The Asset Management Resurgence: From Boring to Top of Mind

January 22, 2020
Speakers

David Vaughn
C|CISO, LPT, GSNA, CISSP
ISSA

Nathan Burke
CMO
Axonius

Bryan Bethelmy
CISO
Mancon
Agenda

• Why the Bad Reputation?
• What Changed?
• Cybersecurity and Asset Management Overview
Why the Bad Reputation?
Traditional ITAM

- **Inventory**
  - Hardware
  - Software
  - Network Assets

- **License Management**
  - Making sure all devices are running licensed software

- **Lifecycle Management**
  - Procurement
  - Decommissioning
  - Updating Inventory
ASSET MANAGEMENT: THE TOYOTA CAMRY OF CYBERSECURITY
The Asset Management Challenge

Jim Schwar
@jimiDFIR

Replying to @MalwareJake

CISO: How many windows hosts do we have?
AV Guy: 7864
Desktop Management: 6321
EDR Team: 6722
CMDB Team: 4848
SIEM Team: 9342

5:55 AM - 8 Feb 2018

540 Retweets 1,023 Likes
Why is Asset Management So Difficult?
Is your agent everywhere it should be?
Which unmanaged devices are connected to privileged networks?
Are your cloud instances covered?
Cloud Asset Compliance

Cloud Asset Compliance Center:

CIS Amazon Web Services Foundations Benchmark Compliance V1.2

<table>
<thead>
<tr>
<th>Rule</th>
<th>Rule Name</th>
<th>Category</th>
<th>Results (Failed/Checked)</th>
<th>Affected Devices/Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Avoid the use of the &quot;root&quot; account</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.2</td>
<td>Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password</td>
<td>Identity and Access Management</td>
<td>1/3</td>
<td>0</td>
</tr>
<tr>
<td>1.3</td>
<td>Ensure credentials accessed for 90 days or greater are disabled</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.4</td>
<td>Ensure access keys are rotated every 90 days or less</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.5</td>
<td>Ensure IAM password policy requires at least one uppercase letter</td>
<td>Identity and Access Management</td>
<td>6/10</td>
<td>7</td>
</tr>
<tr>
<td>1.6</td>
<td>Ensure IAM password policy requires at least one lowercase letter</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.7</td>
<td>Ensure IAM password policy requires at least one symbol</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.8</td>
<td>Ensure IAM password policy requires at least one number</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.9</td>
<td>Ensure IAM password policy requires a minimum length of 14 or greater</td>
<td>Identity and Access Management</td>
<td>4/11</td>
<td>33</td>
</tr>
<tr>
<td>1.10</td>
<td>Ensure IAM password policy prevents password reuse</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.11</td>
<td>Ensure IAM password policy expires passwords within 90 days or less</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.12</td>
<td>Ensure no root account access key exists</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.13</td>
<td>Ensure MFA is enabled for the &quot;root&quot; account</td>
<td>Identity and Access Management</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.14</td>
<td>Ensure hardware MFA is enabled for the &quot;root&quot; account</td>
<td>Logging</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.15</td>
<td>Ensure IAM policies are attached only to groups or roles</td>
<td>Logging</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.16</td>
<td>Ensure IAM policies that allow &quot;all-<em>-</em>&quot; administrative privileges are not created</td>
<td>Logging</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.17</td>
<td>Ensure CloudTrail is enabled in all regions</td>
<td>Logging</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.18</td>
<td>Ensure CloudTrail log file validation is enabled</td>
<td>Logging</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.19</td>
<td>Ensure the S3 bucket CloudTrail logs is not publicly accessible</td>
<td>Logging</td>
<td>0/0</td>
<td>0</td>
</tr>
<tr>
<td>1.20</td>
<td>Ensure CloudTrail trails are integrated with Amazon CloudWatch Logs</td>
<td>Logging</td>
<td>0/0</td>
<td>0</td>
</tr>
</tbody>
</table>
Cloud Asset Compliance
Each tool answers some questions, while begetting other questions that it can’t answer by itself.
1. Is the asset “known” and managed?
2. Where is it?
3. What is it?
4. Is the core software up to date?
5. What additional software is installed?
6. Does it adhere to my security policy?
Modern asset management is the nexus for cybersecurity projects and decisions.
Modern asset management is the nexus for cybersecurity projects and decisions.

- Connect to all existing IT systems, bridging the siloed data sources.
- Correlate to create a unique entry for every asset, viewed from several perspectives.
- Remediate gaps and report on progress toward cybersecurity objectives.