CrowdStrike Integration

DARKTRACE

KEY INTEGRATION FEATURES:

- Retrieve regular endpoint data, including CVE risks, for analysis within Darktrace
- Pull Falcon data for analysis in AI Analyst, triggering both a Darktrace model breach and AI Analyst investigation around high-fidelity CrowdStrike alerts
- Customers with RESPOND/Network can trigger CrowdStrike device quarantines within Darktrace UI via the Falcon Endpoint Protection agent
- Use information from Falcon Spotlight to improve attack path modeling and risk mitigation prioritization in Darktrace PREVENT/E2E

Bidirectional communication between Darktrace and CrowdStrike Falcon API increases the scope and detail of detections and agility in response across endpoints. The integration reduces the need to switch between consoles for investigations, and brings enterprise-wide context and machine learning to endpoint alerts.

DARKTRACE
CROWDSTRIKE

Setting Up the Integration

The Darktrace CrowdStrike integration retrieves data on devices, security events and CVEs from the CrowdStrike Falcon API. Authentication requires the creation of an API client in the Falcon platform and the details provided to Darktrace.

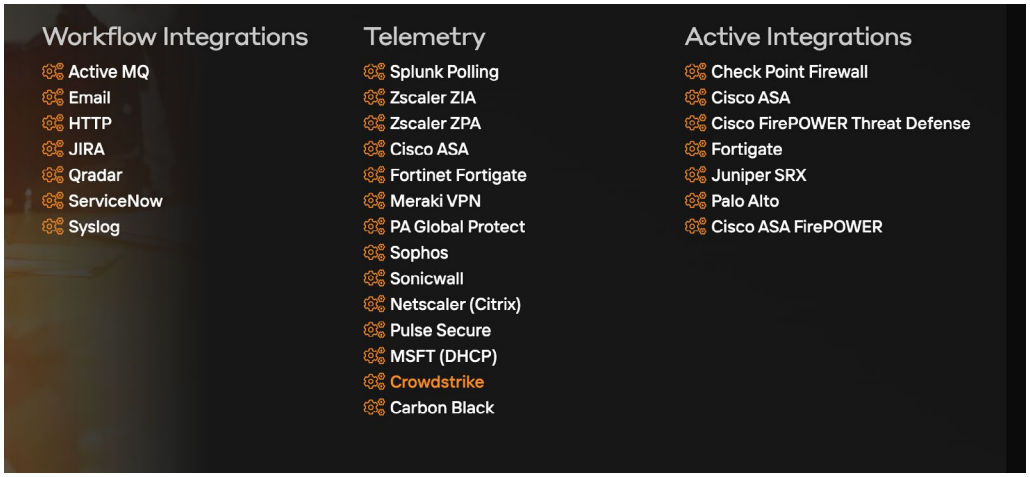

Figure 1: The integration set up within Darktrace's Customer Portal

DARKTRACE DETECT™

Enhance Detection with CVE Data and CrowdStrike Alerts

The integration matches network devices present in the CrowdStrike Falcon platform with those also observed by Darktrace. Matched devices are then enriched in the Threat Visualizer with vulnerability data and, if applicable, CrowdStrike security events.

CVE vulnerability data is retrieved from Falcon Spotlight every 24 hours. This data is added to Device Summary in the Threat Visualizer interface and, where present, shared with Darktrace PREVENT/End-to-End to enhance attack path modelling analysis.

Devices are also tagged to indicate the highest severity category of CVE currently detected by CrowdStrike on the device. CrowdStrike generates security alerts for activity on endpoint devices which are retrieved by the module at regular intervals (default 60 seconds). These events are populated in Darktrace Advanced Search (@type: crowdstrike), inserted into the event log of matched devices referenced in the event and available to Darktrace models.

DARKTRACE RESPOND™

Manually Trigger a CrowdStrike Device Quarantine via the Darktrace UI

Organizations with Darktrace RESPOND can also trigger a manual "Isolate Machine" action against eligible devices using the integration. If activated, Darktrace will instruct CrowdStrike to isolate the device from the network (network contain) using the Falcon Endpoint Protection agent for the time chosen.

DARKTRACE AI ANALYST™

Bring Enterprise-Wide Context to Endpoint Alerts

Darktrace can use EDR alerts as starting points for its investigation, with every EDR alert ingested now triggering AI Analyst. Darktrace takes low-level alerts and investigates around it – drawing from data across cloud, apps, and the network, and try to conclude whether there is more to this EDR alert.

If concludes the EDR alert is part of a bigger incident, Darktrace will generate a report that appears clearly in the UI and can be directly downloaded as a PDF to be shared with other stakeholders. This further automates security operations and alleviates pressure on human teams,

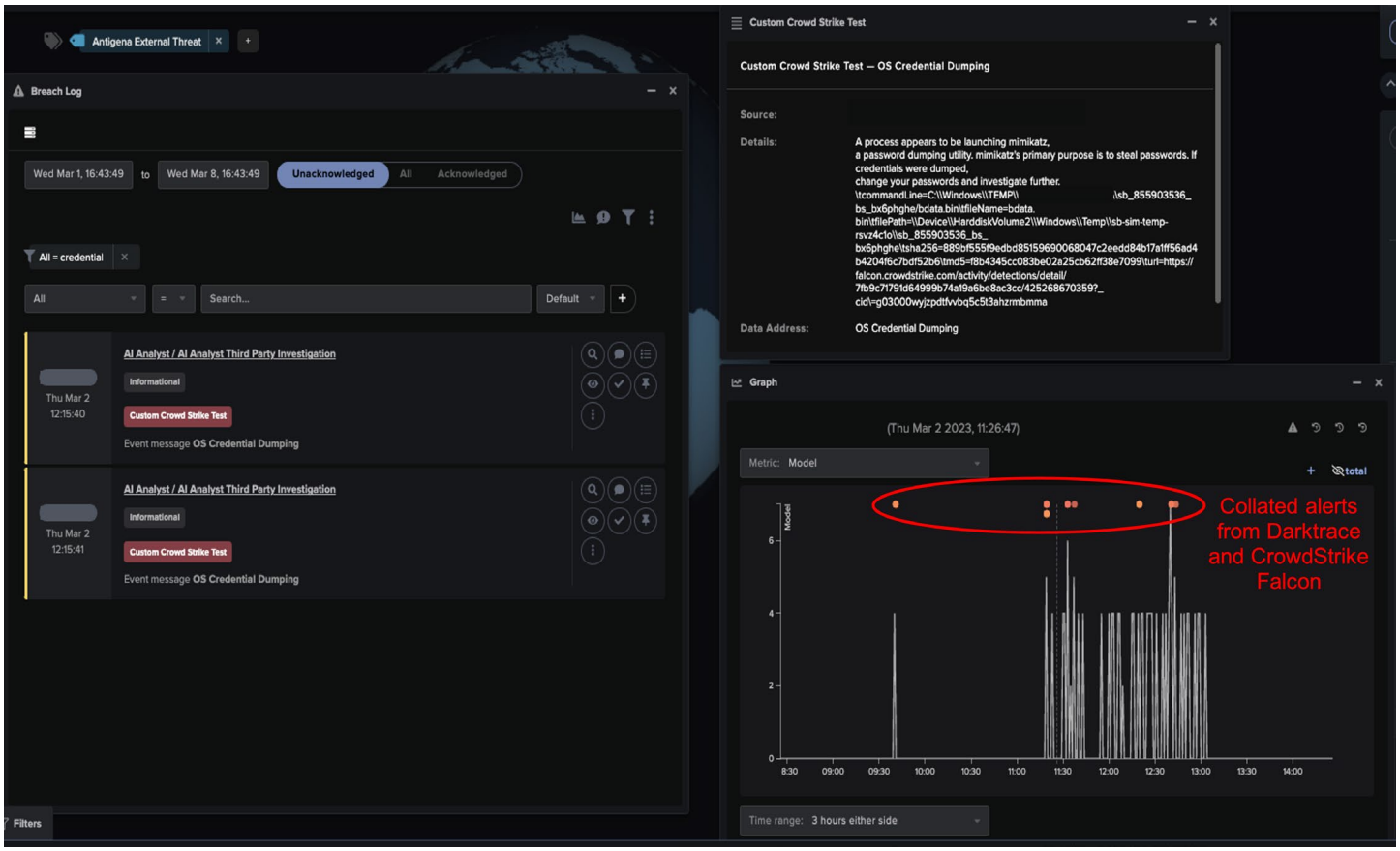

Figure 2: Simulated Mimikatz test run through Darktrace and CrowdStrike Integration. Alerts from both network and the endpoint are collated in one place thanks to AI Analyst.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,100 organizations globally from advanced cyber-threats.

Scan to LEARN MORE