

Accelerate investigations with meaningful and actionable security insights.

Varonis delivers actionable alerts with deep context, including user details, data sensitivity, permissions, geolocation, and device information. These alerts can be seamlessly integrated into Splunk SOAR workflows to create a unified picture of data risk, accelerating triage, investigation, and response.

Centralize incident management and automate threat responses.

Manage all security incidents from one location. Varonis enables organizations to orchestrate and automate workflows to detect threats before they become breaches. Security teams can easily stop attacks in their tracks and limit the damage by automatically killing user sessions, changing passwords, locking accounts, and powering down systems as soon as threats are detected

TRY VARONIS FOR FREE.

See how our cloud-native solution covers all your data security needs.
Get started today at **varonis.com/trial.**