It’s All About Your Assets

Inline Vulnerability and Event Management
Analogy

Let’s kick this off with a story
The Family

Reid is the one with “The Man Perm”
The logical choice

Dad’s 2002 Honda Accord
The not so logical choice

Lifted 1976 Jeep J10 truck with huge mud tires
Logical choice - Context

Advertised / Public Context
- 2002 Honda Accord
- 2.3L 4 cylinder engine
- Automatic transmission
- Reported MPG 26 city / 32 highway

Historical / Acquired Context
- Single owner – Me
- ~120k miles
- No (significant) accidents
- No major issues/weaknesses other than a few recalls and routine maintenance
- Top “safe” driving speed – 80+ MPH
- Average MPG 20-22
Not so logical choice - Context

Advertised / Public Context
- 1976 Jeep J10
- 2nd Largest Engine
  - 5.9L V8 engine
- Manual transmission
- Reported MPG < 10

Historical / Acquired Context
- Before purchase
  - Multiple owners
  - New carburetor
  - Starter might need replaced
  - ~70k miles
  - Leaking coolant
  - Fuel gauge not working
- Soon After purchase
  - Leaking (spraying) oil
  - Maybe leaking power steering fluid
  - Top “safe” drive speed ~55-60 MPH
Gaining context

Car

- Contact previous owner(s)
- Experience - familiarize myself with asset and perform obvious maintenance
- Research available knowledgebases and repositories (online forums, service manuals, etc.)
- Tap into vendor network (auto supply stores)
- Consult an expert (mechanic, transmission shop, etc.)

IT Asset

- Contact owner(s)
- Experience – monitor, patch, configure, investigate, etc.
- Research available knowledgebases and repositories (online forums, CVE/CWE, CIS benchmarks, etc.)
- Tap into vendor network (VM, patch and config. mgmt., etc.)
- Consult an expert (SME, development team, etc.)
Sometimes life imitates work

- Can’t lock doors unless inside lever is down (no spring left)
  - Can’t upgrade Java unless we rewrite application

- Some gauges and displays go in and out
  - Vulnerability goes away comes back next week, repeat

- Fluid leaks from windshield wiper reservoir
  - Memory leak causes of scheduled reboot of application for years until someone bothered to review Static Application Security Testing results below Critical and High

- Car starts better with clutch in but shift lever in reverse
  - Application infrastructure startup sequence can be important

- Better to skip 1st gear most of the time as top speed is 3-5 MPH
  - Should we patch for Specter and Meltdown
Not what I am talking about

- $R = T \times V$
- $R = T \times V \times I \times L$
- $R = \text{LEF} \times \text{LM}$
  - $\text{LEF} = \text{TEF} \times V$
  - $\text{LM} = \text{PL} + \text{SL}$

“A LIST OF PEOPLE WHO ACTUALLY UNDERSTAND IT RISK MANAGEMENT”

Meme: http://www.carmelowalsh.com/tag/memes/
Let’s simplify

- How vulnerable is the asset?
  - Exploit or malware available
  - CVSS 7 or higher

- How critical is the asset?
  - External facing
  - RTO/RPO values

- Who owns the asset?

Theft quadrants – xkcd.com/1698
Take it to the next level

- Who / what understands the asset?
  - Applications installed
  - Applications running
  - Dependencies
  - Baseline Configuration / Ports / Connections
  - Credentials / Authorized Personnel

- Who can approve downtime or make emergency decisions?

- Where is the asset located?

- What behavior is typical?

- What relationships exist?

- Who is responsible for patching and configuring the asset?
Success factors

Where should we focus??
Four Success Factors

- **Accuracy**
  - Findings and data must be accurate in order to increase efficiency and decrease pushback

- **Integration**
  - Security processes should integrate into existing business processes

- **Consolidation**
  - Messaging should be simplified and consolidated to make it easy for asset owners

- **Automation**
  - Anything that can be automated, should be automated
What if we don’t have the talent?

- CISOs number 1 concern for 2018

- Get creative
  - Loaned staff
    - Borrow or hire developers for automation and integration
    - Borrow or hire DevOps or systems engineers to automate patch and configuration management and/or document common issues, resolutions, etc.
  - In-house training
    - Borrow entry-level staff, even without security knowledge, and give them tasks that add value while training (e.g. update asset inventory, attributes, relationships)
Demo Screenshots
Splunk Alert

Listening on Port 4444

{(sourcetype="Unix:ListeningPorts" OR sourcetype="Script:ListeningPorts") dest_port=4444}

Alert: Listening on Port 4444

Description: Server is listening on default Metasploit port of 4444

Alert type: Scheduled

Trigger Conditions

Trigger alert when: Per-Result

Throttle:
Splunk Alert Action

Trigger Actions

When triggered

Create ServiceNow Security Event

Creates a ServiceNow security event using the first log found by this alert search. To set a field below from the log entry, use the $result.x$ syntax - such as $result.host$ to put the host name into node field.

Security Event Values

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>$result.host$</td>
</tr>
<tr>
<td>Type</td>
<td>Security</td>
</tr>
<tr>
<td>Resource</td>
<td>$result.host$</td>
</tr>
<tr>
<td>Source</td>
<td>Splunk</td>
</tr>
<tr>
<td>Severity</td>
<td>1</td>
</tr>
<tr>
<td>Time of Event</td>
<td>$result_time$</td>
</tr>
<tr>
<td>Description</td>
<td>Listener on Default Metasploit Port 4444 $result_raw$</td>
</tr>
</tbody>
</table>

Configuration Item (CI) causing this alert
Type of event to create
Resource affected by or causing this alert
The source of the alert
Severity to assign to the event
Supported format is YYYYMMDDHHmmss[nnn][mmm]
Description of the cause of this event, additional fields and data
Listeners to Trigger Alerts

Fortify Software Security Center

PuTTY

PuTTY[ec2-user@ssc ~]$ nc -l 4444

MSSQL Database Server

C:\Users\admin\Downloads\ncat-portable-5.59BETA1>ncat -l -p 4444
# ServiceNow Events

<table>
<thead>
<tr>
<th>Time of event</th>
<th>Source</th>
<th>Description</th>
<th>Node</th>
<th>Type</th>
<th>Resource</th>
<th>Message key</th>
<th>State</th>
<th>Severity</th>
<th>Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-07-27 22:04:44</td>
<td>Splunk</td>
<td>Listener on Default Metasploit Port 4444...</td>
<td>ssc</td>
<td>Security</td>
<td>ssc</td>
<td>Processed</td>
<td>Critical</td>
<td>Alert0010007</td>
<td></td>
</tr>
<tr>
<td>2018-07-27 22:06:00</td>
<td>Splunk</td>
<td>Listener on Default Metasploit Port 4444...</td>
<td>db.shield.deloitte.com</td>
<td>Security</td>
<td>db.shield.deloitte.com</td>
<td>Processed</td>
<td>Critical</td>
<td>Alert0010006</td>
<td></td>
</tr>
</tbody>
</table>
### ServiceNow Alerts

<table>
<thead>
<tr>
<th>Number</th>
<th>Group</th>
<th>Severity</th>
<th>Priority</th>
<th>State</th>
<th>Source</th>
<th>Description</th>
<th>Node</th>
<th>Configuration item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert0010006</td>
<td></td>
<td>Critical</td>
<td></td>
<td>Open</td>
<td>Splunk</td>
<td>Listener on Default Metasploit Port 4444...</td>
<td>db.shield.deloitte.com</td>
<td>db</td>
</tr>
<tr>
<td>Alert0010007</td>
<td></td>
<td>Critical</td>
<td></td>
<td>Open</td>
<td>Splunk</td>
<td>Listener on Default Metasploit Port 4444...</td>
<td>ssc</td>
<td>ssc</td>
</tr>
</tbody>
</table>
One to Many - Alerts to Events

Quick Response

Alerts
Alert0010006

No records to display

Events
New
Go to

Severity

Critical
2018-07-27 22:04:12
Splunk
db.shield.dealte.com
Security

Critical
2018-07-27 22:06:00
Splunk
db.shield.dealte.com
Security
ServiceNow Alert Rules to Create SI

Alert Action Rule enables you to perform actions on alerts

- **Name**: Create security incidents for critical alerts
- **Active**: Checked
- **Order**: 90

**Alert Filter**
- Classification: Is Security
- Severity: Is Critical

**Action**
- **Auto acknowledge**: Checked
- **Auto open**: Checked
- **Type**: Security Incident (sa_si_incident)
- **Task template**: Security Incident from Event
### ServiceNow Security Incident

#### Draft

<table>
<thead>
<tr>
<th>Number</th>
<th>SIR010005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested by</td>
<td></td>
</tr>
<tr>
<td>Configuration Item</td>
<td>db</td>
</tr>
<tr>
<td>Affected user</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Fairfax</td>
</tr>
<tr>
<td>Category</td>
<td>-- None --</td>
</tr>
<tr>
<td>Subcategory</td>
<td>-- None --</td>
</tr>
</tbody>
</table>

#### Analysis

<table>
<thead>
<tr>
<th>Opened</th>
<th>2018-07-27 22:04:29</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Draft</td>
</tr>
<tr>
<td>Substate</td>
<td>-- None --</td>
</tr>
<tr>
<td>Source</td>
<td>Network Monitoring</td>
</tr>
<tr>
<td>Risk score</td>
<td>92</td>
</tr>
<tr>
<td>Risk score override</td>
<td></td>
</tr>
<tr>
<td>Business impact</td>
<td>1 - Critical</td>
</tr>
<tr>
<td>Priority</td>
<td>1 - Critical</td>
</tr>
<tr>
<td>Assignment group</td>
<td>SRT</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Waldo Sisk</td>
</tr>
</tbody>
</table>

---

*Short description: Security: db.shield.deiattie.com (db.shield.deiattie.com) - Listener on Default Metasploit Port 44407/28/2018 3:04:12 transport=TCP dest_ip=90.0.0.0 dest_port*
ServiceNow Configuration Item
ServiceNow Configuration Item (2)
## ServiceNow Configuration Item (3)

### Related Items
- **Contains - Tracked Configuration files**
  - C:\Windows\System32\drivers\etc\hosts
  - C:\Windows\System32\drivers\etc\networks
  - C:\Windows\System32\drivers\etc\protocol
  - C:\Windows\System32\drivers\etc\services

- **Implement End Point From - Traffic Based Connection Qualifiers**
  - MSSQLSERVER@db
- **Implement End Point From - Nginx Web Servers**
  - Tomcat@ssc:8080
  - Nginx Web Server

- **Runs - MSFT SQL Instances**
  - MSSQLSERVER@db

- **Use End Point From - Tomcats**
  - Tomcat@jira

- **Used by - Tomcats**
  - MSSQLSERVER@db

### Related Links
- Add to Security Case
- Discover now
- Subscribe
- Show Discovery events
<table>
<thead>
<tr>
<th>Display name</th>
<th>Version</th>
<th>Discovery model</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server Developer Edition (64-bit)</td>
<td>13.0.4001.0</td>
<td>Microsoft SQL Server Developer Edition (...</td>
</tr>
</tbody>
</table>
### ServiceNow Configuration Item (6)

<table>
<thead>
<tr>
<th>PID</th>
<th>Name</th>
<th>Command</th>
<th>Parameters</th>
<th>Key parameters</th>
<th>Classify</th>
<th>PPID</th>
<th>Parent</th>
<th>Connecting to</th>
</tr>
</thead>
<tbody>
<tr>
<td>810</td>
<td>conhost.exe</td>
<td>C:\Windows\system32\conhost.exe</td>
<td>177:1 C:\Windows\system32\conhost.exe 0x4</td>
<td>true</td>
<td>7324</td>
<td>splunkd.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>856</td>
<td>chrome.exe</td>
<td>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</td>
<td><em>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</em></td>
<td>true</td>
<td>3,97%</td>
<td>chrome.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>804</td>
<td>chrome.exe</td>
<td>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</td>
<td><em>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</em></td>
<td>true</td>
<td>3,97%</td>
<td>chrome.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>780</td>
<td>chrome.exe</td>
<td>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</td>
<td><em>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</em></td>
<td>true</td>
<td>3,97%</td>
<td>chrome.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>760</td>
<td>chrome.exe</td>
<td>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</td>
<td><em>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</em></td>
<td>true</td>
<td>3,97%</td>
<td>chrome.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>720</td>
<td>svchost.exe</td>
<td>C:\Windows\System32\svchost.exe</td>
<td>C:\Windows\System32\svchost.exe-k mshtml</td>
<td>true</td>
<td>77%</td>
<td>services.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>672</td>
<td>splunkd.exe</td>
<td>C:\Program Files (x86)\SplunkUniversalForwarder\splunkd.exe</td>
<td><em>C:\Program Files (x86)\SplunkUniversalForwarder\splunkd.exe</em></td>
<td>true</td>
<td>77%</td>
<td>services.exe</td>
<td>0.0001</td>
<td>splunkd.exe</td>
</tr>
<tr>
<td>676</td>
<td>chrome.exe</td>
<td>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</td>
<td><em>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</em></td>
<td>true</td>
<td>3,97%</td>
<td>chrome.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>644</td>
<td>ShellExperienceHost.exe</td>
<td>C:\Windows\System32\ShellExperienceHost.exe</td>
<td><em>C:\Windows\System32\ShellExperienceHost.exe</em></td>
<td>true</td>
<td>868</td>
<td>svchost.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>560</td>
<td>dwm.exe</td>
<td>C:\Windows\system32\dwm.exe</td>
<td><em>dwm.exe</em></td>
<td><em>dwm.exe</em></td>
<td>true</td>
<td>956</td>
<td>mfc120u.exe</td>
<td></td>
</tr>
<tr>
<td>564</td>
<td>WUDFHost.exe</td>
<td>C:\Windows\System32\WUDFHost.exe</td>
<td><em>C:\Windows\System32\WUDFHost.exe</em></td>
<td><em>C:\Windows\System32\WUDFHost.exe</em></td>
<td>true</td>
<td>1,028</td>
<td>svchost.exe</td>
<td></td>
</tr>
<tr>
<td>562</td>
<td>chrome.exe</td>
<td>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</td>
<td><em>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</em></td>
<td>true</td>
<td>3,97%</td>
<td>chrome.exe</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ServiceNow Dependency Map Expanded
### ServiceNow Software Vulnerabilities (Before)

<table>
<thead>
<tr>
<th>Number</th>
<th>State</th>
<th>Remediation target</th>
<th>Configuration item</th>
<th>Vulnerability</th>
<th>Risk score</th>
<th>Last found</th>
<th>Defer expiration</th>
<th>Vulnerable software</th>
<th>Created</th>
</tr>
</thead>
</table>

No records to display
ServiceNow Software Vulnerabilities (Config)

Software Asset Management (SAM) creates records listing the software installed. The National Vulnerability Database (NVD) information indicates which particular versions of software have known vulnerabilities within your system. When SAM NVD Vulnerability Detection is enabled, the existing software assets are compared to the NVD database, and vulnerable items are created to track configuration items that you wish to scan.

Detect vulnerabilities using SAM data

CI Filter

Add Filter Condition  Add "OR" Clause

Name ▼ is ▼ db ▼ AND ▼ OR ▼

Vulnerability filter

Add Filter Condition  Add "OR" Clause

-- choose field -- ▼ -- oper -- ▼ -- value --

Save and Create Vulnerable Items
ServiceNow Software Vulnerabilities (After)