CrowdStrike Delivers the Next Generation of SIEM to Power the AI-Native SOC

Falcon Next-Gen SIEM innovations modernize SOC operations with a single, unified platform to deliver full visibility and protection across all workloads; Falcon Insight customers receive 10 gigabytes of third-party data per day at no additional cost

AUSTIN, Texas--(BUSINESS WIRE)--May 7, 2024-- **RSA Conference 2024 --** CrowdStrike (NASDAQ: CRWD) today announced new CrowdStrike Falcon® Next-Gen SIEM innovations to liberate customers from the constraints of legacy SIEM products and power the AI-Native SOC. To accelerate SOC transformation, all Falcon Insight customers will receive 10 gigabytes of third-party data ingest per day at no additional cost to experience the speed and performance of Falcon Next-Gen SIEM.

With breakout times now measured in minutes, stopping breaches requires security operations to match the speed of the adversary. Legacy SIEMs are too slow and complex to deliver the security outcomes customers require. SIEMs have become data dumping grounds, forcing security analysts to navigate multiple data sources, tools and consoles to extract meaning from data and conduct investigations. At the same time, point products positioned as SIEM alternatives struggle with slow search speeds, limited data visualization and investigation options, and a data onboarding process that requires lengthy deployments while driving up overall costs. To give security teams the speed they need to stop breaches, the modern SOC requires a platform that converges data, security and IT, with AI and workflow automation built natively within. With this release, CrowdStrike sets the standard for the next generation of SIEM, engineered to power the AI-native SOC.

“The speed of today’s cyberattacks requires security teams to rapidly analyze massive amounts of data to detect, investigate and respond to threats faster. This is the failed promise of SIEM. Customers are hungry for better technology that delivers instant time-to-value and increased functionality at a lower total cost of ownership,” said George Kurtz, CEO and co-founder, CrowdStrike. “The vast majority of the critical security data is already resident in the Falcon platform, saving the time and cost of data transfer to a legacy SIEM. Our single-agent, single platform architecture unifies native and third-party data with AI and workflow automation to deliver on the promise of the AI-native SOC.”

The AI-Native SOC: Full Visibility. Faster Detection and Response.

Falcon Next-Gen SIEM is the industry’s answer to power the AI-Native SOC, delivering up to 150x faster search performance and an 80% lower total cost of ownership than legacy SIEMs and solutions positioned as SIEM alternatives. New and expanded innovations in the latest Falcon Next-Gen SIEM release include:

Generative AI and Workflow Automation:

- **Charlotte AI for all Falcon Data:** Charlotte AI, CrowdStrike’s Generative AI security analyst which transforms every user into a power user, is now available for all Falcon data in Next Gen SIEM. Analysts can ask any question of Falcon data in the Falcon platform, as well as from product documentation or Knowledge Bases, in plain language and get an answer back in seconds.
- **Investigate with Charlotte AI**: Transforms the speed and efficiency of investigations by automatically correlating all related context into a single incident and generates an LLM-powered incident summary for understanding by security analysts of all skill levels.
- **New GenAI Promptbooks**: New out-of-the-box promptbooks drive the most common analyst workflows across detection, investigation, hunting, and response with velocity. Teams can further define custom prompts to standardize and re-use specific detection and response workflows to go from incident to action with greater speed and efficiency.
- **Native SIEM and SOAR Integration:** Falcon Fusion SOAR provides a newly modernized UI for a drag and drop experience to create playbooks and workflows, accelerating detection, investigation and response. Falcon Next-Gen SIEM includes a growing library of integrations and actions to automate critical security and IT use cases across siloed teams and tools.
- **Automated Investigations and Threat Hunting:** Falcon Fusion SOAR brings workflow automation to threat investigation and hunting. Analysts can automatically query all data in Falcon Next-Gen SIEM and close the loop by visualizing the results or orchestrating action across Falcon and third-party tools.

Rapid Data Ingestion to Consolidate Detection and Response:

- **Expanded Data Ecosystem**: Falcon Next-Gen SIEM includes new and updated connectors to consolidate third-party IT and security data into the unified Falcon platform.
- **New Cloud Connectors:** Includes comprehensive connectors for AWS, Azure, and GCP. AWS coverage includes all key cloud services such as GuardDuty, Security Hub, and S3 Access Logs. Azure connectors include Microsoft Defender for Cloud and Microsoft Exchange Online.
- **Automated Data Normalization on a Common Standard:** Data onboarding is streamlined and made easy with new parsers. Automated normalization of third-party data on the new CrowdStrike Parsing Standard creates a common understanding that drives rapid, accurate detection and response across all data sources.
- **Automated SIEM Data On-boarding**: New data management capabilities make it easy to understand the health, volume,

and status of data ingestion, as well as manage and edit custom parsers to easily bring in new data sources, including on-premises log collectors.

A Modern Analyst Experience with Incident Workbench Innovations:

- **Automated Incident Enrichment:** New automated enrichment capabilities adds context to indicators that an analyst adds to an incident for complete context from the Falcon platform, including adversary TTPs, host and user data and associated vulnerabilities - slashing investigation time.
- **Case Management and Incident Collaboration:** New and enhanced features support analyst collaboration and ease of use, including a simplified user experience with customized views, direct access to Advanced Event Search from the Incident Workbench, severity and naming modification and automated change notifications when another analyst adds a note.
- **Add Threat Intelligence with Custom Lookup Files:** Easily add threat intelligence or custom content to Falcon Next-Gen SIEM to drive searches, without cumbersome manual processes.

Falcon Next-Gen SIEM is generally available. For more information:

- Get a demo at RSA, booth #N-6144
- Register for the virtual AI-Native SOC Summit
- Visit the Falcon Next-Gen SIEM page or request a free virtual test drive.

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.

Learn more: https://www.crowdstrike.com/
Follow us: Blog | Twitter | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

View source version on businesswire.com: https://www.businesswire.com/news/home/20240507009784/en/

Media Contact
Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike, Inc.