Essential Guide

User and Entity Behavior Analytics

Detect advanced threats using machine learning, generate rich contextual insights to understand attacks and streamline incident investigations.

splunk>

Security teams face more challenges than ever — an expanded attack surface, an increased number of vulnerabilities, and a non-stop barrage of cyberattacks, all of which materially increase organizational risk. According to the Splunk State of Security Report 2023, security operations centers (SOCs) have become so overwhelmed that 23% of SOC analysts say they struggle with the high volume of security alerts. There are so many to process that 41% of those alerts are being ignored. This enables threats to slip through an organization's defenses. This can increase mean time to detection (MTTD) and result in lengthy dwell times. In fact, organizations report an average of about 2.24 months of dwell time, and 52% of organizations reported breaches within the last two years.

These challenges are being exacerbated by headwinds fueled by generative AI. According to the recently released Splunk Security Predictions 2024 report, attackers will create AI-designed evasive malware, deep fakes and more authentic social engineering tactics. Plus, new types of assaults will emerge in 2024, including commercial and economic disinformation campaigns, with more targeted attacks against companies' brands and reputations. Ransomware authors will increasingly rely on zero-day threats to infiltrate networks.

Sophisticated cyberattacks like these can be very difficult to uncover and detect. While man-made correlation rules can detect malicious behavior, they should not be solely relied upon to identify 100% of threats in any given environment. Consider the limitations of human-fueled security tactics. Security teams are so overwhelmed by the sheer volume and sophistication of attacks that they have reached, if not exceeded, their capacity to effectively and rapidly observe, orient, decide and take action. A more sound strategy is a combined human and machine approach to scale the SOC team with technology that can streamline and automate key elements of the detection, investigation, response and remediation cycle.

This is where machine learning (ML) changes the dynamic. Machine learning does not presuppose any conditions. It does not assume something is good. Instead, it trains itself, learns what is normal and what is abnormal behavior. Without any inherent bias, it learns from the environment to establish a baseline, and anything that behaves atypically or contrary to that baseline is deemed anomalous.

What is user and entity behavior analytics?

User and entity behavior analytics (UEBA) analyzes the behavior of users and entities, like devices (routers, servers, etc.) and applications, and uses machine learning to detect unusual behaviors. These systems monitor existing user accounts, devices and applications, analyze their access patterns and issue alerts when there is a sign of anomalous behavior. Some examples of potentially anomalous behavior include:

- A user account accessed from an unusual device, browser or geographical location. Alternatively, multiple login attempts for an account and failed login attempts for a user who does not have any record of failed attempts before.
- A user who does not have permission to access files, directories or other resources from a privileged account and is trying to access them, indicating privileged account abuse.
- A user who typically does not download large files, but is observed downloading large files.
- A user suddenly starts transferring large amounts of data, which could indicate that he is exfiltrating sensitive information from the system.
- A user executes unusual commands or run scripts that they usually do not run or that do not align with their job role. For example, someone in the marketing department running a complex database query.
- An application suddenly gets thousands more requests than usual, even if it is not the peak time for users accessing that application. This type of behavior indicates a potential DDOS attack.

How does a UEBA system identify these types of anomalies? The common thread across various forms of cyberattacks is the deviation of a compromised user's or asset's behavior from its past or its peer groups. This change in behavior provides indicators of compromise (IoC) which can be woven together to distinguish a threat.

Behavior of entities — especially users, devices, system accounts and privileged accounts — can be mined to reveal anomalies, even when they occur infrequently and over extended periods of time. A UEBA solution can capture the footprint of these threat actors as they traverse enterprise, cloud and mobile environments, and then run them through its advanced machine learning algorithms to baseline, detect deviations and find anomalies continuously.

These aberrations are then stitched into meaningful sequences over time using pattern detection and advanced correlation to reveal the actual kill chains that are comprehensible and immediately actionable. A kill chain is the true picture of an attack — a sequence of malicious activities resulting in a breach. Frequently, there are several events in each stage of the sequence that reveal the path and behavior of an attacker. In contrast to alerts corresponding to violations of known thresholds, a behavior-based threat detection approach uses machine learning with extreme context awareness to maximize the probability of finding true, hidden threats while minimizing the rate of false positives.

Five essential capabilities of user and entity behavior analytics

The following are five capabilities that any best-of-breed user and entity behavior analytics solution should possess:

1. Coverage across users, entities, devices and applications

Early versions of behavior analytics products simply looked at user behaviors. When evaluating UEBA solutions, be sure the technology analyzes and monitors users and entities. This includes end user behavior, endpoint devices, servers, routers, applications and more. You will want to review all of the coverage areas of any UEBA solution you are considering to ensure comprehensive monitoring across every aspect of your organization.

Furthermore, a best-of-breed UEBA solution should be analyzing data from multiple sources, including:

- Databases like active directory
- Security tools like antivirus, EDR and EPP (endpoint detection and response or endpoint protection platform), intrusion prevention systems (IPS/NGIPS) and, of course, SIEM
- Network security tools like routers, firewalls, identity access and VPN
- Threat intelligence feeds

2. Detection and analysis capabilities fueled by machine learning

Any best-of-breed UEBA solution must go beyond the abilities of correlation rule searches and detections. Despite their ability to detect malicious behavior, man-made correlation rules should not be solely relied upon to identify all threats in any given environment. This is where machine learning can fill the gap. Top-tier UEBA solutions use machine learning to find hidden, unknown threats and anomalous behavior across users, endpoint devices and applications.

How does this work? The UEBA solution creates baselines and ranges of 'normal' behavior and activity for all users and entities. The baseline is run across multiple configurable dimensions and compared to the baseline at the departmental, regional or company level. This allows organizations to identify and track a user who, for instance, normally only prints a few pages, but then suddenly starts printing 50 pages. While that is considered anomalous behavior for that user, another who regularly prints 200 pages a day wouldn't be flagged unless they significantly exceed their normal baseline. This kind of tailored alerting is important because it can be specific to known threats. These conditions can be written quickly to detect future events and are simple enough for security analysts to understand and act upon.

Machine learning allows organizations to solve advanced use cases that should not be managed by conventional approaches alone. UEBA solutions use scalable ML detection capabilities to build on simple detection methods (usually signature-based or correlation rules-based) to enhance overall functionality. While threshold and statistics usually produce higher confidence detections, machine learning models can provide a backstop to find attacks that simple detections might miss.

3. Visibility and contextual awareness that enable fast, decisive action

Any best-of-breed UEBA solution needs to provide security teams with instant visibility and insights that help them rapidly assess risk and detect the presence of any threats in their environment. This is where dashboards and visualizations are especially important. The UEBA solution should have a home dashboard that includes key indicators and panels that provide an overview of the current security posture in your environment. Key indicators should include:

- Threats: a summary of the total number of active threats in your environment
- Anomalies: a summary of the total number of anomalies in your environment
- Users: a summary of the total number of anomalous, known and unknown users

- Devices: a summary of the total number of anomalous internal and external devices
- Apps: a summary of the total number of anomalous apps compared to the number of total apps

The dashboards should also provide detailed contextual information across all key indicators. For instance, views that could be especially important to security analysts include:

- 7-day threats timeline to track threats and identify recent trends in threat activity
- Latest anomalies to see the most recent anomalies identified in your organization
- 7-day anomalies timeline to identify recent anomalies
- Events processing showing the number of active events to ensure event processing is flowing as expected
- 7-day events trend to identify any unexpected changes in event processing

These dashboards and visualizations should give security analysts what they need to start investigative workflows with just a few clicks.

4. Leverages multiple ML-powered models to uncover and eliminate threats

UEBA solutions should run a series of ML-powered threat models over collected anomalies to identify threats that need to be reviewed by SOC analysts. At a minimum, the solution should include:

- **Batch models:** These models and their associated anomaly rules operate on accumulated data stored in the UEBA solution. They analyze ingested data over a larger time frame, such as the last 24 hours, and typically run overnight due to the need to process large amounts of data. Use cases, such as beaconing, function in a mixed mode, where the streaming component identifies events of interest which may be converted into anomalies by offline components.
- **Security analytics models:** A best-of-breed UEBA provides models that can establish a security context and compute security analytics. These models use an array of detection algorithms for security use cases. To enhance the quality of these models, the algorithms re-score anomalies by refining anomaly action and score rules. This includes ranking both internal and external users and providing more personalized detection with threat rules, watchlists, allow and deny lists, and dashboards. You can use anomaly action rules to manage existing anomalies. For example, you can delete or restore anomalies, modify the score or add anomalies to a watchlist. You can also customize anomaly scoring rules to provide more control and consistency across specific anomaly types.
- **Streaming models:** These models process every event as it happens, which is valuable for use cases where the sequence and timing of events is crucial. Streaming models analyze ingested data in real time and determine the impact of that data over a short time frame, such as the past hour. Streaming models can generate anomalies, indicators of compromise (IoCs) or analytics data in a UEBA solution.
- **Threat models:** These models are based on the data and anomalies in the system. Threat models take data aggregation into account, including the data cataloged by the streaming models, to generate threats alerts. UEBA threat rules can flag threats by looking for specific anomaly patterns within a specific window of time. A threat alert is generated each time the anomaly pattern is found. Each threat rule runs on a predefined schedule, depending on the nature of the rule. You should also be able to create custom threat rules to identify verifiable threats in your network, such as specific activities that you want to monitor for policy compliance. Custom threats can apply to users, devices or sessions.

5. Seamless integration with SIEM

Any top-tier UEBA solution should be able to seamlessly integrate with a best-of-breed SIEM solution. A combined SIEM and UEBA solution can enhance machine learning, anomalous user behavior detection, context-enhanced correlation and rapid investigation capabilities. An integrated solution can provide a centralized view for incident investigation and management; leverage the power of both products to gain deeper context about anomalies relative to users, devices and applications; and ultimately help SOC teams better detect and quickly respond to prioritized, high-fidelity threats.

The threat detection capabilities in a UEBA solution can extend the search, pattern and rule-based approaches of a SIEM for detecting threats. Additionally, a best-of-breed UEBA solution uses correlation and pattern detection based on machine learning to deliver automated detection of advanced threats spanning insider threats, account compromise, privileged account abuse, lateral movement, data exfiltration and more. A SIEM typically does not provide this functionality, or if it does, cannot deliver it very easily. Furthermore, a best-of-breed SIEM will usually deliver dynamic and recurring security content updates that empower security teams to proactively stay current with the latest threat detection techniques. Augmenting human-driven correlation rules and searches within a SIEM with the unsupervised machine learning-based threat correlations of a top-tier UEBA solution facilitates more comprehensive and faster threat detection, investigation and response.

Threat use cases addressed by user and entity behavior analytics

Let's dive deeper into some of the user and entity behavior analytics use cases. What are they? How do these attacks work? And how can a user and entity behavior analytics solution address them?

Compromised user account

One of the classic insider use cases is the potential compromise of a trusted user or service account. Best-of-breed user and entity behavior analytics solutions should be able to identify situations where user credentials have been stolen and are being used by an entity other than the authorized user. Detecting shared account usage and generic account abuse falls under this use case as well.

A best-of-breed user and entity behavior analytics solution uses behavior modeling to identify any deviation from normal user activity to determine if someone other than the legitimate owner is operating the account. Detection includes identifying unusual or malicious active directory activity, such as operations on self, terminated users, disabled accounts or account recovery.

Compromised and infected machine (malware)

User and entity behavior analytics solutions can be used to identify endpoints that have been compromised, infected by malware or are otherwise behaving suspiciously. This is different from the compromised user account use case in the sense that malicious activity might be detected on a host, but not necessarily tied to a specific user account (e.g., command and control [C&C] traffic can be identified from a system where no user is currently logged on).

A best-of-breed user and entity behavior analytics solution uses behavior-based modeling to identify malware activity regardless of the delivery mechanism of initial infection. The detection techniques include tracking changes in communication patterns of devices, the nature of communication with external domains or IPs and characteristics of the domains.

Data exfiltration

Unauthorized or malicious data exfiltration by authorized users can occur even if your team already has the ability to detect compromised accounts and endpoints. A best-of-breed user and entity behavior analytics solution can detect loss or theft of private and confidential data from the enterprise across multiple threat vectors, including network security infrastructure (firewalls and proxies), online cloud storage, attached storage (USB) and email.

Lateral movement

Lateral movement by a trusted insider involves a user scanning and expanding access across multiple resources. Detection techniques such as rare access or expanding resource usage are used to identify lateral movement. Resources here can include machines, network file shares or box folders. Accesses can either be network scans, brute force logins or legitimate logins. A best-of-breed user and entity behavior analytics solution should be able to detect lateral movement through anomaly baseline comparisons.

Suspicious behavior/unknown threats

User and entity behavior analytics solutions are very effective at spotting unknown scenarios by identifying anomalies based on deviations in the user/device activity compared with self/peer group baselines, suspicious or malicious activity, alerts from external tools, and correlating them into a threat. Oftentimes, this suspicious account activity and unknown threat demands further investigation. Unknown threats could include malvertising, account compromise, account misuse, policy violations and misconfiguration. These threats are often used by UEBA solutions for content building. Once an unknown scenario is detected, that scenario can then be written into correlation search or threat rules for deterministic detection.

Account misuse

Accidental misuse and deliberate abuse of superuser privileges present critical compliance and privacy risks with potentially severe financial and reputational impacts. A best-of-breed user and entity behavior analytics solution baselines the regular behavior of each account (not just user accounts) and identifies any abnormalities that may indicate excessive usage, rare access, potential sabotage or covering tracks. As the user activity deviates from the peer group and enterprise profile, the UEBA solution's confidence grows. The higher the confidence, the higher the risk. Examples of such detections include, but are not limited to, using service accounts to do VPN or interactive logins, data snooping, deleting audit logs or accessing confidential information.

Contextual intelligence

Best-of-breed user and entity behavior analytics solutions learn a lot about users and entities in the organization to identify anomalies that could be linked to threats. This information is extremely useful for analysts performing alert triage and incident investigations. If an analyst suspects that an endpoint has been compromised, for example, he can use a UEBA solution to learn about the users of that desktop, their regular behavior and even the role of that endpoint in the network. For example, is it a server or a workstation? Is it used for system administration or business function?

Enter Splunk

Splunk User Behavior Analytics (UBA) helps organizations find known, unknown and hidden threats across users, endpoint devices and applications. Despite the name “User Behavior Analytics”, Splunk UBA analyzes both users and entities using multi-dimensional behavior baselines, dynamic peer group analysis and unsupervised machine learning. This allows Splunk UBA to rapidly detect anomalous behavior — such as compromised or misused accounts or devices, IP theft or data exfiltration — and eliminate it.

Using machine learning, Splunk UBA derives sequences and patterns across all anomalies, in addition to other indicators, to filter down and identify the top threats that are critical and actionable.

Amidst all the noise, these threats represent the most likely risk to your business. Splunk User Behavior Analytics addresses security analyst and hunter workflows, requires minimal administration and integrates with existing infrastructure to locate hidden threats.

Need to perform advanced threat detection? Splunk UBA can help you discover anomalies and unknown threats that traditional security tools miss. Need to boost productivity in your SOC? Splunk UBA automates the stitching of hundreds of anomalies into a single threat to simplify and speed up incident investigations. Need to accelerate threat hunting? Use Splunk UBA’s deep investigative capabilities and powerful behavior baselines on any entity, anomaly or threat.

Detect advanced threats and anomalous behavior using machine learning

Splunk UBA uses unsupervised machine learning algorithms to establish baseline behaviors of users, devices and applications, then searches for deviations to detect unknown threats, such as:

- Compromised user account – any deviation of user activity from normal thereby indicating that someone other than the legitimate owner is operating the account.
- Compromised machine – identification of network endpoints that have been compromised, infected by malware or are otherwise behaving suspiciously.
- Data exfiltration – detection of loss or theft of private and confidential data out of the enterprise across multiple threat vectors such as firewalls and proxies, cloud storage, attached storage, or email.
- Lateral movement – a trusted insider user scanning and expanding access across multiple resources.
- Account misuse – accidental misuse or deliberate abuse of superuser privileges.

Enhance visibility and generate rich contextual insights to rapidly assess risk and act decisively

Splunk User Behavior Analytics visualizes threats across multiple phases of an attack to give security analysts a comprehensive understanding of attack root cause, scope, severity and timelines. This context-rich view enables analysts to rapidly assess impact and make informed decisions quickly and confidently. Graph and kill chain analysis provides deep investigative capabilities on any user, entity, anomaly or threat for faster insights.

Simplify and streamline incident investigations and workflows to increase SOC efficiency

Splunk User Behavior Analytics automatically reduces billions of raw events down to tens of threats for rapid review without the need for time-consuming human-fueled detective work performed by an army of highly skilled security and data science professionals. By filtering alerts before they reach the SOC team, Splunk UBA frees up time for security analysts to focus on the most urgent and complex threats.

Pair SIEM with user and entity behavior analytics for comprehensive protection

By combining Splunk User Behavior Analytics’ multi-entity, behavior-based anomaly and threat information with Splunk Enterprise Security’s correlation rules and searches, security teams can establish a potent, wide-reaching defense against the most sophisticated threats. Splunk User Behavior Analytics automatically pushes threat information into Splunk Enterprise Security to create a centralized incident view and an end-to-end investigative workflow.

Get started

Are you ready to learn more about how user and entity behavior analytics can modernize your SOC and help uncover and eliminate the most advanced stealthy threats? Visit the Splunk UBA webpage, take a tour of the product, or speak with a Splunk security expert now.

splunk>

23-490251-Splunk-The Essential Guide to User and Entity Behavior Analytics -EB-106