Machine Learning for Cyber Security

POWERED BY ARUBA EXPERIENCE EDGE

Simon Wilson
Aruba CTO, UK & Ireland
IT SECURITY CHALLENGES

MORE DEVICES, APPS, AND SERVICES
7.6B Enterprise IoT Devices by 2020

EVOLVING SECURITY CHALLENGES
80% Using Valid Credentials

LIMITED RESOURCES AND EXPERTISE
0-2% Growth in Budgets
PROOF OF IDENTITY

ESTABLISHED BEHAVIOR
Behavior Has Many Different Dimensions

User & Entity Behavioral Analytics

- Internal Resource Access
  - Finance servers

- Authentication
  - AD logins

- External Activity
  - C&C, personal email

- Cloud IaaS
  - AWS, Azure

- Exfiltration
  - DLP, Email

- Remote Access
  - VPN logins

- SaaS Activity
  - Office 365, Box

- Physical Access
  - badge logs

ABNORMAL INTERNAL RESOURCE ACCESS
# Machine Learning: Supervised vs Unsupervised

<table>
<thead>
<tr>
<th></th>
<th>Supervised</th>
<th>Unsupervised</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Data</strong></td>
<td>Labelled</td>
<td>Unlabeled</td>
</tr>
<tr>
<td><strong>Prior Knowledge</strong></td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Model Fidelity</strong></td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Logistic Regression</td>
<td>Clustering</td>
</tr>
</tbody>
</table>
Data Sources Feed UEBA

- **Behavior Analytics**
- **Attack Analytics**

### Data Sources

- **IDENTITY**
  - Microsoft
  - Infoblox
  - aruba
  - cisco
- **INFRASTRUCTURE**
  - McAfee
  - Blue Coat
  - juniper
  - aruba
  - cisco
  - Check Point
  - Symantec
- **SaaS**
  - Office 365
  - box
- **IaaS**
  - Microsoft
  - amazon web services
- **ALERTS**
  - paloalto
  - cisco
  - FireEye

### Analyzers

- **SIEM**
- **CASB**

### Consoles / Workflows

- **Risk Score**
- **Risk Profile**
- **Investigation & Response**

### Analyzer Components

- **ENTITY360**
- **ANALYTICS**
- **FORENSICS**
- **DATA FUSION**
- **BIG DATA**
INTROSPECT

Machine-learned user and entity behavioral analytics for enterprise security
Behavior Fingerprinting: User vs DropCam

### User
- DNS
- HTTP
- FTP
- SMTP
- NTP
- MSRPC
- SSH

### DropCam
- DNS
- HTTP
- FTP
- SMTP
- NTP
- MSRPC
- SSH
Behavior Anomaly Detection: Compromised User
100+ Use Cases

Malware activity
Browser exploits
Suspicious file downloads
Suspicious domains
Beaconing
Command and control
SMB based command execution
Protocol violations
Internal Reconnaissance
Lateral Movement
Abnormal Internal Resource Access, including high value assets
**Flight Risk users**
Abnormal print activity
Exfiltration such as large data transfers
Abnormal cloud application usage, including large data/file uploads
Credential theft

Password sharing
**Land speed violations**
Command and Control through DGA/Dictionary DGA
Tunneling
Exfiltration
Privilege escalation
Account Abuse (including service account)
Service ticket request violations
Account creation/deletion
Password changes
**Login rate (success/failure) deviations**
Account Takeover (ATO)
Asset hopping
**Password sharing**
Phishing/Spoofing/Whaling
Exfiltration
Activity to non-affiliated/personal/competitor domains
Disposable email domains
Machine Learning for Cyber Security

Solve the problem of Identity

Automation ≠ Intelligence

Machine Learning will help the security teams identify and focus on the important