User and Entity Behavior Analytics

Shankar Subramaniam

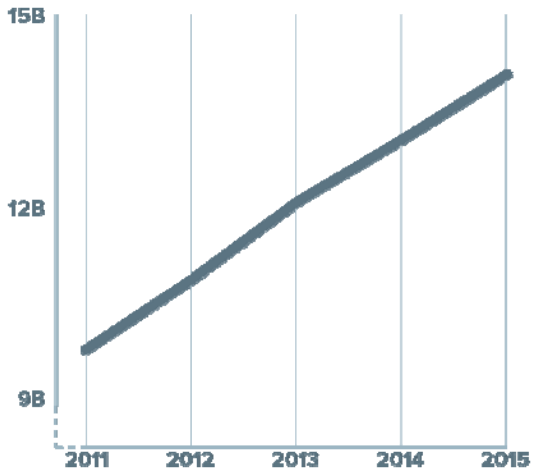
Co-Founder, Niara

Senior Director of Customer Solutions, HPE Aruba Introspect

shasubra@hpe.com

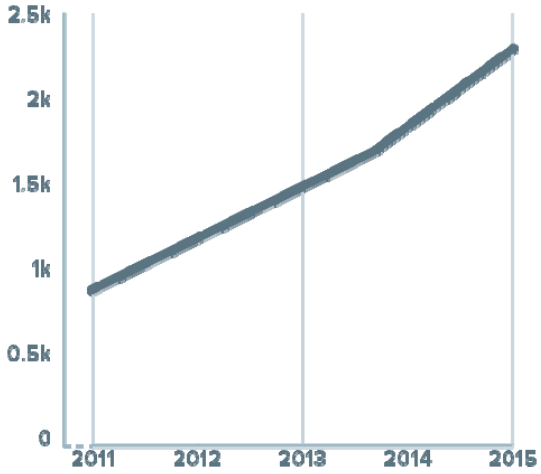
THE SECURITY GAP

SECURITY SPEND

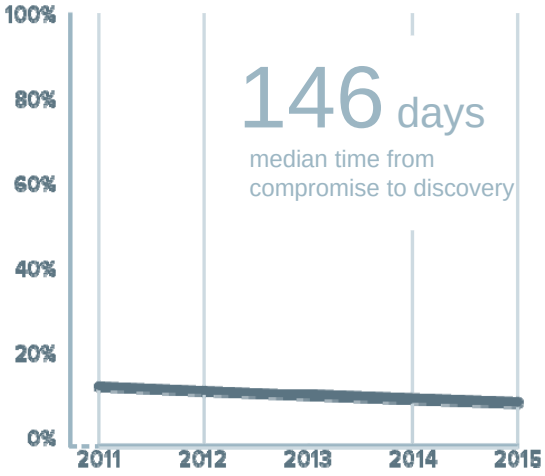


PREVENTION & DETECTION (US $B)

DATA BREACHES



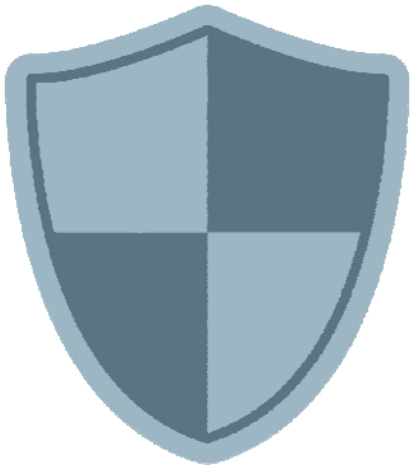
BREACHES



% DISCOVERED INTERNALLY

SOURCES | Mandiant M-Trends 2016, Verizon Data Breach Investigations 2016, IDC 2016

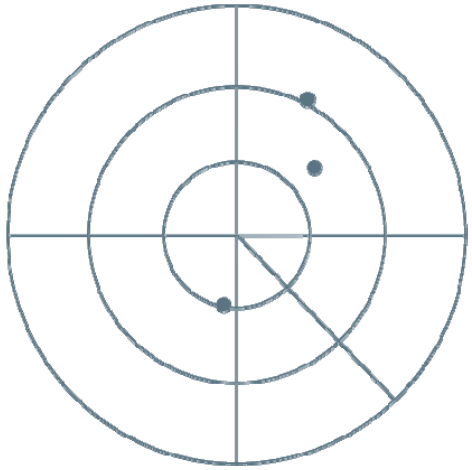
THE PROBLEM



PREVENTION & DETECTION NOT ENOUGH

INCREASINGLY POROUS

+



MONITORING SYSTEMS FALLING SHORT

CANNOT DETECT UNKNOWN THREATS

Attacks involving legitimate credentials

COMPROMISED

40 million credit cards were stolen from Target's severs

STOLEN CREDENTIALS

MALICIOUS

Edward Snowden stole more than 1.7 million classified documents

INTENDED TO LEAK INFORMATION

NEGLIGENT

Employees uploading sensitive information to personal Dropbox for easy access

DATA LEAKAGE

Behavioral Analytics

AUTOMATED DETECTION
of threats inside the organization

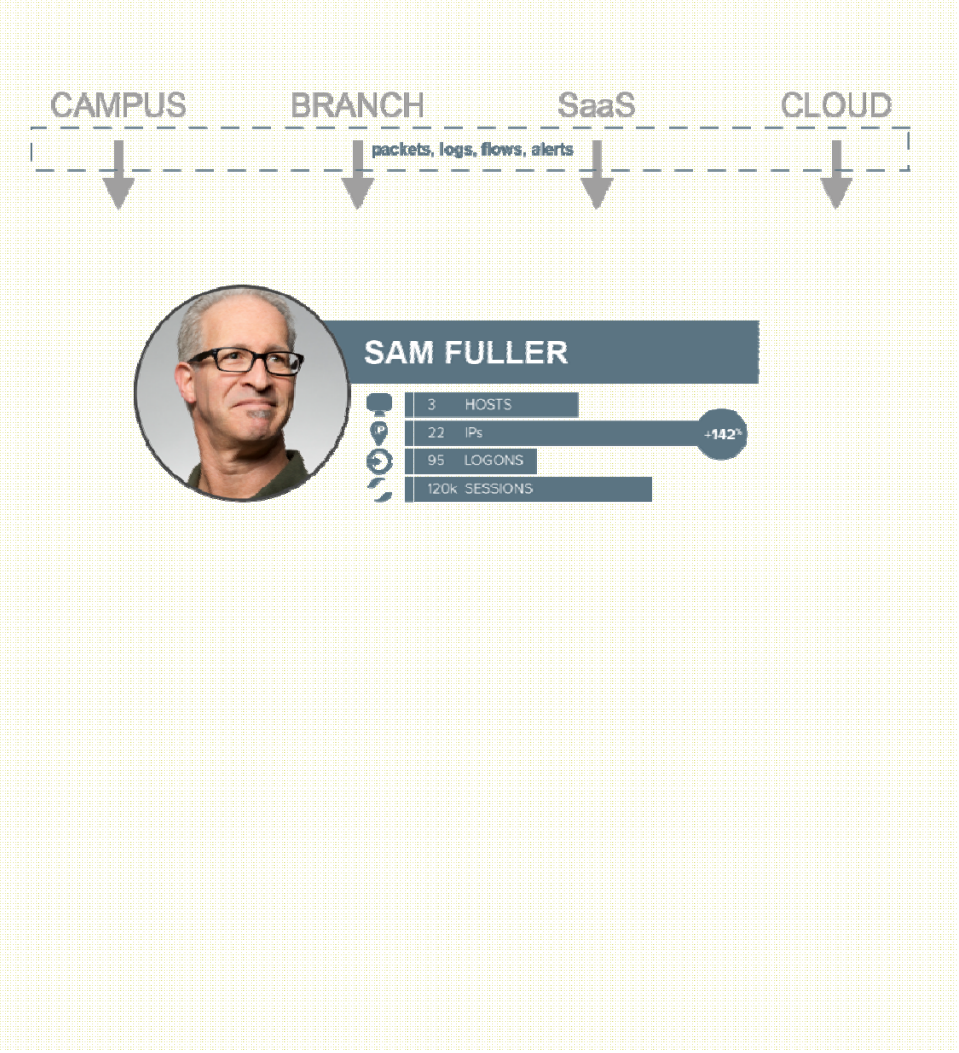
FORCE MULTIPLIER
for security analysts

Basics of Behavioral Analytics

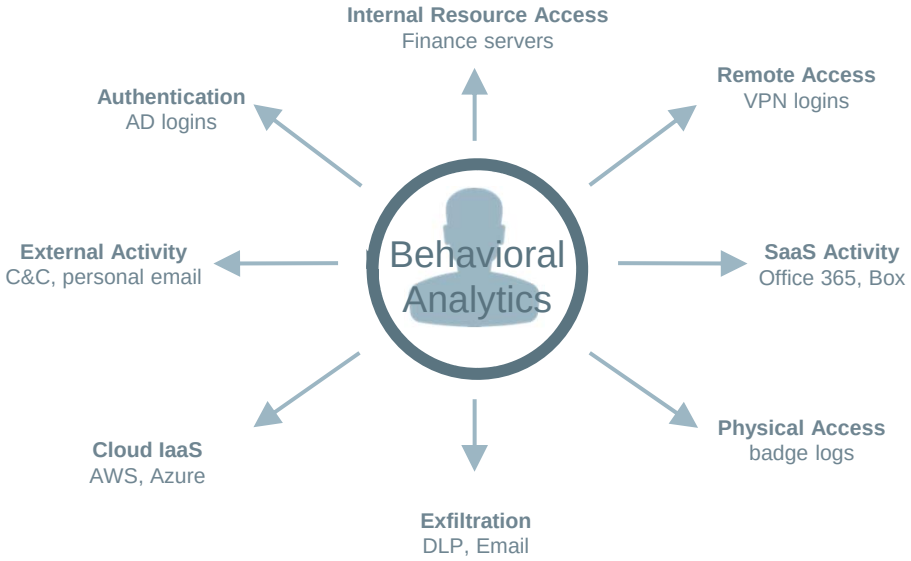
MACHINE LEARNING
UNSUPERVISED
+
SEMI-SUPERVISED

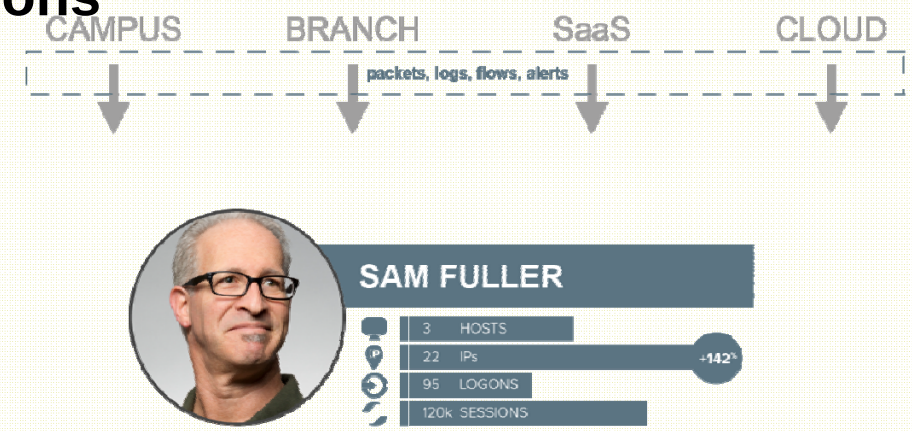
Behavioral Analytics

BASELINES
HISTORICAL
+
PEER GROUP

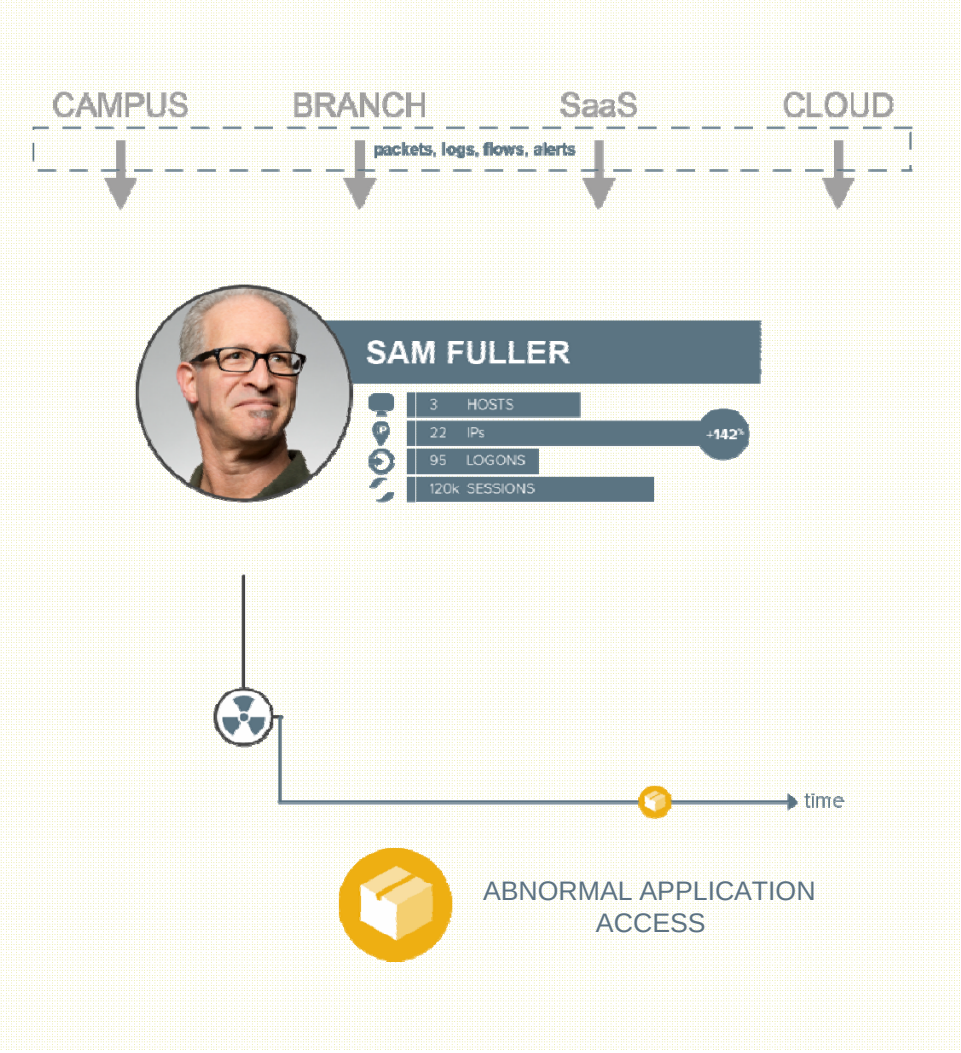


Behavior – Many different dimensions





DETECTING AN ANOMALY



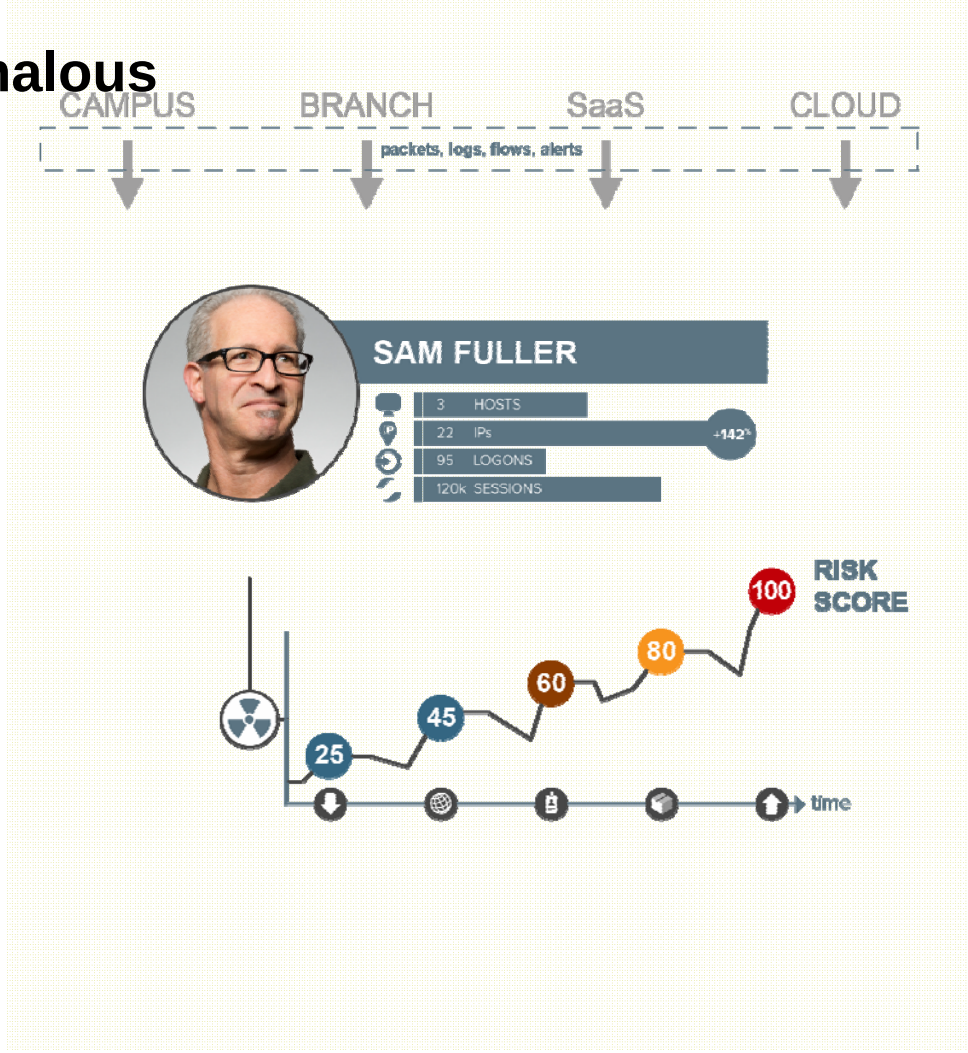
Finding the malicious in the anomalous

MACHINE LEARNING

SUPERVISED
UNSUPERVISED

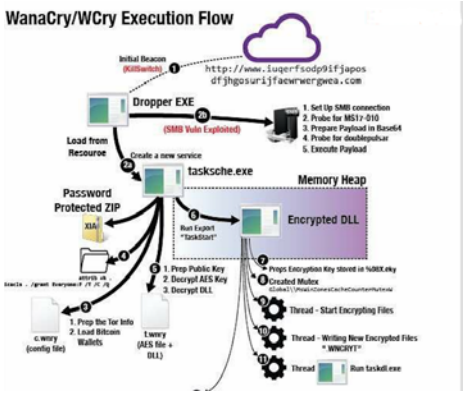
THIRD PARTY ALERTS

DLP
Sandbox
Firewalls
STIX
Rules
Etc.



Ransomware Example

WannaCry Ransomware Attack



Indicators

C&C Communication

SMB based bot scanning

75
RISK SCORE

UEBA

- DGA Detection e.g. iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.], xxlvbrloxvriy2c5[.], sqjolphimrr7jqw6[.], 76jdd2ir2embyv47[.]

- Behavioral Analytics on baseline behavior of systems and detecting anomalous communication patterns

Stateful Risk Score for Compromised System

Data Exfiltration Example

Indicators

Access to internal sensitive information

Moving sensitive data offshore

UEBA

- Abnormal access to internal data

- Abnormal USB writes
- Abnormal Uploads to Box, Dropbox

High Risk Score for user

Abnormal Privileged Insider Activity Example

Indicators	UEBA
Privilege Escalation	• Escalation of privileges for user not entitled to admin role
Abnormal Data access	• Excessive Service Ticket requests • Abnormal data access patterns

High Risk Score for user

Need for dimensionality

Multiple techniques, Expertise in security domain

Supervised	Supervised with manual review	Unsupervised
DNS-DGA (Naïve Bayes) DNS Exfiltration (Logistic Regression)	DNS Tunneling (K-means clustering)	UBA-Server (SVD with Mahalanobis distance) GUEBA (z-score)

Data Source Diversity Matters

Type	Examples	Purpose
Network activity	▪ Firewall ▪ IDS/IPS ▪ Web Proxy ▪ Email ▪ Bro logs, ▪ Network traffic ▪ Network flows	▪ Lateral movement ▪ Abnormal resource access ▪ Browser exploits ▪ Malware activity ▪ Suspicious file downloads ▪ Command and control activity ▪ Beaconing
Remote Access activity	VPN logs	▪ Credential theft, password sharing
Identity	AD, DHCP logs	▪ Credential violations ▪ Account takeover ▪ Privilege escalations
Infrastructure	DNS logs	▪ Command and control activity ▪ Tunneling ▪ Exfiltration
3rd party alerts	FireEye, WildFire alerts	▪ Incorporate alerts into user risk profiles
Threat Intelligence feeds	Commercial & STIX feeds	▪ Perform historical impact assessment
Endpoint Logs	DLP, FIM	▪ Suspicious file activity ▪ USB, cloud based file exfiltration
Physical activity	Badge logs	▪ Building access violations ▪ Tailgating

Lateral Movement

Features	Data Source
Authentication activity ▪ Successful/Failed login activity rates ▪ Password change rates ▪ Odd time of logins ▪ New host logins ▪ Excessive user logons on hosts ▪ Locked/disabled/expired account/restricted workstation logins	▪ AD Logs
Access to internal applications / servers/ peers ▪ Odd time of access (first and last access) ▪ Upload/download deviations ▪ Abnormal activity duration/ session count ▪ New server / application / peer access ▪ Port counts	▪ Packets ▪ NetFlow ▪ Firewall logs

Account Takeover

Features	Data Source
Authentication activity ▪ Service ticket request rates ▪ Unique/New service ticket requests ▪ Account creation/ disable/ lockout / deletion rates ▪ Group change deviations ▪ Locked/disabled/expired account/restricted workstation logins	▪ AD Logs
Access to internal applications/ servers/ peers ▪ Odd time of access (first and last access) ▪ Upload/download deviations ▪ Activity duration/ session counts ▪ New server / application access ▪ New host access ▪ Port counts	▪ Packets ▪ NetFlow ▪ Firewall logs

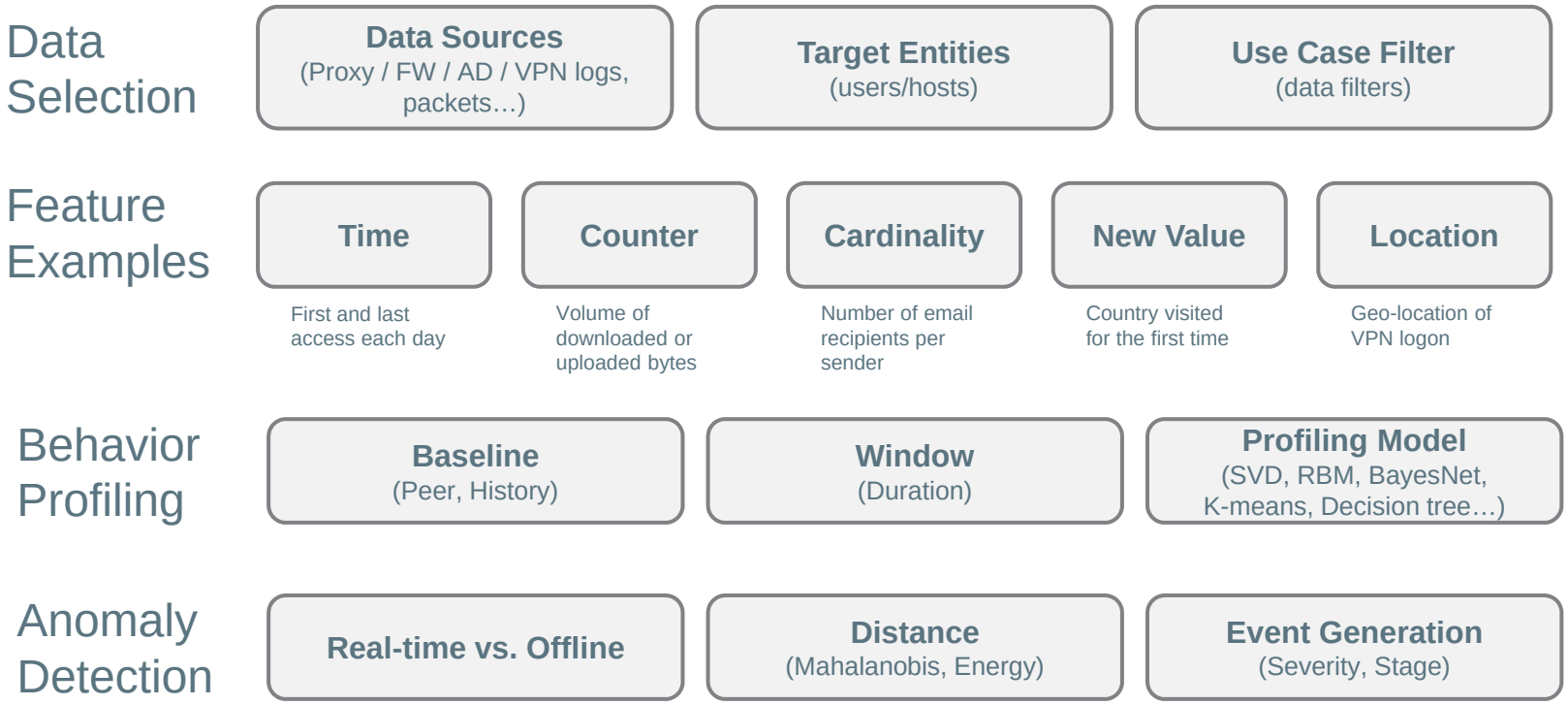
Infiltration / Credential Compromise

Features	Data Source
▪ Land-speed violations: Access from different locations that violate the physical limits of movement between them (city or country) ▪ City: New city access for the first time ▪ Activity duration/ session counts ▪ Bytes in, bytes out ▪ Odd time of access (first and last access)	▪ VPN logs

Exfiltration

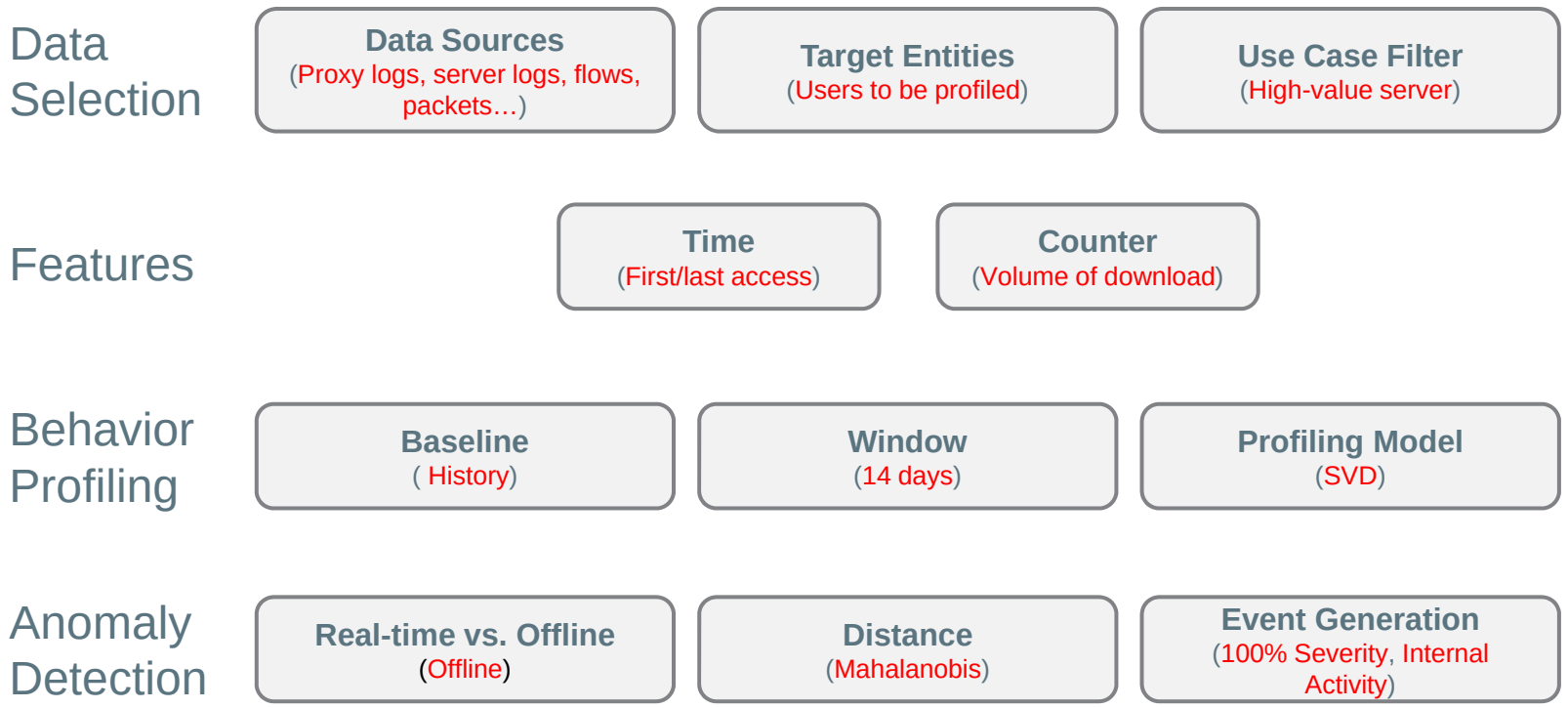
Features	Data Source
▪ DNS-Exfiltration	▪ DNS logs or traffic
Access to internet / external applications / cloud apps ▪ Time of access ▪ Upload/download deviations ▪ Activity duration/ session counts ▪ New server / application access ▪ Port counts ▪ Country visited – New /Counts ▪ Entropy Mismatch	▪ Packets ▪ NetFlow ▪ Firewall logs ▪ Web Proxy logs
Email activity ▪ Odd time of email activity ▪ Upload/download deviations ▪ Attachment size/volumes ▪ Email counts ▪ Suspicious / disposable domains ▪ Activity to non-corporate or non-affiliated domains	▪ Email traffic ▪ Email logs
Endpoint Activity ▪ Volume of data written to USB, first time USB writes ▪ New processes / Registry changes ▪ New file creations/ modifications/ opened/ created ▪ Changes in file read/write/deletes/ permissions	▪ File Integrity Monitoring ▪ DLP logs ▪ Endpoint logs

Generalized Behavioral Analytics



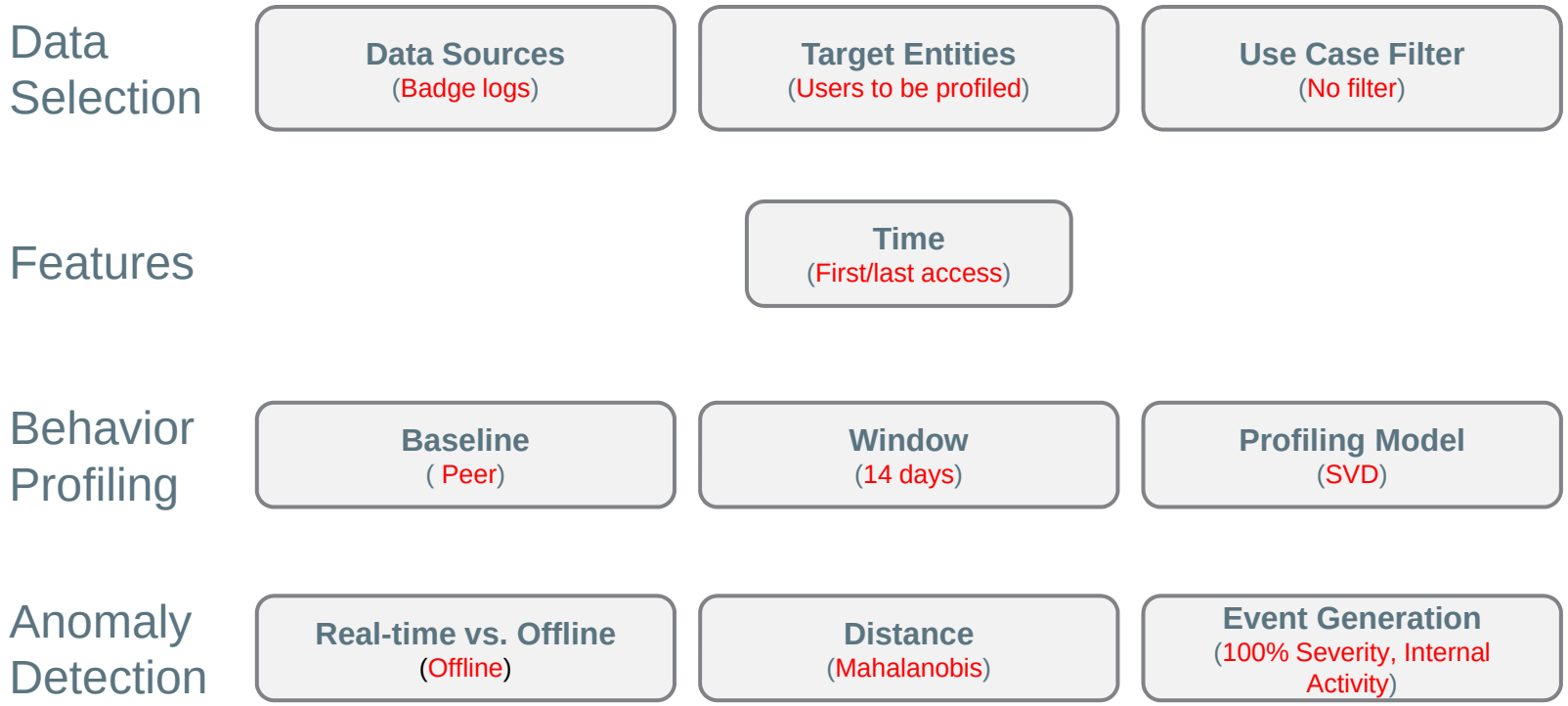
Behavioral analytics for resource access - server

Identifying abnormal access to high value servers by time and download volume



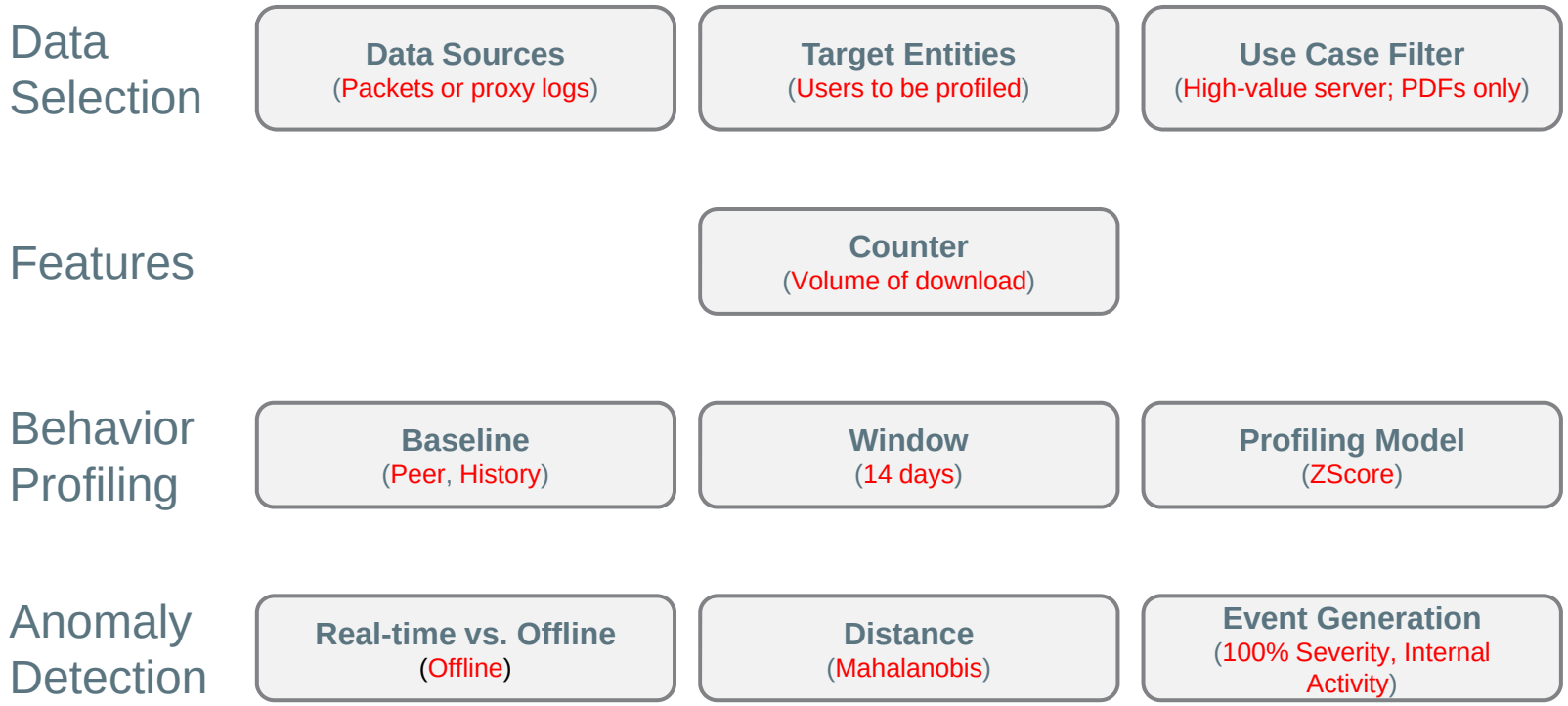
Behavioral Analytics for Resource Access - Building

Identifying abnormal access to physical facility



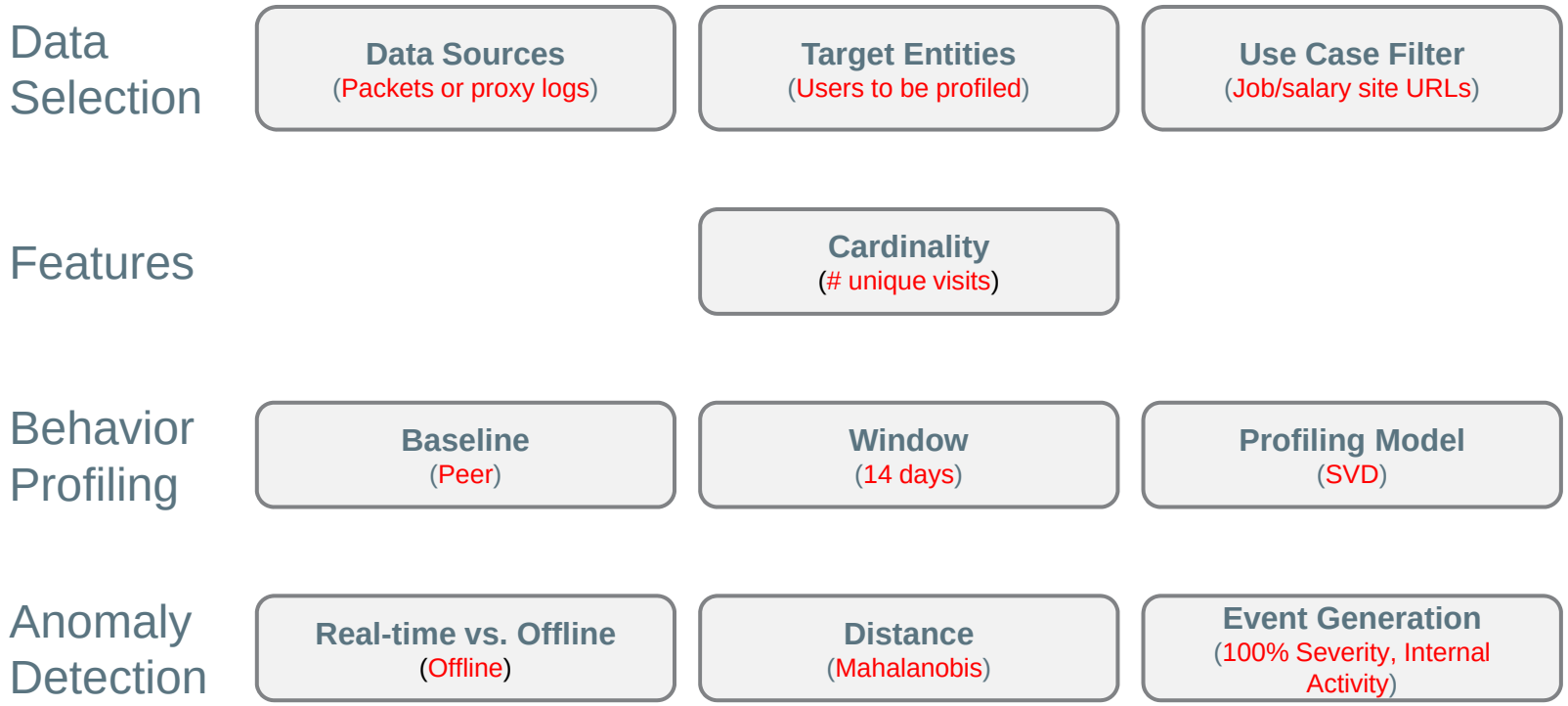
Behavioral Analytics for Resource Access - Files

Detecting abnormally high PDF downloads



Behavioral Analytics for access to job sites

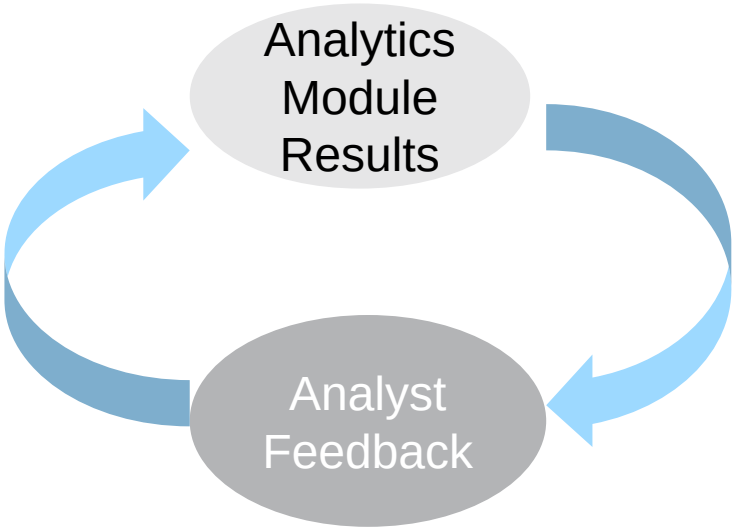
Identifying flight risk users



Differentiated Risk Scoring

- Contextually weighted model
  - Hidden Markov Model
  - Unlike competitors that linearly add up scores for all detected events
  - E.g., a C&C event followed by a privilege escalation event is treated differently from two consecutive C&C events
- Score incorporates:
  - Sequencing of events
  - Distribution of events across kill chain stage
  - Severity and confidence of alerts
- Customer input to shape risk score at a granular level

Adaptive Learning

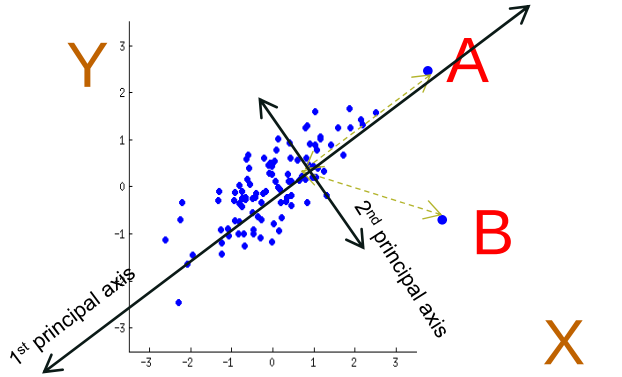


- Incorporate analyst/business context
- Ability to train models for exception handling, risk scoring
- Granular exceptions
  - User/ Application/ Baseline Type
  - E.g., user Bob's access of AWS is exempt from peer detection because he is an admin
  - Global / user specific whitelists
  - E.g., site "xyzinc" facilitates vulnerable PDF file downloads but it is an authorized partner site

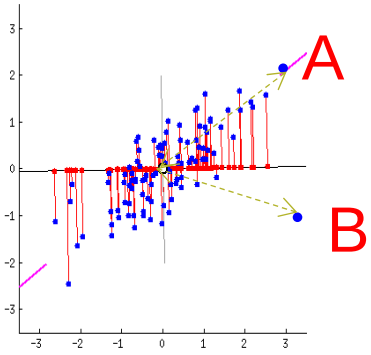
Anomaly detection after applying SVD

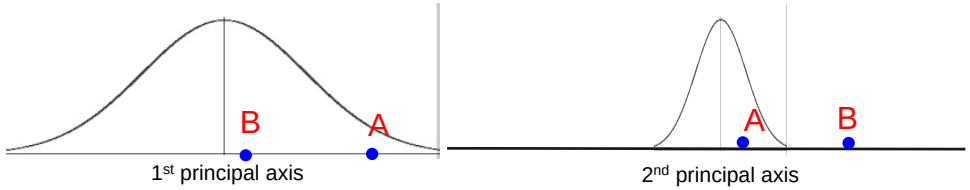
Unsupervised Machine Learning

- In the case of UBA-Server, we have 5 features
  - first/last access time, upload/download volume, number of eflows and duration
- We evaluate Mahalanobis distance, to determine if it is an anomaly
- A score of >60 is an anomaly



X:“time of first access” and Y:“download volume”

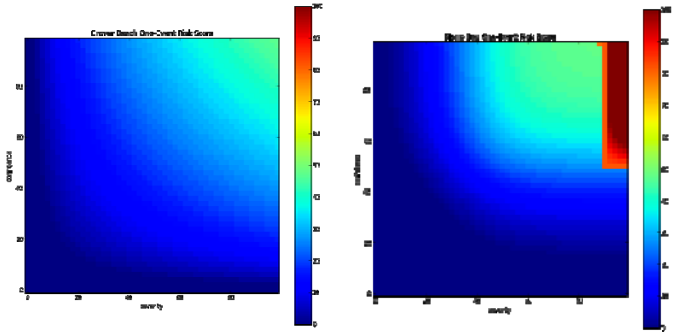




Risk Scoring

Bayesian inference model

Bayes Theorem : $$P(B/A) = \frac{P(A/B) * P(B)}{P(A)}$$



Improvements for ‘single event’ trigger

Risk Score (RS) : $$P(RS/\ f_1, f_2, f_3, f_4) = \frac{P(f_1, f_2, f_3, f_4/RS) * P(RS)}{P(f_1, f_2, f_3, f_4)}$$

$$P(RS/\ f_1, f_2, f_3, f_4) = P(f_1/RS) * P(f_2/RS) * P(f_3/RS) * P(f_4/RS) * P(RS)$$

where,

$$f_1 = \max(\sqrt{severity * confidence * time\_decay})$$

$$f_2 = \sum_{i}^{alerts} \sqrt{(severity * confidence)/100})$$

$$f_3 = \sum_{i}^{attack\ stages} (highest\_sqrt\_of\_sev * conf)$$

$$f_4 = \ln \sum_{i}^{alerts} (\sqrt{severity * confidence * time\_decay})$$

P(RS) is assumed to have a uniform probability distribution

Thank You