Título: UEBA – Identificando ameaças avançadas

Data: 23 de dezembro de 2022

Autora: Jessica Sapucaia (http://aka.ms/jessicasapucaia)

Cargo: Gerente de Produto, Segurança na Nuvem – Microsoft

Visão Geral UEBA

User Entity Behavior Analytics (UEBA), segundo o Gartner, são soluções que através de análise de dados, criam perfis e comportamentos padrão de usuários e entidades (hosts, aplicativos, tráfego de rede e repositório de dados) ao longo do tempo e cruzando com grupos pares na organização. Dessa forma, as atividades anômalas a essas linhas de base padrão, são apresentadas como suspeita.

As soluções de UEBA tem como objetivo atendar principalmente aos seguintes **Cenários de Uso**:

- **Abuso de identidades privilegiadas:** Identificando os usuários que possuem permissões elevadas, e que consequentemente trariam alto impacto caso suas credenciais fossem comprometidas;
- **Usuários e entidades comprometidos:** Invasores que obtiveram acesso a contas de usuários e estão realizando atividades mal-intencionadas no ambiente, trabalhando a cadeia do ataque (*kill-chain*) criando desvios no perfil padrão daquele usuário;
- **Ameaças internas e exfiltração de dados:** Usuários internos mal-intencionados que iniciam processo de coleta de dados e informação confidenciais, com o objetivo de exfiltrá-las, causando potenciais danos financeiros à organização.

Microsoft Sentinel - UEBA

Quando falamos de soluções Microsoft, é o Microsoft Sentinel que contempla a funcionalidade de UEBA.

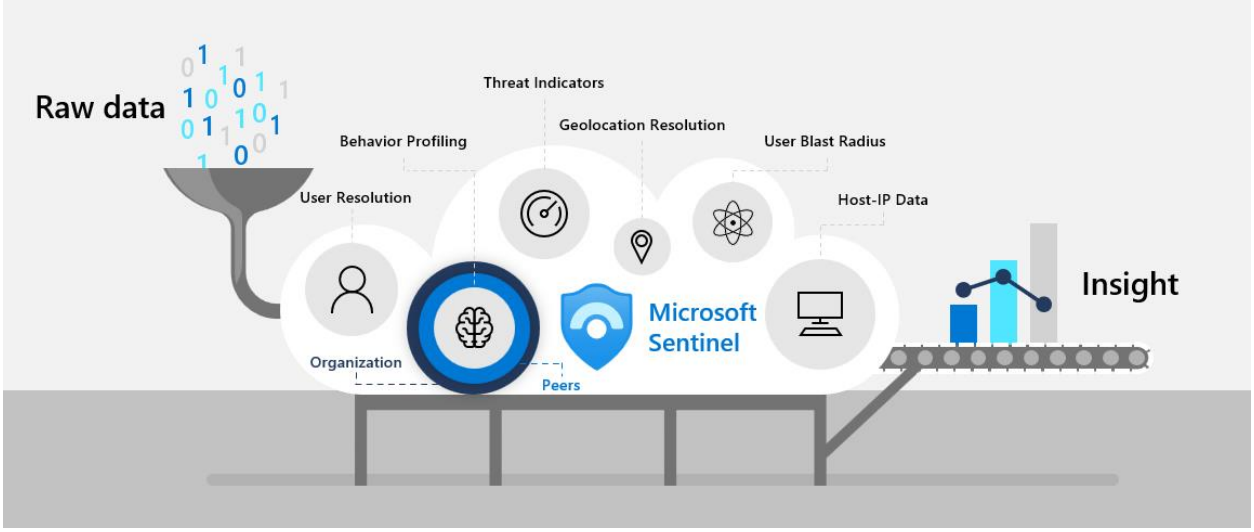
O **Microsoft Sentinel** é a nossa solução nativa da nuvem para *Security Information and Event Management (SIEM), User Entity Behavior Analytics (UEBA) e Security Orchestration, Automation and Response (SOAR).*

No último Quadrante Mágico do Gartner, o Microsoft Sentinel foi considerado o líder de mercado nessas soluções, maiores detalhes podem ser conferidos na publicação oficial do Gartner.

Inteligência e Mecanismos por trás do UEBA

Quando o assunto é UEBA, a utilização de modelos de Aprendizado de Máquina e Inteligência Artificial são imprescindíveis para uma solução eficiente.

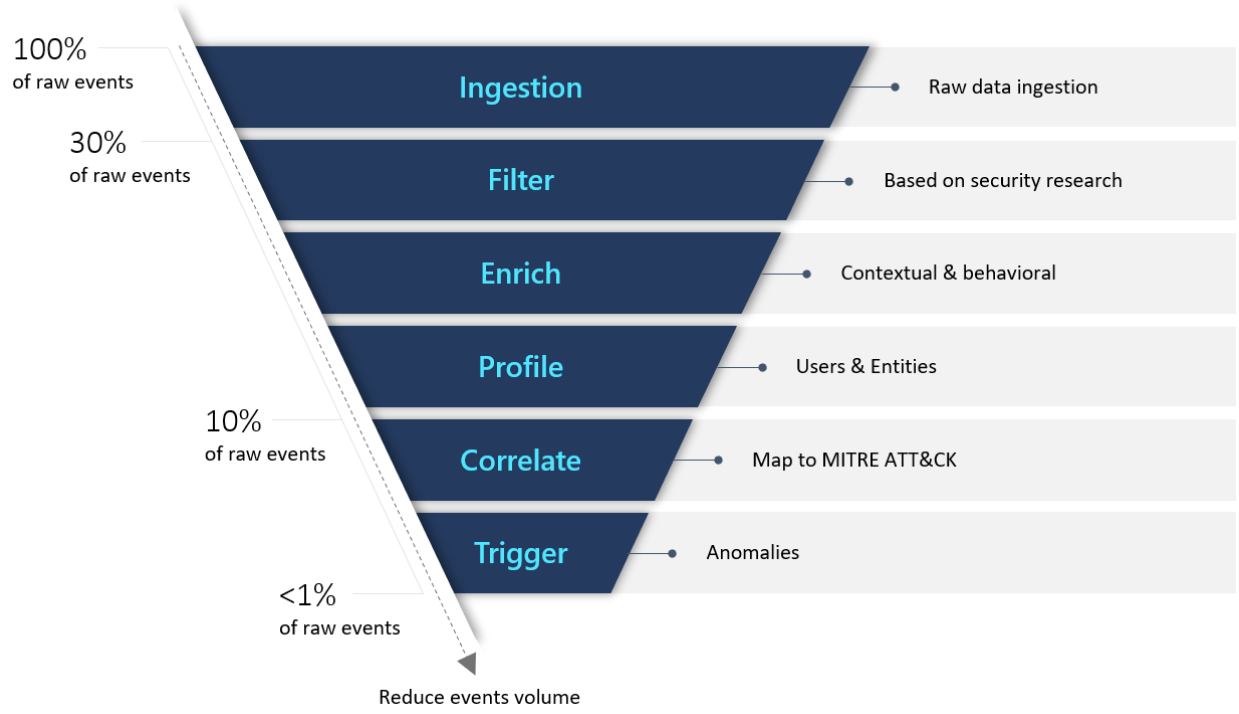
Abaixo podemos observar uma representação gráfica do processo de análise e enriquecimento de dados que acontece no Microsoft Sentinel:



Gostaria de destacar os seguintes pontos da representação acima:

- **Behavior Profiling** - essa fase é o núcleo de todo o processo de UEBA, onde é definida o Perfil de Comportamento daquela entidade, e para realizá-lo, são observados três aspectos da entidade:
    - *User behavior* – processo de avaliação se esse usuário normalmente realiza as atividades apresentadas, análise do perfil padrão
    - *User peers behavior* – através do nosso algoritmo de avaliação dos pares, é analisado se as atividades detectadas são comumente performadas pelos pares daquele usuário
    - *Organzation behavior* – e por último, é realizada uma análise considerando o comportamento e perfil padrão da organização naquele segmento
- **User Blast Radius** – esse item é responsável por calcular o potencial impacto que teria na organização caso essa entidade fosse comprometida. Para realizar isso são considerados dois principais pontos:
    - Privilégios e permissões – caso o usuário seja, por exemplo, Administrador Global do Domínio, o nível de potencial impacto é agravado
    - Posição na hierarquia da organização – quanto mais alto no nível hierárquico, é considerado um risco maior de impacto no cálculo do User Blast Radius

Também é importante compreender o processo de tratativas e filtros realizados no dado puro, para que alertas de alta fidelidade sejam gerados. Abaixo encontramos uma representação gráfica do fluxo que os dados percorrem no Microsoft Sentinel:



Na primeira fase acontece a **ingestão dos dados** puros/dados não tratados (raw data) oriundos das conexões existentes no Microsoft Sentinel, como fontes de dados podemos ter o Azure AD e/ou AD on-premises.

Na segunda fase já é realizado o **filtro** inicial desses dados, mantendo assim as informações que serão relevantes para o restante do processamento e análise.

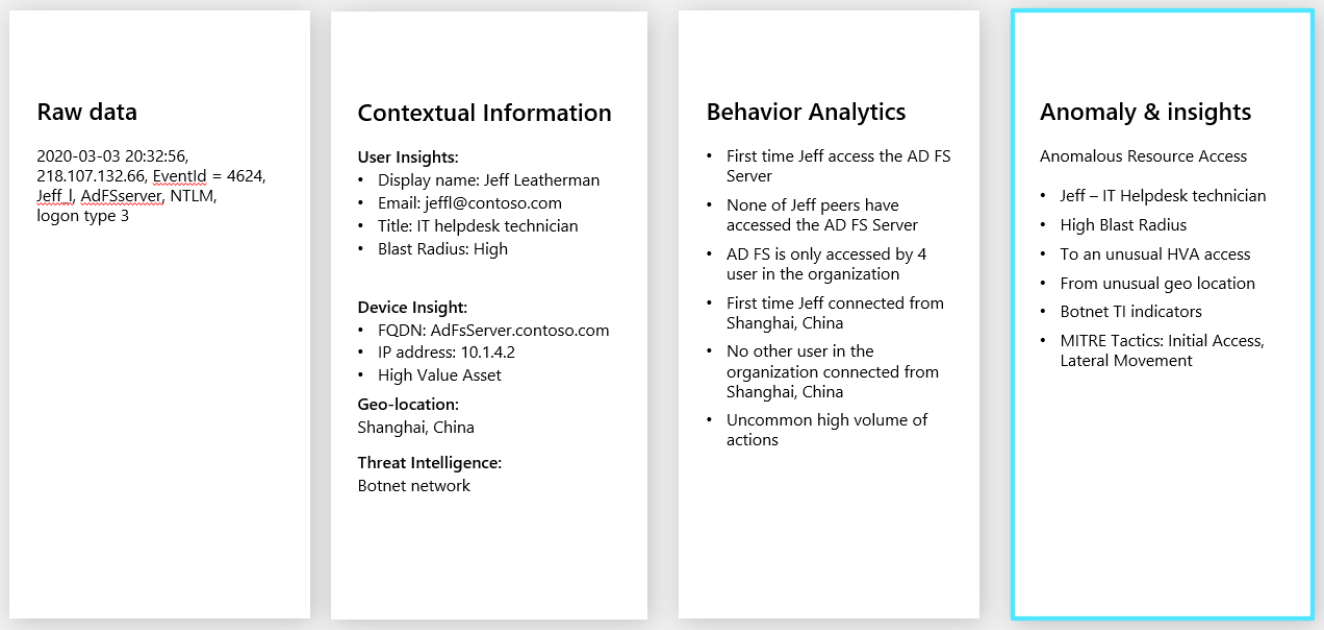
Na terceira fase, acontece o processo de **enriquecimento dos dados**, onde informações que tragam contexto para aquele evento são adicionadas, exemplo: localidade que aquele usuário está definido no AD, grupos de segurança que esse usuário faça parte, dispositivo que foi acessado (avaliando se é um dispositivo considerado High Value Asset, ou seja, dispositivos que executam atividades importantes para a companhia, como um servidor ADFS por exemplo) e etc.

Na quarta fase é realizada a análise do que conhecemos com o **perfil padrão** daquele usuário ou entidade, versus o que foi identificado até o momento com os filtros e enriquecimento dos dados. Para que assim, possamos detectar possíveis ações que estão saindo do padrão definido.

Na quinta fase um **mapeamento com as táticas, técnicas e procedimentos do MITRE ATT&CK** é realizado, para que possamos identificar e responder o mais rápido possível o tipo de ataque que estamos sofrendo.

E por último, na sexta fase é gerado de fato os **alertas com as atividades anômalas** identificadas após toda a análise descrita acima.

Abaixo temos um exemplo de como seria um fluxo real dos dados, o processo de enriquecimento e contexto, avaliação do perfil de comportamento do usuário, pares e organização, para no final gerar o alerta de anomalia.



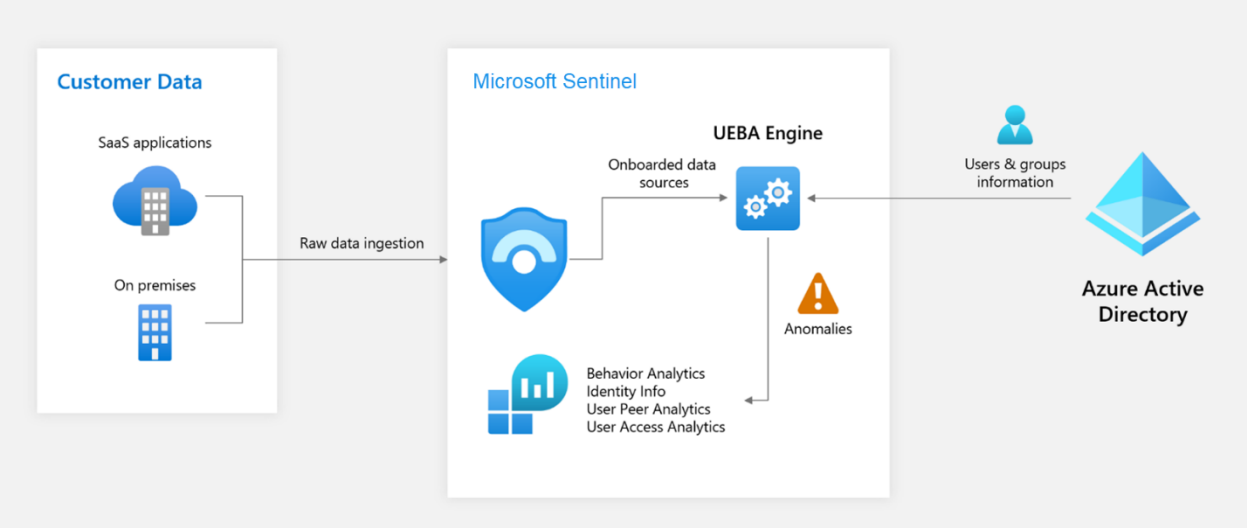
Arquitetura da Solução

O Microsoft Sentinel é uma solução nativa na nuvem, o que não exige infraestrutura de servidores para que o recurso seja habilitado.

As fontes de dados suportadas atualmente para conexão no UEBA são:

- Azure Active Directory
    - Sign-in logs
    - Audit logs
- Azure Activity logs
- Windows Security Events (Active Directory On-Premises)
    - Para utilizar essa fonte de dados é requisito possuir o Microsoft Defender for Identity nos Controladores de domínio

Maiores detalhes das fontes de dados UEBA.



Para maiores informações e documentação completa da solução, indicamos os seguintes recursos:

- Identificar ameaças avançadas com UEBA no Microsoft Sentinel - https://learn.microsoft.com/pt-br/azure/sentinel/identify-threats-with-entity-behavior-analytics
- Tutorial: Investigar incidentes usando dados do UEBA - https://learn.microsoft.com/pt-br/azure/sentinel/investigate-with-ueba?source=recommendations
- Referência do UEBA - https://learn.microsoft.com/pt-br/azure/sentinel/ueba-reference
- Webinar em Inglês sobre UEBA - https://www.youtube.com/watch?v=dLVAkSLKLyQ