D3 SECURITY

CROWDSTRIKE

CrowdStrike Solution Brief

Consolidate without Compromise

Orchestrate intelligent endpoint protection and automated incident response.

CHALLENGES

Many security teams are consolidating their product suite in order to increase integration between tools. They have pursued a best-in-class approach and are now seeing blind spots between tools where linked attacks go unnoticed because detection platforms do not share data. At the same time, users are getting overwhelmed switching between tools and trying to consolidate all relevant information on an alert.

SOLUTION

D3 Smart SOAR integrates with hundreds of security tools, consolidates alert and IoC data into a single platform and automates actions across each individual tool in an environment. This means that users can see all relevant data on an alert in one place and decide how they want to contain the threat. If they want to block an email address, flag an IP, or delete a file from a device they can do it all from a single platform. Security teams no longer need to choose between consolidation and deploying the best solutions in their category.

BUSINESS VALUE

USE CASE CHALLENGE	SOLUTION DESCRIPTION	BENEFITS
Overwhelm Due to Alert Fatigue	Automate alert triaging based on severity and context.	Filter out the noise and focus on high-priority alerts. Automation saves time and allows for quicker threat mitigation.
Difficulty in Threat Hunting	Schedule automated playbooks that run complex queries across multiple data sources to identify potential threats.	Move from reactive to proactive threat identification. Automated threat hunting significantly reduces the time spent on manual queries.
Inefficient Incident Response	Execute predefined playbooks to take immediate actions like isolating affected endpoints using CrowdStrike, all from within the D3 platform.	Execute complex workflows with the click of a button. Conduct all incident response activities from a single interface.

KEY BENEFITS

No more context/tool switching: Consolidate all incident response and threat intel into a single platform.

Faster and more efficient endpoint protection and response: Leverage API-integrations to all of your security tools to automate actions between them.

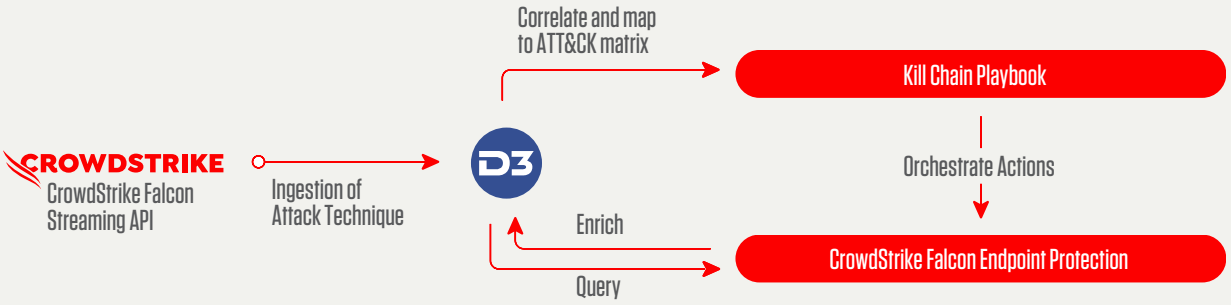
Multi-vendor environments: No limitation to api-based integrations between tools.

Cross-Stack Correlation: Compare indicators of compromise from email, network, and endpoint security data.

TECHNICAL SOLUTION

D3's automated playbooks can be configured to utilize CrowdStrike's Falcon endpoint data, enabling automated or semi-automated threat hunting activities.

D3 SOAR's playbooks are integrated with CrowdStrike's Falcon API, allowing for a range of automated actions, such as endpoint isolation or file quarantine, to be executed directly from the D3 platform.



TECHNICAL SOLUTION

- **Automated Alert Triage:**
  Intelligent sorting of alerts based on severity and context.
- **Proactive Threat Hunting:**
  Schedule automated playbooks to run complex queries and identify hidden threats.
- **Streamlined Incident Response:**
  Execute predefined playbooks for quick containment and remediation actions.

> "D3 was the single vendor that had the most integrations to third-party systems, so in the long run, it will be much cheaper for us to use.
>
> Karsten Thygesen, Chief Technology Officer, Trifork Security

ABOUT D3 SECURITY

D3 SOAR is an award-winning platform for security orchestration, automated investigation and incident response. Think of it like connective tissue for the SOC—D3 ingests events from across the security infrastructure, assesses their criticality, and triggers incident-specific response plans.

Feature-rich integrations with CrowdStrike tools make D3 the perfect command center for event intake, threat intelligence enrichment, malware analysis, and orchestrating actions across endpoints. D3's automation-powered playbooks, MITRE ATT&CK framework, and deep investigative capabilities bring effective and repeatable workflows to all events in your environment.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), 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 two 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.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Learn more: **https://www.crowdstrike.com/**