CrowdStrike Store

Siemplify

CROWDSTRIKE

Data Sheet

SIEMPLIFY: HOLISTIC SECURITY OPERATIONS

Automating the detection of and response to malicious events on the endpoint

CHALLENGES

Some endpoint detection and response (EDR) tools can be ad hoc, manual and labor-intensive when done incorrectly. With trillions of events and an increasing number of adversaries causing growing security alerts, the process of reviewing, researching and responding appropriately to threats can feel daunting.

SOLUTION

Combining EDR and security orchestration, automation and response (SOAR) enables security teams to better manage alerts and reduce manual workloads. With Siemplify and the CrowdStrike Falcon® platform you can ingest endpoint-related alerts, automate data collection to speed up investigation and orchestrate response across all the endpoints — all within one interface.

The Siemplify Security Operations Platform is an intuitive, holistic workbench that makes your security operations smarter, more efficient and more effective. By combining SOAR with context-driven case management, investigation and machine learning, your analysts are more productive, your security engineers are more effective and your managers are more informed about security operations center (SOC) performance.

BUSINESS VALUE

Use Case / Challenges	Solution	Benefits
Streamline malware investigations	Enrich alerts with data about impacted assets and build playbooks to automatically initiate response actions.	Automate case preparation through final response and close cases faster. Turn an investigation into a comprehensive hunt.
Reduce time spent on phishing investigations	Enable playbook creation that incorporates rich endpoint data into your case insights and automates false-positive identification and analysis.	Turn manual, time-consuming tasks into automated processes. Ensure analysts have needed information. Identify and focus on real threats.
Incorporate automated threat hunting	Integrate with existing tools and build playbooks to automatically perform targeted hunting.	Leverage emerging threat intelligence to root out hidden and malicious actors. Automate proactive hunting.

KEY BENEFITS

Slash investigation time and effort: Execute playbooks that automate data collection using CrowdStrike Falcon telemetry to limit the amount of time spent manually cross-referencing information

Remediate threats with a few clicks: Implement immediate remediation actions without having to pivot between systems

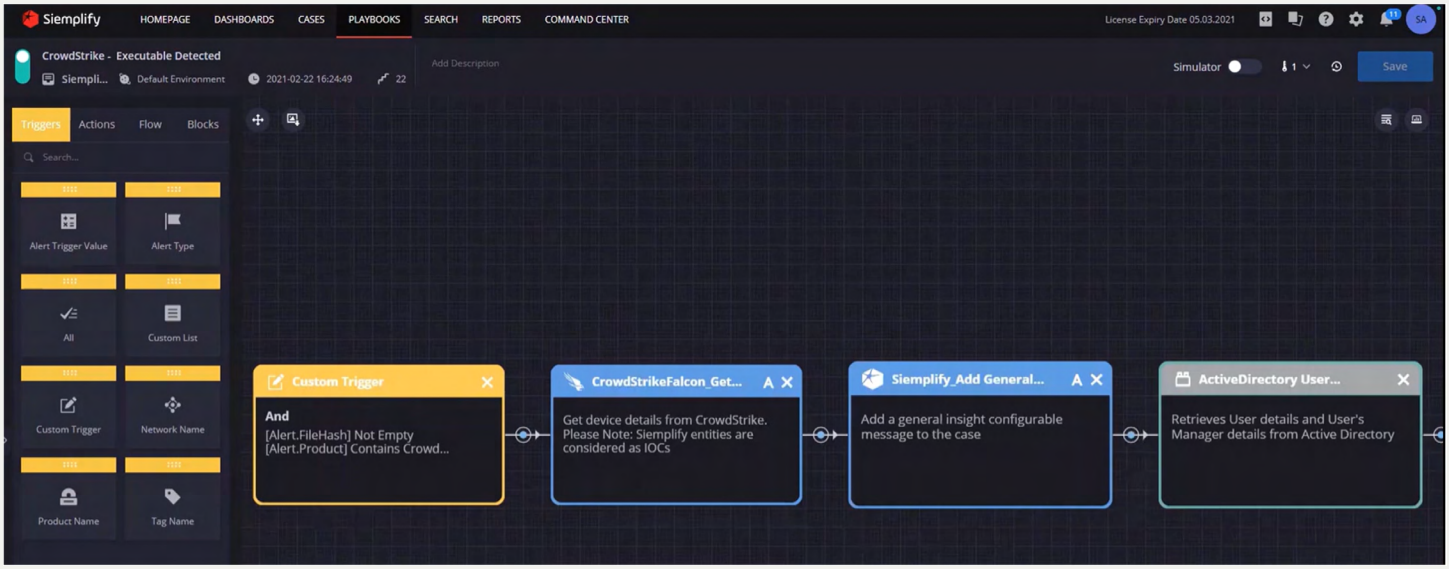
Unify case management: Ingest CrowdStrike's alerts directly into the Siemplify platform to automatically group related alerts into threat-centric cases to expedite threat response

TECHNICAL SOLUTION

Siemplify pulls in Falcon platform events along with metadata from your other tools to efficiently manage cases and automate CrowdStrike remediation actions. Siemplify's intelligent case management groups alerts from your stack of tools to integrate the who, what, when and where of a suspicious endpoint activity without having to pivot between screens.

"Siemplify's SOAR solution has enabled our team to offload manual tasks with automation."

Security Analyst, Retail



KEY CAPABILITIES

- Execute playbooks that automate data collection using Falcon telemetry to limit time spent manually cross-referencing information.
- Leverage the Falcon API for remediation actions such as isolating hosts or killing processes, without having to pivot between systems.
- Ingest Falcon alerts directly or via security information and event management (SIEM) into the Siemplify SOAR platform. Siemplify's patented threat-centric technology automatically groups related alerts into threat-centric cases.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

ABOUT SIEMPLIFY

Siemplify, the leading independent security orchestration, automation and response (SOAR) provider, is redefining security operations for enterprises and MSSPs worldwide. The Siemplify platform is an intuitive workbench that enables security teams to manage their operations from end to end, respond to cyber threats with speed and precision and get smarter with every analyst interaction. Founded in 2015 by Israeli Intelligence experts, with extensive experience running and training security operations centers worldwide, Siemplify has raised $58 million in funding to date and is headquartered in New York, with offices in Tel Aviv.

Learn more at **https://www.siemplify.co** and sign up for a free trial in the CrowdStrike Store.

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**