INTERSET

Interset is now a Micro Focus Company.

Financial service organizations find managing cyber risk increasingly important as they work hard to protect sensitive customer data in the face of more frequent and more targeted attacks. In fact, financial services firms suffer from cyber attacks 300 times more than businesses in other industries (Identity Theft Resource Center®, 2018). Three-quarters of financial services executives agree that cybersecurity is one of the top three risks that will be of increasing importance over the next two years, but only half of these executives feel their institutions have the issue under control (Deloitte, Global Risk Management Survey, 2019). At the core of these organizations' fight against cybercrime is a difficult-to-solve challenge: limited human and financial resources.

Interset user and entity behavioral analytics (UEBA) helps financial services security teams maximize their existing resources and gives them a new lens through which to detect, investigate, and respond to threats—before data is stolen. Using machine learning, Interest UEBA distills billions of events into a prioritized list of high-quality security leads to focus and accelerate the efforts of your security operations center (SOC). Interset's machine learning models, combined with an intuitive user interface (UI), accelerate threat detection and investigation from weeks to minutes

Why Interset

Financial services organizations have important assets to protect, whether it is customer information, intellectual property, or both. Unfortunately, existing approaches to protecting these assets continuously fall short, leaving security teams to contend with rigid, rules-based analytics, fragmented security ecosystems, and a never-ending barrage of alerts—most of which are false alarms. Meanwhile, these teams are expected to flawlessly protect against critical threats like data exfiltration and unauthorized network access.

Interset is uniquely positioned to find the threats that matter for enterprises with valuable data to protect, limited security resources, and significant surface area to monitor—characteristics common among financial institutions. Unlike other solutions, Interset UEBA bypasses rules and thresholds and instead assesses the potential risk of a user or entity in your enterprise based on mathematical probability and unsupervised machine learning models. This approach, combined with Interset's native big-data architecture, allows your security team to detect difficult-to-find threats with speed and at scale.

Detect. Investigate. Respond.

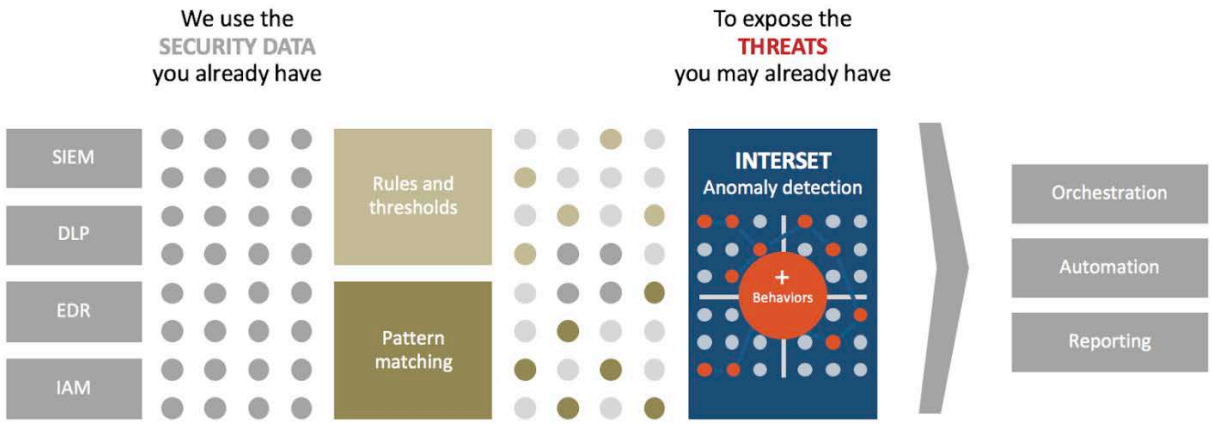


Figure 1 | Interset UEBA views your existing security data through a new lens in order to identify hidden threats by looking for anomalous behavior. This produces high-quality threat leads, allowing your security teams to respond and remediate quickly and effectively.

Using supervised machine learning—a type of artificial intelligence (AI) that doesn't need labels—Interset's algorithms extract available entities (users, machines, IP addresses, servers, printers, etc.) from within log files and observe events that involve these entities to determine expected behavior—a measurement we call "unique normal." As new information comes through the analytics process, events are evaluated against previously observed behavior to assess potential risk.

With this process of baselining and scoring, Interset UEBA boosts the efficiency and speed at which security teams detect, triage, investigate, and respond to threats. Interset's output risk assessments can be used to initiate actions via automation, orchestration, and alerting solutions to execute faster-than-human actions as risks are found. Interset also provides downloadable reports summarizing immediate organizational risks.

Threat Detection Use Caqų

Insider Threat

- At-Risk employee
- High-Risk Employees
- Account Misuse
- Privilege Account Misuse
- Terminated Employee Activity

Data Breach

- Data Staging
- Data Exfiltration
- Email Exfiltration
- Print Exfiltration
- USB Exfiltration
- Unusual data access
- Unusual uploads

Advanced Threat

- Compromised Account
- Internal Recon
- Unusual Traffic
- Abnormal Processes
- Unusual Applications
- Infected Host
- Malicious Tunneling
- Bot Detection

IP Theft

- Mooching
- Snooping
- Interactions with dormant resources/files
- High Risk IP/Data Access
- Lateral Movement

Fraud

- Transaction Abuse
- Expense Fraud

[illegible]

[illegible]

[illegible]

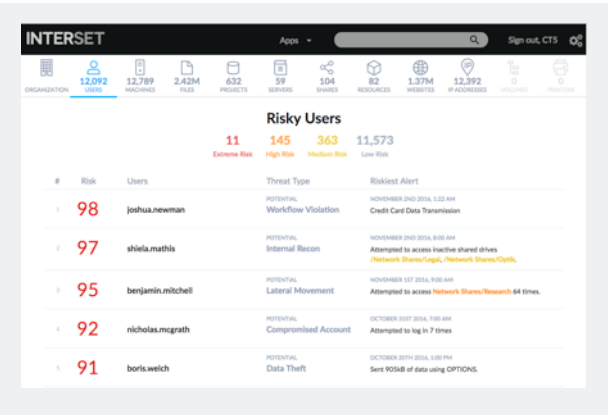
[illegible]

1. [illegible] Qll entities within the enterprise with analytics to display group ed by entity type.

   This screenshot shows Qlist of users in, with a presentation that displays them inorder of risk score from highest to lowest.

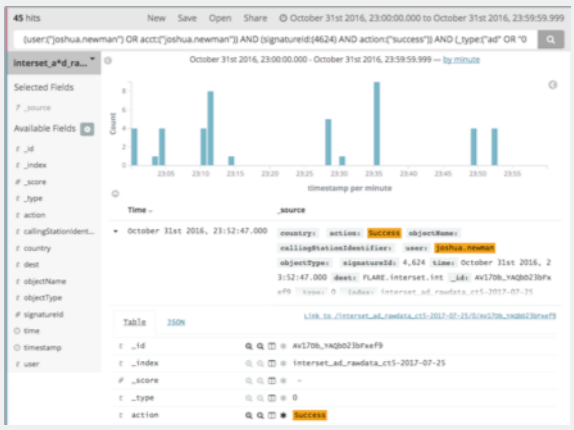
2. When any entity is viewed [illegible]

3. When viewing an entity, a display of the alerts associated with the entity can be seen below the timeline view. They can be filtered by associated entities and types of risk and, because they display in chronological order linked to the timeline view, it is simple to see a narrative of the unfolding behavior in the context of other events.



4. Clicking on any of the alerts allows for examination that shows the event in context of the user's baseline and other relevant entities in the enterprise. The risk associated with the alert is displayed, and the model that triggered the alert is described in detail. Note that the user's baseline is compared to both itself, as well as to other similar entities. These similar entities are identified through statistically determined peer groups.

5. The raw events that triggered an alert are only one click away. In addition to seeing the actual contents of the log file responsible for the analytics, users have the ability to enter additional queries using this interface.



INTERSET

Contact **sales@interset.com**

Interset, now a part of Micro Focus, equips security teams with analytics to detect, investigate, and respond to threats before data is stolen. Our user and entity behavioral analytics augments existing security tools and leverages machine learning to measure the unique footprint of systems and users—distilling billions of events into a handful of prioritized threat leads. What used to take months, now takes minutes. A member of the In-Q-Tel portfolio, Interset is trusted to protect critical data and infrastructure in the finance, high tech manufacturing, healthcare, utility, and energy industries. Visit us at Interset.AI. Visit us at **interset.ai**, and follow us on **Twitter**, **LinkedIn**, and **Facebook**.