Getting started with UBA

With Splunk User Behavior Analytics, you can discover abnormalities and unknown threats that traditional security tools miss; automate stitching of hundreds of anomalies into a single threat; and use deep investigative capabilities and powerful behavior baselines on any entity, anomaly, or threat. The pages in this guided learning path will help you get started.

- UBA Product Tour

Use cases

If you are considering purchasing Splunk User Behavior Analytics, the use cases described below will help you become familiar with what you can accomplish. If you are already a customer, skip to the next page in this path to get started.

Account misuse

Accidental misuse and deliberate abuse of superuser privileges yield critical compliance and privacy risks with potentially severe financial consequences and damage to your company's reputation. Splunk User Behavior Analytics baselines the regular behavior of each accounts and identifies abnormalities that may indicate excessive usage, rare access, potential sabotage, or covering tracks. Splunk User Behavior Analytics's confidence grows as a user's activity deviates from the user's peer group profile and the enterprise profile. The higher the confidence, the higher the risk. Examples of such detections include using service accounts to do VPN or interactive logins, data snooping, deleting audit logs, and accessing confidential information.

Compromised user account

Splunk User Behavior Analytics identifies situations where user credentials have been stolen and are being used by someone other than the authorized human user or application. This use case can also detect shared account usage and generic account abuse. Splunk User Behavior Analytics uses behavior modeling to identify any deviation of user activity from normal thereby indicating that someone other than the legitimate owner is operating the account. Detection encompasses identifying unusual or malicious AD activity such as operations on self, terminated users, disabled accounts, and account recovery.

Compromised and infected machine

Splunk User Behavior Analytics can identify compromised network endpoints that are infected by malware or are otherwise behaving suspiciously. This differs from the Compromised User Account use case in that malicious activity might be detected on a host but not necessarily linked to a specific user account. For example, command and control traffic can be identified from a system where no user is currently logged in. Behavior-based modeling enables Splunk
User Behavior Analytics to identify malware activity irrespective 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, or characteristics of the domains.

**Contextual intelligence**

Splunk User Behavior Analytics learns 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. For example, if an analyst suspects that an endpoint has been compromised, the analyst can use Splunk User Behavior Analytics to learn about that desktop's users, their regular behavior, and even the role of that endpoint in the network. For example, is the endpoint a server or a workstation, and is it used for system administration or business functions?

**Data exfiltration**

Unauthorized or malicious data exfiltration may occur even by action of authorized users. As a result, this use case is focused on identifying this type of activity, which is necessary even when the ability to detect compromised accounts and endpoints is in place. Splunk User Behavior Analytics detects loss or theft of private and confidential data out of enterprise across multiple threat vectors such as network security infrastructure including firewall and proxies, online cloud storage, attached storage including USB devices, and email.

**Lateral movement**

Lateral movement involves a trusted insider 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 be machines, network file shares, box folders etc. Accesses can either be network scans, brute force logins or legitimate logins.

**Suspicious behavior and unknown threats**

In cases when there are not enough pre-defined signatures or correlations to cover some scenarios, Splunk User Behavior Analytics can effectively identify unknown scenarios by identifying anomalies based on deviations in the user or device activity in comparison with self or peer group baselines, suspicious or malicious activity, and alerts from external tools and correlating them into a threat. These suspicious account activities and unknown threats often demand further investigation and can lead to other potential threats such as malvertising, account compromise, account misuse, policy violations, or misconfiguration. The Suspicious Behavior / Unknown Threats use case is often used for content building. When an unknown scenario is detected, the scenario can be written into correlation search or threat rules for deterministic detection.