THE CASE FOR BUILDING YOUR OWN SOC AUTOMATIONS

NATHANAEL KENYON
ABOUT ME

• 20 YEARS EXPERIENCE IN INFORMATION TECHNOLOGY WITHIN MILITARY, GOVERNMENT AND PRIVATE SECTORS

• MBA, CISSP, GXPN, GAWN, GMOB, GPYC, GNFA, GPen, GCIA, GCIH, GCFE, GSEC
HAS THIS EVER HAPPENED TO YOU?

- **Salesperson “misrepresented product capabilities”**
- **Tool changes required you to make adjustments to your processes**
THE PURPOSE OF SOAR TOOLS

• Alleviate Staff shortages
• Reduce routine and burdensome work for analysts
• Reduce the number of tools an analyst has to interact with
• Improve Workflow management
Why should you build your own SOC automations?

- There is no magic product that will do everything for you.
- The new security, automation, orchestration and response (SOAR) tools will not help you if you do not have your processes defined and the ability implement custom integrations. (Even if the salesperson says it will.)
- Trying to do it yourself will tell you if you really need a new tool and give you valuable experience that will help you if you do purchase SOAR tools.
PEOPLE, PROCESSES AND TECHNOLOGY

• Adequately trained staff will be more successful with lesser tools than poorly trained staff with best of breed, top of the line tools

• There is an information security skills shortage in part because there are so many technologies that have to be secured

• People bring skills, process is how you apply the skills, improving both of these is more important than acquiring new technology
MAXIMIZING YOUR ANALYST

- Analysts should be investigating and mitigating threats
- Advanced analysts should be hunting for threats
- Make sure job tasks are appropriate for skill level
- Have analysts train and share knowledge with each other
SKILLS INVENTORY

• A human resource tool to help ensure that employees are a good fit for job/task needs

• Used to collect information about your analyst regarding their skills, abilities and experiences

• Include what skills/areas the analyst would like to improve in
“O” IS FOR ORCHESTRATION

- **Orchestration** – the organizing and coordination of workflow
  - Establishing written procedures (Use Cases)
  - Have your analyst write their individual use cases
“A” IS FOR AUTOMATION

- Automate all the things
- Use automation for consistency and time savings
- There will always be a gap between what is available out of the box with your tools and what you will need
- Develop the skills within your team to write custom automations
MAXIMIZING YOUR CURRENT TOOL SET

- Too many tools is a problem
- Implement all the features of the tools you have before you add more tools.
- Maximize by minimizing
PURCHASE CONSIDERATIONS

• ARE YOU GETTING FULL VALUE FROM THE TOOLS YOU CURRENTLY HAVE?
• DO YOUR ANALYSTS HAVE THE TIME TO LEARN ANOTHER TOOL OR PROCESS?
• IS IT POSSIBLE THAT ACQUIRING A NEW TOOL COULD MAKE THINGS WORSE?
Initial
- Processes are ad hoc
- It is often a reactive and chaotic environment.

Repeatable
- Basic processes are in place.
- Still more of a reactive environment.

Defined
- Processes are well documented and implemented.

Managed
- The processes are evaluated based on the data that is collected.

Optimizing
- The environment has become proactive.
- Qualitative feedback allows for process improvement.
# MITRE ATT&CK Framework

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command And Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Items</td>
<td>21 Items</td>
<td>56 Items</td>
<td>28 Items</td>
<td>60 Items</td>
<td>20 Items</td>
<td>19 Items</td>
<td>17 Items</td>
<td>13 Items</td>
<td>9 Items</td>
<td>21 Items</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript</td>
<td>Bash_profile and Bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
<td></td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>CMSTP</td>
<td>Accessibility Features</td>
<td>Binary Padding</td>
<td>Binary Padding</td>
<td>Hashing</td>
<td>Hashing</td>
<td>Application Deployment Software</td>
<td>Communication Through Removable Media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Command-Line Interface</td>
<td>AppCert DLLs</td>
<td>Access Token Shimming</td>
<td>BITS Jobs</td>
<td>Brute Force</td>
<td>Brute Force</td>
<td>Clipboard Data</td>
<td>Data Compressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Control Panel Items</td>
<td>Authorization</td>
<td>AppCert DLLs</td>
<td>AppCert DLLs</td>
<td>Clear Command History</td>
<td>Credential Discovery</td>
<td>Data Encrypted</td>
<td>Data Compressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>Execution through API</td>
<td>Bypass User Account Control</td>
<td>Bypass User Account Control</td>
<td>Bypass User Account Control</td>
<td>Code Signing</td>
<td>Clear Command History</td>
<td>Extortion Over Alternative Protocol</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing via Service</td>
<td>Execution through Module Load</td>
<td>DLL Search Order Hijacking</td>
<td>DLL Search Order Hijacking</td>
<td>DLL Search Order Hijacking</td>
<td>Component Firmware</td>
<td>Clear Command History</td>
<td>Extortion Over Command and Control Channel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>Exploitation for Client Execution</td>
<td>DLL Hijacking</td>
<td>DLL Hijacking</td>
<td>DLL Hijacking</td>
<td>Component Object Model Hijacking</td>
<td>Clear Command History</td>
<td>Extortion Over Other Network Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td>Graphical User Interface</td>
<td>Exploitation for Privilege Escalation</td>
<td>Extra Window Memory Injection</td>
<td>Extra Window Memory Injection</td>
<td>Control Panel Items</td>
<td>Clear Command History</td>
<td>Extortion Over Physical Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>InstallUtil</td>
<td>Extra Window Memory Injection</td>
<td>File System Permissions Weakness</td>
<td>File System Permissions Weakness</td>
<td>DCShadow</td>
<td>Clear Command History</td>
<td>Extortion Over Physical Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launchl</td>
<td>Local Job Scheduling</td>
<td>Fakedas/Decode/Decode Files or Information</td>
<td>Fakedas/Decode/Decode Files or Information</td>
<td>Fakedas/Decode/Decode Files or Information</td>
<td>Debfuscate/Decode/Decode Files or Information</td>
<td>Clear Command History</td>
<td>Extortion Over Physical Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malta</td>
<td>PowerShell</td>
<td>Faking Tools</td>
<td>Faking Tools</td>
<td>Faking Tools</td>
<td>Faking Tools</td>
<td>Clear Command History</td>
<td>Extortion Over Physical Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled Task</td>
<td>Scripting</td>
<td>File System Permissions Weakness</td>
<td>File System Permissions Weakness</td>
<td>File System Permissions Weakness</td>
<td>File System Permissions Weakness</td>
<td>Clear Command History</td>
<td>Extortion Over Physical Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Execution</td>
<td>Service Execution</td>
<td>Hashing</td>
<td>Hashing</td>
<td>Hashing</td>
<td>Hashing</td>
<td>Clear Command History</td>
<td>Extortion Over Physical Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signed Binary Proxy Execution</td>
<td>Signed Script Proxy Execution</td>
<td>Hypervisor</td>
<td>Hypervisor</td>
<td>Hypervisor</td>
<td>Hypervisor</td>
<td>Clear Command History</td>
<td>Extortion Over Physical Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Source</td>
<td>Executable File</td>
<td>Executable File</td>
<td>Executable File</td>
<td>Executable File</td>
<td>Clear Command History</td>
<td>Extortion Over Physical Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source after Fileẫme</td>
<td>Source</td>
<td>Executable File</td>
<td>Executable File</td>
<td>Executable File</td>
<td>Executable File</td>
<td>Clear Command History</td>
<td>Extortion Over Physical Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command And Control**
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control
- Custom Crypto Protocols
- Data Encoding
- Data Obfuscation
- Domain Fronting
- FallBack Channels
- Multi-Hop Proxy
- Multi-Stage Channels
- Multibad Communication
- MultiLayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocols
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
FINAL TAKE AWAY

- **Utilize your analysts to help develop your orchestration and automation procedures**
- **Maximize the current tools that are already in your SOC before adding more tools**
- **Use CMM and MITRE ATT&CK to find areas for improvement**
RESOURCES

• **Splunk Boss Of The Soc (BOTS)**
  
  • **BOTS dataset is not Splunk dependent**
  
  • [HTTP://EXPLORE.SPLUNK.COM/BOTS_1_0_DATASETS](HTTP://EXPLORE.SPLUNK.COM/BOTS_1_0_DATASETS)
  
  
  • [HTTPS://SPLUNKBASE.SPLUNK.COM/APP/3985/#/DETAILS](HTTPS://SPLUNKBASE.SPLUNK.COM/APP/3985/#/DETAILS)

• **Mitre att&ck Framework**
  
  • [HTTPS://ATTACK/MITRE.ORG/](HTTPS://ATTACK/MITRE.ORG/)