CROWDSTRIKE

Medium Enterprise Pharmaceuticals Company

Introduction

This case study of a medium enterprise pharmaceuticals company is based on a November 2023 survey of CrowdStrike Threat Intelligence customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

> "One more step closer to validating the exposed data and threat actor."
>
> "Pre-filter results with follow-up calls with analysts are helpful."

Challenges

The business challenges that led the profiled company to evaluate and ultimately select CrowdStrike Threat Intelligence:

- What challenges did you or your team experience before using Falcon Intelligence Recon+?
  - Our current detection capabilities were mostly internal and we were concerned about underground threats
  - We were concerned about brand abuse on social media or forums
  - We were concerned about risks to VIPs or executives mentioned on forums

Use Case

The key features and functionalities of CrowdStrike Threat Intelligence that the surveyed company uses:

- The surveyed user is part of the Cyber Security Oversight & Risk Team.
- Which features of Falcon Intelligence Recon+ do you find most useful?
  - Assistance from CrowdStrike experts pre-filtering alerts
  - Domain "take-down" reports and assistance

Results

The surveyed company achieved the following results with CrowdStrike Threat Intelligence:

- Why did you choose CrowdStrike Falcon Intel Recon + over others?
  - Assistance from CrowdStrike analysts
  - Recon + covers multiple use cases, valuable to multiple teams without an increase in costs
- Please rate the following capabilities of CrowdStrike Falcon Intel Recon+ compared to the competition:
  - Continuous coverage of underground forums, marketplaces, etc: Better
  - Discovery of typo squatted domains: Better
  - Monitoring assistance from CrowdStrike Experts: Significantly Better
  - User Experience via Falcon Portal: Better
  - Notification capabilities to other members inside our outside the team: Better
  - Vulnerability Intelligence: Better
- What benefits did your organization realize following the deployment of CrowdStrike Falcon Intelligence Recon+?
  - Improved awareness of key eCrime trends (Ransomware campaigns, Access Broker trends …)
  - We can inform our leadership more reliably about emerging threats as they unfold
- In your best estimate, by what percent did CrowdStrike improve the following?
  - Improved our threat risk awareness: 50-75%
  - Increased depth of incident investigations: 50-75%
  - Helped to mitigate external threats before they became a problem: 25-50%
  - Reduced our global risk posture: 25-50%
  - Improved effectiveness of our patching efforts: 50-75%

Company Profile

The company featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Company Size:
Medium Enterprise

Industry:
Pharmaceuticals

About CrowdStrike Threat Intelligence

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:

CrowdStrike

CrowdStrike Threat Intelligence