Microsoft Security

Microsoft Sentinel

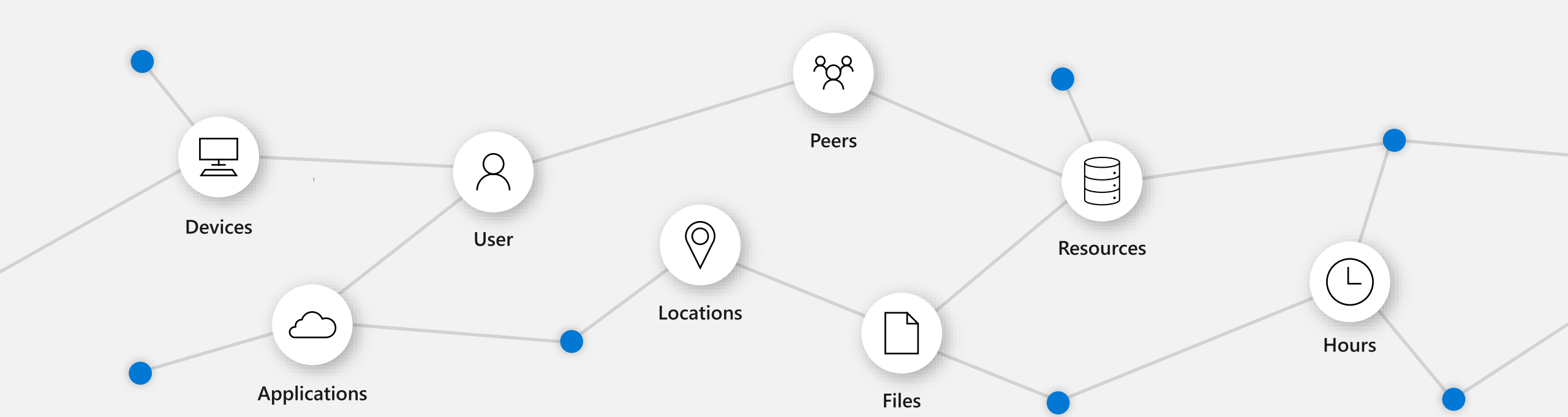
User and Entity Behavior Analytics (UEBA)

Zachary (Zach) Riffle

User and Entity Behavior Analytics

User Entity Behavior Analytics (UEBA) solutions use analytics to **build profiles** and behaviors of **users and entities** (hosts, applications, network traffic and data repositories) **across time and peer group horizons**. Activity that is anomalous to these standard baselines is presented as suspicious.

Gartner

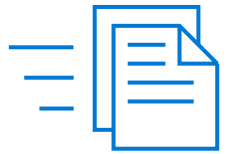


User and Entity Behavior Analytics Use Cases

Abuse of privileged identities

Compromised user and entity

Insider Threat



Data exfiltration

Introducing Microsoft Sentinel User and Entity Behavior Analytics

Our approach – Keep it simple!

Detect anomalies based on entity behavior profiling

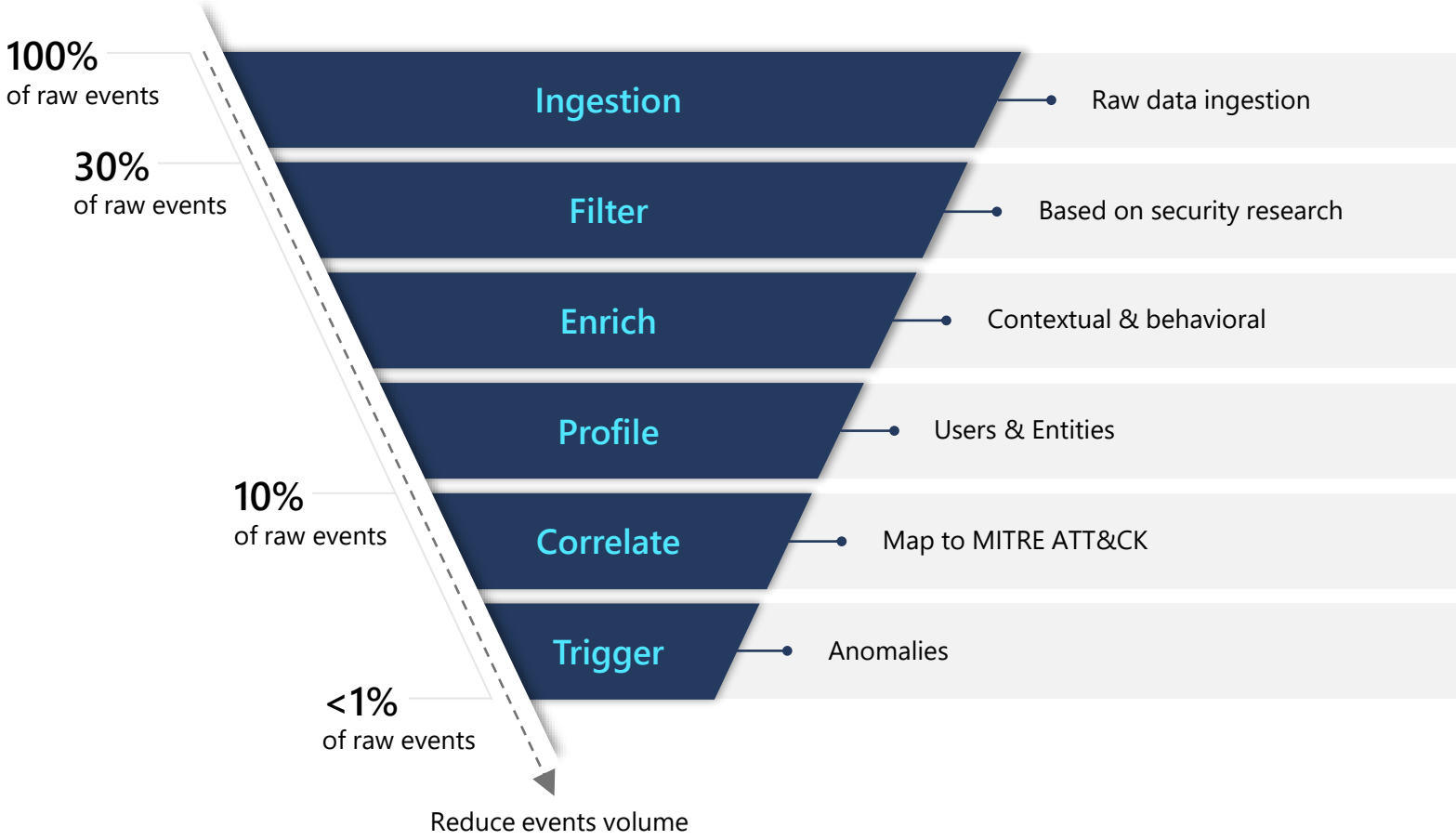
Investigation & hunting with **contextual and behavioral information**

Entity pages provides clear insight, timeline and investigation prioritization

Instant security value following quick & simple onboarding

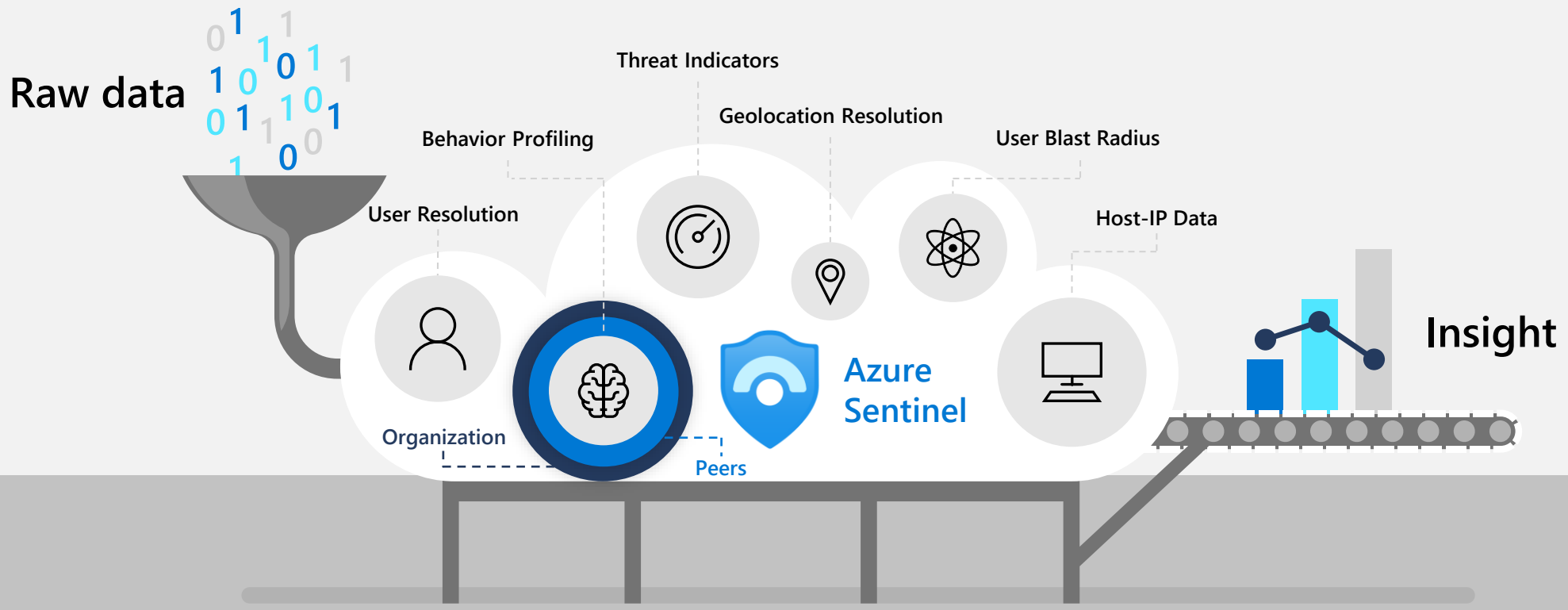
Focus on what's Important

User and Entity Behavior Analytics leverage Microsoft security experts to define scenarios based on real life attacks, mapped to MITRE ATT&CK



ATT&CK®

User and Entity Behavior Analytics Engine



Transforming raw data to anomalies & Insights

Raw data

2023-03-03 20:32:56,
218.107.132.66, EventId = 4624,
Jeff_I, FinanceSRV, NTLM,
logon type 3

Contextual Information

User Insights:
Display name: Jeff Leatherman

- Email: jeffl@contoso.com
- Title: IT helpdesk technician
- Blast Radius: High
- Dormant Account:
  12.07.22 – 03.03.2023

Device Insight:

- FQDN: FinanceSRV.contoso.com
- IP address: 10.1.4.2
- High Value Asset
- Asset Owner: Dan Marino
- Device is unmanaged

Geo-location:
Pyongyang, North Korea

Threat Intelligence:
Botnet network

Behavior Analytics

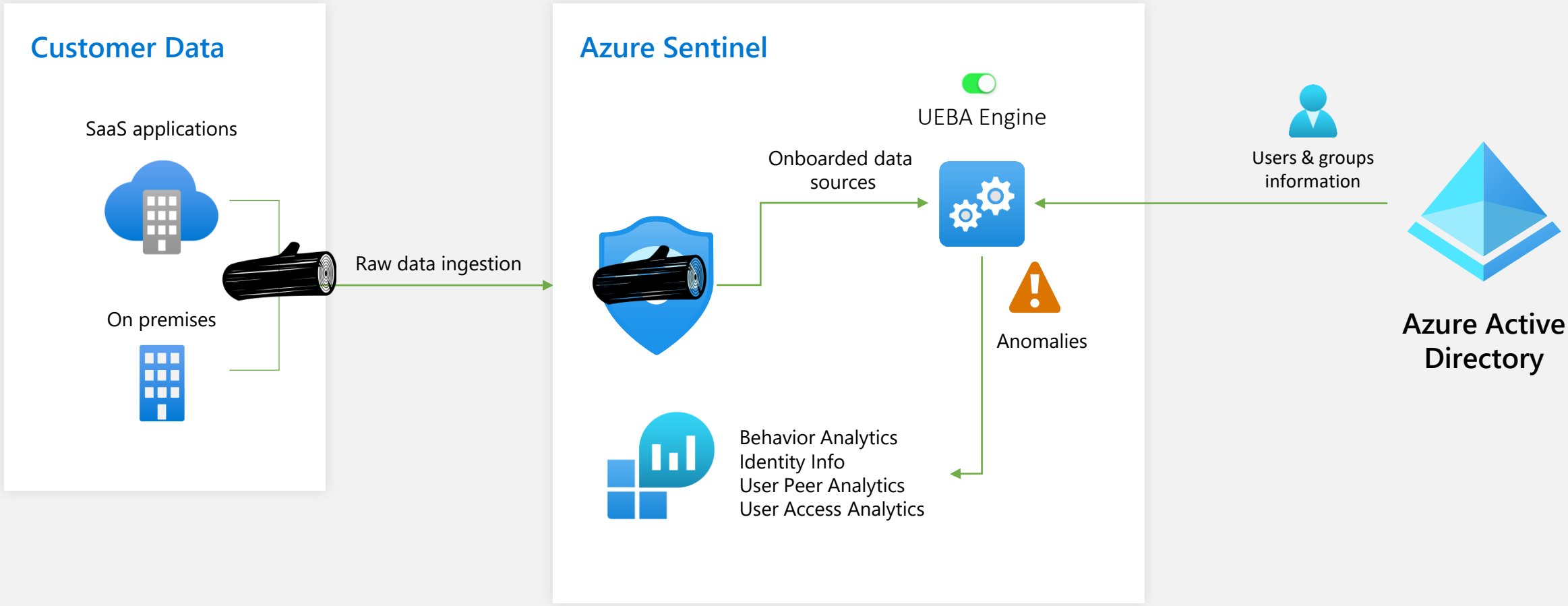
- First time Jeff access the FinanceSRV
- None of Jeff's peers have accessed the FinanceSRV
- FinanceSRV is only accessed by 4 users in the organization
- First time Jeff connected from Pyongyang, North Korea
- No other user in the organization connected from Pyongyang, North Korea

Anomaly & insights

Anomalous Resource Access

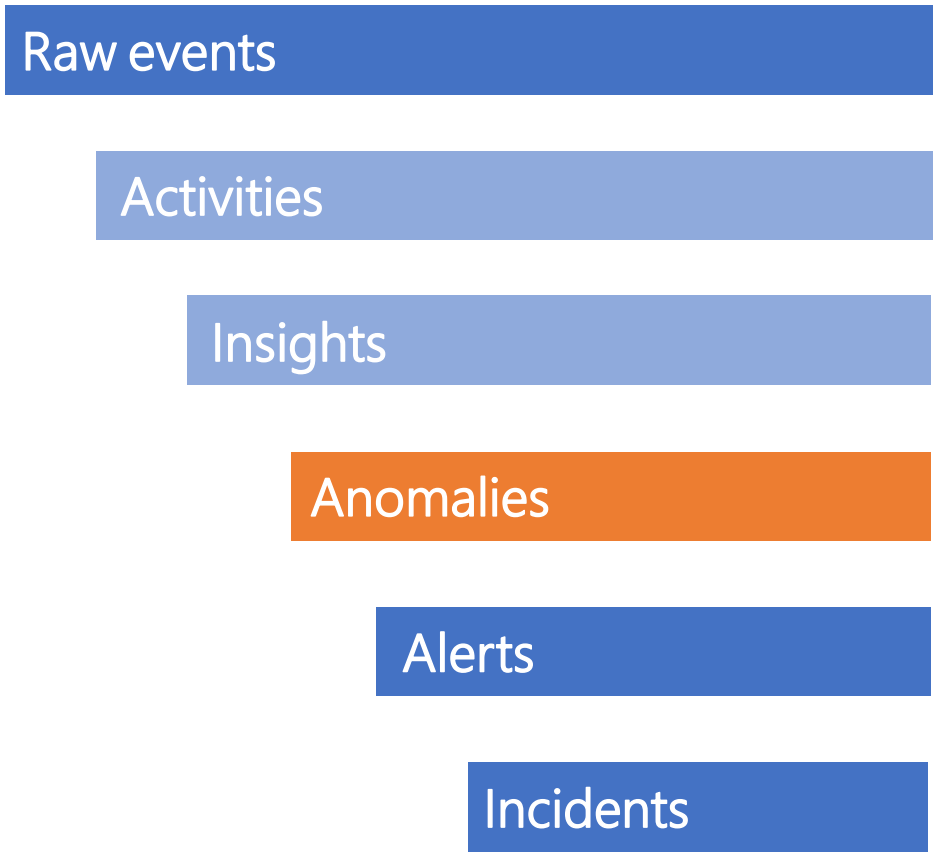
- Jeff – IT Helpdesk technician
- Recently dormant
- High Blast Radius
- To an unusual HVA access
- From unusual geo location
- Botnet TI indicators
- MITRE Tactics: Initial Access, Lateral Movement

Architecture Overview



UEBA Anomalies

Behavioral anomalies, based on dynamic baselines created for each entity across various data inputs.



Behavior	Data Source	Activity
Sign-in	Azure	Sign-in
	Windows security	4624
	Pulse Secure	NWC23464

Any kind of anomaly

Anomalous sign-in
(Persistence | Valid Accounts)

Demo