CrowdStrike Store

Data Sheet

CYBERRES ARCSIGHT INTELLIGENCE: ENDPOINT DATA AND BEHAVIORAL ANALYTICS

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

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

CyberRes 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, date 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 recon, or low and slow attacks. Once identified, threat leads can be passed on to your security team or the CrowdStrike Falcon OverWatch™ 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 CrowdStrike Store at **store.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 CrowdStrike 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.

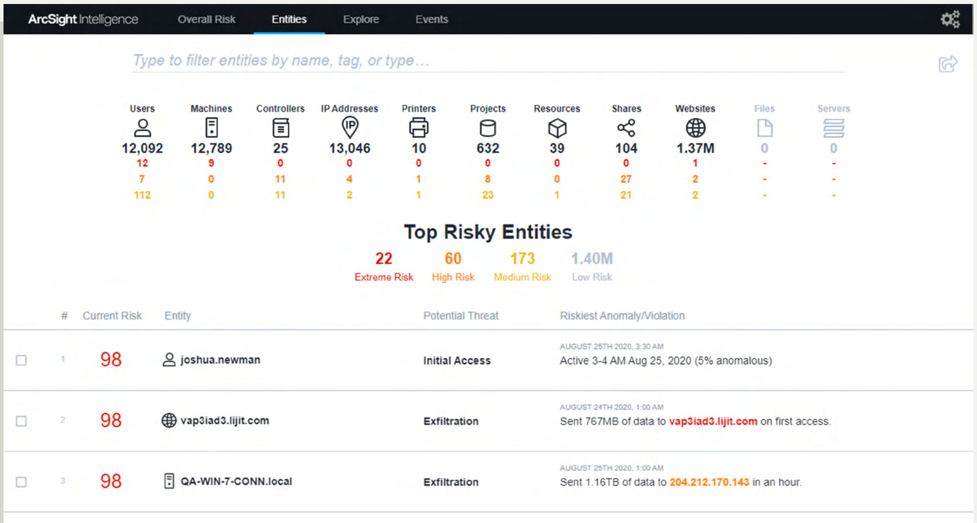
KEY BENEFITS

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

ArcSight Intelligence Dashboard (Demo)



Users	Machines	Controllers	IP Addresses	Printers	Projects	Resources	Shares	Websites	Files	Servers
12,092	12,789	25	13,046	10	632	39	104	1.37M	0	0
12	9	0	0	0	0	0	0	1	-	-
7	0	11	4	1	8	0	27	2	-	-
112	0	11	2	1	23	1	21	2	-	-

Top Risky Entities

22	60	173	1.40M
Extreme Risk	High Risk	Medium Risk	Low Risk

	#	Current Risk	Entity	Potential Threat	Riskiest Anomaly/Violation
□	1	98	joshua.newman	Initial Access	AUGUST 25TH 2020, 3:30 AM Active 3-4 AM Aug 25, 2020 (5% anomalous)
□	2	98	vap3iad3.lijit.com	Exfiltration	AUGUST 24TH 2020, 1:00 AM Sent 767MB of data to vap3iad3.lijit.com on first access.
□	3	98	QA-WIN-7-CONN.local	Exfiltration	AUGUST 25TH 2020, 1:00 AM Sent 1.16TB of data to 204.212.170.143 in an hour.

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.

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 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 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 and request a trial of ArcSight Intelligence at

www.microfocus.com/products/arcsight-intelligence.

ABOUT CYBERRES

CyberRes, a Micro Focus line of business, brings the expertise of one of the world's largest security portfolios to help our customers navigate the changing threat landscape by building both cyber and business resiliency within their teams and organizations. CyberRes helps enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

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