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

DATA BREACHES

PREVENTION & DETECTION (US $B)

# BREACHES

% DISCOVERED INTERNALLY

146 days
median time from
compromise to discovery

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 servers

**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

BASELINES
HISTORICAL
+
PEER GROUP

SAM FULLER

3 HOSTS
22 IPs
95 LOGINS
120k SESSIONS

CAMPUS
BRANCH
SaaS
CLOUD

packets, logs, flows, alerts
Behavior – Many different dimensions

- Internal Resource Access
  - Finance servers
- Authentication
  - AD logins
- External Activity
  - C&C, personal email
- Cloud IaaS
  - AWS, Azure
- Remote Access
  - VPN logins
- SaaS Activity
  - Office 365, Box
- Physical Access
  - Badge logs
- Exfiltration
  - DLP, Email

---

SAM FULLER

- 3 Hosts
- 22 IP
- 95 Logons
- 120 Sessions
DETECTING AN ANOMALY

Internal Resource Access
Finance servers

Behavioral Analytics

ABNORMAL APPLICATION ACCESS

SAM FULLER

3 HOSTS
22 IPS
95 LOGONS
120K SESSIONS

time

CAMPUS BRANCH SaaS CLOUD

packets, logs, flows, alerts
Finding the malicious in the anomalous

MACHINE LEARNING
SUPERVISED
UNSUPERVISED

THIRD PARTY ALERTS
DLP
Sandbox
Firewalls
STIX
Rules
Etc.

SUPERVISED
UNSUPERVISED
MACHINE LEARNING
DLP
Sandbox
Firewalls
STIX
Rules
Etc.

SAM FULLER

RISK SCORE

time
Ransomware Example

Indicators

C&C Communication

• DGA Detection e.g.
  iuqerfsodp9ifjaposdfjgosuriijaewrwegwea[.],
  xxlvbrloxxvriy2c5[.], sqjolphimr7jqw6[.],
  76jdd2ir2embyv47[.]

SMB based bot scanning

• 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

75 RISK SCORE
Abnormal Privileged Insider Activity Example

Indicators

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

UEBA
Need for dimensionality

Multiple techniques, Expertise in security domain

<table>
<thead>
<tr>
<th>Supervised</th>
<th>Supervised with manual review</th>
<th>Unsupervised</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS-DGA (Naïve Bayes)</td>
<td>DNS Tunneling (K-means clustering)</td>
<td>UBA-Server (SVD with Mahalanobis distance)</td>
</tr>
<tr>
<td>DNS Exfiltration (Logistic Regression)</td>
<td></td>
<td>GUEBA (z-score)</td>
</tr>
</tbody>
</table>
## Data Source Diversity Matters

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

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

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

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

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

Data Selection
- **Data Sources**
  - (Proxy / FW / AD / VPN logs, packets…)
- **Target Entities**
  - (users/hosts)
- **Use Case Filter**
  - (data filters)

Feature Examples
- **Time**
  - First and last access each day
- **Counter**
  - Volume of downloaded or uploaded bytes
- **Cardinality**
  - Number of email recipients per sender
- **New Value**
  - Country visited for the first time
- **Location**
  - Geo-location of VPN logon

Behavior Profiling
- **Baseline**
  - (Peer, History)
- **Window**
  - (Duration)
- **Profiling Model**
  - (SVD, RBM, BayesNet, K-means, Decision tree…)

Anomaly Detection
- **Real-time vs. Offline**
- **Distance**
  - (Mahalanobis, Energy)
- **Event Generation**
  - (Severity, Stage)
Behavioral analytics for resource access - server

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

### Data Selection
- **Data Sources**: (Proxy logs, server logs, flows, packets…)
- **Target Entities**: (Users to be profiled)
- **Use Case Filter**: (High-value server)

### Features
- **Time**: (First/last access)
- **Counter**: (Volume of download)

### Behavior Profiling
- **Baseline**: (History)
- **Window**: (14 days)
- **Profiling Model**: (SVD)

### Anomaly Detection
- **Real-time vs. Offline**: (Offline)
- **Distance**: (Mahalanobis)
- **Event Generation**: (100% Severity, Internal Activity)
Behavioral Analytics for Resource Access - Building

Identifying abnormal access to physical facility

**Data Selection**
- **Data Sources**: Badge logs
- **Target Entities**: Users to be profiled
- **Use Case Filter**: No filter

**Features**
- **Time**: First/last access

**Behavior Profiling**
- **Baseline**: Peer
- **Window**: 14 days
- **Profiling Model**: SVD

**Anomaly Detection**
- **Real-time vs. Offline**: Offline
- **Distance**: Mahalanobis
- **Event Generation**: 100% Severity, Internal Activity
Behavioral Analytics for Resource Access - Files

Detecting abnormally high PDF downloads

Data Selection
- Data Sources: (Packets or proxy logs)
- Target Entities: (Users to be profiled)
- Use Case Filter: (High-value server; PDFs only)

Features
- Counter: (Volume of download)

Behavior Profiling
- Baseline: (Peer, History)
- Window: (14 days)
- Profiling Model: (ZScore)

Anomaly Detection
- Real-time vs. Offline: (Offline)
- Distance: (Mahalanobis)
- Event Generation: (100% Severity, Internal Activity)
Behavioral Analytics for access to job sites
Identifying flight risk users

<table>
<thead>
<tr>
<th>Data Selection</th>
<th>Data Sources</th>
<th>Target Entities</th>
<th>Use Case Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Packets or proxy logs)</td>
<td>(Users to be profiled)</td>
<td>(Job/salary site URLs)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Features</th>
<th>Cardinality</th>
<th>(# unique visits)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Behavior Profiling</th>
<th>Baseline</th>
<th>Window</th>
<th>Profiling Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Peer)</td>
<td>(14 days)</td>
<td>(SVD)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Anomaly Detection</th>
<th>Real-time vs. Offline</th>
<th>Distance</th>
<th>Event Generation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Offline)</td>
<td>(Mahalanobis)</td>
<td>(100% Severity, Internal Activity)</td>
</tr>
</tbody>
</table>
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:**

\[
P(B / A) = \frac{P(A / B) * P(B)}{P(A)}
\]

**Risk Score (RS):**

\[
P(RS / f_1, f_2, f_3, f_4) = \frac{P(RS / f_1, f_2, f_3, f_4) * P(RS)}{P(f_1, f_2, f_3, f_4)}
\]

\[
\]

where,

\[
f_1 = \text{max} (\sqrt{\text{severity} * \text{confidence} * \text{time}\_\text{decay}})
\]

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

\[
f_3 = \sum_{i}^{\text{attack\_stages}} (\text{highest\_sqrt\_of\_sev} * \text{conf})
\]

\[
f_4 = \ln \sum_{i}^{\text{alerts}} (\sqrt{\text{severity} * \text{confidence} * \text{time}\_\text{decay}})
\]

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