ThreatSTOP & CrowdStrike:
Extending Falcon Protection to the Entire Network

Block APT Attacks Automatically

The threat landscape changes fast, but ThreatSTOP and CrowdStrike's integrated solution moves even faster to mitigate serious threats.

By leveraging security and threat intelligence automation, new emerging Indicators (IOCs) identified by CrowdStrike can be added to firewall and DNS rules at machine speed, outpacing threat actors and their efforts to avoid detection. Complete your continuous 360-degree breach prevention by extending Falcon coverage to every device, even IoT and agent-less hosts.

Close the Gap, Protect Everything

Full coverage requires network-layer IP and DNS protection that protects every endpoint, even those traditionally hard to secure such as IoT, BYOD and guest devices where Falcon Host can't be easily deployed.

The solution creates an automated bridge between Falcon X and existing, customer-owned network enforcement devices like Firewalls, Routers and DNS servers. This SaaS automation ensures IP connections and DNS requests related to threats and actors identified by CrowdStrike are proactively blocked and reported.

Joint Solution Features

- Broad compatibility allows easy, rapid deployment to your security stack
- Real-time Falcon X intelligence applied as dynamic network traffic policy
- Automated threat blocking and policy updates, no manual effort
- Custom black-and-white listing, accepts custom 3rd party TI feeds
- Advanced web reporting shows blocked threats and devices involved
- Granular policy customization built upon more than 900 TI feeds

Instant Security from Threat Intelligence

Unlike traditional threat intelligence implementations where indicators are used reactively in assessing attacks and threats that have already entered the network, ThreatSTOP and CrowdStrike's integrated solution uses highly accurate, award-winning threat intelligence to proactively defend networks and stop breaches before they can happen. Thanks to the cloud native platforms and automation, this is accomplished with no new hardware or hands-on effort.

Solve Security Challenges

Challenge:

Anticipating and preventing attacks before they happen by proactively blocking communication with high confidence IoCs yields significant security results, but accomplishing it requires large multi-vendor purchases and skilled dedicated staff to manage it.

Solution:

Leverage the power of automation that delivers real time operationalized threat intelligence as a cloud-based integration between CrowdStrike's Falcon X Intelligence and your existing firewalls, routers, DNS servers, and more.

Customer Benefit:

By automating real-time updates to network traffic enforcement points , security teams can ensure their network doesn't communicate with threat actors and the infrastructure used to carry out attacks. Protection is proactive and instantaneous, removing the time-consuming and manual workflows that otherwise increase false positives and dwell time.

Evaluate the integrated solution in your own network.
Start a trial today at: www.threatstop.com/crowdstrike