Find Unknown Threats with ArcSight Intelligence for CrowdStrike

Swiftly reveal hidden threats with endpoint data and behavioral analytics.

CrowdStrike and ArcSight Intelligence at a Glance:

Uncover:

Combine rich CrowdStrike endpoint data with advanced Behavioral Analytics to uncover traditionally difficult-to-find threats.

Detect:

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

Respond:

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.

Introduction

The combined analytical powers of ArcSight Intelligence's Behavioral Analytics with the rich Falcon sensor data from CrowdStrike enables visibility of hard-to-find threats inside your organization. And, it couldn't be easier to get started. Simply log in, head over the CrowdStrike App Store, 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 insider threats and anomalous activities in your CrowdStrike data, which may be threatening your organization. You are then provided with access to ArcSight Intelligence's state-of-the-art threat hunting user interface that highlights instances of risky anomalous behaviors and prioritized lists of the riskiest entities in your organization.

If you are worried you won't have the time or staff to monitor ArcSight Intelligence's insights—don't worry! ArcSight Intelligence offers an optional add-on threat hunting service comprised of a team of security professionals who provide ongoing threat hunting on a weekly, bi-weekly, or daily schedule. In addition, ArcSight Intelligence's extensible API enables your team to orchestrate event notifications to your existing "pane of glass", ticketing systems and even your SOAR platform.

Challenges

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

Micro Focus ArcSight Intelligence allows your security team to see CrowdStrike Falcon's detailed and accurate 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, date or time of work, unusual machines—ArcSight Intelligence adds 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 recon, or low and slow attacks. Once identified, threat leads can be passed on to your security team or the CrowdStrike OverWatch service for further investigation.

Contact us at **CyberRes.com**
Like what you read? Share it.

Use Cases

- **Find insider threats:** Leveraging CrowdStrike's rich endpoint data, ArcSight Intelligence behavioral analytics can help uncover malicious or negligent insiders by learning the "unique normal" behavior of each and every user or entity in your enterprise and by 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 CrowdStrike's 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 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 or entity's peers, to assess potential risk.
- **Focused investigation with prioritized threat leads:** ArcSight Intelligence behavioral analytics 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.

Customer Testimonial

At a major hospitality company, ArcSight Intelligence utilized rich CrowdStrike Falcon endpoint data—process, user and machine activity—to detect a well-executed, nation-state-level Red Team attack. The customer was able to uncover the entire attack lifecycle via behavioral indicators and gave the company's security team the right context to respond to attack. The following attack characteristics were identified:

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

About Micro Focus ArcSight Intelligence

Micro Focus ArcSight Intelligence Behavioral Analytics gives security teams a new lens through which to find and respond to difficult-to-find insider threats or targeted outside attacks. Bypassing rules and thresholds, 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 at **www.microfocus.com/integrations-interset-crowdstrike**.

CyberRes
A Micro Focus Line of Business