securonix

CROWDSTRIKE

SOLUTION BRIEF

Bi-Directional Integration Delivers Complete Endpoint Visibility and Protection

An Integrated Approach to Prevent Breaches

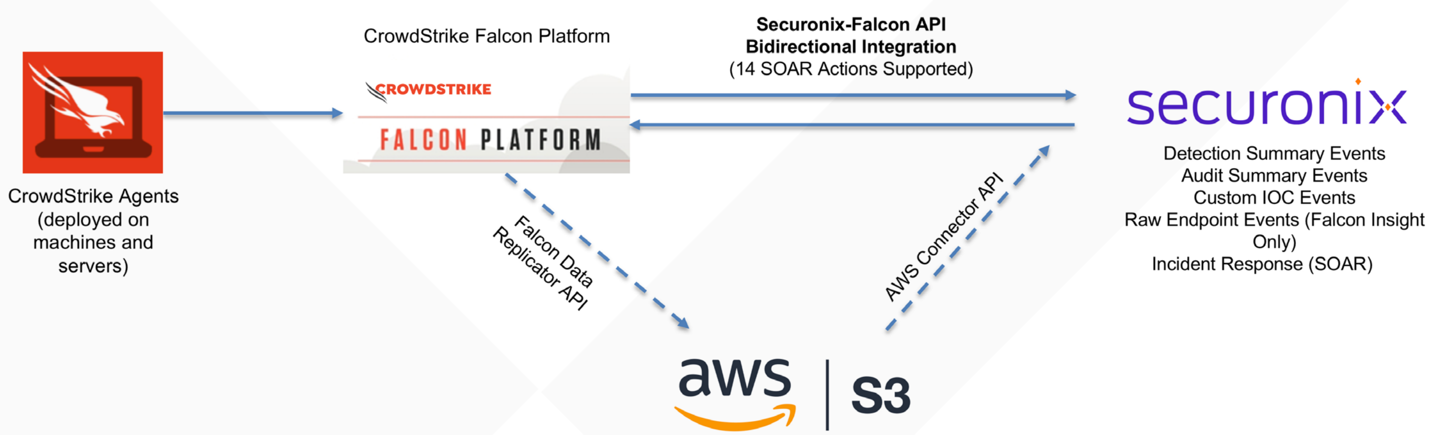
Businesses face an increasingly complex threat landscape. Cloud, cloud applications, and the internet of things (IoT) only complicate the situation. A harmonized and integrated security platform is the only way for organizations to stay ahead.

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.

Securonix and CrowdStrike Integrated Architecture


CrowdStrike Agents (deployed on machines and servers)
CrowdStrike Falcon Platform
CROWDSTRIKE
FALCON PLATFORM
Securonix-Falcon API
Bidirectional Integration
(14 SOAR Actions Supported)
securonix
Detection Summary Events
Audit Summary Events
Custom IOC Events
Raw Endpoint Events (Falcon Insight Only)
Incident Response (SOAR)
Falcon Data Replicator API
AWS Connector API
aws
S3

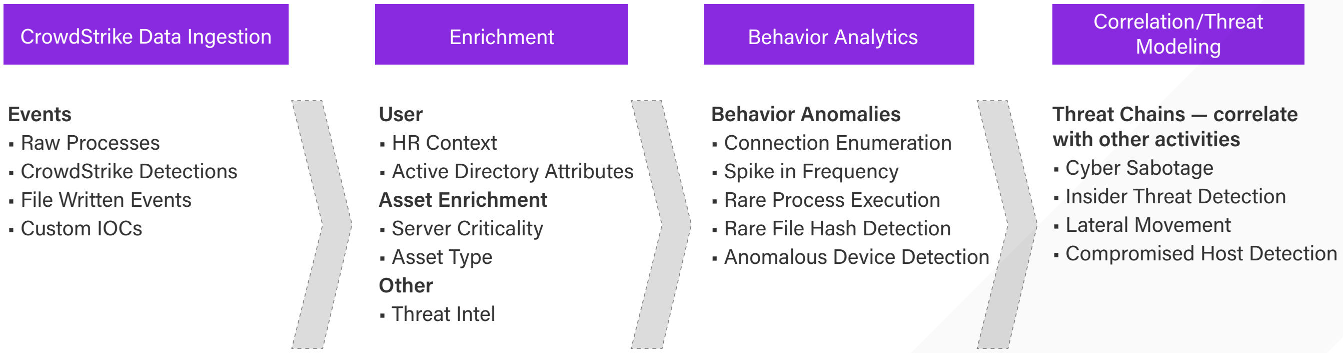
Securonix CrowdStrike API Integration

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, imformation gathering and management of detection status	The Falcon Query API allows bidirectional integration with ▪ 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

Shared Deployment Model for Risk Mitigation

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.



CrowdStrike Data Ingestion

Events
- Raw Processes
- CrowdStrike Detections
- File Written Events
- Custom IOCs

Enrichment

User
- HR Context
- Active Directory Attributes

Asset Enrichment
- Server Criticality
- Asset Type

Other
- Threat Intel

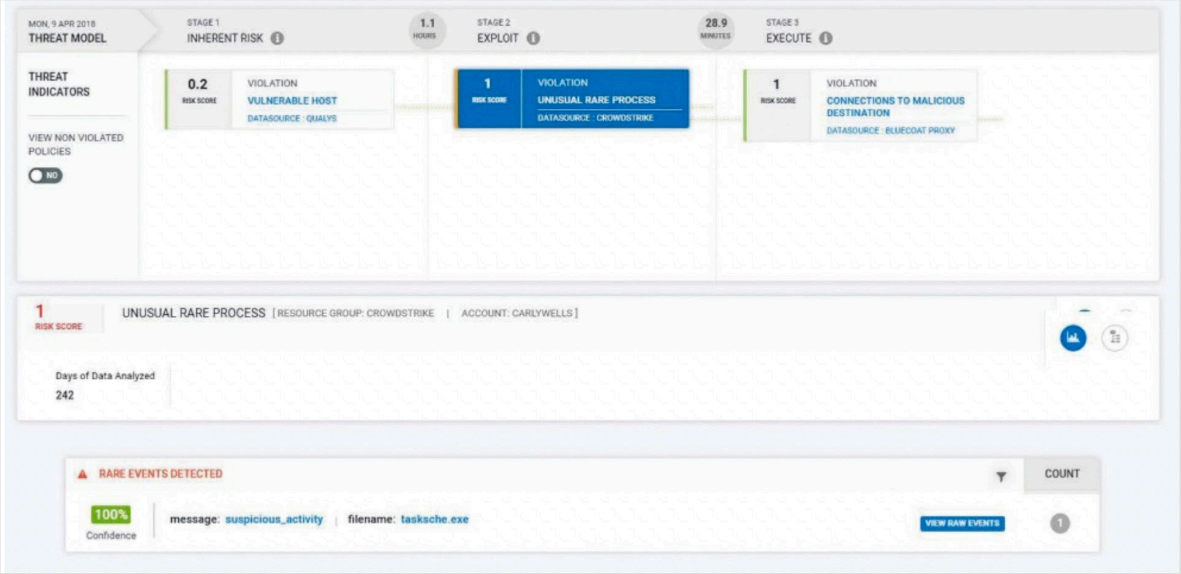
Behavior Analytics

Behavior Anomalies
- Connection Enumeration
- Spike in Frequency
- Rare Process Execution
- Rare File Hash Detection
- Anomalous Device Detection

Correlation/Threat Modeling

Threat Chains — correlate with other activities
- Cyber Sabotage
- Insider Threat Detection
- Lateral Movement
- Compromised Host Detection

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.



MON, 9 APR 2018
THREAT MODEL

STAGE 1 INHERENT RISK — 1.1 HOURS — STAGE 2 EXPLOIT — 28.9 MINUTES — STAGE 3 EXECUTE

THREAT INDICATORS

0.2 RISK SCORE — VIOLATION: VULNERABLE HOST — DATASOURCE : QUALYS

1 RISK SCORE — VIOLATION: UNUSUAL RARE PROCESS — DATASOURCE : CROWDSTRIKE

1 RISK SCORE — VIOLATION: CONNECTIONS TO MALICIOUS DESTINATION — DATASOURCE : BLUECOAT PROXY

VIEW NON VIOLATED POLICIES: NO

1 RISK SCORE — UNUSUAL RARE PROCESS [RESOURCE GROUP: CROWDSTRIKE | ACCOUNT: CARLYWELLS]

Days of Data Analyzed: 242

RARE EVENTS DETECTED

100% Confidence — message: suspicious_activity | filename: tasksche.exe — COUNT 1

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.

Solution Benefits

- **Analyze endpoint threats** in wider context of the organization in order to identify advanced threats.
- Use endpoint user data to **enrich behavioral analysis** and add additional depth to our 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.

Use Cases

- Abnormal numbeer 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 Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.
For more information visit securonix.com

About CrowdStrike

CrowdStrike is a global cybersecurity leader that 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, 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, the Falcon platform enables partners to rapidly build best-in-class integrations to deliver customer-focused solutions that provide scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value. For More Information visit www.crowdstrike.com