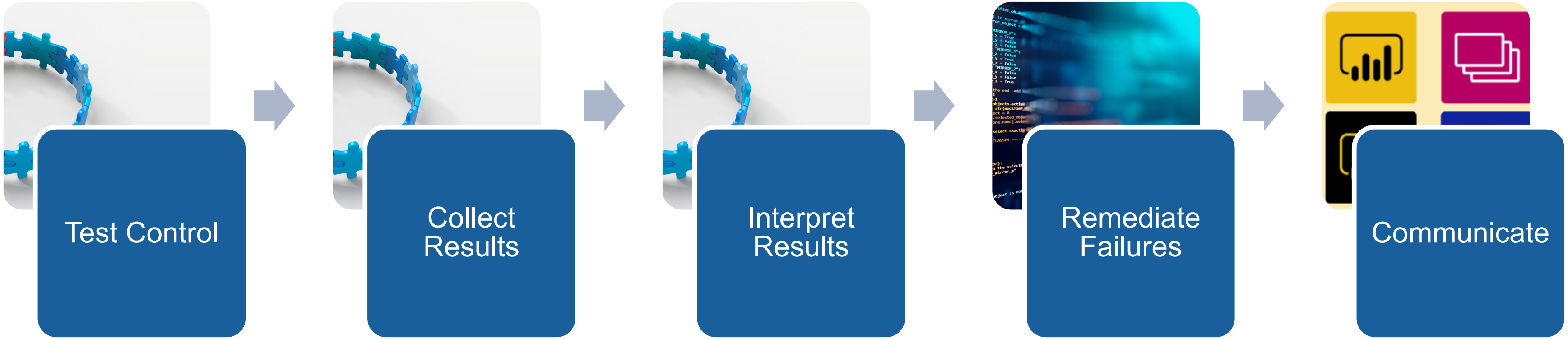
The Aaron’s Company, Inc.

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



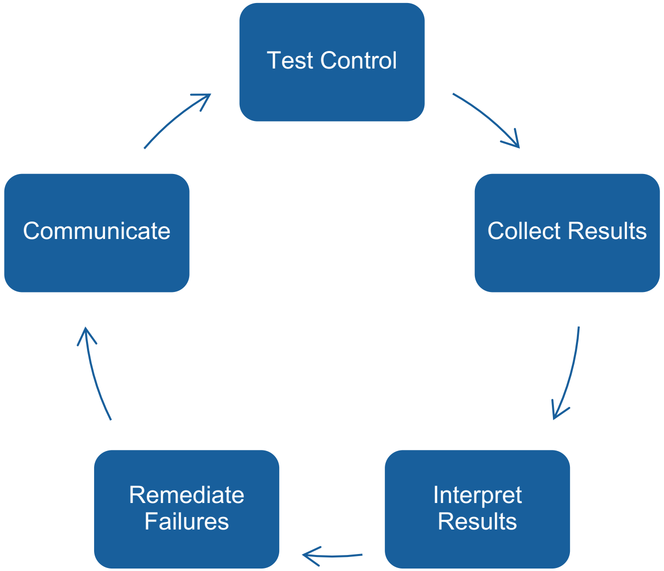
Test Control

Collect Results

Interpret Results

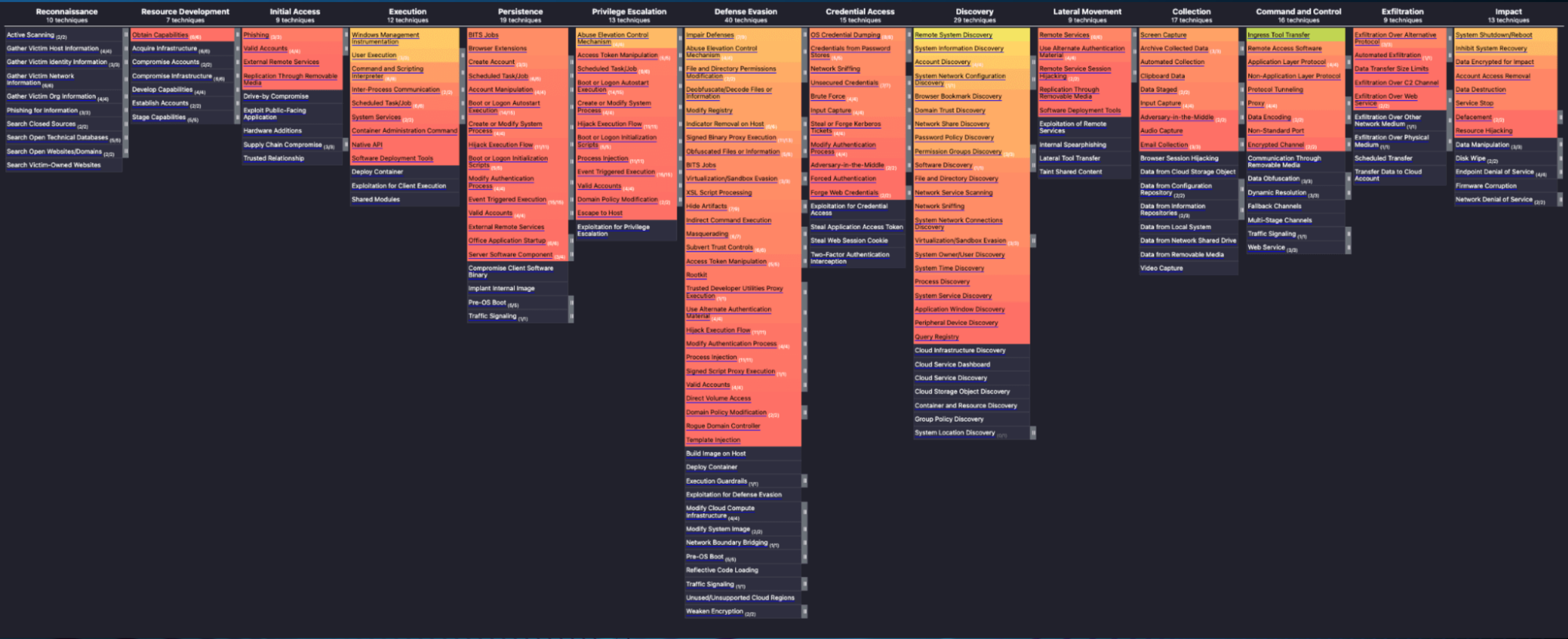
Remediate Failures

Communicate



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

Direct Correlation to MITRE ATT&CK Matrix



Reconnaissance
10 techniques

- Active Scanning (2/2)
- Gather Victim Host Information (4/4)
- Gather Victim Identity Information (3/3)
- Gather Victim Network Information (6/6)
- Gather Victim Org Information (4/4)
- Phishing for Information (3/3)
- Search Closed Sources (2/2)
- Search Open Technical Databases (5/5)
- Search Open Websites/Domains (2/2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Obtain Capabilities (6/6)
- Acquire Infrastructure (6/6)
- Compromise Accounts (2/2)
- Compromise Infrastructure (6/6)
- Develop Capabilities (4/4)
- Establish Accounts (2/2)
- Stage Capabilities (5/5)

Initial Access
9 techniques

- Phishing (3/3)
- Valid Accounts (4/4)
- External Remote Services
- Replication Through Removable Media
- Drive-by Compromise
- Exploit Public-Facing Application
- Hardware Additions
- Supply Chain Compromise (3/3)
- Trusted Relationship

Execution
12 techniques

- Windows Management Instrumentation
- User Execution (3/3)
- Command and Scripting Interpreter (8/8)
- Inter-Process Communication (2/2)
- Scheduled Task/Job (6/6)
- System Services (2/2)
- Container Administration Command
- Native API
- Software Deployment Tools
- Deploy Container
- Exploitation for Client Execution
- Shared Modules

Persistence
19 techniques

- BITS Jobs
- Browser Extensions
- Create Account (3/3)
- Scheduled Task/Job (6/6)
- Account Manipulation (4/4)
- Boot or Logon Autostart Execution (14/15)
- Create or Modify System Process (4/4)
- Hijack Execution Flow (11/11)
- Boot or Logon Initialization Scripts (5/5)
- Modify Authentication Process (4/4)
- Event Triggered Execution (15/15)
- Valid Accounts (4/4)
- External Remote Services
- Office Application Startup (6/6)
- Server Software Component (3/4)
- Compromise Client Software Binary
- Implant Internal Image
- Pre-OS Boot (5/5)
- Traffic Signaling (1/1)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4/4)
- Access Token Manipulation (5/5)
- Scheduled Task/Job (6/6)
- Boot or Logon Autostart Execution (14/15)
- Create or Modify System Process (4/4)
- Hijack Execution Flow (11/11)
- Boot or Logon Initialization Scripts (5/5)
- Process Injection (11/11)
- Event Triggered Execution (15/15)
- Valid Accounts (4/4)
- Domain Policy Modification (2/2)
- Escape to Host
- Exploitation for Privilege Escalation

Defense Evasion
40 techniques

- Impair Defenses (7/9)
- Abuse Elevation Control Mechanism (4/4)
- File and Directory Permissions Modification (2/2)
- Deobfuscate/Decode Files or Information
- Modify Registry
- Indicator Removal on Host (6/6)
- Signed Binary Proxy Execution (11/13)
- Obfuscated Files or Information (5/6)
- BITS Jobs
- Virtualization/Sandbox Evasion (3/3)
- XSL Script Processing
- Hide Artifacts (7/9)
- Indirect Command Execution
- Masquerading (6/7)
- Subvert Trust Controls (6/6)
- Access Token Manipulation (5/5)
- Rootkit
- Trusted Developer Utilities Proxy Execution (1/1)
- Use Alternate Authentication Material (4/4)
- Hijack Execution Flow (11/11)
- Modify Authentication Process (4/4)
- Process Injection (11/11)
- Signed Script Proxy Execution (1/1)
- Valid Accounts (4/4)
- Direct Volume Access
- Domain Policy Modification (2/2)
- Rogue Domain Controller
- Template Injection
- Build Image on Host
- Deploy Container
- Execution Guardrails (1/1)
- Exploitation for Defense Evasion
- Modify Cloud Compute Infrastructure (4/4)
- Modify System Image (2/2)
- Network Boundary Bridging (1/1)
- Pre-OS Boot (5/5)
- Reflective Code Loading
- Traffic Signaling (1/1)
- Unused/Unsupported Cloud Regions
- Weaken Encryption (2/2)

Credential Access
15 techniques

- OS Credential Dumping (8/8)
- Credentials from Password Stores (5/5)
- Network Sniffing
- Unsecured Credentials (7/7)
- Brute Force (4/4)
- Input Capture (4/4)
- Steal or Forge Kerberos Tickets (4/4)
- Modify Authentication Process (4/4)
- Adversary-in-the-Middle (2/2)
- Forced Authentication
- Forge Web Credentials (2/2)
- Exploitation for Credential Access
- Steal Application Access Token
- Steal Web Session Cookie
- Two-Factor Authentication Interception

Discovery
29 techniques

- Remote System Discovery
- System Information Discovery
- Account Discovery (4/4)
- System Network Configuration Discovery (1/1)
- Browser Bookmark Discovery
- Domain Trust Discovery
- Network Share Discovery
- Password Policy Discovery
- Permission Groups Discovery (3/3)
- Software Discovery (1/1)
- File and Directory Discovery
- Network Service Scanning
- Network Sniffing
- System Network Connections Discovery
- Virtualization/Sandbox Evasion (3/3)
- System Owner/User Discovery
- System Time Discovery
- Process Discovery
- System Service Discovery
- Application Window Discovery
- Peripheral Device Discovery
- Query Registry
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Group Policy Discovery
- System Location Discovery (0/1)

Lateral Movement
9 techniques

- Remote Services (6/6)
- Use Alternate Authentication Material (4/4)
- Remote Service Session Hijacking (2/2)
- Replication Through Removable Media
- Software Deployment Tools
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Taint Shared Content

Collection
17 techniques

- Screen Capture
- Archive Collected Data (3/3)
- Automated Collection
- Clipboard Data
- Data Staged (2/2)
- Input Capture (4/4)
- Adversary-in-the-Middle (2/2)
- Audio Capture
- Email Collection (3/3)
- Browser Session Hijacking
- Data from Cloud Storage Object
- Data from Configuration Repository (2/2)
- Data from Information Repositories (2/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Video Capture

Command and Control
16 techniques

- Ingress Tool Transfer
- Remote Access Software
- Application Layer Protocol (4/4)
- Non-Application Layer Protocol
- Protocol Tunneling
- Proxy (4/4)
- Data Encoding (2/2)
- Non-Standard Port
- Encrypted Channel (2/2)
- Communication Through Removable Media
- Data Obfuscation (3/3)
- Dynamic Resolution (3/3)
- Fallback Channels
- Multi-Stage Channels
- Traffic Signaling (1/1)
- Web Service (3/3)

Exfiltration
9 techniques

- Exfiltration Over Alternative Protocol (3/3)
- Automated Exfiltration (1/1)
- Data Transfer Size Limits
- Exfiltration Over C2 Channel
- Exfiltration Over Web Service (2/2)
- Exfiltration Over Other Network Medium (1/1)
- Exfiltration Over Physical Medium (1/1)
- Scheduled Transfer
- Transfer Data to Cloud Account

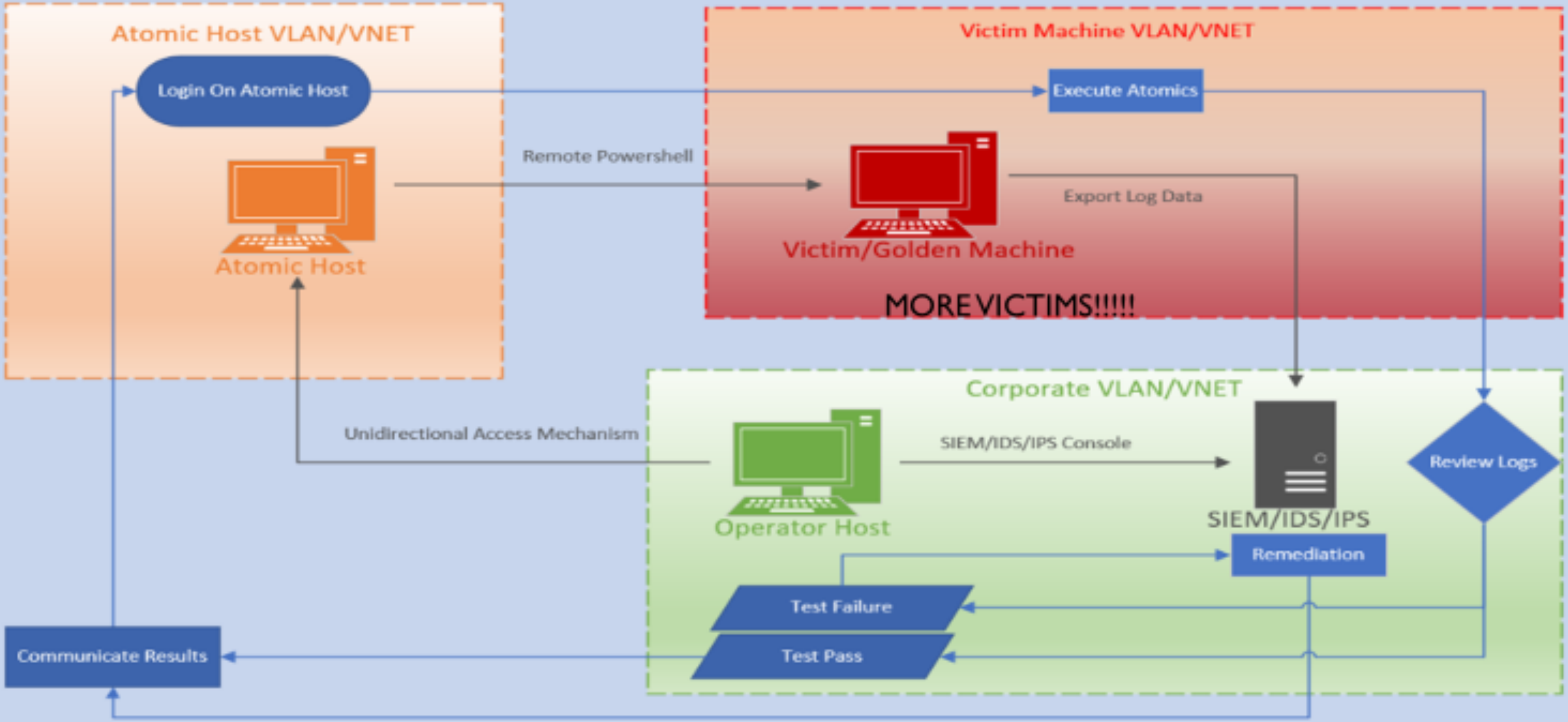
Impact
13 techniques

- System Shutdown/Reboot
- Inhibit System Recovery
- Data Encrypted for Impact
- Account Access Removal
- Data Destruction
- Service Stop
- Defacement (2/2)
- Resource Hijacking
- Data Manipulation (3/3)
- Disk Wipe (2/2)
- Endpoint Denial of Service (4/4)
- Firmware Corruption
- Network Denial of Service (2/2)

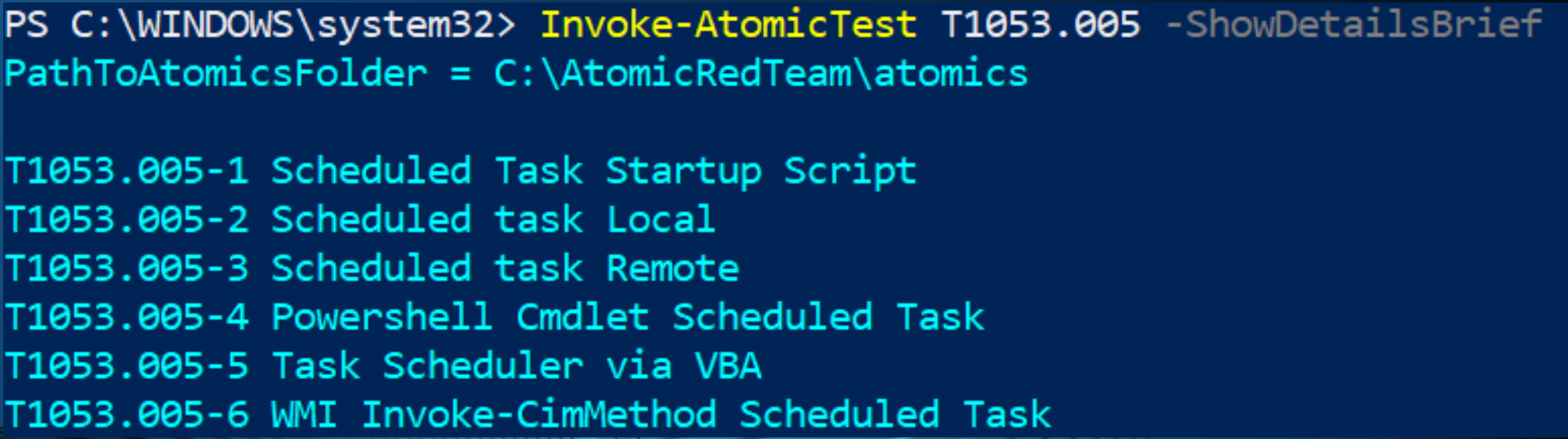
CSO50 | The Aaron's Company, Inc.

PRODUCED BY CSO

SAMPLE ARCHITECTURE



GOING NUCLEAR – ATOMIC RED TEAM

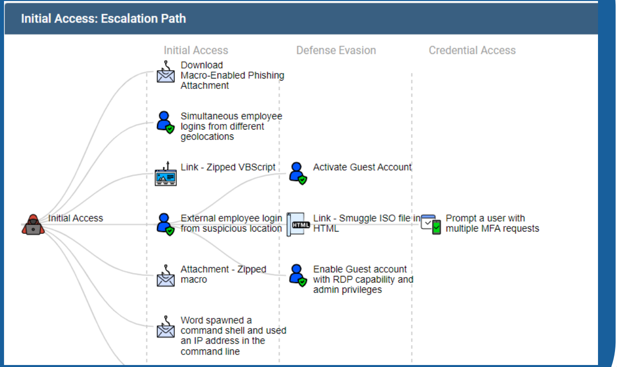


```
PS C:\WINDOWS\system32> Invoke-AtomicTest T1053.005 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

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
```

vectr

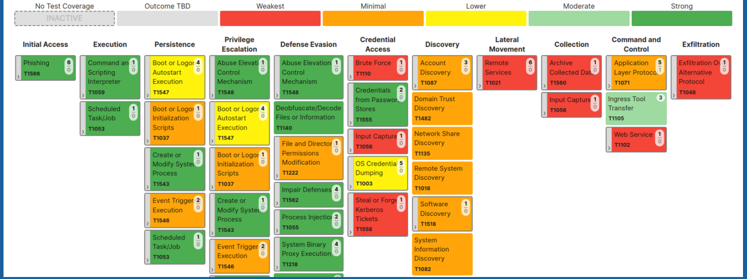
Visualize Attack Paths



Initial Access: Escalation Path

Initial Access
Defense Evasion
Credential Access
Initial Access
Download Macro-Enabled Phishing Attachment
Simultaneous employee logins from different geolocations
Link - Zipped VBScript
Activate Guest Account
External employee login from suspicious location
HTML
Link - Smuggle ISO file in HTML
Prompt a user with multiple MFA requests
Attachment - Zipped macro
Enable Guest account with RDP capability and admin privileges
Word spawned a command shell and used an IP address in the command line

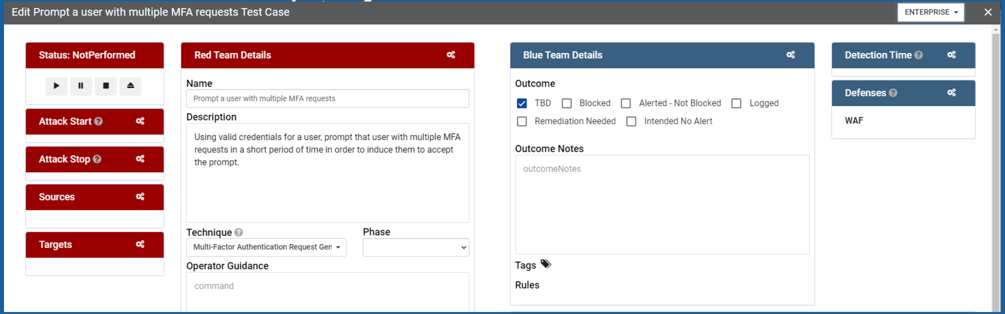
Heat Map Visualization of MITRE ATT&CK Relationship



No Test Coverage	Outcome TBD	Weakest	Minimal	Lower	Moderate	Strong
INACTIVE						

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Phishing T1566 6 0	Command an Scripting Interpreter T1059 1 0	Boot or Logon Autostart Execution T1547 4 0	Abuse Elevati Control Mechanism T1548 1 0	Abuse Elevation Control Mechanism T1548 1 0	Brute Force T1110 1 0	Account Discovery T1087 3 0	Remote Services T1021 6 0	Archive Collected Data T1560 1 0	Application Layer Protocol T1071 5 1	Exfiltration Ov Alternative Protocol T1048 1 0
	Scheduled Task/Job T1053 1 0	Boot or Logon Initialization Scripts T1037 1 0	Boot or Logon Autostart Execution T1547 4 0	Deobfuscate/Decode Files or Information T1140	Credentials from Passwor Stores T1555 2 0	Domain Trust Discovery T1482		Input Capture T1056 1 0	Ingress Tool Transfer T1105 3	
		Create or Modify Systen Process T1543 1 0	Boot or Logon Initialization Scripts T1037 1 0	File and Director Permissions Modification T1222 1 0	Input Capture T1056 1 0	Network Share Discovery T1135			Web Service T1102 1 0	
		Event Trigge Execution T1546 2 0	Create or Modify Systen Process T1543 1 0	Impair Defenses T1562 4 0	OS Credentia Dumping T1003 5 0	Remote System Discovery T1018				
		Scheduled Task/Job T1053 1 0	Event Trigger Execution T1546 2 0	Process Injection T1055 2 0	Steal or Forge Kerberos Tickets T1558 1 0	Software Discovery T1518 1 0				
				System Binary Proxy Execution T1218 4 0		System Information Discovery T1082				

Red Team/Blue Team



Edit Prompt a user with multiple MFA requests Test Case

Status: NotPerformed

Red Team Details

Name: Prompt a user with multiple MFA requests

Description: Using valid credentials for a user, prompt that user with multiple MFA requests in a short period of time in order to induce them to accept the prompt.

Technique: Multi-Factor Authentication Request Gen

Phase:

Operator Guidance: command

Blue Team Details

Outcome

☑ TBD ☐ Blocked ☐ Alerted - Not Blocked ☐ Logged

☐ Remediation Needed ☐ Intended No Alert

Outcome Notes: outcomeNotes

Tags

Rules

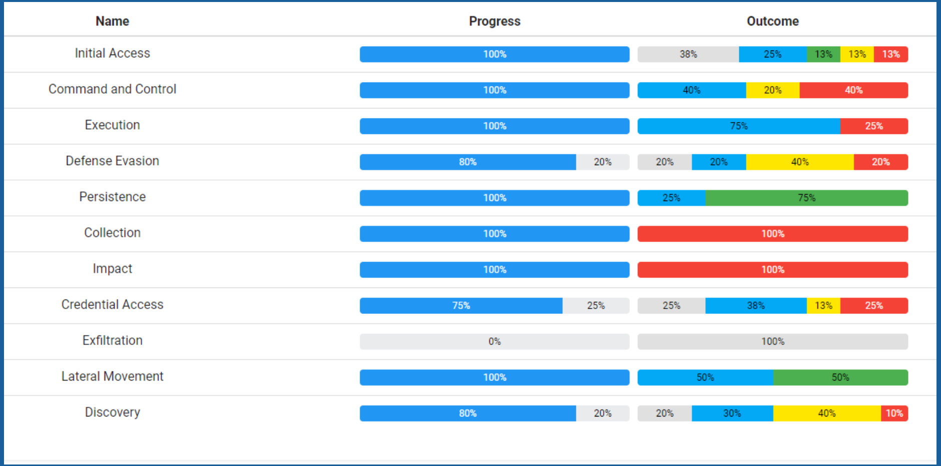
Defenses: WAF

CSO50

PRODUCED BY CSO

Example Metrics

Encompassing Test Coverage



Name	Progress	Outcome
Initial Access	🟦 100%	⬜ 38% 🟦 25% 🟩 13% 🟨 13% 🟥 13%
Command and Control	🟦 100%	🟦 40% 🟨 20% 🟥 40%
Execution	🟦 100%	🟦 75% 🟥 25%
Defense Evasion	🟦 80% ⬜ 20%	⬜ 20% 🟦 20% 🟨 40% 🟥 20%
Persistence	🟦 100%	🟦 25% 🟩 75%
Collection	🟦 100%	🟥 100%
Impact	🟦 100%	🟥 100%
Credential Access	🟦 75% ⬜ 25%	⬜ 25% 🟦 38% 🟨 13% 🟥 25%
Exfiltration	⬜ 0%	⬜ 100%
Lateral Movement	🟦 100%	🟦 50% 🟩 50%
Discovery	🟦 80% ⬜ 20%	⬜ 20% 🟦 30% 🟨 40% 🟥 10%

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