CrowdStrike Marketplace

ArcSight Intelligence
by opentext

CROWDSTRIKE

Data Sheet

# ArcSight Intelligence: Endpoint Data and Behavioral Analytics

Swiftly reveal hidden and unknown threats, including insiders and advanced persistent threats (APTs)

## Challenge

Some threats, such as insider threats and targeted outside attacks, are notoriously difficult to detect. These “unknown” threats manifest in complex ways and avoid detection because they don’t have fixed signatures or known patterns of attack by which they can be easily spotted. Instead, they often fly under the radar by purposely or inadvertently leveraging privileged access to commit fraud, sabotage operations or swipe intellectual property.

## Solution

ArcSight Intelligence allows your security team to see detailed and accurate CrowdStrike Falcon® endpoint data using behavioral intelligence to detect threats or actors that may be hiding in your enterprise. By shining a new light on user information — abnormal login frequency, unexpected day or time of work, unusual machines — ArcSight Intelligence’s behavioral analytics add valuable context to help you see threats that you might otherwise miss. With the right user context, you can detect unusual login patterns, sudden or unusual file or system activity, user impersonation, internal reconnaissance, or “low and slow" attacks. Once identified, threat leads can be passed on to your security team or the CrowdStrike® Falcon OverWatch™ managed threat hunting service for further investigation.

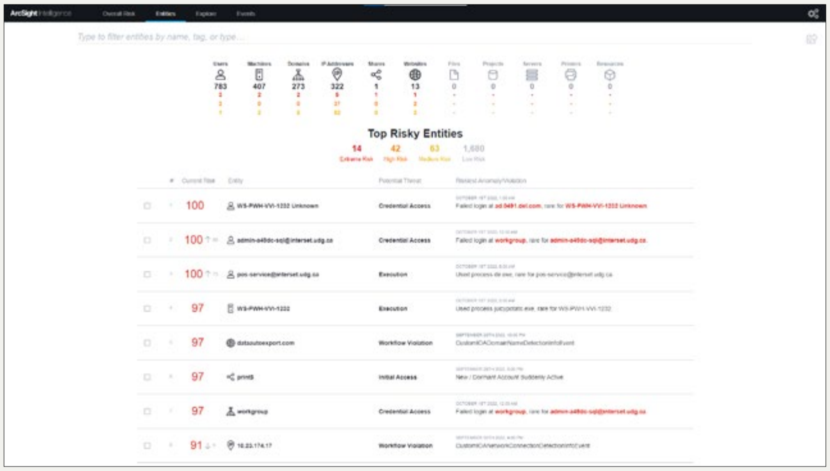
Getting started with the combined analytical powers of ArcSight Intelligence’s behavioral analytics with the rich Falcon sensor data from CrowdStrike couldn’t be easier. Simply visit the CrowdStrike Marketplace at **marketplace.crowdstrike.com** and click on the ArcSight Intelligence application. Once you click the “Try it free” button, ArcSight Intelligence automatically gains access to your Falcon sensor data. There’s no software to deploy, no machines to manage—everything happens on your behalf in the cloud. After 30 days of data collection, ArcSight Intelligence’s machine learning engine has all it needs to begin detecting anomalous activities in your Falcon data that may be threatening your organization. You are then provided with access to ArcSight Intelligence’s state-of-the-art threat hunting user interface, which highlights instances of risky anomalous behaviors and provides prioritized lists of the riskiest entities in your organization.

## Key Benefits

Combine rich CrowdStrike Falcon endpoint data with advanced behavioral analytics to uncover traditionally difficult-to-find threats.

Detect insider threats or targeted attacks by learning the normal, unique behavior of every entity and detecting the most unusual or suspicious behaviors

Distill billions of endpoint events into a list of prioritized threat leads, reducing alert fatigue and allowing you to focus on the threats that matter



| Users | Machines | Domains | IP Addresses | Shares | Websites | Files | Projects | Servers | Printers | Resources |
|---|---|---|---|---|---|---|---|---|---|---|
| 783 | 407 | 273 | 322 | 1 | 13 | 0 | 0 | 0 | 0 | 0 |
| 2 | 2 | 2 | 5 | 1 | 1 | - | - | - | - | - |
| 3 | 0 | 0 | 27 | 0 | 2 | - | - | - | - | - |
| 1 | 2 | 8 | 52 | 0 | 2 | - | - | - | - | - |

Top Risky Entities

| 14 | 42 | 63 | 1,680 |
|---|---|---|---|
| Extreme Risk | High Risk | Medium Risk | Low Risk |

| # | Current Risk | Entity | Potential Threat | Related Anomaly/Violation |
|---|---|---|---|---|
| □ | 100 | WS-PWH-VVI-1232 Unknown | Credential Access | [illegible]<br>Failed login at ad.0491.del.com, rare for WS-PWH-VVI-1232 Unknown |
| □ | 100 ↑ | admin-a48dc-sql@interset.udg.ca | Credential Access | [illegible]<br>Failed login at workgroup, rare for admin-a48dc-sql@interset.udg.ca. |
| □ | 100 ↑ | pos-service@interset.udg.ca | Execution | [illegible]<br>Used process dir.exe, rare for pos-service@interset.udg.ca |
| □ | 97 | WS-PWH-VVI-1232 | Execution | [illegible]<br>Used process juicypotato.exe, rare for WS-PWH-VVI-1232 |
| □ | 97 | datautoexport.com | Workflow Violation | [illegible]<br>CustomIOADomainNameDetectionInfoEvent |
| □ | 97 | print$ | Initial Access | [illegible]<br>New / Dormant Account Suddenly Active |
| □ | 97 | workgroup | Credential Access | [illegible]<br>Failed login at workgroup, rare for admin-a48dc-sql@interset.udg.ca |
| □ | 91 ↓ | 10.23.174.17 | Workflow Violation | [illegible]<br>CustomIOANetworkConnectionDetectionInfoEvent |

## Use Cases

- **Find insider threats:** Leveraging CrowdStrike's rich endpoint data, ArcSight Intelligence can help uncover malicious or negligent insiders by learning the "unique normal" behavior of each and every user or entity in your enterprise and identifying new behaviors that are unusual or suspicious.
- **Discover targeted attacks:** Outsider attacks can often present "insider" characteristics. For example, an attacker may use valid credentials to infiltrate a system and swipe high-value data. ArcSight Intelligence identifies the behavioral leads within Falcon endpoint data that may indicate a bad actor has gained access to your network or systems.

## Key Capabilities

- **Anomaly detection with advanced analytics:** ArcSight Intelligence leverages built-in unsupervised machine learning models to extract available entities (users, machines, IP addresses, servers, printers, etc.) from within log files and observe relevant events to determine expected behavior. New events are evaluated against previously observed behavior, as well as the behavior of a user's or entity's peers, to assess potential risk.
- **Focused investigation with prioritized threat leads:** ArcSight Intelligence combines unsupervised machine learning with mathematical probability to calculate risk scores that will tell you which entities are the most suspicious.
  This allows ArcSight Intelligence to distill billions of events into a handful of prioritized threat leads, eliminating alert fatigue and allowing you to focus on investigating the threats that really matter.

## About ArcSight Intelligence

ArcSight Intelligence, previously recognized as Interset, gives security teams a new lens through which to find and respond to difficult-to-find insider threats or targeted outside attacks. Bypassing rules andthresholds, ArcSight Intelligence uses unsupervised machine learning to measure the unique digital footprint of systems and users. ArcSight Intelligence then distills billions of events into a prioritized list of high-quality security leads to focus and accelerate the efforts of the security operations center (SOC). What used to take months, can now take minutes. Learn more and request a trial of ArcSight Intelligence at www.arcsight.com/intelligence.

**Start a Free Trial**

Learn more at **www.crowdstrike.com**

For an online consumer retailer, ArcSight Intelligence combined with rich CrowdStrike Falcon endpoint data — process, user and machine activity — detected a well-executed red team attack. The customer was able to uncover the entire attack lifecycle via behavioral indicators, giving the company's security team the right context to respond to the attack. The following attack characteristics were identified:

- Compromised accounts
- Remote exploit
- OWA profiling
- Password guessing
- Lateral movement
- IP address and attack tool

## About CrowdStrike

**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.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**