Identity Driven Security

Javier Dominguez
Identity and Information Protection Technical Specialist
On-premises / Private cloud

THE WORLD BEFORE MOBILITY & CLOUD

users  devices  apps  data
On-premises / Private cloud

CLOUD APPS & SAAS SERVICES

now
Office 365
Dynamics 365
salesforce
MOBILE AND PERSONAL DEVICES
ORGANIZATION & SOCIAL IDENTITIES
Dynamics 365

One strong identity
at the center of your business

On-premises / Private cloud
WHY IDENTITY IS IMPORTANT

- 81% of breaches are caused by credential theft
- 73% of passwords are duplicates
- 80% of employees use non-approved apps for work
IDENTITY & ACCESS MANAGEMENT
PROVE USERS ARE AUTHORIZED AND SECURE BEFORE GRANTING ACCESS TO APPS AND DATA

Protect at the front door
Simplify access to devices and apps
Safeguard your credentials
Traditional IT security tools have problems

- **Complexity**: Initial setup, fine-tuning, and creating rules and thresholds/baselines can take a long time.

- **Prone to false positives**: You receive too many reports in a day with several false positives that require valuable time you don’t have.

- **Designed to protect the perimeter**: When user credentials are stolen and attackers are in the network, your current defenses provide limited protection.
Security data explosion

- Useful Data
- Web server logs
- Windows Event logs, Linux syslog
- Network logs
- SaaS services audit information
- Data center security token service
- Cloud service logs
Weak independent alert streams

This escalation backlog includes tickets generated more than 8 hours ago. Please prioritize and triage the backlog to confirm the activity.

<table>
<thead>
<tr>
<th>Created</th>
<th>Severity</th>
<th>Task</th>
<th>Assigned To</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/27/2016</td>
<td></td>
<td></td>
<td></td>
<td>Sever Data Health</td>
</tr>
<tr>
<td>3/1/2016</td>
<td></td>
<td></td>
<td></td>
<td>Event Count Outliers</td>
</tr>
<tr>
<td>3/1/2016</td>
<td></td>
<td></td>
<td></td>
<td>Failed Logins</td>
</tr>
<tr>
<td>3/1/2016</td>
<td></td>
<td></td>
<td></td>
<td>Failed Logins</td>
</tr>
<tr>
<td>3/2/2016</td>
<td></td>
<td></td>
<td></td>
<td>Event Count Outliers</td>
</tr>
<tr>
<td>3/2/2016</td>
<td>Fake</td>
<td>Fake</td>
<td>Fake</td>
<td>Firewall Change</td>
</tr>
</tbody>
</table>
Burden of triage

Active alerts to triage

<table>
<thead>
<tr>
<th>Escalation Backlog (Active escalations older than 24 hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Date</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>4/2/2013 12:05:15 PM</td>
</tr>
<tr>
<td>4/4/2013 7:04:12 AM</td>
</tr>
<tr>
<td>4/5/2013 7:05:04 AM</td>
</tr>
<tr>
<td>4/6/2013 7:04:42 AM</td>
</tr>
<tr>
<td>4/9/2013 5:06:33 AM</td>
</tr>
<tr>
<td>4/10/2013 11:17:54 PM</td>
</tr>
<tr>
<td>4/10/2013 10:14:52 AM</td>
</tr>
<tr>
<td>4/10/2013 5:40:42 PM</td>
</tr>
</tbody>
</table>
Interpretability of Alerts

Automated Account Security Alerts

Anomaly are found on [redacted]

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>[redacted]</td>
<td>link</td>
</tr>
</tbody>
</table>

Excel Sheet:

<table>
<thead>
<tr>
<th>Day</th>
<th>Account</th>
<th>ActivityId</th>
<th>DeviceNameCertificates</th>
<th>CreateOSVersion</th>
<th>GetMaxUpdateDomain</th>
<th>GetMultiAddAddress</th>
<th>GetOSVersions</th>
<th>GetStagingStatus</th>
<th>GetTenantCertificate</th>
<th>GetTenantGenerations</th>
<th>GetTenants</th>
<th>GetTransportPublicCertificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>by1-dts</td>
<td>c40fbd79-46b-413b-a11-4279b96e564</td>
<td>36</td>
<td>10</td>
<td>1</td>
<td>12</td>
<td>20</td>
<td>3</td>
<td>8</td>
<td>6</td>
<td>22</td>
<td>24</td>
</tr>
</tbody>
</table>

Graph:

[Graph showing data trends]
Lack of Feedback
How Machine Learning can help

Reduce triage of burden by PRIORITIZING ALERTS

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Overall Triage Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Triage-P1</td>
</tr>
<tr>
<td></td>
<td>Triage-P1</td>
</tr>
<tr>
<td></td>
<td>Triage-P1</td>
</tr>
<tr>
<td></td>
<td>Not-For-Ticketing</td>
</tr>
<tr>
<td></td>
<td>Not-For-Ticketing</td>
</tr>
<tr>
<td></td>
<td>Not-For-Ticketing</td>
</tr>
<tr>
<td></td>
<td>Not-For-Ticketing</td>
</tr>
</tbody>
</table>

COMBINING INDEPENDENT ALERT STREAMS and providing informed scoring

Each alert combines multiple points:

- Is the sequence of API calls unusual for this account?
- Is the IP address unusual?
- Does the time of access look normal?

*Typical Ops orgs anomaly detection, more 8 different weaker streams are combined*
How Machine Learning can help

Incorporating Analyst/User Feedback to Improve the System Signal

Providing Interpretable Results

When we get an alert, we’re informed exactly why the ML system feels it is anomalous. Not a black box.

<table>
<thead>
<tr>
<th>Unusual UserAgent</th>
<th>Logins Eval</th>
<th>Unusual Location</th>
<th>Failed Login</th>
<th>Unusual IP</th>
<th>Unusual Activity</th>
<th>Overall Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>37</td>
<td>324</td>
<td>197106</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>64</td>
<td>134460</td>
</tr>
<tr>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>0</td>
<td>521308</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>33648</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3048</td>
<td>0</td>
<td>129</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>94</td>
</tr>
</tbody>
</table>
How ML is different

Traditional Programming

Data → Program → Computer System → Output

Machine Learning

Data → Output + Assumptions → Computer System → Program
Machine Learning for security is difficult

Lack of ground truth
Data labeled as an attack is rare
Datasets are imbalanced

Disproportionate cost of false negative (missing an attack)

Constantly changing environment

Adversarial setting: deliberately avoiding detection
Advanced Threat Detection for Identities

Behavioral Analytics + Detection of advanced attacks and security risks = Advanced Threat Detection

POWERED BY MACHINE LEARNING
INTELLIGENT SECURITY GRAPH ENABLES

- Signal Breadth
- Integrated Intelligence
- Machine Learning/AI
Microsoft Identity Security at Glance

- **Automatically detect/defect**
  - 1.5 million attacks per day

- **Identify**
  - 30K potentially compromised users per day

- **Bootnet data/infected machines from Microsoft DCU**
  - >9 M

- **Azure AD Directories**
  - More than 700 M user accounts on Azure AD

- **Every day the Identity ML system processes**
  - >10 TB of data

- **1.2 Billion devices scanned each month**

- **>42k third-party applications used with Azure AD each month**

- **>18 billion Web sites scanned**

- **>15 billion authentications every day from consumer/commercial**
Cloud-powered protection

- Gain insights from a consolidated view of machine learning based threat detection
- Remediation recommendations
- Risk severity calculation
- Risk-based conditional access automatically protects against suspicious logins and compromised credentials
Detecting suspicious activities on prem

- Abnormal resource access
- Account enumeration
- Net Session enumeration
- DNS enumeration
- SAM-R Enumeration

- Abnormal authentication requests
- Abnormal resource access
- Pass-the-Ticket
- Pass-the-Hash
- Overpass-the-Hash

- Skeleton key malware
- Golden ticket
- Remote execution
- Malicious replication requests
- Abnormal Modification of Sensitive Groups

- Reconnaissance
- Compromised Credential
- Lateral Movement
- Privilege Escalation
- Domain Dominance

Abnormal working hours
Brute force using NTLM, Kerberos, or LDAP
Sensitive accounts exposed in plain text authentication
Service accounts exposed in plain text authentication
Honey Token account suspicious activities
Unusual protocol implementation
Malicious Data Protection Private Information (DPAPI) Request

MS14-068 exploit (Forged PAC)
MS11-013 exploit (Silver PAC)
Who is accessing? What is their role? Is the account compromised?

Where is the user based? From where is the user signing in? Is the IP anonymous?

Which app is being accessed? What is the business impact?

Is the device healthy? Is it managed? Has it been in a botnet?

What data is being accessed? Is it classified? Is it allowed off premises?
CONDITIONAL ACCESS

IF
- Privileged user?
- Credentials found in public?
- Accessing sensitive app?
- Unmanaged device?
- Malware detected?
- IP detected in Botnet?
- Impossible travel?
- Anonymous client?
- Compromised device?
- Pass the Ticket?
- What content is accessed?

User risk
- High
- Medium
- Low

Session risk
- High
- Medium
- Low

THEN
- Allow access
- Require MFA
- Force password reset
- Deny access
- Limit access
HOW CAN YOU SIMPLIFY ACCESS TO DEVICES & APPS?
Passwordless strong authentication via multiple factors

- PC + PIN or Biometrics
- PC + Companion Device
- PC supported Biometrics: fingerprint & facial
- Companion Device can support other biometrics options (e.g.: EKG)

Supported on any Windows 10 device

>100 devices supporting biometrics
MAKING WINDOWS HELLO WORK FOR EVERY ENVIRONMENT
WHAT IS FIDO?

- Security on premises and web
- Secure mobile user credentials
- Secure authentication

FIDO BOARD MEMBERS
USE DEVICE AUTHENTICATION TO AUTOMATICALLY PROVIDE ACCESS TO APPS
HOW DO YOU PROTECT USER & ADMINISTRATOR CREDENTIALS?
Can you protect credentials against Pass-the-Hash and other similar classes of attacks?

Can you restrict and monitor the use of privileged credentials?

How are the credentials stored in your devices?
HOW HELLO PROTECTS CREDENTIALS

Strong authentication via multiple factors
- Uses two factors for authentication (e.g.: PC + PIN or Biometric)
- Asymmetrical Keys (i.e: Private/Public)

User credentials protected by hardware
- Hardware generated credential (keys)
- Credential isolated and protected by hardware

Secure biometrics
- Hardened biometric implementation in Windows & hardware
- Anti-spoofing and brute-force protection
#1 go-to attack for hackers: Pass the Hash

Used in nearly every major breach for lateral movement

Credential Guard uses Windows Defender System Guard to hardware isolate authentication and authentication data away from system

Fundamentally breaks derived credential theft even when OS is fully compromised
PROTECT PRIVILEGED IDENTITIES
Discover, restrict, and monitor privileged identities

Enforce on-demand, just-in-time administrative access when needed

Use Alert, Audit Reports and Access Review
Thank You