Use The Tools You Have: Threat Detection and Hunting in Azure

Daryl Novak | Director, Information Security - NewSignature
Who Am I?

- Director, Information Security at New Signature – building new Managed Security services based on Microsoft toolsets
- ~20 years working with Microsoft technologies- starting with SMS 1.2
- Started in security through patch management (SMS), expanded into Identity, Endpoint and Datacenter security, then shifted to the Cloud!
Points to cover

• Reference Architectures – MS Cybersecurity, Zero Trust

• Azure Active Directory & Identity Protection
  • Licensing
  • Risk Events
  • User Risk and Sign-in Risk Policies
  • Examples

• Azure Security Center
  • Threat Protection

• Azure Sentinel
  • Connectors
  • Analytics Rules
  • Incidents
  • Hunting
Responsibility Zones

Who’s Job is it Anyway?

https://aka.ms/sharedresponsibility

- Always retained by customer
- Varies by Service Type
- Transfers to Cloud Provider
Cybersecurity Reference Architecture

April 2019 - https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

Roadmaps and Guidance
1. Present Slide
2. Hover for Description
3. Click for more information

Securing Privileged Access
1. Office 365 Security
2. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365
- Secure Score
- Customer Lockbox

Dynamics 365

Information Protection

Conditional Access – Identity Perimeter Management

Cloud App Security
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM

Cloud Information Protection (AIP)
- Discover
- Classify
- Protect
- Monitor
- Hold Your Own Key (HYOK)

AIP Scanner
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
- Azure SQL
  - Threat Detection
  - Encryption & Data Masking
- Azure SQL Info Protection

Microsoft Azure

Hybrid Cloud Infrastructure

On Premises Datacenter(s)
- Azure Firewall
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Azure Monitor
- Backup & Site Recovery
- VMs
- Secure Appliances
- Express Route
- NGFW
- Edge DLP
- SSL Proxy
- IPS/IDS
- Azure Stack
- Shielded VMs
- Windows Server 2019 Security
  - Window 10 + just Enough Admin, HyperV Containers, Nano server, and more...

Intranet Servers
- Privileged Access Workstations (PAWs)

IoT and Operational Technology
- Windows 10 IoT
- Azure IoT Security
- Azure Sphere

IT Security Architecture
- IoT Security Maturity Model
- Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)
Zero Trust

Reference Architecture
Azure Active Directory and Identity Protection

https://aka.ms/AzureADandYou
Azure AD Licensing

- Azure AD Free edition does offer a list of users flagged for risk and an overview of risk events.

- Azure AD Premium P1 (EMS E3 or M365 E3) includes much more detail as to the nature of each risk.

- Azure AD Premium P2 (EMS or M365 E5) includes all risk event details and allows for risk-based conditional access policies and MFA registration policies.
Azure Active Directory Basics

- Identity is the new perimeter!

- Anyone, anywhere in the world can sign in to your Azure AD accounts (assuming they pass MFA and your conditional access policies...)

- Examine who is assigned to privileged roles. Do they really really need to use a built-in role to do their job?

- Audit your sign-in logs. Why are failures happening?

- Conditional Access Policies apply after authentication has occurred. They may prevent access to data but accounts can still be sprayed

- Use Exchange Authentication Policies to block legacy auth
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Status</th>
<th>IP Address</th>
<th>Client App</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/06/2019</td>
<td>21:47:15</td>
<td>Fi</td>
<td>101.231.140.218</td>
<td>Other clients; IMAP</td>
<td>Shanghai, Shanghai Shi, CN</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:44:32</td>
<td>Si</td>
<td>221.1.177.2</td>
<td>Other clients; IMAP</td>
<td>Zhouchengzhen, Shandong, CN</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:44:11</td>
<td>A</td>
<td>187.72.160.39</td>
<td>Other clients; IMAP</td>
<td>Belo Horizonte, Minas Gerais, BR</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:43:59</td>
<td>R</td>
<td>41.128.185.155</td>
<td>Other clients; IMAP</td>
<td>Al Qahirah, Al Qahirah, EG</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:43:40</td>
<td>R</td>
<td>61.153.54.38</td>
<td>Other clients; IMAP</td>
<td>Quzhou, Zhejiang, CN</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:42:49</td>
<td>A</td>
<td>181.143.17.66</td>
<td>Other clients; IMAP</td>
<td>Medellin, Antioquia, CO</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:42:24</td>
<td>L</td>
<td>177.135.101.101</td>
<td>Other clients; IMAP</td>
<td>Sao Paulo, Sao Paulo, BR</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:42:20</td>
<td>L</td>
<td>177.135.101.101</td>
<td>Other clients; IMAP</td>
<td>Sao Paulo, Sao Paulo, BR</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:42:14</td>
<td>H</td>
<td>112.24.104.228</td>
<td>Other clients; IMAP</td>
<td>Xicheng Qu, Beijing Shi, CN</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:41:52</td>
<td>R</td>
<td>60.246.1.99</td>
<td>Other clients; IMAP</td>
<td>Macau, Macau, MO</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:40:13</td>
<td>B</td>
<td>112.16.214.182</td>
<td>Other clients; IMAP</td>
<td>Hangzhou, Zhejiang, CN</td>
</tr>
<tr>
<td>06/06/2019</td>
<td>21:40:09</td>
<td>B</td>
<td>112.16.214.182</td>
<td>Other clients; IMAP</td>
<td>Hangzhou, Zhejiang, CN</td>
</tr>
</tbody>
</table>
Azure AD Identity Protection

- Azure AD Identity Protection provides several functions to help detect and respond to unauthorized access:
  - Alerting and logging of preconfigured risk events associated with sign-ins and aggregation of these to provide User Risk score corresponding to the likelihood a specific user is compromised
  - MFA Registration Policies
    - User Risk Policies
    - Sign-in Risk Policies
  - User and Sign in Risk Policies can automate containment and remediation upon detection of a risk event
## Azure AD Identity Protection Risk Events

<table>
<thead>
<tr>
<th>Risk Event</th>
<th>Severity</th>
<th>Detection Type / Noisiness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unfamiliar Sign-In Properties</td>
<td>Medium</td>
<td>Realtime- Greatly improved specificity with Modern Auth. Recently became better at handling Activesync legacy auth</td>
</tr>
<tr>
<td>Sign-ins from anonymous IP address</td>
<td>Medium</td>
<td>Realtime- Quite noisy, no distinction between TOR or commercial privacy VPNs- improvements coming</td>
</tr>
<tr>
<td>Impossible travel to atypical locations</td>
<td>Medium</td>
<td>Offline- Reasonably good indicator of compromise</td>
</tr>
<tr>
<td>Sign-ins from infected devices</td>
<td>Low</td>
<td>Offline- Seldom seen, difficult to reliably associate public IP with a specific host</td>
</tr>
<tr>
<td>Leaked Credentials</td>
<td>High</td>
<td>Offline- Rarely seen, high specificity, low sensitivity</td>
</tr>
<tr>
<td>Sign-ins from IP addresses with suspicious activity</td>
<td>Medium</td>
<td>Offline- Rarely seen, but will often trigger multiple alerts across multiple users with failed signins from a suspect IP</td>
</tr>
</tbody>
</table>

Sign-in Risk Policy

- Azure AD Identity Protection provides two main forms of automated response which work in different ways.

- Sign-in risk policies apply to specific sign-in attempts. The following settings are available:
Sign-in Risk Policy - Sign in Allowed

Help us protect your account

We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity.

Next

For added security, we need to further verify your account

How do you want us to verify your account?

robyn@aad161.ccsctp.net
Text me at +X X0XXX00X66

We've sent you a text message with a verification code.
163136

Sign in

Use a different verification option
Sign out and sign in with a different account
More information
Sign-in Risk Policy- Sign in Blocked

- If the policy is configured to block sign-in, administrative help will be needed
- Signing in from an familiar device or location may work
User Risk Policy

- User risk policies operate on the aggregate risk that the user is compromised, based on the user’s active Risk events
Your account security is at risk

A security alert has been triggered for your account. This might be because we noticed suspicious account activity or we found your email and password posted in a public location.

To help you—and only you—get back into matt@aad178.csctp.net, we need to verify that it’s yours.

Next

For added security, we need to further verify your account

How do you want us to verify your account?

user9@aadiptest.onmicrosoft.com
Text me at +X.XXXXXXXXXX66

We've sent you a text message with a verification code.

Enter verification code

Sign in

Use a different verification option
Sign out and sign in with a different account
More information

Update your password

Since someone else may have had access to your account, you need to choose a new password. Don't use the same password that you use for other sites.

View details

user9@aadiptest.onmicrosoft.com
Current password
New password
Confirm password

Update password and sign in
Your account has been blocked

A security alert has been triggered for your account. This might be because we noticed suspicious account activity or we found your email and password posted in a public location. Please contact your admin.

If you think you’re seeing this error by mistake, contact your admin and report the following details:
• Triggered by Azure Active Directory Identity Protection.
• App name: Office 365
• IP address: 131.107.159.58
• Device Platform: Windows 10
• Device State:
  • Signed in as user2@aadiptest.onmicrosoft.com
  • Correlation ID: 6e896043-93dc-4975-96ad-d7639bde5e53
  • Time stamp: 2016-02-08 19:59:52Z

User Risk Policy- Sign in Blocked

• If the policy is configured to block sign-in, administrative help will be needed to reset the password
Welcome to Azure AD Identity Protection’s new ‘Overview’.

Data range = 30 days

New risky users detected

User risk level = All

Medium risk users

15
- Medium risk users detected.
- Investigate users and reset passwords.

Unprotected risky sign-ins

16 / 777 risky sign-ins last week
- Protect these sign-ins by configuring your sign-in risk policy.

Identity Secure Score

175 / 263
- Monitor and improve your identity security posture.

Configure user risk policy >

New risky sign-ins detected

Sign-in risk type = Real-time
- Sign-in risk level = All

Count

09/08 09/15 09/22 09/29
- Count
- Unprotected
- Protected
### Risky users

<table>
<thead>
<tr>
<th>Application</th>
<th>Status</th>
<th>Date</th>
<th>IP Address</th>
<th>Location</th>
<th>Risk State</th>
<th>Risk Level</th>
<th>Risk Level (Aggregate)</th>
<th>Risk Level (Real-Time)</th>
<th>Conditional Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>O365 Suite UX</td>
<td>Failure</td>
<td>9/27/2019, 3:35:24 PM</td>
<td>41.13...</td>
<td>Lagos, Lagos, NG</td>
<td>At risk</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Failure</td>
</tr>
<tr>
<td>O365 Suite UX</td>
<td>Failure</td>
<td>9/27/2019, 3:33:26 PM</td>
<td>41.13...</td>
<td>Lagos, Lagos, NG</td>
<td>At risk</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Failure</td>
</tr>
</tbody>
</table>

Users can have detections on sign-ins that are currently not supported in the Sign-ins report. Such risky sign-ins do not appear here. To see all the detections in the last 90 days, please go to the 'Risk history' tab.
<table>
<thead>
<tr>
<th>DATE</th>
<th>APPLICATION</th>
<th>STATUS</th>
<th>IP ADDRESS</th>
<th>LOCATION</th>
<th>CONDITIONAL ACCESS</th>
</tr>
</thead>
</table>

**Details**

- **Request ID**: [Redacted]
- **Correlation ID**: [Redacted]
- **User**: [Redacted]
- **Username**: [Redacted]
- **User ID**: [Redacted]
- **Application**: O365 Suite UX
- **Application ID**: [Redacted]
- **Resource**: Windows Azure Active Directory
- **IP address**: 41.138.169.136
- **Location**: Lagos, Lagos, NG
- **Date**: 9/27/2019, 3:35:24 PM
- **Status**: Failure
- **Sign-in error code**: 53003
- **Failure reason**: Access has been blocked due to conditional access policies.
- **Client app**: Browser
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Application</th>
<th>Status</th>
<th>IP Address</th>
<th>Client App</th>
<th>Operating System</th>
<th>Location</th>
<th>Conditional</th>
<th>MFA Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/29/2019</td>
<td>6:58:44 PM</td>
<td>Microsoft Office</td>
<td>Interrupted</td>
<td></td>
<td></td>
<td></td>
<td>Sydney, New South Wales, AU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9/29/2019</td>
<td>6:00:48 PM</td>
<td>Microsoft Office</td>
<td>Success</td>
<td></td>
<td>Unknown</td>
<td>Windows 7</td>
<td>Sydney, New South Wales, AU</td>
<td></td>
<td>Not Applied</td>
</tr>
<tr>
<td>9/26/2019</td>
<td>9:18:10 PM</td>
<td>Office365 Shell WCSS</td>
<td>Success</td>
<td></td>
<td>Browser</td>
<td>Windows 7</td>
<td>Sydney, New South Wales, AU</td>
<td></td>
<td>success</td>
</tr>
<tr>
<td>9/26/2019</td>
<td>9:17:57 PM</td>
<td>Bynder</td>
<td>Success</td>
<td></td>
<td>Browser</td>
<td>Windows 7</td>
<td>Sydney, New South Wales, AU</td>
<td></td>
<td>success</td>
</tr>
<tr>
<td>Risk State</td>
<td>Risk Level</td>
<td>Last Updated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>--------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>10/2/2019, 3:51:44 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Low</td>
<td>10/1/2019, 3:28:18 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/30/2019, 11:29:38 AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/30/2019, 9:28:34 AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/29/2019, 7:23:39 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Low</td>
<td>9/29/2019, 5:22:45 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/27/2019, 8:13:28 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>High</td>
<td>9/27/2019, 3:39:27 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/27/2019, 3:25:03 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>High</td>
<td>9/26/2019, 8:43:37 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/25/2019, 9:10:30 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>High</td>
<td>9/25/2019, 12:17:50 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/24/2019, 3:21:04 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/24/2019, 1:57:01 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/24/2019, 1:08:27 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Risky Users

Welcome to Azure AD Identity Protection's advanced "Risky users" view. Manage all your risky users here.

<table>
<thead>
<tr>
<th>RISK STATE</th>
<th>RISK LEVEL</th>
<th>RISK LAST UPDATED</th>
</tr>
</thead>
<tbody>
<tr>
<td>At risk</td>
<td>Medium</td>
<td>9/20/2019, 1:22:43 PM</td>
</tr>
</tbody>
</table>

**Details**

- **View user's sign-ins**
- **View user's risky sign-ins**
- **View user's risk detections**
- **Reset password**
- **Confirm user compromised**
- **Dismiss user risk**
- **Block user**
- **Investigate with Azure ATP**

**Basic Info**

- **User**: [Redacted]
- **Roles**: [Redacted]
- **Username**: [Redacted]
- **User ID**: [Redacted]

- **Risk state**: At risk
- **Risk level**: Medium
- **Risk last updated**: 9/20/2019, 1:22:43 PM

**Office location**: New York, New York, United States of America
**Department**: [Redacted]
**Mobile phone**: [Redacted]
Risk detections (Preview)

Welcome to Azure AD Identity Protection's advanced 'Risky detections' view. Manage all your risk detections here.

Detection time: Last 1 month  Show dates as: Local  User:  Detection type: None Selected  Risk state: 2 selected  Risk level: None Selected  

<table>
<thead>
<tr>
<th>DETECTION TIME</th>
<th>LOCATION</th>
<th>DETECTION TYPE</th>
<th>RISK STATE</th>
<th>RISK LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/20/2019, 1:17:43 PM</td>
<td>64.12... Balch Springs, Texas, US</td>
<td>Atypical travel</td>
<td>At risk</td>
<td>Medium</td>
</tr>
<tr>
<td>DATE</td>
<td>APPLICATION</td>
<td>STATUS</td>
<td>IP...</td>
<td>OPERATING SYSTEM</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------</td>
<td>----------</td>
<td>---------</td>
<td>------------------</td>
</tr>
<tr>
<td>9/20/2019</td>
<td>Office 365 Exchange Online</td>
<td>Success</td>
<td>2602...</td>
<td>Ios</td>
</tr>
<tr>
<td>9/20/2019</td>
<td>Microsoft Office</td>
<td>Success</td>
<td>64.12...</td>
<td>Windows 7</td>
</tr>
<tr>
<td>9/20/2019</td>
<td>Microsoft Office</td>
<td>Failure</td>
<td>64.12...</td>
<td>Windows 7</td>
</tr>
<tr>
<td>9/20/2019</td>
<td>Office 365 Exchange Online</td>
<td>Success</td>
<td>2602...</td>
<td>Ios</td>
</tr>
<tr>
<td>9/20/2019</td>
<td>Office 365 Exchange Online</td>
<td>Success</td>
<td>2602...</td>
<td>Ios</td>
</tr>
<tr>
<td>9/20/2019</td>
<td>Office 365 Exchange Online</td>
<td>Success</td>
<td>2602...</td>
<td>Ios</td>
</tr>
<tr>
<td>9/20/2019</td>
<td>Office 365 Exchange Online</td>
<td>Success</td>
<td>107.7...</td>
<td>Ios</td>
</tr>
<tr>
<td>9/20/2019</td>
<td>Cisco Webex</td>
<td>Success</td>
<td>38.11...</td>
<td>Windows 7</td>
</tr>
<tr>
<td>9/20/2019</td>
<td></td>
<td>Success</td>
<td>38.11...</td>
<td>Windows 7</td>
</tr>
</tbody>
</table>

Details

- **Grant Controls**
  - require domain-joined device: Success
  - block: Not Applied
  - require compliant device: Not Applied
  - require multi-factor authentication: Not Applied
  - require multi-factor authentication: Not Applied
Azure Security Center

• You need to upgrade to the Standard plan to access advanced threat protection features and alerting

• Agents need to be deployed to existing VM resources, and should be set to autodeploy for all new resources by policy

• ASC also helps deploy endpoint protection solutions to your virtual servers, and assess those you have deployed yourself

• Security Recommendations and Threat Detection is also available for PaaS workloads

Threat Protection

• Azure Security Center is capable of generating Security Alerts of the following types:
  
  • Virtual Machine Behavioral Analysis
  • Network Analysis
  • SQL Database and SQL Data Warehouse Analysis
  • Contextual Information

• Alerts are scored by severity and can be automatically correlated into Incidents

https://docs.microsoft.com/en-ca/azure/security-center/security-center-detection-capabilities
Retirement...

• A number of Azure Security Center features were retired July 31, 2019. Of note:
  • Events Dashboard
  • Custom alert rules
  • Security Alerts investigation
  • A subset of security solution integrations (NGF, WAF, CEF, Advanced Threat Analytics, AAD IP)

• The main reason these were removed from ASC is the introduction of....

What is Azure Sentinel?

- **SIEM** – Security Incident and Event Management
  - Collect data and generate correlated alerts

- **SOAR** – Security Orchestration, Automation and Response
  - Do something useful about it

- Data is stored in a Log Analytics workspace
  - Kusto Query Language used for queries and alert rules

- Charged on consumption – Sentinel + Log Analytics
  - MS security providers free

https://docs.microsoft.com/en-ca/azure/sentinel/overview
Azure Sentinel Connectors

- Built-in connectors for many common data sources and formats
- Some require additional agents or configuration
  - TI connector requires publishing of TI data to Graph Security API
- Connectors from Microsoft security providers offer the ability to automatically create incidents for alerts coming from these providers
- If a connector isn’t available and can’t be connected via the CEF connectors, custom connectors can be created- Sentinel allows query time parsing so rigid data structures and transformation isn’t necessary
Analytics Rules

• Analytics rule templates are now available out of the box
  • Check out the community at https://aka.ms/ASICommunity

• Types of rules:
  • Scheduled (KQL Query based)
  • Microsoft Security (other MS security platforms like ASC)
  • Fusion (AI based - multistaged attack)
  • ML Behavior Analytics (currently bringing Identity Protection-like analysis to SSH logins)

• Custom rules are all of the Scheduled type, and Scheduled templates can be freely modified

• Currently, only Scheduled rules can automatically trigger a playbook
Azure Sentinel - Analytics

RULES BY SEVERITY

Active rules

Advanced Multistage Attack Detection

Description
By using Fusion technology that’s based on machine learning, Azure Sentinel can automatically detect multistage attacks by combining anomalous behaviors and suspicious activities that are observed at various stages of the kill chain. Azure Sentinel then generates incidents that would otherwise be very difficult to catch. These incidents excise two or more alerts or activities. By design, these incidents are low volume, high fidelity, and high severity - which is why this detection is turned ON by default.

There are currently 35 incident types that include a combination of suspicious Azure Active Directory sign-in events followed by anomalous Office 365 activity.

To detect these multistage attacks, the following data connectors must be configured:

- Azure Active Directory Identity Protection
- Microsoft Cloud App Security

For a full list and description of each scenario that is supported for these multistage attacks, go to https://aka.ms/SentinelFusion.
Define the logic for your new analytic rule.

```
Rule query
SigninLogs
| where TimeGenerated >= ago(1d)
| summarize peridentityAuthCount = count() by Identity, locationString = strcat(tostring(LocationDetails)
| summarize distinctAccountCount = count(), identityList = makeset(Identity) by locationString
| extend identityList = if(distinctAccountCount<10, identityList, "multiple (>10)")
| join kind=anti
```

Any time details set here will be within the scope defined below in the Query scheduling fields.

**Map entities - more entities coming soon!**

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis.

<table>
<thead>
<tr>
<th>ENTITY TYPE</th>
<th>COLUMN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>Defined in query</td>
</tr>
<tr>
<td>Host</td>
<td>Choose column</td>
</tr>
<tr>
<td>IP address</td>
<td>Choose column</td>
</tr>
</tbody>
</table>

**Query scheduling**

- Run query every
  - 5
  - Hours
- Lookup data from the last
  - 5
  - Hours
Select a playbook to be run automatically when your analytic rule generates an alert.

**Selected playbook**: `[✓]` ConnectServiceNow

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>TRIGGER KIND</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectServiceNow</td>
<td>Enabled</td>
<td>Azure Sentinel</td>
</tr>
</tbody>
</table>
Validation passed.

**Analytic rule details**

Name
Description
Tactics
Severity
Status

**Medium**

**Enabled**

**Detection settings**

**Rule query**

```sql
| where TimeGenerated >= ago(1d) 
| summarize perIdentityAuthCount=count() by identity, locationString= strcat(tostring(LocationDetails["countryOrRegion"]), "/", tostring(LocationDetails["state"]), "/", tostring(LocationDetails["city"]), "/", tostring(LocationDetails["geoCoordinates"])) 
| summarize distinctAccountCount = count(), identityList=makeSet(identity) by locationString 
| extend identityList = if(distinctAccountCount < 10, identityList, "multiple (>10)") 
| join kind= anti 
| SigninLogs 
| where TimeGenerated < ago(1d) 
| project locationString= strcat(tostring(LocationDetails["countryOrRegion"]), "/", tostring(LocationDetails["state"]), "/", tostring(LocationDetails["city"]), "/", tostring(LocationDetails["geoCoordinates"])) 
| summarize priorCount = count0 by locationString 
| on locationString 
| where distinctAccountCount > 1 // select threshold above which #new accounts from a new location is deemed suspicious 
| extend AccountCustomEntity = identityList 
| Every 5 hours 
| Last 5 hours data 
| Rule threshold 
| Trigger alert if query returns more than 1 results 
```

**Rule frequency**

**Rule period**

**Rule threshold**
Investigating Incidents

• Incidents are opened for triggered analytics rules

• Incidents can be assigned to investigators, comments added, and the status and severity can be modified- providing basic workflow tools

• Investigation is highly dependent on entities surfaced through the alert query

• Currently available entities:
  • Host
  • IP
  • User
  • Timestamp

• Entities allow pivoting and correlation of alerts in the Investigation pane
Multiple failed user log on attempts to an app

**Description**

Activity policy 'Multiple failed user log on attempts to an app' was triggered by 'Daryl Novak'.

**Tags**

- 

**Last update time**

10/04/19, 4:29 PM

**Creation time**

10/04/19, 3:06 PM

**Close reason**

N/A

**Evidence**

- N/A

- 1

- 0

- View full details
Multiple failed user log on attempts to an...
Multiple failed user log on attempts to an app
Multiple failed user log on attempts

Severity: High
Status: In Progress
Owner: Daryl@systemcenteradmin.com

Last incident update time: 2019-10-04, 4:29:34 PM

Timeline
Info
Entries
Help
Multiple failed user log on attempts

Severity: High
Status: In Progress
Owner: Daryl@systemcenteradmin.com
Last incident update time: 2019-10-04, 4:29:34 PM

Related alerts:
- Related bookmarks:
- Least active accounts on Azure:
  - More...

- Multiple failed u...
- daryl
- 192.168.1.23
- Microsoft Azure
- Failed login attempt...
- Brute force attack...
- + 309 Failed log...
Multiple failed user log on attempt.

Severity: High
Status: In Progress
Owner: Daryl@systemcenteradmin.com
Last incident update time: 2019-10-04, 4:29:34 PM

Attached data:
- 102.0.201.232
- Microsoft Azure
- Failed login attempt:
  - 301 Failed login...
Multiple failed user log on attempts to an app

Entities (3)
- 192.0.212.232
- Microsoft Azure
- daryl

Alerts (3)
- Multiple failed user log on attempts to an app
- Failed login attempts to Azure Portal
- Brute force attack against Azure Portal

Bookmarks (0)
No results
Multiple failed user log on attempts

Brute force attack against Azure Portal
- Failed login attempts to Azure Portal
  2019-09-24, 2:03:54 PM
  Identifies failed login attempts in the Azure Active Directory...
- Brute force attack against Azure Portal
  2019-10-04, 2:43:26 PM
  Identifies evidence of brute force activity against Azure Po...
- Multiple failed user log on attempts ...
  2019-10-04, 3:06:03 PM
  Activity policy 'Multiple failed user log on attempts to an a...
Hunting in Sentinel

• Workbooks allow you to visualize trends and drill down into anomalies
  • Many connectors come with Workbook templates, or you can create your own

• Hunting queries allow you to group and organize KQL queries by datasource and MITRE ATT&CK category and create bookmarks for interesting findings
  • Its very easy to run all your hunting queries simultaneously

• Notebooks let you deploy Jupyter notebooks to the free Azure Notebooks service
  • You can also deploy them locally or elsewhere into a
let timeRange = ago('d');
SigninLogs
  | where TimeGenerated >= timeRange
  | where AppDisplayName contains "Azure Portal"
  // 50126 - Invalid username or password, or invalid on-premises username or password.
  // 588287 - The user doesn't exist in the tenant.
  | where ResultType in ("50126", "588278")
  | extend OS = DeviceDetail.operatingSystem, Browser = DeviceDetail.browser
  | extend StatusCode = tostring(Status.errorCode), StatusDetails = tostring(Status.additionalDetails)
  | extend State = tostring(LocationDetails.state), City = tostring(LocationDetails.city)
  | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), IPAddress = makeset(IPAddress), DistinctIPCount = dcount(IPAddress), makeset(OS), makeset(Browser), StatusArray = Status.errorCode
Completed

<table>
<thead>
<tr>
<th>StatusCode</th>
<th>StatusDetails</th>
<th>State</th>
<th>timestamp [UTC]</th>
<th>AccountCustomEntity</th>
<th>UserDisplayName</th>
<th>UserPrincipalName</th>
<th>AppDisp</th>
</tr>
</thead>
<tbody>
<tr>
<td>50126</td>
<td></td>
<td>Ontario</td>
<td>10/4/2019, 6:46:38.74 PM</td>
<td><a href="mailto:daryl@systemcenteradmin.com">daryl@systemcenteradmin.com</a></td>
<td>Daryl Novak</td>
<td><a href="mailto:daryl@systemcenteradmin.com">daryl@systemcenteradmin.com</a></td>
<td>Azure Portal</td>
</tr>
</tbody>
</table>
let timeRange = ago(7d);

SigninLogs
where TimeGenerated >= timeRange
where AppDisplayName contains "Azure Portal"
  // 50126 - Invalid username or password, or invalid on-premises username or password.
  // 50820 - The user doesn’t exist in the tenant.
where ResultType in ("50126", "50820")

extend OS = DeviceDetail.operatingSystem, Browser = DeviceDetail.browser
extend StatusCode = toString(Status.errorCode), StatusDetails = toString(Status.additionalDetails)
extend State = toString(LocationDetails.state), City = toString(LocationDetails.city)
summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), IPAddressxes = makeset(IPAddress)

### Completed

<table>
<thead>
<tr>
<th>StatusCode</th>
<th>StatusDetails</th>
<th>State</th>
<th>timestamp [UTC]</th>
<th>AccountCustomEntity</th>
</tr>
</thead>
<tbody>
<tr>
<td>50126</td>
<td></td>
<td>Ontario</td>
<td>10/4/2019, 6:16:38.740 PM</td>
<td><a href="mailto:daryl@systemcenteradmin.com">daryl@systemcenteradmin.com</a></td>
</tr>
</tbody>
</table>

- **UserDisplayName** | Daryl Nowak
- **UserPrincipalName** | daryl@systemcenteradmin.com
- **AppDisplayName** | Azure Portal
- **ResultType** | 50126
- **ResultDescription** | Invalid username or password or invalid on-premise username or password.
- **StatusCode** | 50126
- **Location** | CA
- **State** | Ontario
- **StartTimeUtc [UTC]** | 2019-10-04T18:46:38.74Z
- **EndTimeUtc [UTC]** | 2019-10-05T17:53:13.051Z
- **IPAddressxes** | ["192.0.212.232"]
<table>
<thead>
<tr>
<th>Name</th>
<th>Created By</th>
<th>Tags</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed attempt to access Azure Portal - 532...</td>
<td>@systemcenteradmin.com</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**Event time**
2019-10-04, 2:46:38 PM

**Tags**
```
+
```

**Entities**
- **Account**: daryl@systemcenteradmin.com
- **UserDisplayName**: Daryl Novak
- **UserPrincipalName**: daryl@systemcenteradmin.com

**Query result row**

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserDisplayName</td>
<td>Daryl Novak</td>
</tr>
<tr>
<td>UserPrincipalName</td>
<td><a href="mailto:daryl@systemcenteradmin.com">daryl@systemcenteradmin.com</a></td>
</tr>
</tbody>
</table>
Failed attempt to access Azure Portal - 532047ff8d97

Daryl@systemcenteradmin.com

Last updated by

2019-10-05, 3:32:56 PM

Last bookmark update time
Using the Notebooks locally or in other environments

Azure Sentinel will provision notebooks and supporting modules for you in Azure Notebooks. You can also download the notebooks and modules and use them locally in a supported Python environment (Anaconda is recommended) or another notebook hosting environment such as Azure Databricks or a JupyterHub environment that supports Python 3.6 or later.

Azure Sentinel Notebooks Include:

- **Alert Investigation and Hunting**
  Quickly triage different classes of alerts by enriching them with related activity and events from multiple data sources.

- **Endpoint Host Guided Hunting**
  Hunt for signs of a compromise by drilling down into the security relevant activities related to specific endpoint hosts.

- **Office Logon Anomalies Guided Hunting**
  Investigate suspicious logons in Office365 data by visualizing geographic data and displaying unusual logon patterns.
Threat Intel - Check the IP Address for known malicious addresses

Lookup in Azure Sentinel Bring-Your-Own-Threat-Intel

```
In [19]:
# Lookup in Sentinel Bring-Your-Own-Threat-Intel (or IPReputation/Blacklists)
# The Ti Kql query - we're substituting the IP address to search for
Ti_query = r'''
BYOTthreatIntelv1_CL
| where NetworkIP_s == '(ip)'
| project TimeGenerated, ExternalIndicatorId_s, ThreatType_s,
Description_s, Active_s, TrafficLightProtocolLevel_s,
ConfidenceScore_s, ThreatSeverity_s, ExpirationDateTime_t,
IndicatorId_s, NetworkIP_s, Type
'''.format(ip=alert_ip_entities[0].Address)

# run the query, convert to a dataframe and display any result
kql = query Ti_query
Ti_query_df = kql_raw_result_.to_dataframe()
if len(Ti_query_df) > 0:
    display(Ti_query_df.T)
```

<table>
<thead>
<tr>
<th>TimeGenerated</th>
<th>2019-02-17 02:54:12.096000</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExternalIndicatorId_s</td>
<td>Botnet Indicator:1549501989M5525</td>
</tr>
<tr>
<td>ThreatType_s</td>
<td>Botnet</td>
</tr>
<tr>
<td>Description_s</td>
<td>This is a botnet indicator generated in RFC5737 documentation space. Take no action on any observables set in this indicator.</td>
</tr>
<tr>
<td>Active_s</td>
<td>True</td>
</tr>
<tr>
<td>TrafficLightProtocolLevel_s</td>
<td>Green</td>
</tr>
<tr>
<td>ConfidenceScore_s</td>
<td>0</td>
</tr>
<tr>
<td>ThreatSeverity_s</td>
<td>0</td>
</tr>
<tr>
<td>ExpirationDateTime_t</td>
<td>2019-02-07 02:13:08.520000</td>
</tr>
<tr>
<td>IndicatorId_s</td>
<td>fe16b36b64741ec1c73918971811620e38b26d69d20e5eb20953dcaacda075</td>
</tr>
<tr>
<td>NetworkIP_s</td>
<td>23.97.60.214</td>
</tr>
<tr>
<td>Type</td>
<td>BYOTthreatIntelv1_CL</td>
</tr>
</tbody>
</table>
In [19]:

```
# Get an API key for Virus Total
vt_key = nbtools.GetEnvironmentKey(env_var='VT_API_KEY',
    help_str='To obtain an API key sign up here https://www.virustotal.com/
    prompt='Virus Total API key: ')

vt_key.display()
```

HTML(value='To obtain an API key sign up here https://www.virustotal.com/')</p>

```
HBox(children=(Text(value=''), description='Virus Total API key:', layout=Layout(width='50%'), style=Description)
```

In [20]:

```
# Lookup the IP Addresses in Virus Total using the matcpy VTLookup class
vt_lookup = seクトools.VT Lookup(vt_key.value, verbosity=2)

# Let's look for our other C2 IPs - we don't expect our simulated attack
# address to appear in VT.
# Note, because we're using a free VirusTotal API key here we're limited to
# 4 requests per minute so some requests may error out.
for ip in vt_lookup.ip_entities:
    vt_lookup.lookup_loc(observable=ip.Address, ioc_type='ipv4')
vt_lookup.results.dropna(axis='columns')
```

Error parsing response to JSON: "31.148.220.53", type "ipv4". (Source index 0)
Error parsing response to JSON: "103.225.168.159", type "ipv4". (Source index 0)
Parting thoughts

• Security is (still) hard

• Carefully design your architectures for security and use the tools available to you to catch what you miss – then improve your architecture based on your findings!

• Identity is the new perimeter, zero trust, least privilege - all catchy phrases but they distill important (and messy) concepts

• Security is (still) everyone’s job
Thanks for attending!

THANK YOU
YOU HAVE GOOD SECURITY SKILLS

Daryl.Novak@newsignature.com
darylnovak
@darylnovak