Silk Security: Operationalize Exposure Management Risk Resolution

Bridge the gap between detecting security findings and fixing them

Challenges

The adoption of new technologies, DevOps approaches and cloud services has expanded the enterprise attack surface, and at the same time attackers have developed more automated techniques to exploit security exposures and unremediated vulnerabilities. With siloed legacy tools, security teams lack a consolidated view to understand where risks are the most elevated — potentially leaving their environments exposed. Current tool-centric approaches operate in a silo without enough risk or business value context to drive prioritization, relying on manual assessments that slow collaboration with the teams responsible for fixing exposure. Without consistently prioritizing remediation actions for exposures, organizations are left open to vulnerabilities and potential breaches.

Solution

Silk Security's integration with CrowdStrike Falcon® Exposure Management enables security teams to consolidate visibility across the extended enterprise attack surface, identify elevated risks based on correlated insights and specific context, and enable cross-functional collaboration for the risk resolution process. Organizations can seamlessly prioritize and proactively remediate critical vulnerabilities using correlated asset intelligence and custom asset labeling and rules from Silk Security and CrowdStrike to effectively see and understand vulnerability business impact.

Once security teams have identified a high-risk priority, Silk's AI-driven remediation responsibility assignment helps identify who is responsible for a fix implementation. Through extended bidirectional integrations with ticketing and workflow systems, Silk can then automate the process of issuing tickets and provide a centralized view into activity and fixer feedback across multiple ticketing systems to drastically accelerate the remediation lifecycle.

Key benefits

- Operationalize remediation of CrowdStrike Falcon Exposure Management risk findings with ownership assignment, ticketing tools integration and fix status reporting

- Enrich risk prioritization with additional environmental insights, business context and custom asset labels

- Centrally track progress and the state of resolution fix by criticality, team and SLA timeline

- Identify asset coverage gaps where CrowdStrike Falcon is not present and compare tool usage to improve operational efficiency

silk.

Use Case/Challenge	Solution	Benefits
Manage risk with remediation operationalization	Silk leverages rich vulnerability data from CrowdStrike to provide prioritization context and automated discovery of the team responsible for remediating findings, with third-party bidirectional ticketing system integrations for assignments and a centralized activity dashboard	Maintain a consistent process for assigning, monitoring and reporting remediation fixes and automated endpoint actions
Simplify tracking and monitoring	Silk's workflow integration manages and tracks exceptions and reassignment status, and monitors remediation SLAs based on criticality or other key metrics	Track trends by risk criticality, and measure how teams are performing over time and in comparison with each other to improve overall operations and output
Extend technology risk understanding	Integrate and normalize findings from CrowdStrike and other third-party detection tools, and correlate with asset linking	Determine which remediations will be high-impact fixes, and understand which assets to focus on for optimal risk reduction

Technical solution

By translating consolidated security findings from CrowdStrike Falcon Exposure Management and other security detection tools into actionable operational remediation tasks for the right owners, Silk empowers security teams to transform how they resolve, track and audit cyber risk. The Silk platform consolidates and correlates rich vulnerability and cloud security findings from the CrowdStrike Falcon® platform into a unified risk framework to bridge the gap between detecting security findings and fixing them to ensure a best-in-class security posture.
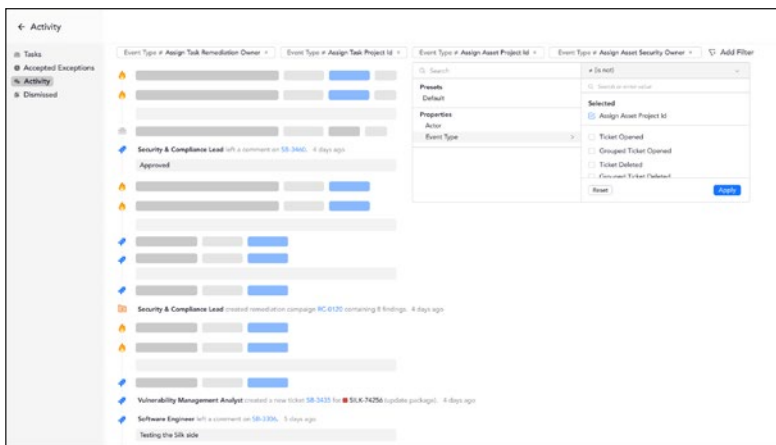
Silk's consolidated activity dashboard

"Silk has positively impacted both the productivity and the efficiency of the security team in identifying risks to the business, as well as how the function of security is integrated into our development processes. The security team can collaborate more closely with development teams responsible for the fix implementation of identified priorities and improve our overall risk profile."

Frank Baalbergen, CISO, Mendix

Key capabilities

Accelerate Mean Time to Resolution: Manage a single, streamlined ticketing process for finding, fixing, assigning and reporting on vulnerability and exposure resolution — whether implemented remediation, automated patch or accepted exception.

Centralize Visibility into Risk: Understand how your teams and the tools they are using are performing through a consolidated dashboard, and measure the effectiveness of the remediation process.

Silk Security is a trusted CrowdStrike Falcon Fund Partner providing risk resolution and operationalization capabilities, leveraging the Falcon platform's telemetry and vulnerability insights for a hardened security posture.

About Silk Security

Silk is the first platform for unified risk prioritization and resolution — built by practitioners for practitioners. Silk automates technology risk assessment and prioritization by consolidating, correlating and contextualizing findings across tools, and facilitates operationalization with predictive ownership assignment, bidirectional workflow communication and end-to-end tracking and reporting of resolution tasks.

Silk Security was founded by three entrepreneurs with over 40 years of combined experience in the cybersecurity space with a proven track record of building successful cybersecurity products from inception.

Learn More

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.