



Bi-Directional Integration Delivers Complete Endpoint Visibility and Protection

Businesses face an increasingly complex threat landscape. Cloud, cloud applications, and the internet of things (IoT) only complicate the situation. A harmonized and integrated security platform is the only way for organizations to stay ahead.

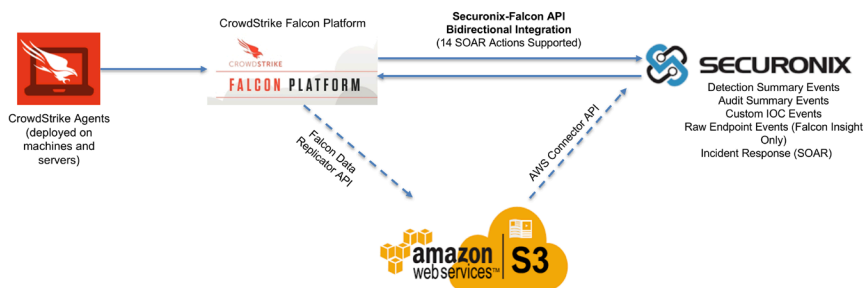
The Securonix platform delivers unlimited scale, powered by advanced analytics, behavior detection, threat modeling, and machine learning. It increases your security through improved visibility, actionability, and security posture, while reducing management and analyst burden.

CrowdStrike Falcon endpoint protection unifies the technologies required to successfully stop breaches, including next-generation antivirus, endpoint detection and response, IT hygiene, 24/7 threat hunting, and threat intelligence.

When integrated, Securonix and CrowdStrike provides continuous breach prevention in a single agent and proactively detects viruses, malware, ransomware, and other known and unknown threats.

Solution Benefits

- Analyze endpoint threats in the wider context of the organization in order to identify advanced threats.
- Use endpoint user data to enrich behavioral analysis and add additional depth to your security analytics.
- Identify and mitigate risks related to insider behavior activity.
- Proactively detect and respond to virus, malware, ransomware, and other known and unknown threats.

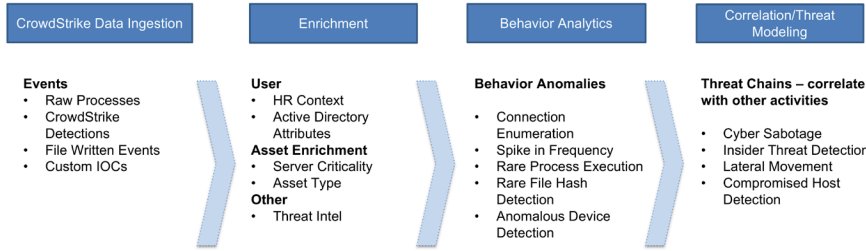


Securonix CrowdStrike API Integration

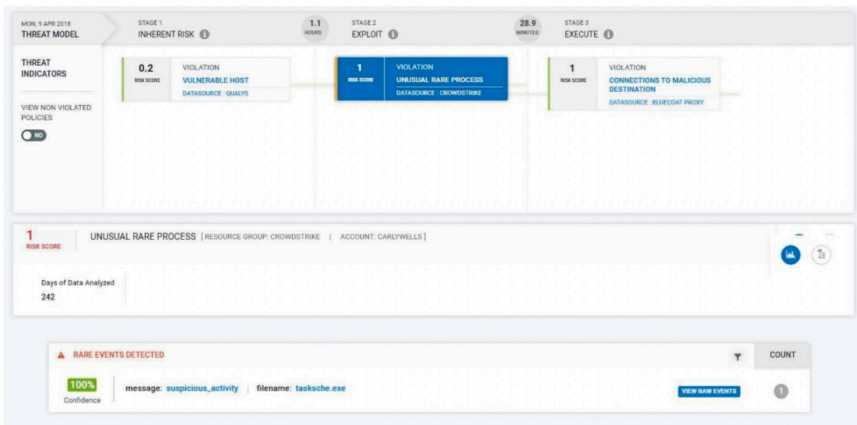
Securonix integrates with multiple CrowdStrike APIs in order to detect and respond to threats. Each API provides a separate subset of information.

Crowdstrike API	Data Ingested/Sent	Description
Falcon Streaming API	Real time detections and audit events from CrowdStrike	The Falcon Streaming API allows collection of real-time events and alerts from instances as they occur within a single data stream, providing a low-latency, high throughput delivery mechanism
Falcon Data Replicator (requires Falcon Insight)	Raw events from endpoints and servers	The Falcon Data Replicator API allows extraction of all raw events from endpoint data. This data can be used for correlation with other security feeds.
Falcon Query API	Bidirectional integration with Custom IOCs, information gathering and management of detection status	The Falcon Query API allows bidirectional integration with <ul style="list-style-type: none"> • Upload of IOCs (Indicators of Compromise) for monitoring • Device information about systems with the Falcon agent installed • Searches for IOCs and related processes • Management of detection status • Automate incident response actions

Securonix collects CrowdStrike security events in real time and enriches them with additional data for further analysis. Securonix behavior analytics uses self-learning to baseline normal behavior patterns and detect anomalous threats.



Securonix assigns a risk score to events. Based on the context of the user's behavior, it can elevate the risk score. Threats with a risk score above a set threshold can trigger predefined threat playbook actions to mitigate the threat.



Integration with the Falcon Query API allows for 14 different security orchestration automation and response (SOAR) actions including:

- **IOCs:** Create, Get, Get Details, Update, and Delete
- **Threat Hunting:** Hunt File, Domain
- Process Information and Details
- Device Details
- Detection Details, Detection Search, Set Detection State, and Detection Aggregates

Securonix also uses CrowdStrike endpoint data to create data insights and visualize cybersecurity threats, risks, and compliance metrics.

Combined, Securonix and CrowdStrike provide visibility, analytics, and response protection to mitigate risks related to insider behavior activity.

Use Cases

- Abnormal number of high severity endpoint alerts.
- Rare command parameters, rare file hashes, rare process and path, and rare ports used by a process. (All high severity endpoint alerts.)
- Use of credential dumper endpoints.
- Virus and malicious code outbreaks.
- Vulnerable endpoint monitoring.
- Infected endpoint monitoring.
- IOS buffer overflow.
- Possible malware outbreak. (Same infection on multiple hosts.)
- Abnormal number of services created.
- Suspicious DLL injections observed.

About CrowdStrike

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence, the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. For more information visit www.crowdstrike.com.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.