ARES | IT-SECURITY

Marcus Osterloh

Measuring Cyber Security with MITRE ATT&CK

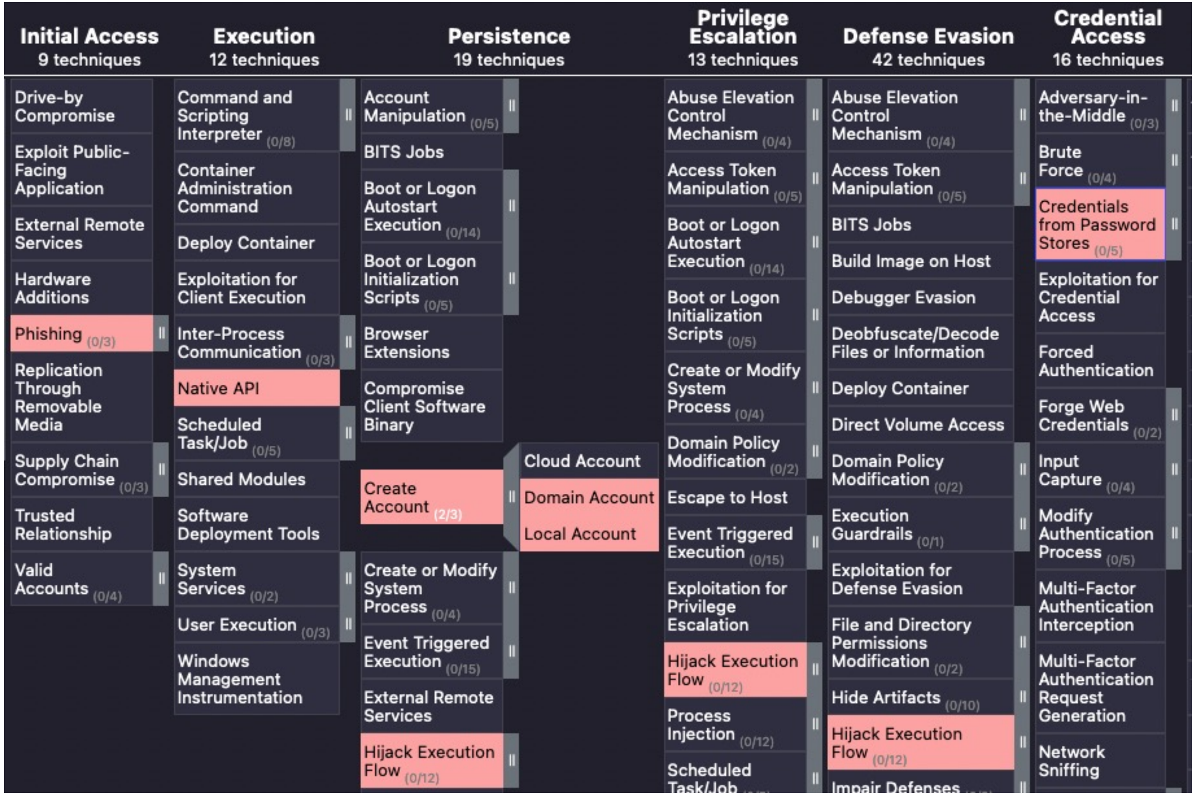
# whoami

- Marcus Osterloh – marcus.osterloh@ares-it-sec.de
- Head of Ares IT-Security
- Master IT-Sec @ RUB, Pentester, Security Engineer, etc.
- Background: Offense, Defense, Scientist
- Loves Bouldering

Why Measuring Cyber Security?

- Distributed **Responsibilities** and **changing** Environment
- Security teams are **not in control** of the environment
- **Making security assumption** about the environment
- **Overview** of the current security state and monitoring
- Build security on **confidence**

What is MITRE ATTA&CK?



Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
12 techniques

- Command and Scripting Interpreter (0/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (2/3)
  - Cloud Account
  - Domain Account
  - Local Account
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/12)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job

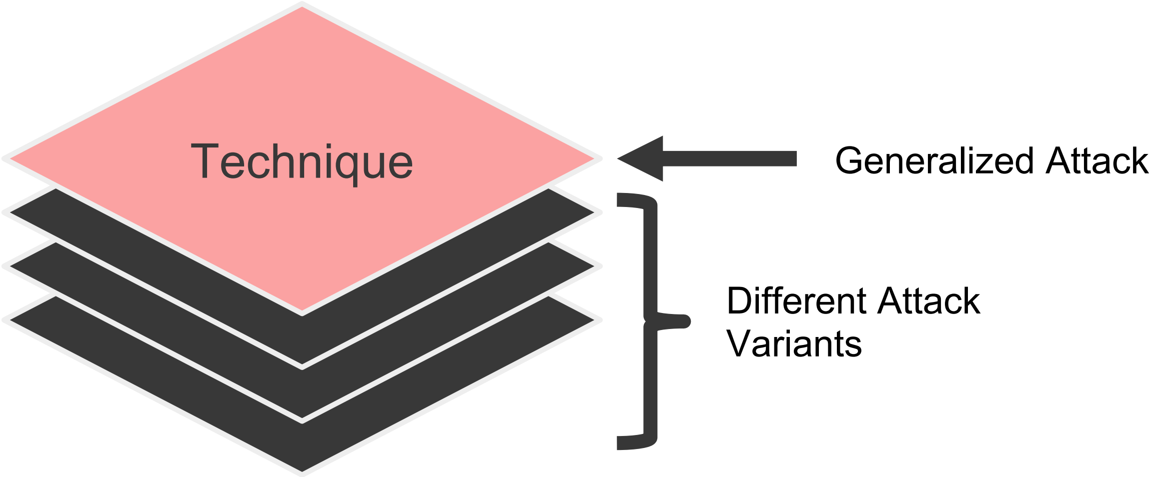
Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (0/12)
- Impair Defenses

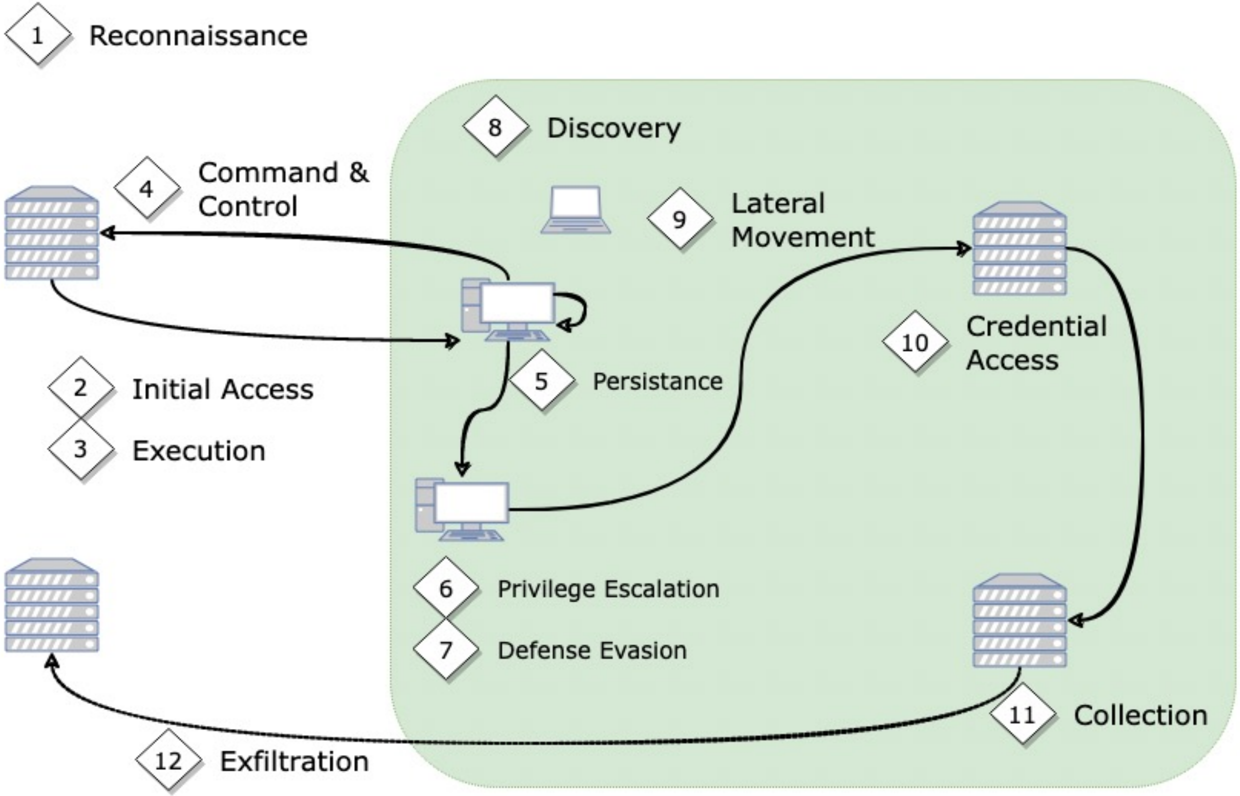
Credential Access
16 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing

Consider Different Attack Perspectives



Why Using MITRE ATT&CK?

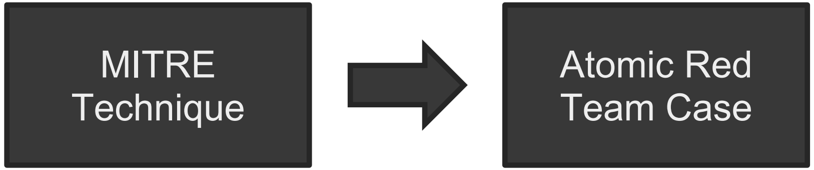


How to Measure?

- Red Teaming
- Penetration Testing
- Vulnerability Scanning
- Offensive/Defensive Tool XYZ
- Model Test Cases:
  Specific Security Condition must hold

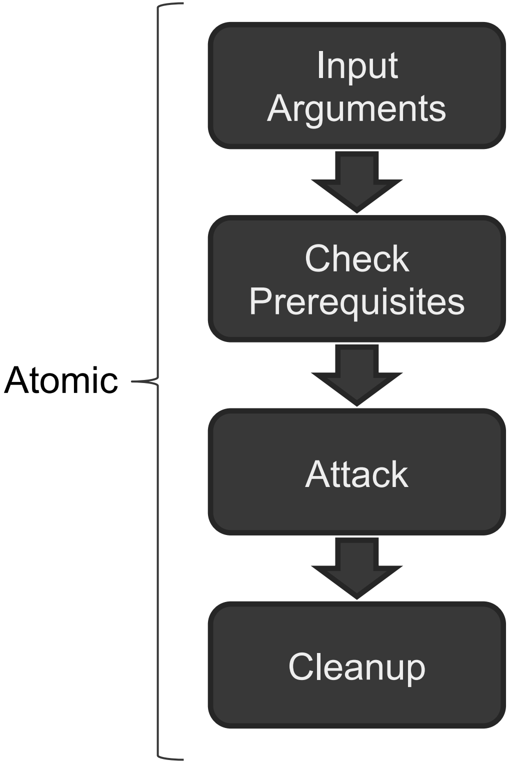
How to Measure?

- Red Teaming
- Penetration Testing
- Vulnerability Scanning
- Offensive/Defensive Tool XYZ
- Model Test Cases:
  Specific Security Condition must hold



MITRE Technique → Atomic Red Team Case

Model Your Attacks



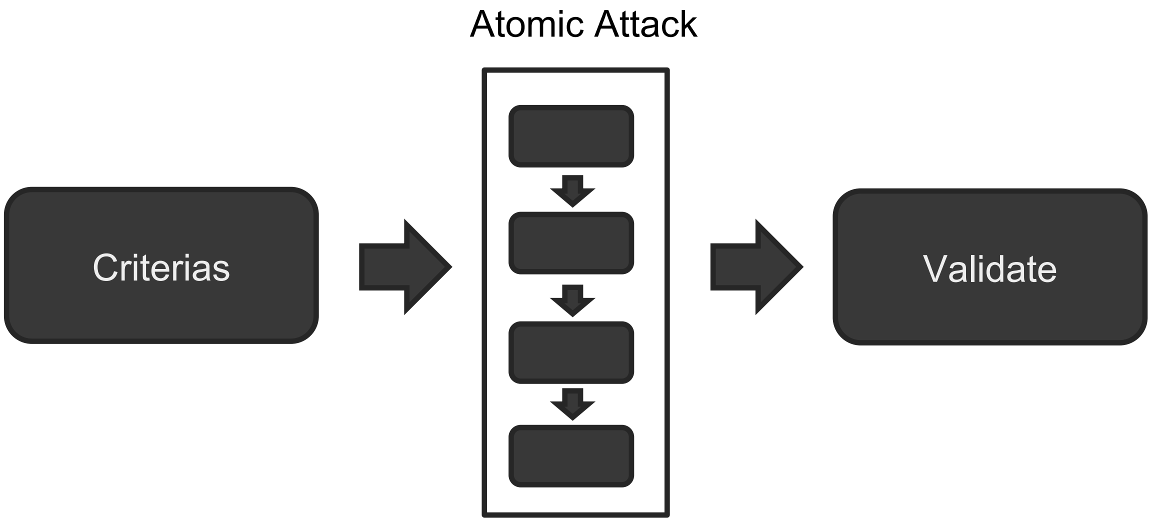
```
source_file = “C:\atomics\T1106\src\stage1.cs“
output_file = “'%tmp%\stage1.exe'“
```

```
dir C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
```

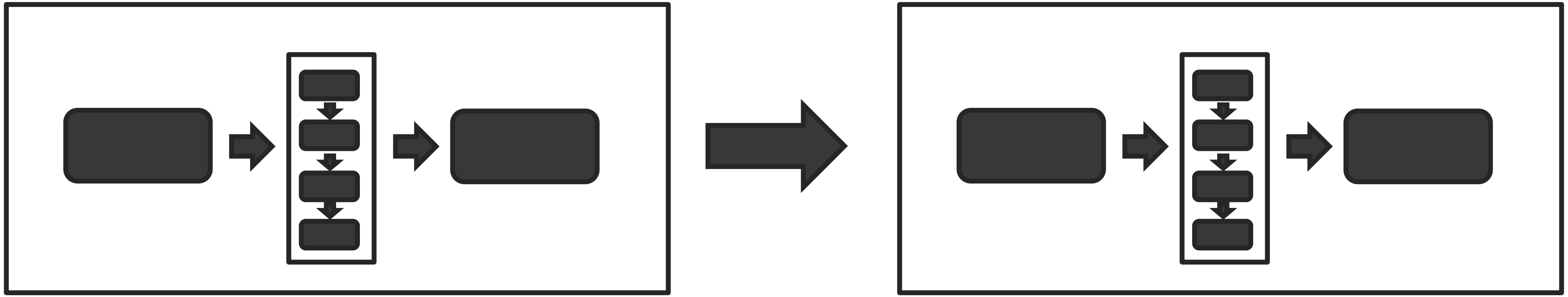
Exec: `C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /out:"#{output_file}" /target:exe #{source_file}`
Exec: `#{output_file}`

```
rm #{source_file}
rm #{output_file}
```

Model Your Attacks with Criterias



Think in Flows



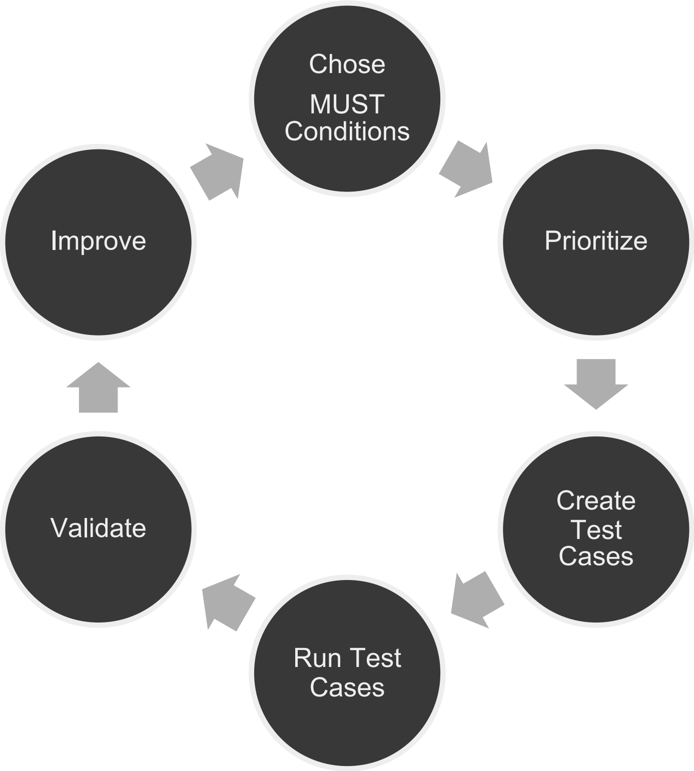
Attack 1

…

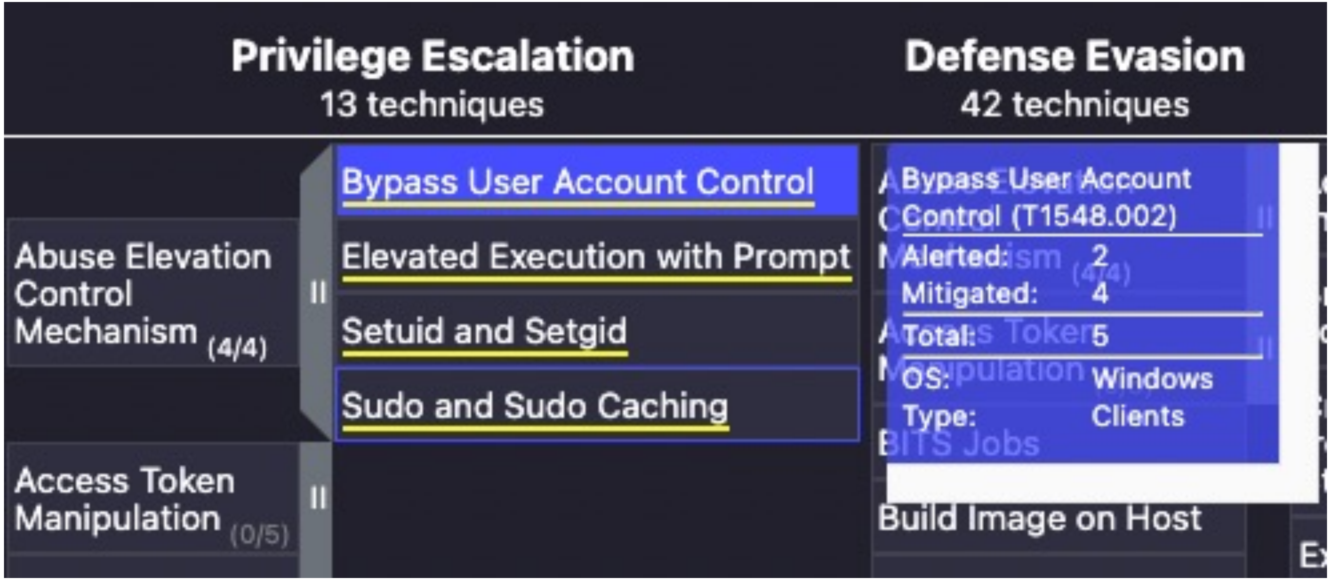
Attack N

Single attacks can be administrative bahaviour!

How to use ATT&CK?



MITRE Measurement



Privilege Escalation
13 techniques

Defense Evasion
42 techniques

Abuse Elevation Control Mechanism (4/4)

- Bypass User Account Control
- Elevated Execution with Prompt
- Setuid and Setgid
- Sudo and Sudo Caching

Access Token Manipulation (0/5)

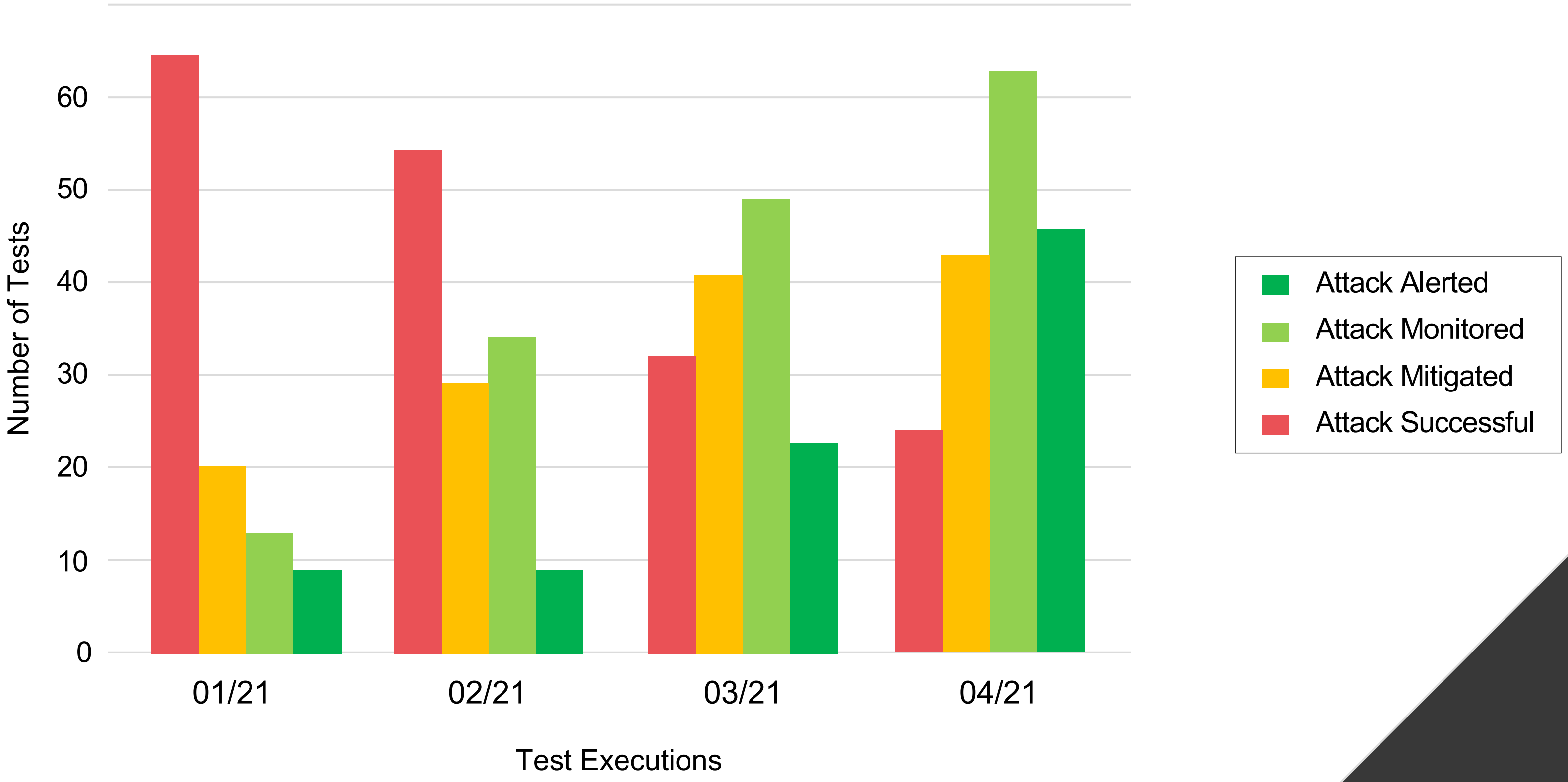
Bypass User Account Control (T1548.002)

Alerted:	2
Mitigated:	4
Total:	5
OS:	Windows
Type:	Clients

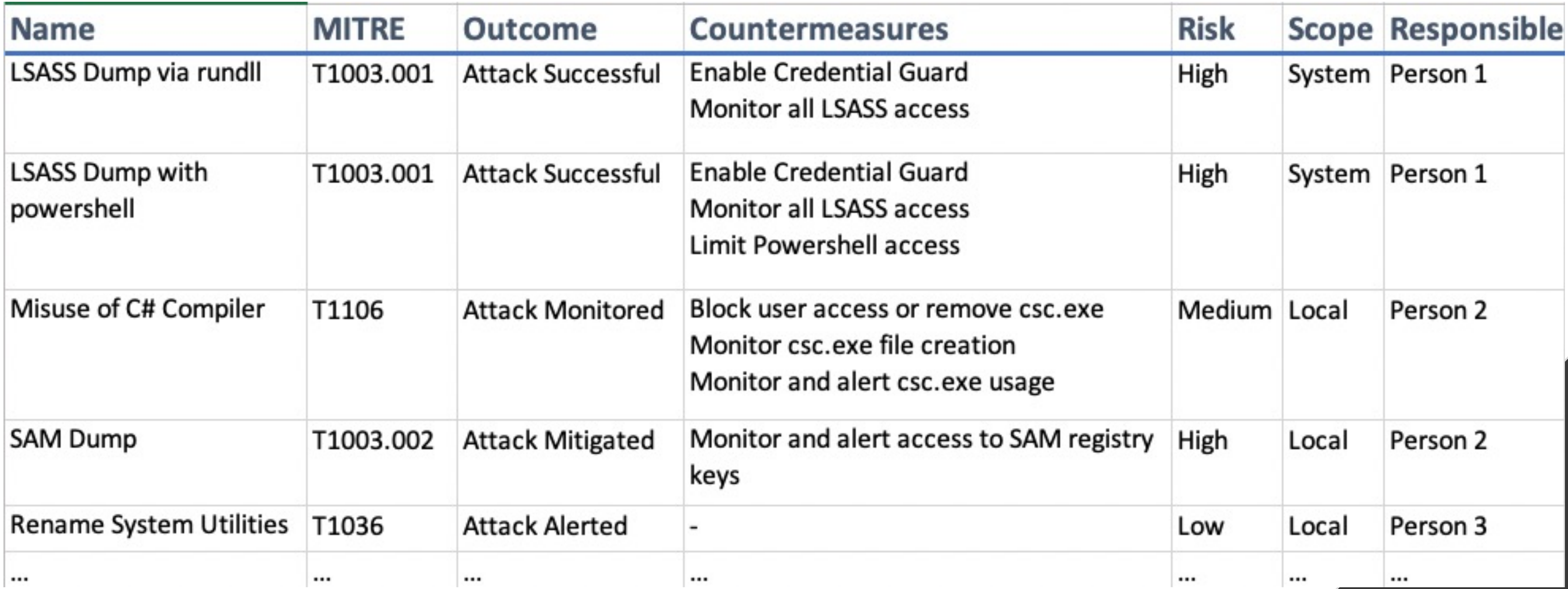
BITS Jobs

Build Image on Host

Measure and Overview



Track with Details and Actions



Name	MITRE	Outcome	Countermeasures	Risk	Scope	Responsible
LSASS Dump via rundll	T1003.001	Attack Successful	Enable Credential Guard Monitor all LSASS access	High	System	Person 1
LSASS Dump with powershell	T1003.001	Attack Successful	Enable Credential Guard Monitor all LSASS access Limit Powershell access	High	System	Person 1
Misuse of C# Compiler	T1106	Attack Monitored	Block user access or remove csc.exe Monitor csc.exe file creation Monitor and alert csc.exe usage	Medium	Local	Person 2
SAM Dump	T1003.002	Attack Mitigated	Monitor and alert access to SAM registry keys	High	Local	Person 2
Rename System Utilities	T1036	Attack Alerted	-	Low	Local	Person 3
...	...	...	...	...	...	...

Advantages of the Strategy

- Provides a reproducable methodology for security measure test
- Recognize changes in the infrastructure
- Identifies security and monitoring gaps
- Flows avoid isolated „attacks“
- Your security becomes verifiable

Questions

?