Silverfort & CrowdStrike SIEM for risk and incident monitoring

SIEM is a key component in security teams' detection and response capabilities. However, a SIEM is only as effective as the data it receives, and when it comes to identity-based attacks that exploit compromised credentials, traditional IAM solutions often lack the depth needed to detect malicious activity in progress. Silverfort and CrowdStrike address this persistent visibility gap by continuously delivering rich, real-time identity threat data into the CrowdStrike Falcon Next-Gen SIEM environment. This integration equips security and SOC teams with continuous visibility into authentication-based risks for faster and more effective threat detection and response.

Accelerated detection of identity-based threats

The integration between Silverfort and CrowdStrike Falcon® Next-Gen SIEM delivers unified visibility into identity-based threats by combining real-time authentication telemetry with CrowdStrike's endpoint and network analytics. Silverfort continuously delivers authentication threat signals directly into the CrowdStrike SIEM environment, including Risk and Incident events such as suspicious logins, credential abuse, and lateral movement attempts.

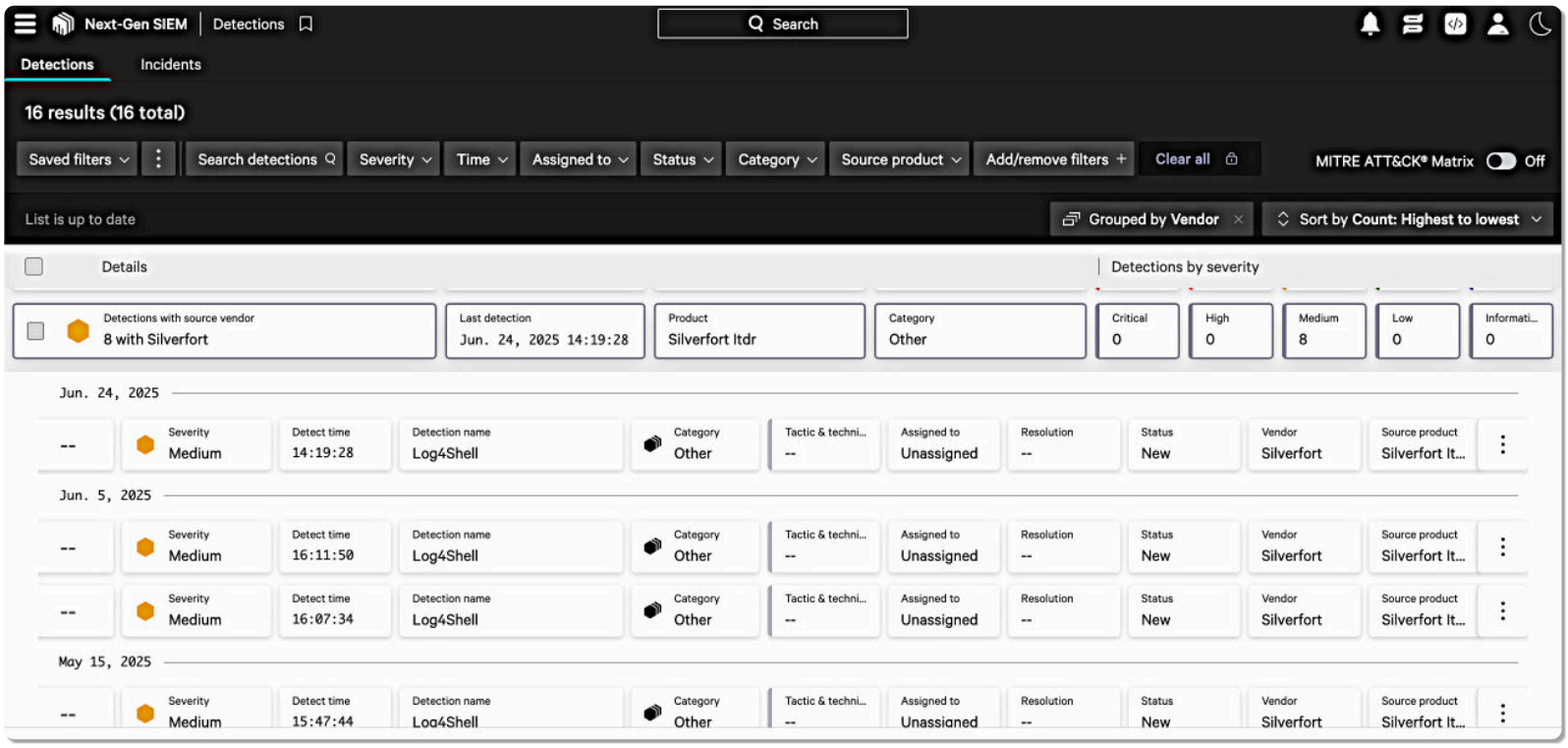
This enriched data enables SOC teams to centralize identity threat data alongside broader endpoint and network telemetry, which accelerates the speed and accuracy of threat detection. Now SOC analysts gain faster, context-rich insights directly within their SIEM environment, eliminating the need for manual correlation across disparate systems. This streamlines incident response, enabling quicker detection, deeper cross-domain context, and more confident, precise action on identity threats.

How Silverfort for CrowdStrike SIEM works

Through a seamless API-based integration, Silverfort continuously delivers identity-centric risk and incident events to CrowdStrike's SIEM. These events include real-time alerts for high-risk behaviors such as MFA fatigue attacks, excessive failed login attempts, and suspicious authentications across both on-prem and cloud environments.

CrowdStrike ingests this data into its SIEM dashboards and detection engines, where it is correlated with host activity, endpoint behavior, and network telemetry. This unified view streamlines investigations, reduces alert fatigue, and enhances the effectiveness of incident response.

SOC teams no longer need to manually stitch together identity signals from multiple tools. Silverfort's identity data and insights are automatically embedded into CrowdStrike's workflows, enabling faster triage, greater context, and more efficient mitigation of identity-based threats.



Example of a security alert generated by Silverfort with severity sent to Crowdstrike EDR via API for investigation and response.

Key benefits

Threat detection capabilities
Enables real-time identification of identity-based threats such as brute force attacks and lateral movement.

Intelligence integration
Delivers dynamic identity threat intelligence directly into CrowdStrike SIEM dashboards for faster, more informed decision-making.

Context correlation across domains
Ensures identity-based risks are automatically analyzed alongside endpoint and network data for full situational awareness.

Security operations efficiency
Unifies identity threat monitoring within the broader security ecosystem to streamline workflows and improve operational effectiveness.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.