Draft: UEBA for Sentinel

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Concepts

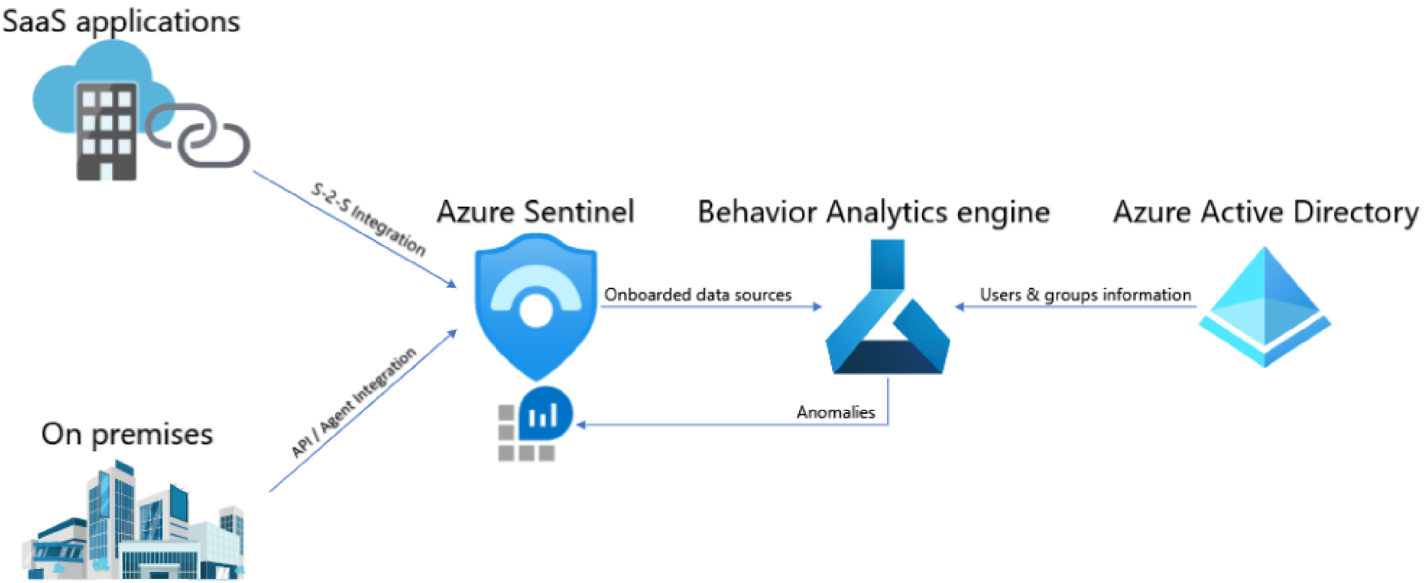
What is Entity Behavior Analytics?

Identifying internal threat sources in your organization, and their potential impact, has always been a labor-intensive process. Sifting through alerts, connecting the dots, and active hunting all add up to massive amounts of effort expended with minimal returns, and the possibility of many internal threats simply evading discovery. Azure Sentinel's Entity Behavioral Analytics (UEBA) eliminates the drudgery from your analysts' workloads and the uncertainty from their efforts, and delivers high-fidelity, actionable intelligence, so they can focus on investigation and remediation. As Azure Sentinel collects logs and alerts from all of its connected data sources, it analyzes them and builds baseline behavioral profiles of your organization's entities (users, hosts, IP addresses, applications etc. across time and peer group horizon. Using a variety of techniques and machine learning capabilities, Sentinel can then identify anomalous activity and help you determine if an asset has been compromised. Not only that, but it can also figure out the relative sensitivity of particular assets, identify peer groups of assets, and evaluate the potential impact of any given compromised asset (its "blast radius"). Armed with this information, you can effectively prioritize your investigation and incident handling.

Entity Page

When you select any entity (user, host, IP address...) in an alert or an investigation, you will land on an entity page, which is basically a portfolio of relevant information about that entity. Each type of entity has its own unique page, since information about users and about hosts will not be of the same type. On the user entity page, you will find basic information about the user, a list of recent events involving the user, summary counts of various types of alerts.

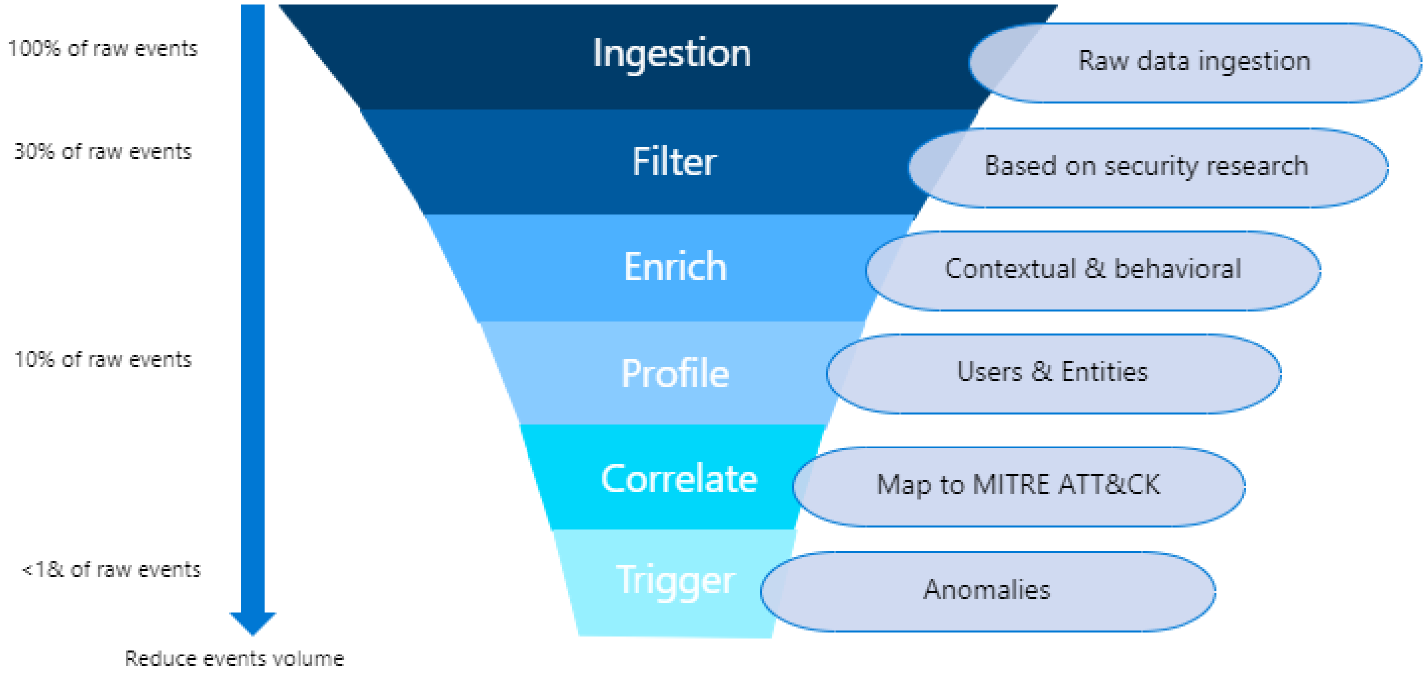
Architecture Overview



Maximized Value

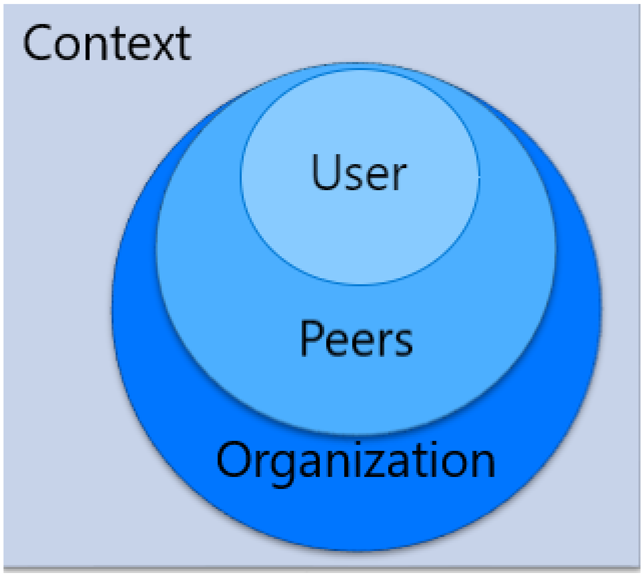
Inspired by Gartner's definition for UEBA solutions, Sentinel Entity Behavioral Analytics provides a "top-down" approach based on 3 different dimensions.

- Use Cases – Researching for relevant attack scenarios that put various entities as victims or pivot points in an attack chain, and adapting those attack vectors into MITRE ATT&CK's tactics, techniques, and sub techniques terminology, Sentinel EBA focuses only on the most valuable logs each data source can provide.
- Data Sources – While seemingly supporting Azure data sources, 3rd party data sources are thoughtfully chosen to provide data that matches our threat use cases.
- Analytics – Using various ML algorithms, evidence of anomalous activities are presents in enrichments such as: first time activity, uncommon activity, contextual information, and more. All evidence is provided in a clear, to the point manner, where a TRUE statement represses an anomaly.



Anomalies provide 'Evidence' that helps SecOps get a clear understanding of the context, and the profiling of the user. The evidence includes information about:

- Context – Geo location, device information & TI
- User behavior
- User Peers behavior
- Organization behavior



Behavior Analytics Table

All the enriched data from connected data source is contained within the Behavior Analytics Table. The table is constructed by the following schema:

Scoring:

Each activity is scored with “Investigation Priority Score” – which determine the probability of a specific user performing a specific activity, based on behavioral learning of the user and their peers. Activities identified as the most abnormal receive the highest scores (on a scale of 0-10).

Example:

https://techcommunity.microsoft.com/t5/microsoft-security-and/prioritize-user-investigations-in-cloud-app-security/ba-p/700136

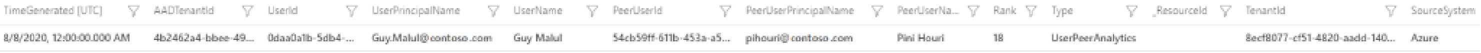
Using KQL, we can query the Behavioral Analytics Table.

For example – in case we’d like to find all the users that failed to login to an Azure, while it was the first attempt to connect from a certain country and is even uncommon for their peers, we can use the following query:

```
BehavorialAnalytics

| where ActivityType == "FailedLogOn"

| where FirstTimeUserConnectedFromCountry == True

| where CountryUncommonlyConnectedFromAmongPeers == True
```

User Peers Metadata Table & Notebook

User peers metadata provides an important context in threat detections, in investigating an incident, and in hunting for a potential threat. Security Analyst can observe the normal activities of the peers of a user to get insights of if the user activities are abnormal comparing to his/her peers. UserPeerAnalytics table provides a ranked list of peers of a user based on the user's group membership in Azure Active Directory. For example, if the user is Guy Malul, Peer Analytics calculates all of Guy's peers based on his mailing list, security groups, etc. and provides all his peers in the top 20 ranking in the table. The screenshot below shows the schema of UserPeerAnalytics table and an example of a row in the table. One of the peers of Guy is Pini. His peer rank is 18. TF-IDF algorithm is used to normalize the weigh for calculating the rank, smaller the group higher the weight.



TimeGenerated [UTC]	AADTenantId	UserId	UserPrincipalName	UserName	PeerUserId	PeerUserPrincipalName	PeerUserNa...	Rank	Type	_ResourceId	TenantId	SourceSystem
8/8/2020, 12:00:00.000 AM	4b2462a4-bbee-49...	0daa0a1b-5db4-...	Guy.Malul@contoso.com	Guy Malul	54cb59ff-611b-453a-a5...	pihouri@contoso.com	Pini Houri	18	UserPeerAnalytics		8ecf8077-cf51-4820-aadd-140...	Azure

Permission Analytic Table & Notebook

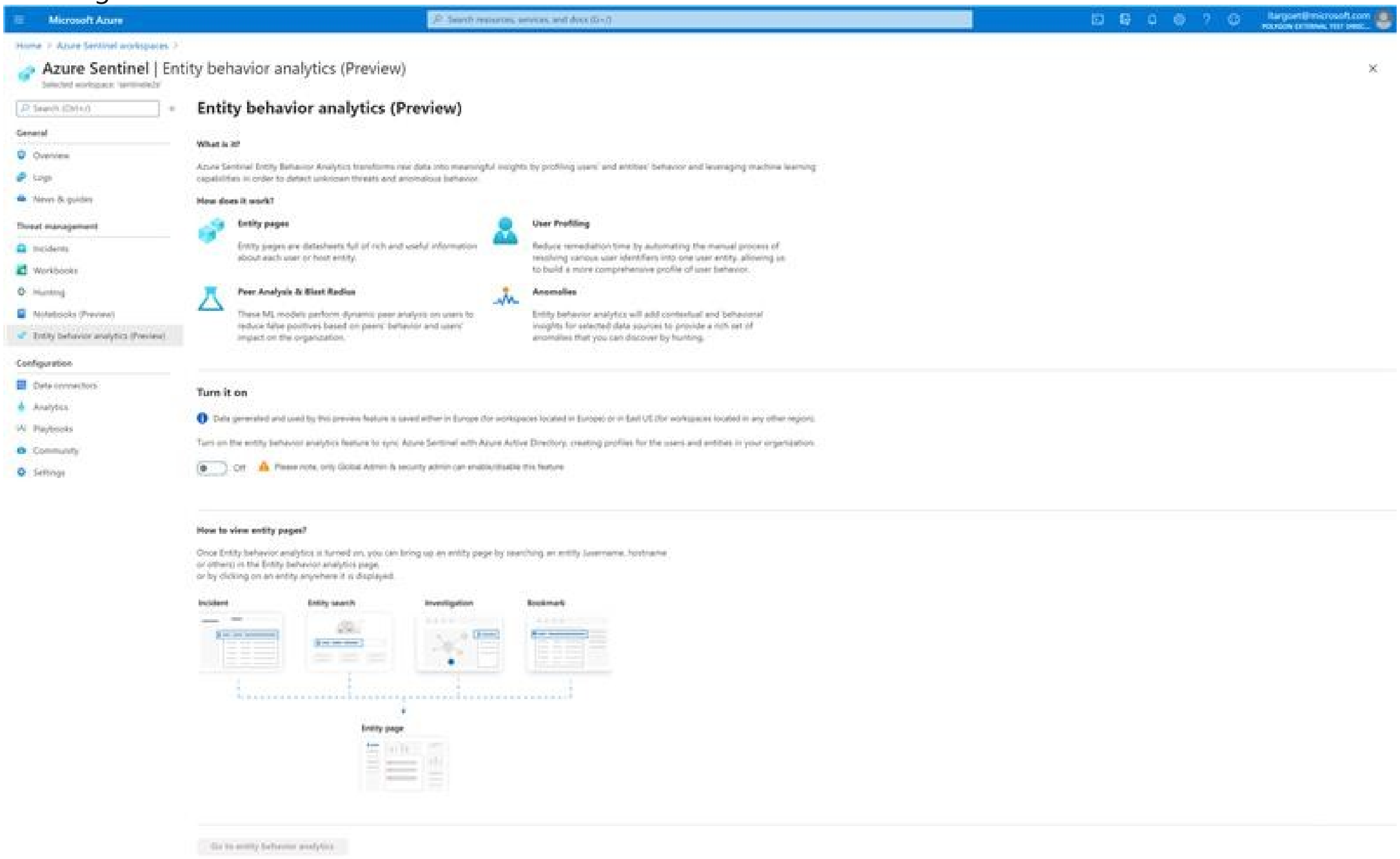
UserAccessAnalytics table provides the direct or transitive access to Azure resources for a given user. For example, if the user under investigation is Jane Smith, user Access Analytics calculates all the Azure subscriptions that she either can access directly, via groups or service principals transitively. It also lists all the Azure Active Directory security groups of which Jane is a member. The screenshot below shows an example row in UserAccessAnalytics table. Source entity is the user or service principle account, Target entity is the resource that the source entity has access to. The value of Access level and Access type depend on the access control model of the target entity. You can see Jane has Contributor access to Azure subscription Contoso Azure Production 1. The access control model of the subscription is RBAC.

Hunting Queries & Exploration Queries

Entity Behavior Analytics provides out-of-the-box set of hunting queries, exploration queries and a workbook. Those will present the enriched data the system generates focused on specific use cases that can indicate anomalous behavior. A great addition to the already existing queries and workbooks that exist in Sentinel. More information regarding hunting in sentinel, and the investigating graph, can be found here: https://docs.microsoft.com/en-us/azure/sentinel/hunting

How-to-guides

Enabling UEBA



Microsoft Azure
Search resources, services, and docs (G+/)
POLYGON EXTERNAL TEST DIREC...
Home > Azure Sentinel workspaces >
Azure Sentinel | Entity behavior analytics (Preview)
Selected workspace: 'sentinelw2z'
Search (Ctrl+/)
General
Overview
Logs
News & guides
Threat management
Incidents
Workbooks
Hunting
Notebooks (Preview)
Entity behavior analytics (Preview)
Configuration
Data connectors
Analytics
Playbooks
Community
Settings
Incident
Entity search
Investigation
Bookmark
Entity page
Go to entity behavior analytics

Entity behavior analytics (Preview)

What is it?

Azure Sentinel Entity Behavior Analytics transforms raw data into meaningful insights by profiling users' and entities' behavior and leveraging machine learning capabilities in order to detect unknown threats and anomalous behavior.

How does it work?

Entity pages

Entity pages are datasheets full of rich and useful information about each user or host entity.

User Profiling

Reduce remediation time by automating the manual process of resolving various user identifiers into one user entity, allowing us to build a more comprehensive profile of user behavior.

Peer Analysis & Blast Radius

These ML models perform dynamic peer analysis on users to reduce false positives based on peers' behavior and users' impact on the organization.

Anomalies

Entity behavior analytics will add contextual and behavioral insights for selected data sources to provide a rich set of anomalies that you can discover by hunting.

Turn it on

Data generated and used by this preview feature is saved either in Europe (for workspaces located in Europe) or in East US (for workspaces located in any other region).

Turn on the entity behavior analytics feature to sync Azure Sentinel with Azure Active Directory, creating profiles for the users and entities in your organization.

○ Off ⚠ Please note, only Global Admin & security admin can enable/disable this feature

How to view entity pages?

Once Entity behavior analytics is turned on, you can bring up an entity page by searching an entity (username, hostname or others) in the Entity behavior analytics page,
or by clicking on an entity anywhere it is displayed.