INTERSET

Solution Brief

We Uncover the Threats that Matter

Interset Security Analytics

Interset user and entity behavioral analytics (UEBA) detects and responds to threats before your data is stolen. It distills billions of events, generating a prioritized list of high-quality security leads to focus and accelerate the efforts of security operations centers (SOC).

Unlike other solutions, Interset bypasses rules and thresholds and instead assesses potential risk based on mathematical probability and machine learning models. These machine learning models, combined with a highly intuitive user interface (UI), accelerate threat detection and investigation from days or weeks to minutes.

Interset's UEBA makes SOC teams more effective at threat hunting, triage, and investigation. Its advanced mathematical algorithms leverage AI and machine learning to automatically and constantly mine billions of data points to reveal indicators of insider threats, data breaches, advanced persistent threats (APT), IP theft, and fraud.

Threat Detection Use Cases

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

Advanced Threat Detection

Interset's mathematically based approach increases enterprise-wide risk visibility, accelerates threat detection time, improves SOC efficiency, and increases the ROI of existing security investments such as SIEMs. By relieving alert fatigue, security teams are able to focus on the threats that matter and have a measured response to measured risk.

Interset significantly improves a security team's ability to detect threats and enable focus on response and remediation. Interset's security analytics platform is Apache Hadoop®-based and processes many common types of system data, including authentication, file/data repository, NetFlow, web proxy, client endpoint, printer, and more— with speed and at scale. The output risk assessments that Interset produces can be used to initiate actions via automation, orchestration, and alerting solutions to execute faster-than-human actions as risks are uncovered.

Interset Threat Detection Platform

Interset's UEBA is built from the ground-up to execute unsupervised machine learning algorithms at enormous scale using an Apache Hadoop compute architecture. These algorithms extract the available entities (users, machines, IP Addresses, web servers, printers, etc.) from within log files and observes events that include these entities in order to determine what is normal or expected behavior. As new information comes through the analytics process, it is evaluated against previously observed behavior to assess potential risk.

Interset's solution is unique because it is the only one that natively uses ***unsupervised*** machine learning algorithms to discover new patterns and subsequently find new threats. It can track the relative potential security risk of not of just users, but also file shares, servers, repositories, external websites, printers, and more.

Understanding the Analytics Processing

Interset's analytics are powered by over 400 built-in unsupervised machine learning models that take log-file-based events and produce an assessment of the potential risk an entity may pose to the enterprise. Using these models, Interset's analytics processing undertakes two primary tasks as each new event moves through the system:

1. **Baseline:** The event is incorporated into the behavioral model that serves as the mathematical basis for describing the expected behavior of an entity.
2. **Scoring:** The same event is compared against the model to determine if it varies from normal or expected behavior for the entity.

The outcome from these two tasks is a value that represents the probability that the event is expected, as shown by Figure 1 below:

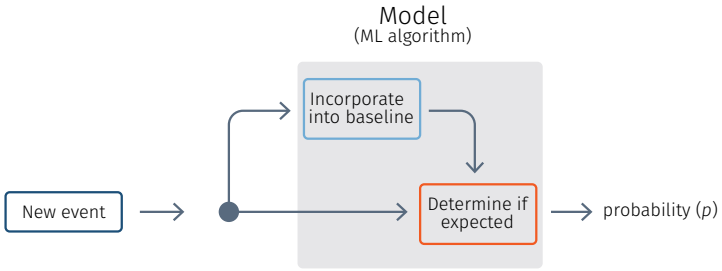


Figure 1 | Processing events in a model: As a new event enters the analytics process it is processed twice in each model for which it is eligible. First, it is incorporated into the behavior baseline for the entity. Then it is examined to determine the probability that it is an expected or normal event.

Figure 2 | Probability & weighting yield alert severity: If the probability calculation of the model indicates unusual behavior, a weighting is incorporated with this finding to calculate the severity of the alert for the entities involved.

If the probability scored by the model is at all unusual (falls outside of the expected range), then weighting is applied. When the probability and the weighting values are combined, an alert is produced with a characterization as low, medium, high, or extreme, as shown in Figure 1 above. Interset's weightings are pre-configured and, out-of-the-box, but may be modified by customers via both graphical user interface (GUI) and REST API. The weighting allows for the relative risks of particular types of behavioral anomalies to be balanced against one another in order to reflect the security concerns of the enterprise.

Alerts are associated with the entities whose behaviors spawned them. Both the number and severity of the alerts associated with an entity serve to raise its risk score. A risk score is a value between zero (0) and one hundred (100) that represents the relative potential risk an entity represents to the enterprise. A score near the lower end of the scale (closer to 0) represents an entity that is acting in a relatively normal manner; a score at the upper end (near 100) represents not only abnormal behavior, but also acts that have a significant amount of potential risk.

The figure below represents the analytical process running end-to-end. It shows how many events running through multiple models all contribute the risk score of an entity.

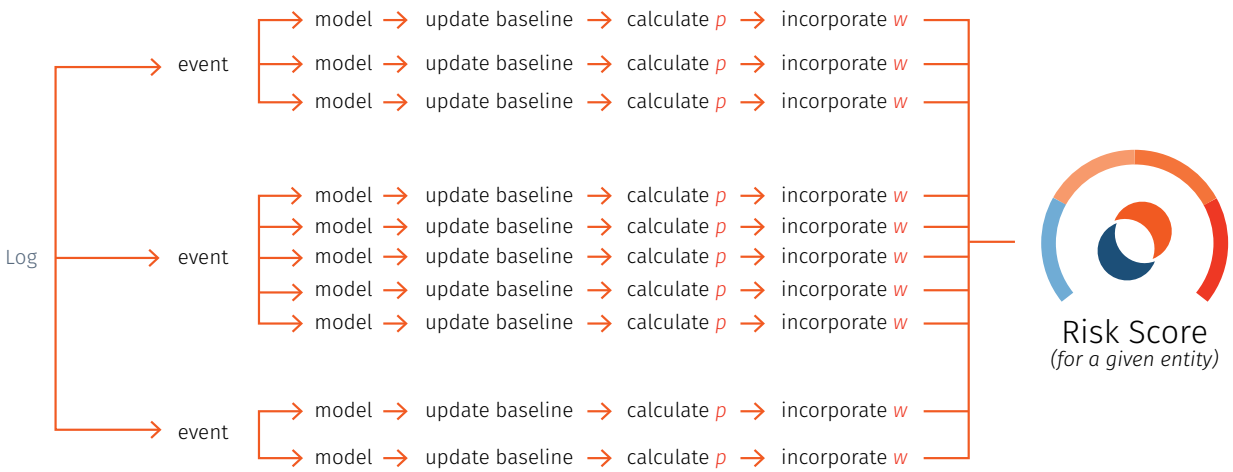


Figure 3 | Events fire models, models generate alerts, and alerts raise entity risk scores: As a log is parsed, events are extracted. Events may be eligible for processing by the built-in behavioral models. Within each model, the event is incorporated into the observed baseline and then scored to determine the probability of unusual behavior for a relevant entity. If unusual, a weighting is incorporated into the alert. The result is an alert that, as it is linked to the involved entity, drives the risk score for the entity in the overall analytical output.

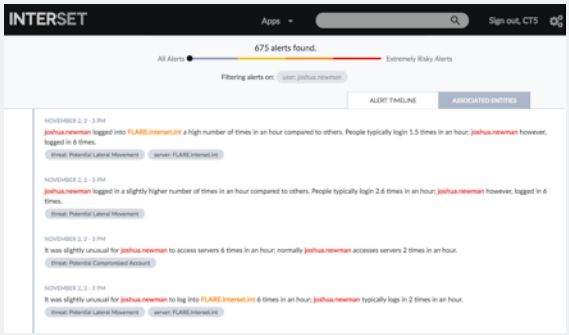
Viewing Entities Exhibiting Potential Risk

The primary mechanism for interacting with Interset from a security practitioner standpoint is the web-based dashboard. The dashboard serves to allow users to quickly and easily determine which entities represent the greatest potential risk to the enterprise. As these entities are identified, the dashboard allows for drill-down into the results so that the potential risk can be understood in the context of the generated alerts and, if desired, the raw events that produced them.

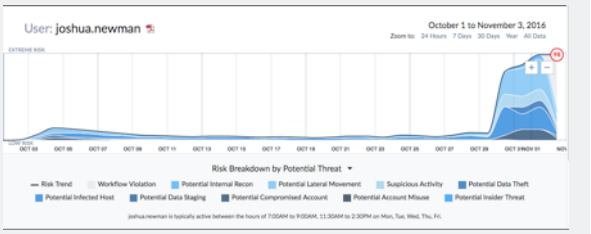
The following series of screenshots show a drill-down from the list of riskiest users, down to the raw event level.
Table 1: Screenshots of the Interset dashboard showing navigation through the analytical results.

1. All of the entities within the enterprise with analytics to display can be viewed within the Interset dashboard, grouped by entity type.

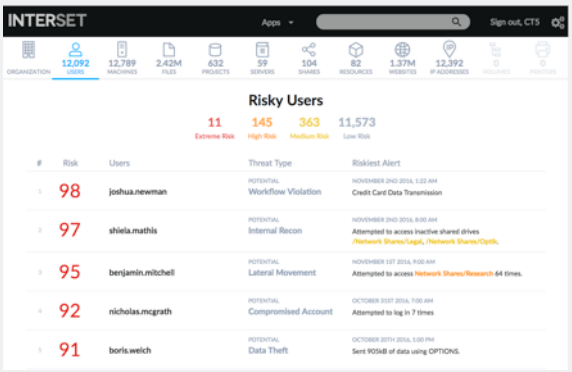
   This screenshot shows the list of users in the organization, with a presentation that displays them in order of risk score from highest to lowest.



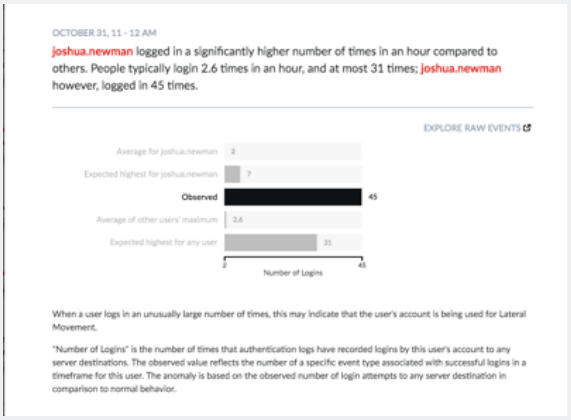
2. When any entity is viewed (in this case, a user), their risk score over time is displayed in a timeline view. This perspective shows not only the change in risk score, but also broadly characterizes the types of behavior that drove it.



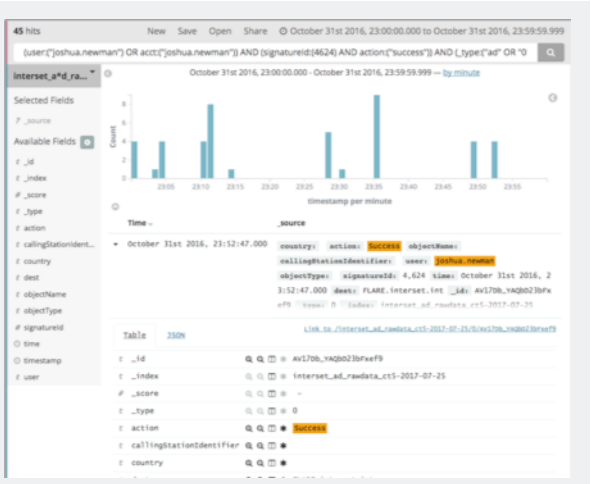
3. When viewing an entity, a display of the alerts associated with the entity can be seen below the timeline view. They can be filtered by associated entities and types of risk and, because they display in chronological order linked to the timeline view, it is simple to see a narrative of the unfolding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



Integrating Interset into the Enterprise

When evaluating how the Interset analytics product fits within the scope of an existing enterprise ecosystem, as shown below in Figure 3, there are two primary considerations:

Source System Log Files: Getting data from the location where they are generated into Interset with the right structure and with the necessary content for analytics to run successfully.

Security Ecosystem Integration: As noted above, the results of Interset analytics can be viewed in the built-in dashboard. To fully leverage this information, most enterprises choose to create automated handoffs between the Interset product and existing security or incident response applications.

Figure 3 | Interset works within an existing enterprise ecosystem: Interset consumes logs from source systems throughout the enterprise and uses the compute power of an Apache Hadoop® Data Lake to conduct behavioral analytics on the events they contain. The analytical outcome is made available for viewing in a dashboard and can hand-off automated actions throughout the security ecosystem to support appropriate responses to potential risks.

Hadoop Architecture

The Interset product is built natively on Apache Hadoop. Both the Hortonworks and Cloudera distributions of Hadoop are supported, but the out-of-the-box installation is shipped with Hortonworks data platform by default.

As shown below in Figure 4, the architecture of Interset is best understood in the context of how data is processed. There are four main groupings:

Acquire Data: This portion of the process is devoted to the acquisition of data, performance of any required transformations to make the data ready for analytics, and movement of that data to required locations for subsequent steps.

Create Baselines: This is where all operations related to the baselining and scoring activities that form the core value proposition of the Interset platform are performed. Interset creates baselines for every single entity. This means a baseline for every one of 12,000 users for example, simultaneously a baseline for each one of 2.42 M files and each printer, machine, IP address etc.

Detect Anomalies: In this step, Interset analyzes data and performs calculations to detect unusual events, determine severity, and produce risk scores for entities.

Threat Leads: Once analytics is complete, results are moved into an intuitive, human-friendly user interface to make it fast and easy to follow up and handoff to an automated orchestration and response systems.

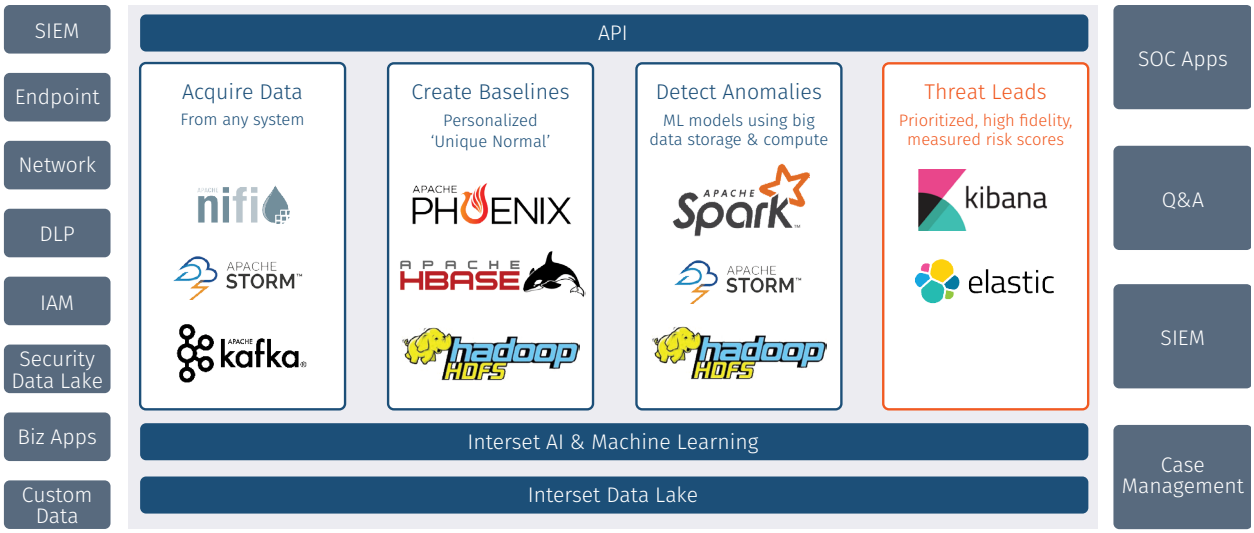


Figure 4 | Interset architecture by phased grouping: The left-to-right flow shows the three main groupings of the Big Data platform that underpins the Interset process. Acquire data involves the transportation and transformation of data to make it available for analytics. The second step, Create unique baselines continuously measures and baselines all available data to determine "unique normal" for entities such machines, printers, people, peer groups and the enterprise as a whole. The 3rd step: Detect, Measure and Score anomalies analyzes data, performs the calculations to detect unusual events, determine severity, and produce risk scores for entities. Finally, step 4: High quality threat leads are produced for intuitive viewing

Summary

Interset's threat detection platform leverages sophisticated mathematical models, presented via an intuitive UI to enable security teams to accelerate threat detection and investigation from days or weeks to minutes.

The prioritized list of high-quality security leads focuses and accelerates the efforts of SOC teams for easier and faster threat detection, threat hunting, triage, and investigation. Its advanced mathematical algorithms leverage AI and machine learning to automatically and constantly mine billions of data points to reveals indicators of insider threats, data breaches, advanced persistent threats (APT), IP theft, and fraud.

For enterprises with valuable data to protect, limited security resources, and significant surface area to monitor, Interset is uniquely positioned to find the threats that matter.

About Interset, a Micro Focus company

Interset, a security analytics company— and part of the Micro Focus Security, Risk, and Governance portfolio— augments existing security tools and empowers security teams to identify and respond to the threats that matter before data is stolen. Interset's user entity behavioral analytics (UEBA) and machine learning threat detection platform leverages AI and machine learning to measure the unique digital footprint of systems and users, distilling billions of events into a handful of prioritized threat leads. What used to take months, can now take minutes. Interset is backed by In-Q-Tel and trusted to protect critical data in finance, critical infrastructure, high-tech manufacturing, healthcare, utility, and energy industries.

Visit us at **interset.ai,** and follow us on **Twitter**, **LinkedIn**, and **Facebook**.