MODEL-DRIVEN SECURITY: IT’S CLOSER THAN YOU THINK

Jim Routh
CSO
Aetna
@jmrouth1
Session objectives

1. Share some examples of model-driven security
2. Introduce you to the world of unconventional controls
3. Identify talent development challenges
Evolution from conventional to unconventional controls

- NIST CSF 800-53
- ISO 27001
- HiTrust

Cyber Security

Conventional

Un-Conventional
This is the reason that phishing, spear-phishing, and whaling attacks are directed against individuals. ... Almost all national and industry phishing laws and regulations include a stipulation that businesses and organizations must create, implement, and maintain a security awareness training program.

NIST SP 800-177
SEPTEMBER, 2016

Domain based Message Authentication, Reporting and Conformance (DMARC) was conceived to allow email senders to specify policy on how their mail should be handled, the types of security reports that receivers can send back, and the frequency those reports should be sent. Standardized handling of SPF and DKIM removes guesswork about whether a given message is authentic, benefitting receivers by allowing more certainty in quarantining and rejecting unauthorized mail.
Different tactics require different controls

Sender

- DMARC
- Sinkhole newly registered domains
- Apply domain attributes to inbound filters
- Brand protection services

Impostor
- Spoof
- Look-Alike Domain
- Display Name Deception

Authentic
- Compromised Account
- Account Owner

End user education TBD

Phishing
Using email traffic data, the system learns the unique fingerprint of all email senders into your enterprise.

This durable identity trust model is used to stop all messages that do not prove they should be trusted.

- **29,231** servers sent email for an enterprise on a single day.
- **312** servers for the enterprise.
- **4,641** servers owned by service providers.
- **9,732** benign email forwarders.
- **14,526** malicious senders.
Comparing Aetna in-bound email and correlating it with billions of emails every day from the largest email providers using machine learning models applied in real time enables filtering of email based on sending domain attributes to divide the mail stream into trusted and untrusted streams.
Privilege user & activity management activity

1. Reduce the number of privilege users

2. Provide context to monitoring and change admin tool choice

3. Implement data analytic techniques to determine behavioral patterns
Behavioral analysis is the cornerstone
Privileged Access Management (PAM)

Implement and consolidate access monitoring, alerting, and response utilizing all available access and identity data (policy and event) to identify anomalies:

- Provide clear understanding of privileged access
- Ensure appropriate access is not being misused
- Target investigations & follow up

Event email is sent:

- When unusual activity is detected within a 24-hour period
- To the employee’s manager
- And contains attachment of Anomalous Activity Report

This results in a substantial ‘false-positive’ reduction, as well as an increased business awareness of privileged access.
Over 3 billion user IDs and passwords were stolen in 2016

Source: Shape Security
Criminals use credentials for account takeover

40% In 2016, data breaches increased by

51% of consumers suffered some kind of security incident in 2016, including a stolen password or breached account

81% of hacking related breaches leveraged stolen or weak passwords

3 Billion In one breach- Yahoo 2013

Sources: 2017 Verizon DBIR Report; Identity Theft Resource Center (ITRC) and CyberScout
The trouble with passwords...

- Most people use less than 5 passwords for all accounts
  - 50% of those haven’t changed their password in the last 5 years

- Reuse makes them easy to compromise
  - 39% of adults use the same password for many of their online accounts

- They are difficult to remember
  - 25% of adults admit to using less secure passwords, because they are easier to remember

Sources: Pew research; Telesign research
If I were a criminal...

I would use **Sentry MBA** for credential stuffing. I’d take log in credentials and try them on different domains. I’d get a 2% hit, meaning 2% of the credentials I use will give me control of the account.

I can get a 4% return by using the domain name in front of the password.

10,000 credentials = 200 or 400 accounts that I own.

---

Sources: [https://krebsonsecurity.com/tag/sentry-mba/](https://krebsonsecurity.com/tag/sentry-mba/)
A simpler and more secure experience

Aetna is leading the way in introducing advanced authentication methods into the health care sector.

- Our consumers no longer need to rely on traditional usernames and passwords when logging into Aetna applications.
- Authentication, once a single event, is now integrated into the application transparently and continuously.
- We’re adjusting controls and analytic capabilities to create friction for the threat adversaries while reducing friction for our users.
Continuous risk-based authentication

- Risk score calculated
- Continual authentication without impacting the user experience
- Risk score determines how much and what access to provide
- 30-60 user attributes assessed
Authentication framework for mobile & web

- One framework
- Multiple authentication tools
- Change controls without changing applications
- Across mobile and web
- Policy-driven authentication model
Model-driven security controls have arrived

- Inbound email protection
- Continuous behavioral based authentication
- Privileged User Monitoring
- High risk user monitoring
- Endpoint protection using Machine Learning
- Fraud management models
- Dynamic access provisioning
- Voice biometrics for fraud detection
The Models are driving security

Security Controls → Data Aggregation → Data Analysis → Results
The Models are driving security

Data Aggregation → Data Analysis → Security Controls
<table>
<thead>
<tr>
<th>Model/Policy Name</th>
<th>Description</th>
<th>Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Risk user - Departing User Sending self email</td>
<td>Users with future term date in UltiPro sending email to personal email accounts</td>
<td>Workforce</td>
</tr>
<tr>
<td>Restrict SSN email for High Risk users</td>
<td>Provide a daily list of all users with a risk score over 80 so they are restricted from sending email with SSN data.</td>
<td>Workforce</td>
</tr>
<tr>
<td>Events By Restricted Users</td>
<td>High volumes of privileged activity</td>
<td>Workforce</td>
</tr>
<tr>
<td>Off hours activities</td>
<td>Unusual evening privileged activity</td>
<td>Workforce</td>
</tr>
<tr>
<td>Week end login events</td>
<td>Unusual weekend privileged activity</td>
<td>Workforce</td>
</tr>
<tr>
<td>Unauthorized password changes</td>
<td>Vaulted accounts that have passwords changed by an unauthorized ID</td>
<td>Workforce</td>
</tr>
<tr>
<td>Self-Privilege Escalation</td>
<td>Admin granting privileges to themselves</td>
<td>Workforce</td>
</tr>
<tr>
<td>Account Compromise: Multiple Failed Logins/ Possible Configuration Issue</td>
<td>Multiple Failed Logins/ Possible Configuration Issue</td>
<td>Workforce</td>
</tr>
<tr>
<td>Unusual amount of password reset events</td>
<td>Unusual amount of password reset events</td>
<td>Workforce</td>
</tr>
<tr>
<td>Unusual amount of Failed Password changes</td>
<td>Unusual amount of Failed Password changes</td>
<td>Workforce</td>
</tr>
<tr>
<td>Purging of Audit Logs</td>
<td>A user purges an audit log from a server</td>
<td>Workforce</td>
</tr>
<tr>
<td>Model/Policy Name</td>
<td>Description</td>
<td>Effects</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Register new bank followed by transaction over threshold</td>
<td>If a person changes banking information and performs a financial transaction same day</td>
<td>Consumer</td>
</tr>
<tr>
<td>Account email address changed followed by password reset request</td>
<td>Account email address changed followed by password reset request</td>
<td>Consumer</td>
</tr>
<tr>
<td>Financial Activity greater than threshold</td>
<td>Financial Activity greater than threshold</td>
<td>Consumer</td>
</tr>
<tr>
<td>Brute Force Attack</td>
<td>high number of failed login attempts</td>
<td>Consumer</td>
</tr>
<tr>
<td>Prevent Vault Checkout for High Risk Users</td>
<td>Require additional verification before allowing a vaulted ID to be checked out by a high risk user</td>
<td>Workforce</td>
</tr>
<tr>
<td>Geographic Activity without Physical Access</td>
<td>Logical Account activity at Geo location where there is no Physical Account activity</td>
<td>Workforce</td>
</tr>
<tr>
<td>Physical/Geographic Location Mismatch</td>
<td>Logical Account Geo location not matching Physical Account Geo location.</td>
<td>Workforce</td>
</tr>
<tr>
<td>Accounts Creation and deletion in a day</td>
<td>Accounts created by the admin, used and then deleted in the same day</td>
<td>Workforce</td>
</tr>
<tr>
<td>Accounts Enable and Disable in a day</td>
<td>Accounts enabled by the admin, used and then disabled in the same day</td>
<td>Workforce</td>
</tr>
<tr>
<td>Potential Access Misuse Attempt (Wanderer) - Badge</td>
<td>User is getting failed access at multiple access point</td>
<td>Workforce</td>
</tr>
<tr>
<td>Abnormal Access using Multiple Cards - Badge</td>
<td>Person is using temporary badge and permanent badge in short timeframe</td>
<td>Workforce</td>
</tr>
<tr>
<td>Rare Badge Access Anomaly</td>
<td>User accesses badge outside his normal historical behavior</td>
<td>Workforce</td>
</tr>
<tr>
<td>Potential Access Breach Attempt - Badge Stats model</td>
<td>User is getting high number of failed access</td>
<td>Workforce</td>
</tr>
</tbody>
</table>
Model Inventory Management

GS Model Catalog

Platform

Status

Model Type
- Behavioral
- Rule

Model Status 1
- UA
- Null
- Development
- Planning
- Production
- Testing

Processing Platform
- AEM
- AEM/Surround
- Analytic Data Platform
- BPO
- Crowded
- PS Security
- Next Generation Authentic
- Name
- Pindrop
- Splunk ES

Model Status 1
- UA
- Null
- Development
- Planning
- Production
- Testing

Function

Processing Platform
- AEM
- AEM/Surround
- Analytic Data Platform
- BPO
- Crowded
- PS Security
- Next Generation Authentic
- Name
- Pindrop
- Splunk ES

Focus Area

Number of Models
- 15

Number of Models
- 10

Number of Models
- 64

Number of Models
- 45

Number of Models
- 13

Number of Models
- 9

Number of Models
- 10

Number of Models
- 9

Number of Models
- 5

Number of Models
- 4

Number of Models
- 2

Number of Models
- 1

Number of Models
- 1

Total Models: 231
- Production: 142
- Testing: 89
What are Models?

\[ e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \]

\[ \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}} \]

Mathematical formulation of observed events
Vendor Analytics Ecosystem

Various models in production from a variety of vendors
Custom Fraud Analytic Models

- HSA Burst Model
- FSA Burst Model
- Merchant Spike
- HSA Employer Breach
- FSA Employer Breach
- Cardholder Fraud
- HSA Individual Fraud
- FSA Individual Fraud
- Targeted Merchant

Daily Report
Model Data and Workflow

Dataflow

Threat Detection

Storage & Analytics

Analytics

Storage & Analytics

Analytics

Workflow Orchestration

- Alerts
- Playbooks
- Auto Bots

NGA

Fraud

Network Events & Security Logs

36 production flows
6+ Billion events/day

36 production flows
6+ Billion events/day

Dataflow

Analytics

Storage & Analytics

Analytics

Analytics

Storage & Analytics

Analytics

Network Events & Security Logs

Fraud

NGA

36 production flows
6+ Billion events/day
Data Scientist meet Security Professional
QUESTIONS?

routhj@aetna.com

https://www.linkedin.com/in/jmrouth/