The Aaron’s Company, Inc.

Security Control Validation on a Budget
Business Case

• We wanted a security control validation solution, but not the price tag
• Atomic Red Team and Vectr.io were used as a starting point
• Resulted in a more robust, customizable, and automated solution
Security Control Validation Process

1. Test Control
2. Collect Results
3. Interpret Results
4. Remediate Failures
5. Communicate
The process flow is as follows:

1. **Test Control**: Simulate attack against DLP, EDR, etc.
2. **Collect Results**: Storage options can be SIEM, ELK, etc.
3. **Interpret Results**: Hands on or automated pass/fail examination
4. **Remediate Failures**: Adjust Security Control to alert appropriately for specific attack
5. **Communicate**: Format, Review, and Report test results

The cycle then restarts with **Test Control**.
Direct Correlation to MITRE ATT&CK Matrix

[Image of a detailed matrix correlating various attack vectors and techniques to the MITRE ATT&CK framework]
SAMPLE ARCHITECTURE

Atomic Host VLAN/VNET
- Login On Atomic Host
- Remote Powershell

Victim Machine VLAN/VNET
- Execute Atomics
- Export Log Data

MORE VICTIMS!!!!!!

Corporate VLAN/VNET
- Unidirectional Access Mechanism
- SIEM/IDS/IPS Console

Operator Host
- Communicate Results
- Test Failure
- Test Pass

SIEM/IDS/IPS
- Remediation

Review Logs
GOING NUCLEAR – ATOMIC RED TEAM

PS C:\WINDOWS\system32> Invoke-AtomicTest T1053.005 -ShowDetailsBrief
PathToAtomsFolder = C:\AtomicRedTeam\atomics

T1053.005-1 Scheduled Task Startup Script
T1053.005-2 Scheduled task Local
T1053.005-3 Scheduled task Remote
T1053.005-4 Powershell Cmdlet Scheduled Task
T1053.005-5 Task Scheduler via VBA
T1053.005-6 WMI Invoke-CimMethod Scheduled Task
Visualize Attack Paths

Heat Map Visualization of MITRE ATT&CK Relationship

Red Team/Blue Team
Example Metrics

Encompassing Test Coverage

Retest and Relate

- Emphasize when a test is repeated
- Relationship to other tests in cycle
- Relationship to other tests against same security control

- * Blue = Alert & Block
- * Green = Alert & No Block
- * Yellow = Expected Behavior
- * Red = Remediation Needed
The Aaron’s Team

- John Dearman, Security Architect
- Tyler Compton, Lead Security Engineer
- Jonathan Buckner, Junior Security Engineer