CrowdStrike Store

RAPID7

CROWDSTRIKE

Data Sheet

RAPID7: INSIGHTIDR FOR FASTER THREAT DETECTION

Accelerate threat discovery, investigation and response by combining the power of CrowdStrike Falcon with Rapid7's leading software-as-a-service (SaaS) SIEM

CHALLENGES

Security teams are facing constant and accelerated change, from monitoring remote teams to sprawling attack surfaces and fast-moving threat landscapes — and the only thing certain is uncertainty for security operations center (SOC) teams. But many tools today make it unnecessarily challenging for teams to be agile or to scale with the needs of their modern environments.

In fact, many legacy tools intended to help teams monitor their environments often make it more difficult, as teams are caught in the weeds of rule configuration, operations, hardware setup, chasing false positives and constantly switching context to stitch together the full picture. This noise distracts analysts from real threats, leaves teams vulnerable to attack and makes it nearly impossible to effectively respond to threats.

SOLUTION

InsightIDR, Rapid7's software-as-a-service (SaaS) security information and event management (SIEM) tool, integrates with CrowdStrike Falcon Insight™ endpoint detection and response (EDR) to unite endpoint telemetry and detections alongside user, network, cloud, deception technology and other critical security alerts, providing a powerful and comprehensive view of the environment.

Leveraging InsightIDR's attribution engine, every endpoint alert is enriched with user and asset information, giving analysts a single efficient view of the complete threat impact. The investigations timeline also aggregates related events from around the environment, so that SOC teams can quickly understand the scope of the attack. By combining InsightIDR and Falcon Insight, teams can focus on what matters most: finding and remediating threats fast, no matter where they start.

KEY BENEFITS

Accelerate your time to value by leveraging Falcon Insight EDR to ingest endpoint telemetry into InsightIDR

Get the complete picture with all of your critical security data in one place: endpoint, user, network, cloud, deception technology and other critical security alerts

Respond faster with user and asset attribution on every alert, and with relevant events across the entire environment pulled into a single investigation timeline

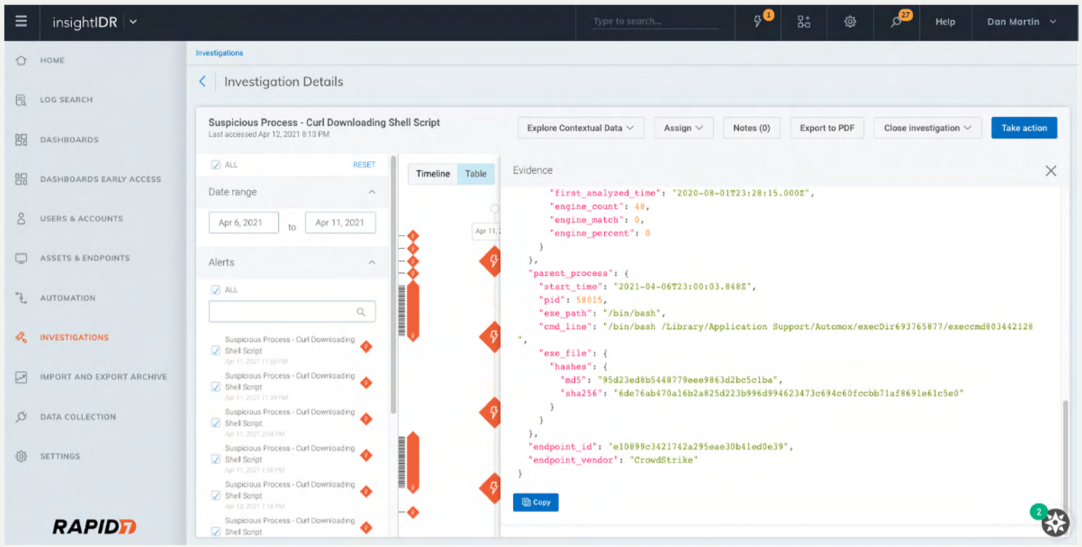
RAPID7: INSIGHTIDR FOR FASTER THREAT DETECTION

BUSINESS VALUE

Use Case / Challenges	Solution	Benefits
Complete environment coverage: Analysts have a limited view of the environment and jump between many tools, causing inefficiencies.	InsightIDR combines alerts and telemetry from the CrowdStrike Falcon® platform, alongside user, network, cloud and deception technology and other security alerts.	By combining CrowdStrike's endpoint capabilities with InsightIDR's detections from across the environment, analysts have a single, comprehensive view and can more effectively identify and respond to threats.
High-fidelity detections: Teams are plagued with false positives that exhaust resources and distract from real threats.	Rapid7's global managed detection and response (MDR) SOC experts and data science teams manage and curate InsightIDR's out-of-the-box detections library.	With expertly vetted detections and Rapid7's attribution engine marrying events across the network to users and assets, analysts have the context and information they need to act with confidence.
Investigation details and automation: Once a security event has happened, many teams are unsure of what to do next.	InsightIDR provides a complete timeline of all events related to an attack, and with security orchestration and automation (SOAR) from Rapid7 InsightConnect, customers can immediately kick off workflows to isolate and respond to threats.	When an attack inevitably happens, InsightIDR enables teams to have the context, guidance and tools to understand the complete impact and extinguish threats quickly and thoroughly.

TECHNICAL SOLUTION

1. Falcon Insight EDR collects enriched endpoint telemetry data
2. Falcon Insight integrates with the Rapid7 Insight cloud to ingest data into InsightIDR
3. Security teams can investigate and respond to threats from across the entire environment in a single hub



KEY CAPABILITIES

- Accelerate next-gen SIEM deployment with enriched data from the Falcon platform
- Eliminate blind spots with a complete view of your environment in one place
- Find and respond to threats faster, with automation, reliable alerting and correlated events in a single timeline

ABOUT RAPID7

Organizations around the globe rely on Rapid7 technology, services and research to securely advance. The visibility, analytics and automation delivered through its Insight cloud simplifies the complex and helps security teams reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks.

InsightIDR — Rapid7's cloud-native SaaS SIEM — leverages insights from Rapid7's global services and threat intelligence network, to provide highly reliable out-of-the-box detections across modern, hybrid environments. With InsightIDR, customers have the scale they need to grow, the expert coverage to detect stealthy threats early and reliably, and the context and automation to respond quickly and confidently.

Learn more: **https://www.rapid7.com/insightidr**

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.