CrowdStrike Store

MICRO FOCUS Interset

CROWDSTRIKE

Data Sheet

# MICRO FOCUS INTERSET UEBA: UNKNOWN THREAT DETECTION

Combining endpoint data with user and entity behavioral analytics (UEBA) to swiftly reveal hidden threats

## 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

Micro Focus Interset UEBA allows your security team to see the CrowdStrike Falcon® platform'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 log-in frequency, date or time of work, unusual machines — Interset adds valuable context to help you see threats that you might otherwise miss. With the right user context, you can detect unusual log-in patterns, sudden or unusual file or system activity, user impersonation, internal reconnaissance, and low and slow attacks. Once identified, threat leads can be passed on to your security team or the CrowdStrike® Falcon OverWatch™ threat hunting team for further investigation.

## KEY BENEFITS

Combines rich CrowdStrike endpoint data with advanced UEBA to uncover traditionally difficult-to-find threats.

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

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

# TECHNICAL SOLUTION

Getting started with the combined analytical powers of Interset's UEBA and CrowdStrike's rich Falcon sensor data couldn't be easier. Simply log in to your Falcon UI console, head over to the CrowdStrike App Store and click on the Interset UEBA application. Once you click the "Try it free" button, Interset 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, Interset's machine-learning engine has all it needs to begin using the data to detect anomalous activities that may be threatening your organization. You are then provided with access to Interset's state-of-the-art threat-hunting user interface, which highlights instances of risky anomalous behaviors and prioritized lists of the riskiest entities in your organization.

# USE CASES

- **Find insider threats:** Leveraging CrowdStrike's rich endpoint data, Interset UEBA can help uncover malicious or negligent insiders by learning the unique patterns of behavior of each 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 steal high-value data. Interset UEBA identifies the behavioral clues 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:** Interset UEBA 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:** Interset UEBA combines unsupervised machine learning with mathematical probability to calculate risk scores that will tell you which entities are the most suspicious. This allows Interset 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.

## INTERSET UEBA: A REAL-WORLD SUCCESS STORY

At a major hospitality company, Interset UEBA combined with rich CrowdStrike Falcon endpoint data — including process, user and machine activity — detected 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 the attack. The following attack characteristics were identified:

Compromised accounts

Remote exploit

Outlook Web Access (OWA) profiling

Password guessing

Lateral movement

IP address and attack tool

# ABOUT MICRO FOCUS INTERSET

Micro Focus Interset User and Entity Behavioral Analytics (UEBA) 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, Interset uses unsupervised machine learning to measure the unique digital footprint of systems and users. Interset 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/interset.**

# ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), 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 over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.



**Start Free Trial**
**of Next-Gen AV**

Learn more **www.crowdstrike.com**