How does Endpoint Detection use the MITRE ATT&CK Framework?

Apurva Virkud, Muhammad Adil Inam, Andy Riddle, Jason Liu,
Gang Wang, Adam Bates
University of Illinois Urbana-Champaign






Finding metrics to evaluate security systems has been historically challenging.

MITRE ATT&CK Coverage

Check Point offers the widest coverage of the MITRE ATT&CK matrix

65% more MITRE ATT&CK coverage than average out-of-the-box SIEMs

Stellar Cyber Launches MITRE ATT&CK Coverage Analyzer for Partners and Customers

CrowdStrike Achieves 99% Detection Coverage in First-Ever MITRE ATT&CK Evaluations for Security Service Providers

SentinelOne leads in the latest MITRE ATT&CK Evaluation with 100% prevention

MITRE ATT&CK Coverage: Vectra AI provides over 90%

Carbon Black Delivers MITRE ATT&CK™ Coverage with Zero Delayed Detections & Zero Tainted Detections

SafeBreach Enhances ATT&CK Coverage with Industry Scenarios Focused on Top-16 MITRE TTPs

Rapid7 Delivers Complete Kill Chain Coverage

MITRE ATT&CK Coverage

Check Point offers the widest coverage of the MITRE ATT&CK matrix

65% more MITRE ATT&CK coverage than average out-of-the-box SIEMs

Stellar Cyber Launches MITRE ATT&CK Coverage Analyzer for Partners and Customers

CrowdStrike Achieves 99% Detection Coverage in First-Ever MITRE ATT&CK Evaluations for Security Service Providers

SentinelOne leads in the latest MITRE ATT&CK Evaluation with 100% prevention

MITRE ATT&CK Coverage: Vectra AI provides over 90%

Carbon Black Delivers MITRE ATT&CK™ Coverage with Zero Delayed Detections & Zero Tainted Detections

SafeBreach Enhances ATT&CK Coverage with Industry Scenarios Focused on Top-16 MITRE TTPs

Rapid7 Delivers Complete Kill Chain Coverage

MITRE ATT&CK Coverage

There is a risk for misinterpretation with the ATT&CK coverage metric.

CrowdStrike Achieves 99% Detection Coverage in First-Ever MITRE ATT&CK Evaluations for Security Service Providers

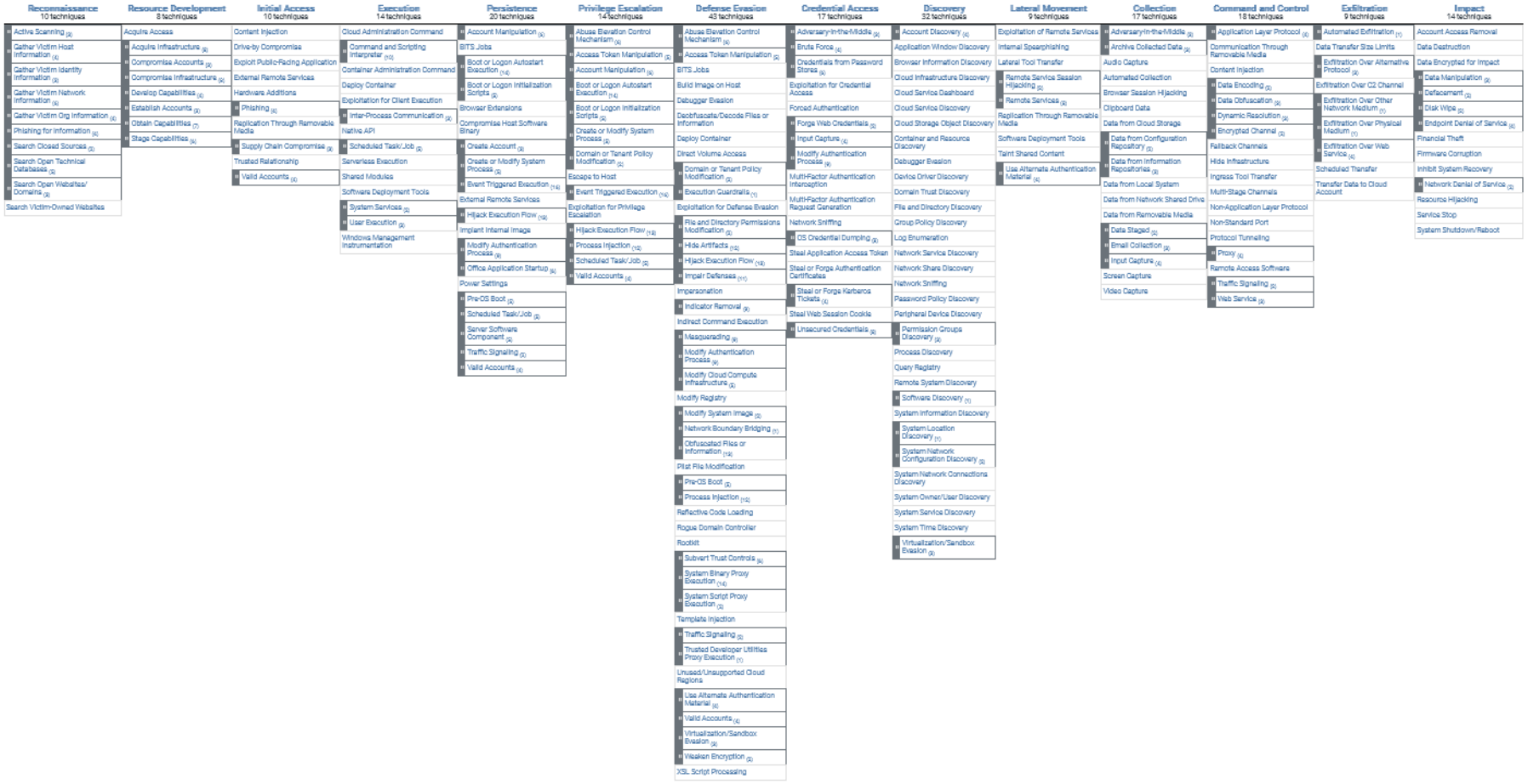
"99% Coverage = 99% Secure"

Should customers rely on ATT&CK coverage to choose a security system for their enterprise?

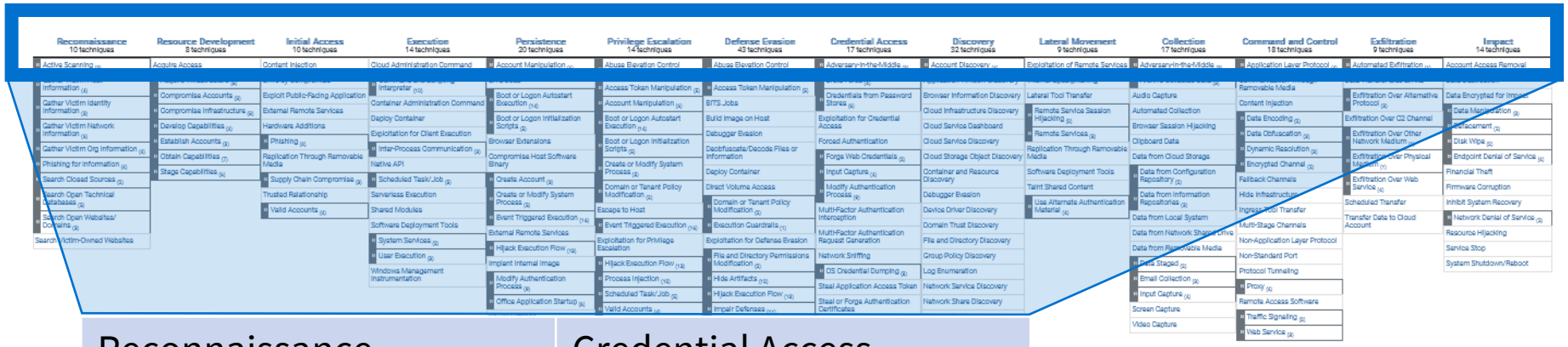
MITRE ATT&CK Coverage

Is ATT&CK coverage a suitable metric to evaluate endpoint detection systems?

MITRE ATT&CK


Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (4)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/ Domains (3)
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (8)
Develop Capabilities (4)
Establish Accounts (3)
Obtain Capabilities (7)
Stage Capabilities (6)
Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (10)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (3)
Native API
Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (3)
Windows Management Instrumentation
Persistence
20 techniques
Account Manipulation (5)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Host Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (16)
External Remote Services
Hijack Execution Flow (12)
Implant Internal Image
Modify Authentication Process (9)
Office Application Startup (6)
Power Settings
Pre-OS Boot (3)
Scheduled Task/Job (5)
Server Software Component (5)
Traffic Signaling (2)
Valid Accounts (4)
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
Account Manipulation (5)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain or Tenant Policy Modification (2)
Escape to Host
Event Triggered Execution (16)
Exploitation for Privilege Escalation
Hijack Execution Flow (12)
Process Injection (12)
Scheduled Task/Job (5)
Valid Accounts (4)
Defense Evasion
43 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (10)
Hijack Execution Flow (12)
Impair Defenses (11)
Impersonation
Indicator Removal (9)
Indirect Command Execution
Masquerading (8)
Modify Authentication Process (9)
Modify Cloud Compute Infrastructure (5)
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Obfuscated Files or Information (12)
Plist File Modification
Pre-OS Boot (3)
Process Injection (12)
Reflective Code Loading
Rogue Domain Controller
Rootkit
Subvert Trust Controls (6)
System Binary Proxy Execution (14)
System Script Proxy Execution (5)
Template Injection
Traffic Signaling (2)
Trusted Developer Utilities Proxy Execution (1)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (4)
Valid Accounts (4)
Virtualization/Sandbox Evasion (3)
Weaken Encryption (2)
XSL Script Processing
Credential Access
17 techniques
Adversary-in-the-Middle (3)
Brute Force (4)
Credentials from Password Stores (6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (9)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Unsecured Credentials (8)
Discovery
32 techniques
Account Discovery (4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Location Discovery (1)
System Network Configuration Discovery (2)
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Adversary-in-the-Middle (3)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (2)
Data from Information Repositories (3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Screen Capture
Video Capture
Command and Control
18 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Content Injection
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (2)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (4)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
14 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

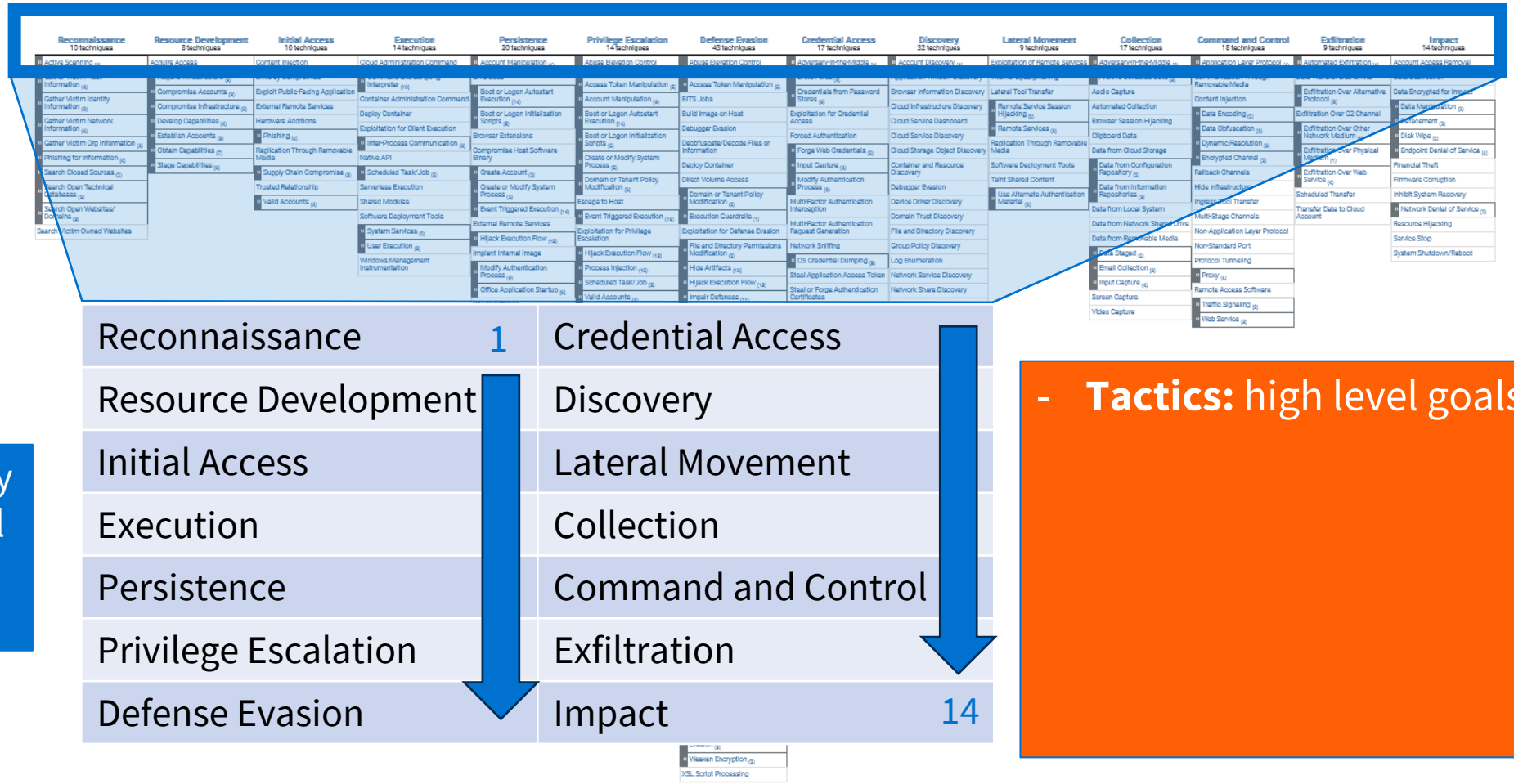
MITRE ATT&CK



Reconnaissance	Credential Access
Resource Development	Discovery
Initial Access	Lateral Movement
Execution	Collection
Persistence	Command and Control
Privilege Escalation	Exfiltration
Defense Evasion	Impact

- **Tactics:** high level goals

MITRE ATT&CK

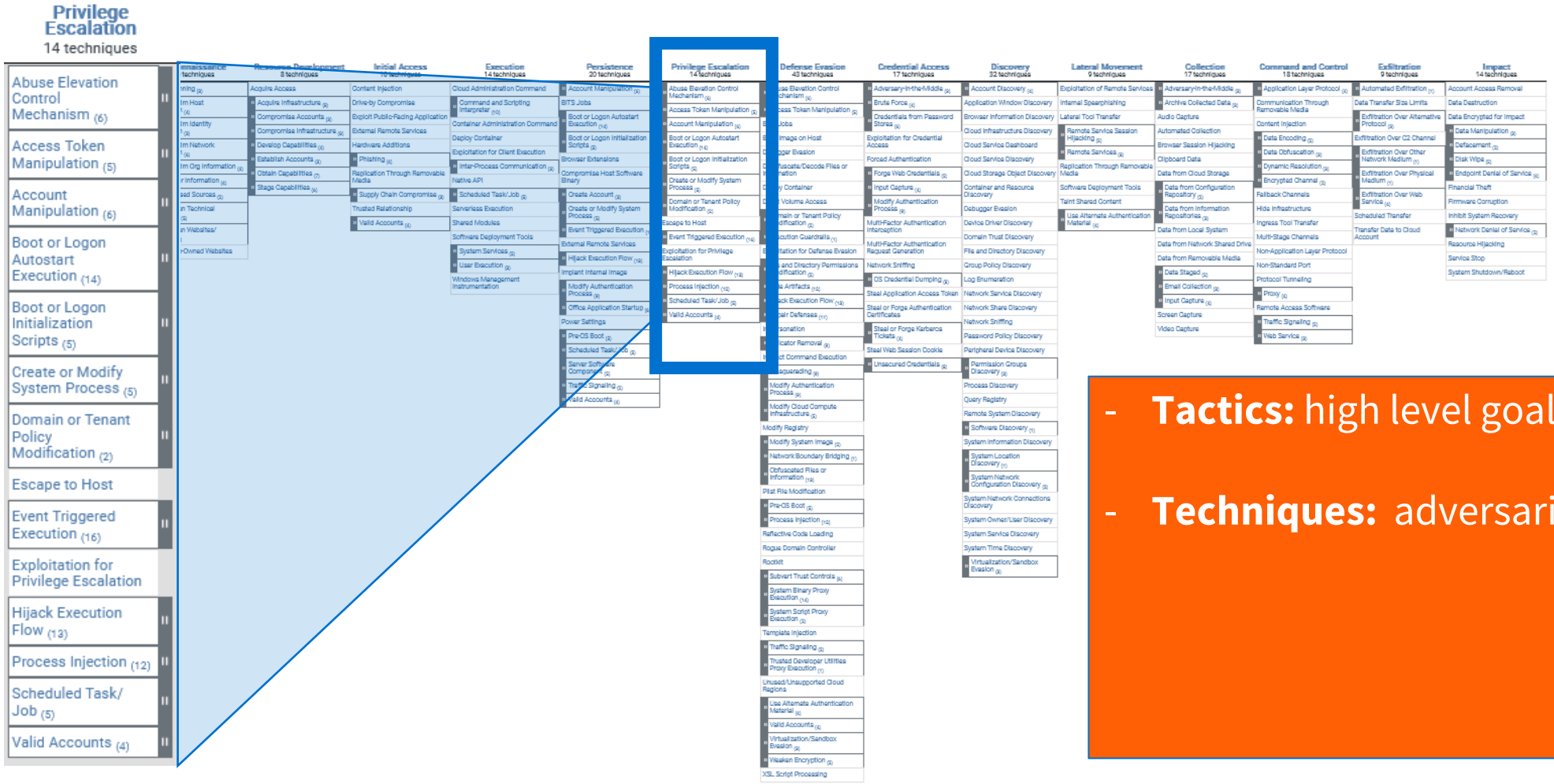


Reconnaissance	1	Credential Access	
Resource Development		Discovery	
Initial Access		Lateral Movement	
Execution		Collection	
Persistence		Command and Control	
Privilege Escalation		Exfiltration	
Defense Evasion		Impact	14

Approximately chronological order during an attack

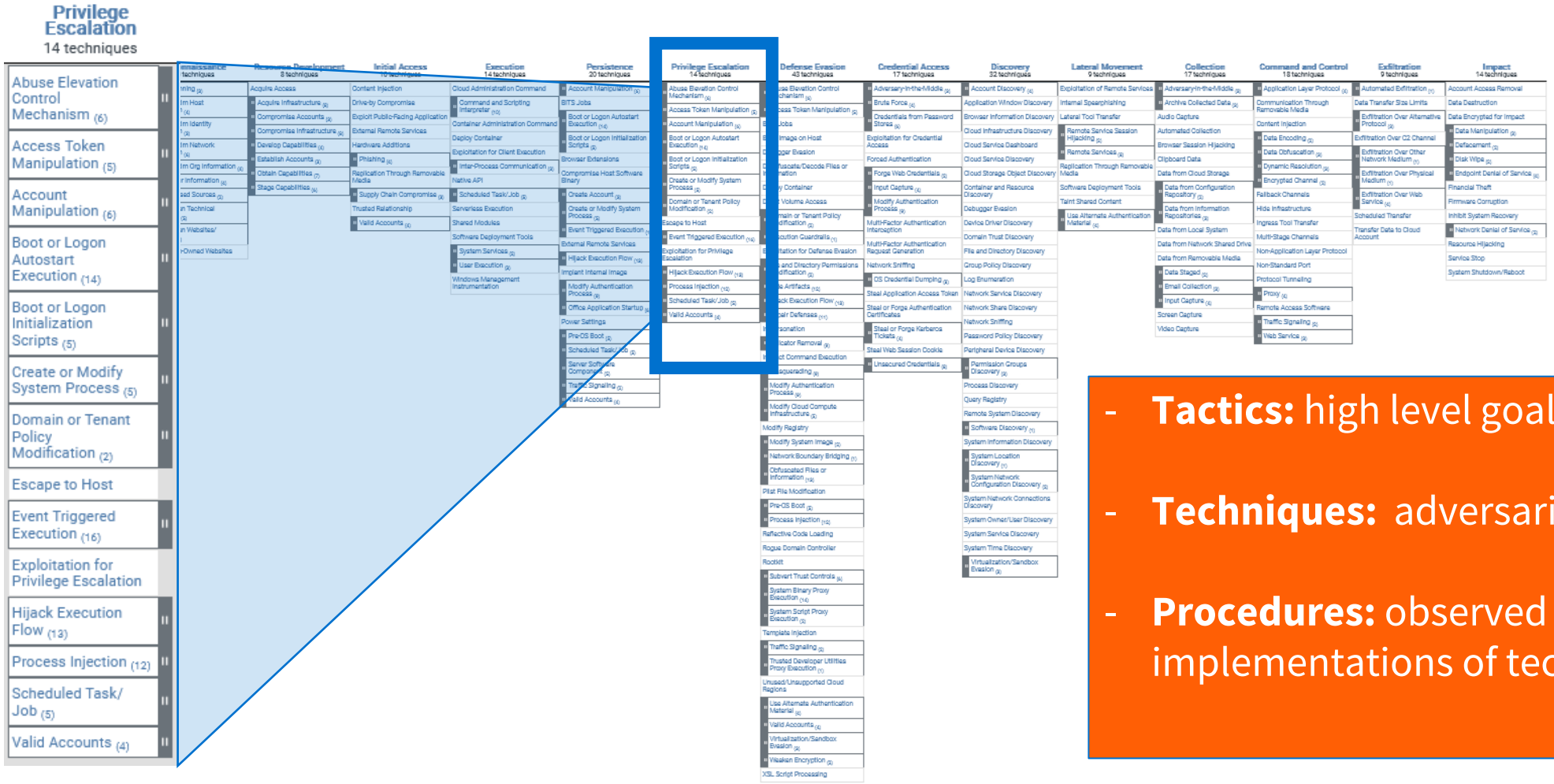
- **Tactics:** high level goals

MITRE ATT&CK



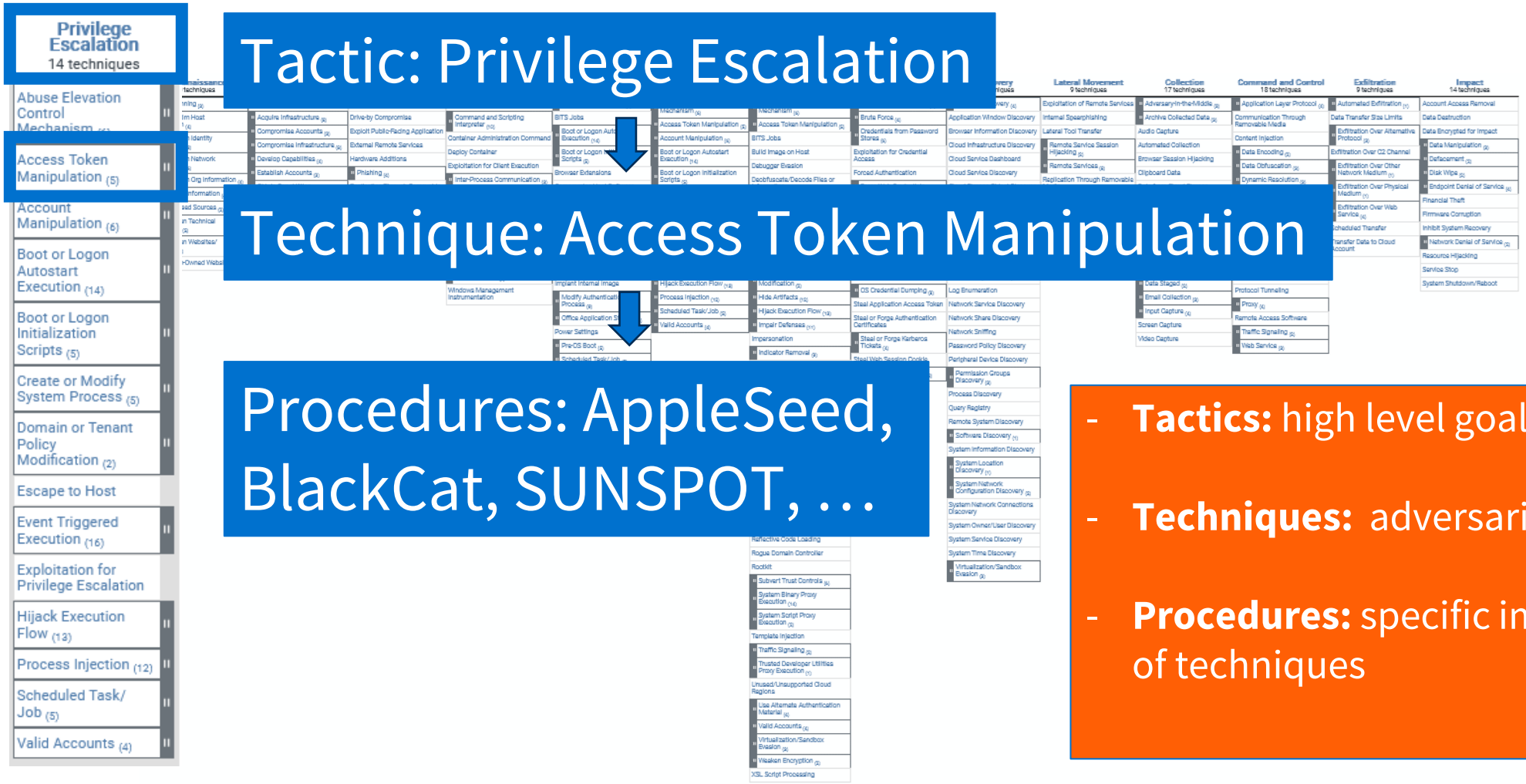
- **Tactics:** high level goals
- **Techniques:** adversarial actions

MITRE ATT&CK



- **Tactics:** high level goals
- **Techniques:** adversarial actions
- **Procedures:** observed implementations of techniques

MITRE ATT&CK



- **Tactics:** high level goals
- **Techniques:** adversarial actions
- **Procedures:** specific implementation of techniques

Endpoint Detection

Carbon Black

```
process_name:wevtutil.exe
and process_cmdline:cl*
and -process_cmdline:clicktorun*
and -process_cmdline:AnyConnect\.evtx*
```

T1070 (Indicator Removal)
Defense Evasion

Splunk

```
(Processes.process_name="RDPWInst.exe"
  OR Processes.original_file_name= "RDPWInst.exe")
AND Processes.process IN ("* -i*", "* -s*",
    "* -o*", "* -w*", "* -r*")
```

T1021 (Remote Services)
Defense Evasion

Elastic

```
event.category : (network or network_traffic)
and network.transport:tcp
and (destination.port: 26
     or (event.dataset:zeek.smtp
         and destination.port: 26))
```

T1048 (Exfilt. Over Alt. Prtcl)
Command & Control,
Exfiltration

Endpoint Detection

Carbon Black

```
process_name:wevtutil.exe
and process_cmdline:cl*
and -process_cmdline:clicktorun*
and -process_cmdline:AnyConnect\.evtx*
```

T1070 (Indicator Removal)
Defense Evasion

Splunk

```
(Processes.process_name="RDPWInst.exe"
  OR Processes.original_file_name= "RDPWInst.exe")
AND Processes.process IN ("* -i*", "* -s*",
    "* -o*", "* -w*", "* -r*")
```

T1021 (Remote Services)
Defense Evasion

Elastic

```
event.category : (network or network_traffic)
and network.transport:tcp
and (destination.port: 26
     or (event.dataset:zeek.smtp
         and destination.port: 26))
```

T1048 (Exfilt. Over Alt. Prtcl)
Command & Control,
Exfiltration

Rules

Vendor tagged techniques and tactics

Endpoint Detection

Carbon Black

```
process_name:wevtutil.exe
and process_cmdline:cl*
and -process_cmdline:clicktorun*
and -process_cmdline:AnyConnect\.evtx*
```

T1070 (Indicator Removal)
Defense Evasion

Splunk

```
(Processes.process_name="RDPWInst.exe"
  OR Processes.original_file_name= "RDPWInst.exe")
AND Processes.process IN ("* -i*", "* -s*",
    "* -o*", "* -w*", "* -r*")
```

T1021 (Remote Services)
Defense Evasion

Elastic

```
event.category : (network or network_traffic)
and network.transport:tcp
and (destination.port: 26
     or (event.dataset:zeek.smtp
         and destination.port: 26))
```

T1048 (Exfilt. Over Alt. Prtcl)
Command & Control,
Exfiltration

Rules

Vendor tagged techniques and tactics

Endpoint Detection

Carbon Black

```
process_name:wevtutil.exe
and process_cmdline:cl*
and -process_cmdline:clicktorun*
and -process_cmdline:AnyConnect\.evtx*
```

T1070 (Indicator Removal)
Defense Evasion

Splunk

```
(Processes.process_name="RDPWInst.exe"
  OR Processes.original_file_name= "RDPWInst.exe")
AND Processes.process IN ("* -i*", "* -s*",
    "* -o*", "* -w*", "* -r*")
```

T1021 (Remote Services)
Defense Evasion

Elastic

```
event.category : (network or network_traffic)
and network.transport:tcp
and (destination.port: 26
     or (event.dataset:zeek.smtp
         and destination.port: 26))
```

T1048 (Exfilt. Over Alt. Prtcl)
Command & Control,
Exfiltration

Rules → Exist on the Procedural level of ATT&CK!

Vendor tagged techniques and tactics

Endpoint Detection

Carbon Black

```
process_name:wevtutil.exe
and process_cmdline:cl*
and -process_cmdline:clicktorun*
and -process_cmdline:AnyConnect\.evtx*
```

Splunk

```
(Processes.process_name="RDPWInst.exe"
  OR Processes.original_file_name= "RDPWInst.exe")
AND Processes.process IN ("* -i*", "* -s*",
    "* -o*", "* -w*", "* -r*")
```

Elastic

```
event.category : (network or network_traffic)
and network.transport:tcp
and (destination.port: 26
     or (event.dataset:zeek.smtp
         and destination.port: 26))
```

90% coverage of ATT&CK

==

At least 1 detection rule for 90% of ATT&CK techniques

Rules → Exist on the Procedural level of ATT&CK!

Vendor tagged techniques and tactics

Endpoint Detection

```
process_name:wevtutil.exe
and process_cmdline:cl*
```

```
    or (event.dataset:zeek.smtp
        and destination.port: 26))
```

Technique coverage doesn't tell us about how many procedural level threats we can detect!

90% coverage of ATT&CK

==

At least 1 detection rule for 90% of ATT&CK techniques

Rules → Exist on the Procedural level of ATT&CK!

Vendor tagged techniques and tactics

How is MITRE ATT&CK integrated with real-world endpoint detection products?

Dataset

	Carbon Black	Splunk	Elastic	Sigma
Type of Ruleset	commercial, proprietary	commercial, open-source	commercial, open-source	crowdsourced
# ATT&CK Tagged Rules	867	911	473	2195
Metadata Field				
Name of Attack	✓	✓	✓	✓
Description	✓	✓	✓	✓
ATT&CK Technique(s)	✓	✓	✓	✓
Confidence	✓	✓		
Risk Score		✓	✓	
Severity Score	✓		✓	

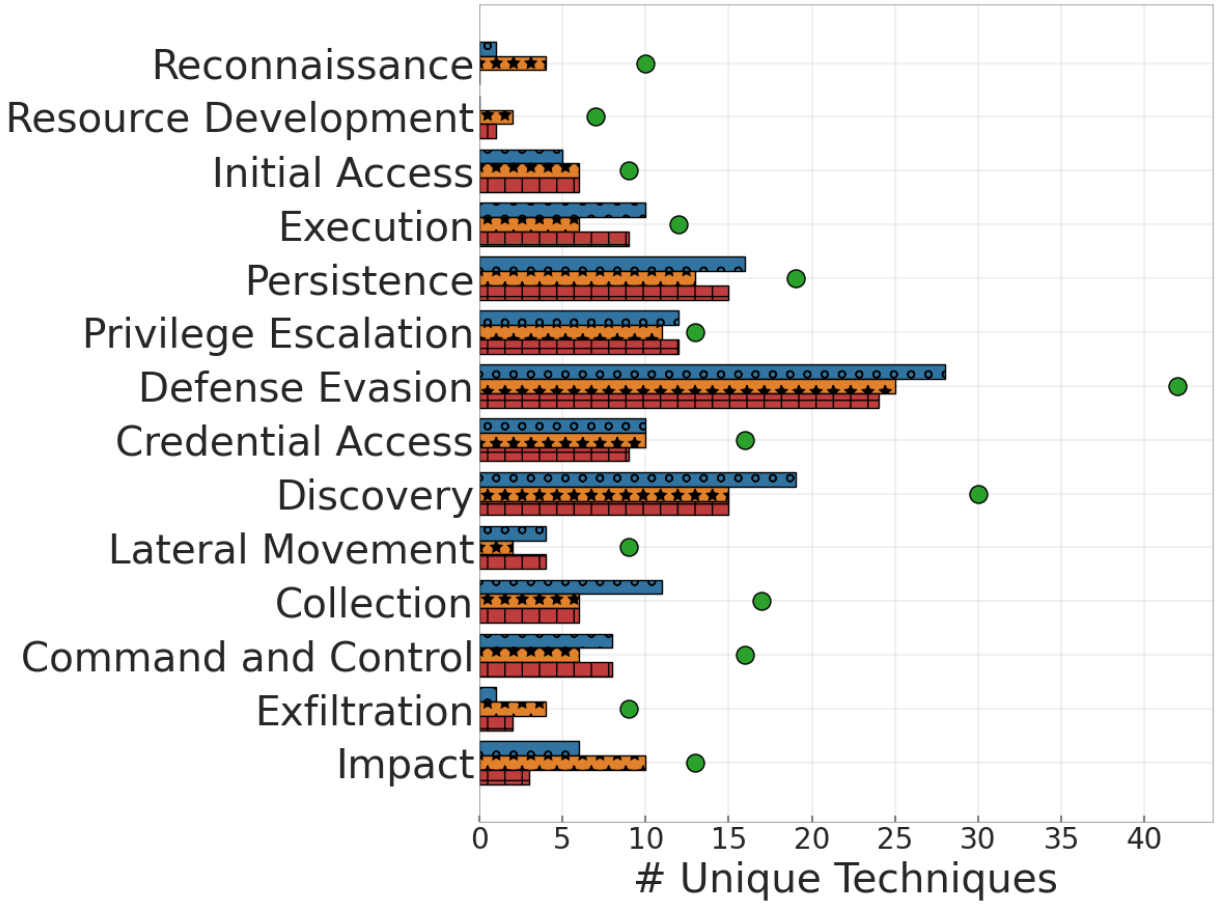
Research Questions

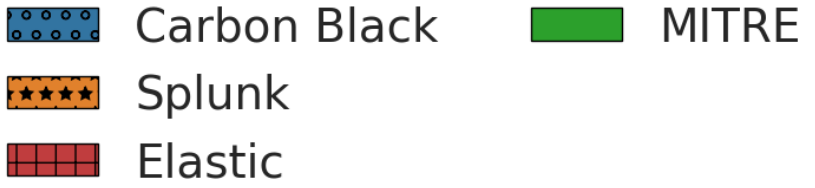
1. **How do products use ATT&CK?**

2. Why don’t products detect all of ATT&CK?

3. How consistently do products apply ATT&CK?

Technique Coverage under each Tactic

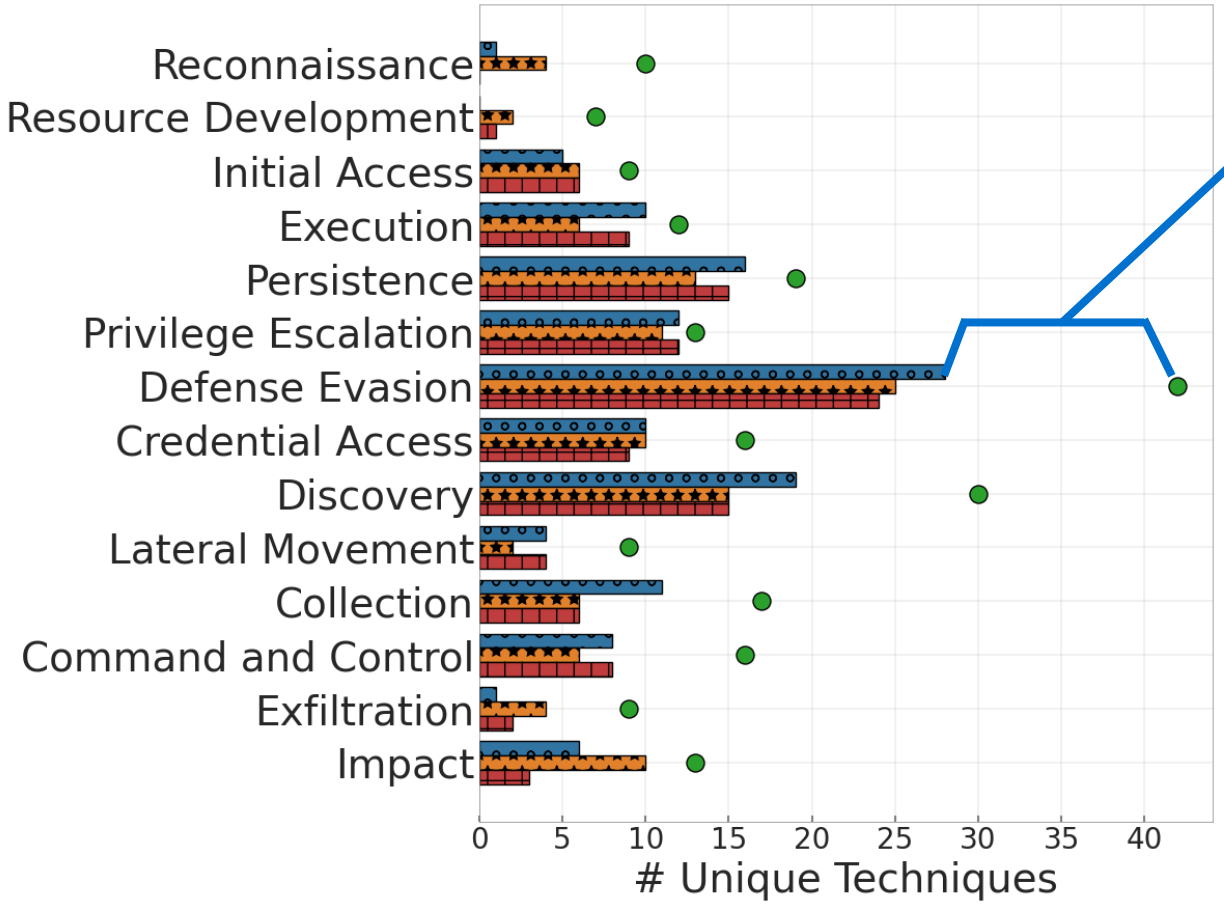




Findings:

- Products prioritize the same tactics and techniques.
- Coverage across all products combined is far from 100%.

Technique Coverage under each Tactic



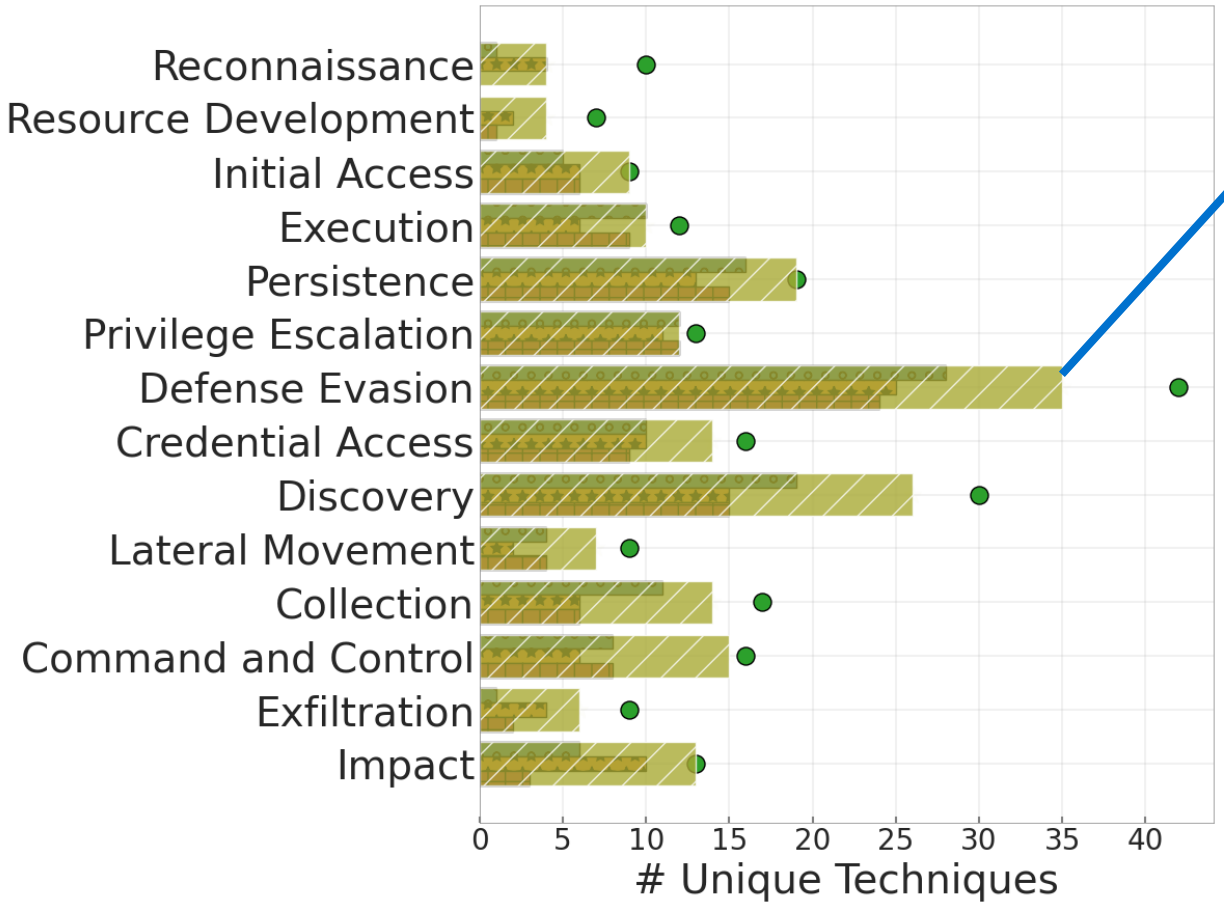
Number of techniques under a tactic not covered by each product

Carbon Black
Splunk
Elastic
MITRE

Findings:

- Products prioritize the same tactics and techniques.
- Coverage across all products combined is far from 100%.

Technique Coverage under each Tactic



Number of techniques under a tactic covered by all products combined

Carbon Black
Splunk
Elastic
MITRE
Union

Findings:

- Products prioritize the same tactics and techniques.
- Coverage across all products combined is far from 100%.

Impact of Risk/Severity/Confidence on Coverage

Metric	Filter	Carbon Black	Splunk	Elastic
Baseline	No Filter	55%	52%	48%
Risk	>= Med.	/	43%	42%
	>= High	/	25%	26%
Severity	>= Med.	52%	/	42%
	>= High	46%	/	26%
Confidence	>= Med.	/	51%	/
	>= High	/	46%	/

Findings:

- When filtering out low and medium severity/risk rules, ATT&CK technique coverage is halved for both Splunk and Elastic.

Impact of Risk/Severity/Confidence on Coverage

Metric	Filter	Carbon Black	Splunk	Elastic
Baseline	No Filter	55%	52%	48%
Risk	>= Med.	/	43%	42%
	>= High	/	25%	26%
Severity	>= Med.	52%	/	42%
	>= High	46%	/	26%
Confidence	>= Med.	/	51%	/
	>= High	/	46%	/

Findings:

- When filtering out low and medium severity/risk rules, ATT&CK technique coverage is halved for both Splunk and Elastic.

Impact of Risk/Severity/Confidence on Coverage

Metric	Filter	Carbon Black	Splunk	Elastic
Baseline	No Filter	55%	52%	48%
Risk	>= Med.	/	43%	42%
	>= High	/	25%	26%
Severity	>= Med.	52%	/	42%
	>= High	46%	/	26%
Confidence	>= Med.	/	51%	/
	>= High	/	46%	/

Findings:

- When filtering out low and medium severity/risk rules, ATT&CK technique coverage is halved for both Splunk and Elastic.

Research Questions

1. How do products use ATT&CK?

2. **Why don’t products detect all of ATT&CK?**

3. How consistently do products apply ATT&CK?

Qualitative Analysis of Unimplemented Techniques

Three coders independently analyze **53 techniques that were not implemented in any of the three commercial products.**

Findings:

- Many techniques are difficult (if not impossible) to implement as effective detection rules.

Label	Techniques	Example
Ineffective Detection Method	21 (39.6%)	T1480
Targeting Non-Host Infrastructure	13 (24.5%)	T1584
Client-specific	9 (17.0%)	T1528
Vague Detection Method	9 (17.0%)	T1602
Targeting Third Parties	8 (15.1%)	T1591
Provenance-based Detection	4 (7.5%)	T1578
Involving Low-level Behavior	3 (5.7%)	T1200
Involving Removable Media	3 (5.7%)	T1025
Involving Human Factors	1 (1.9%)	T1598
Reason Unknown	2 (3.8%)	T1217
Total Unique Techniques	53	

Top Reasons for Unimplemented Techniques

Explanation	# Techniques	Example
Ineffective Detection Method	21 (39.6%)	T1480 (Execution Guardrails): MITRE ATT&CK explicitly mentions that this behavior is difficult to detect.
Targeting Non-Host Infrastructure	13 (24.5%)	T1584 (Compromise Infrastructure): Suggested active Internet scanning of remote infrastructure is not suitable for endpoint detection.
Client-specific	9 (17.0%)	T1528 (Steal Application Access Token): Detection requires knowledge of customer-specific services or parameters.

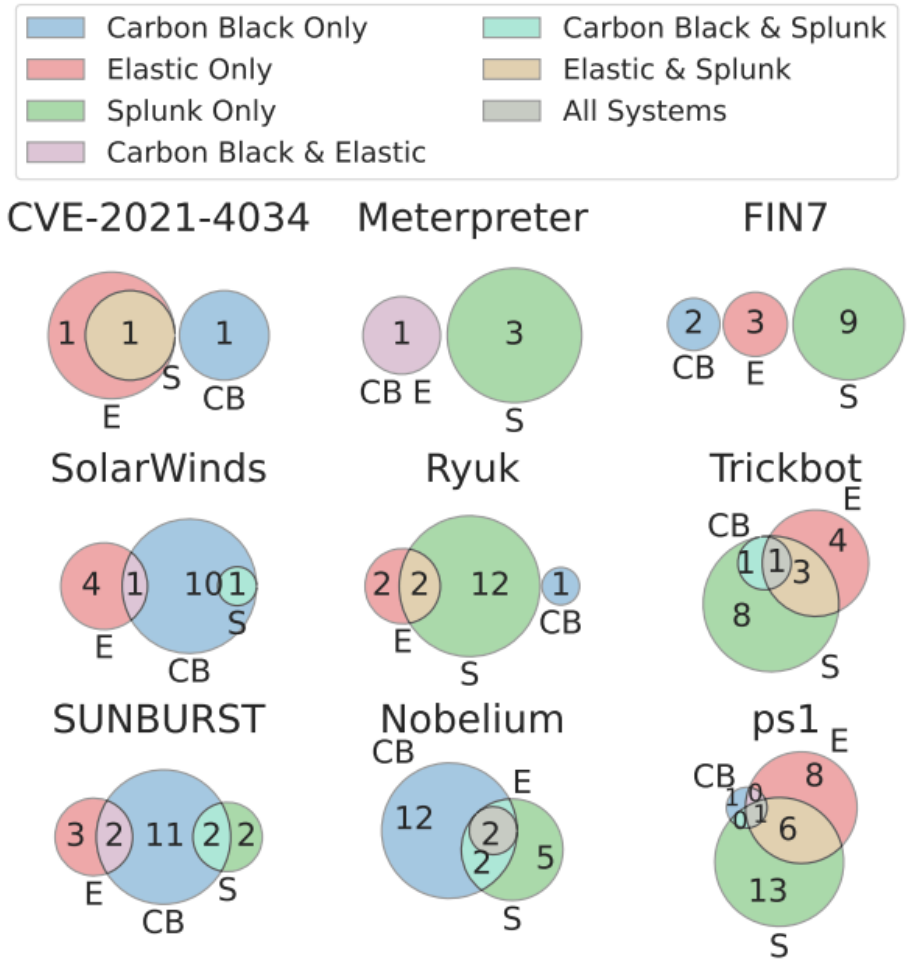
Research Questions

1. How do products use ATT&CK?

2. Why don’t products detect all of ATT&CK?

3. **How consistently do products apply ATT&CK?**

Technique Consistency for the Same Malicious Entities

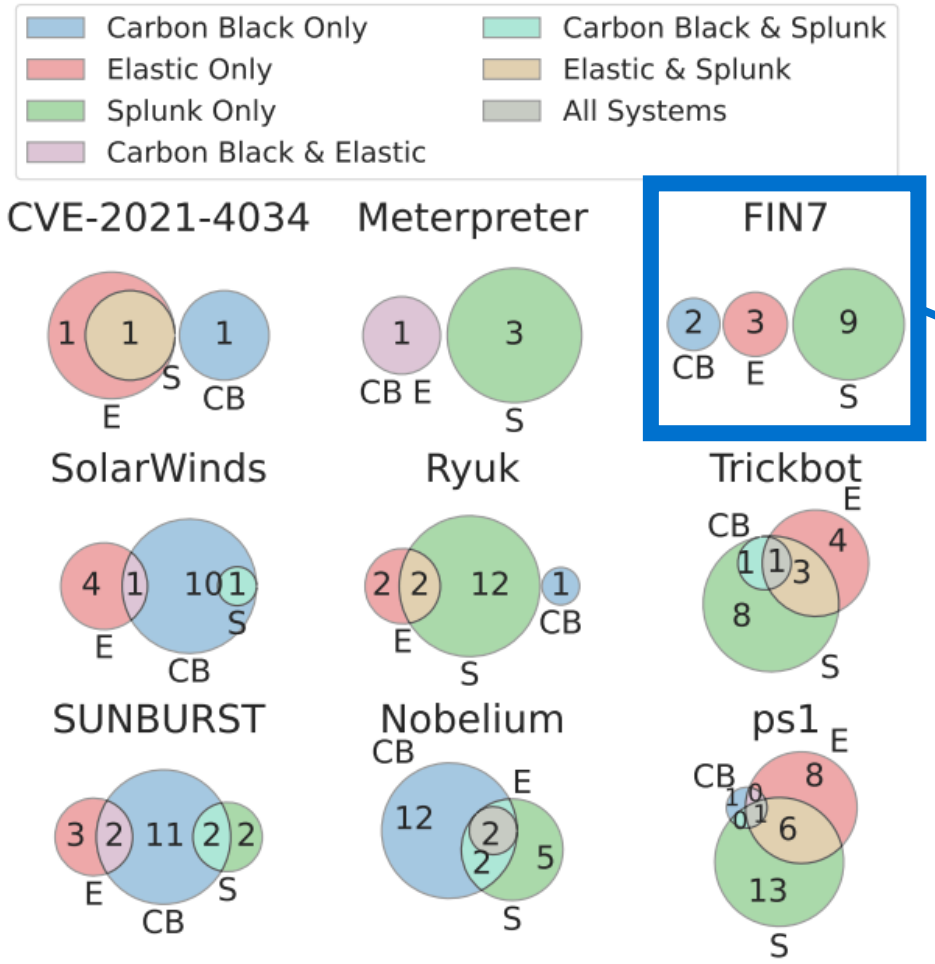


Identify rules are created to address a common malicious entity.

Findings:

- Even when products try to detect the same threat, they rarely use the same ATT&CK techniques to describe it!

Technique Consistency for the Same Malicious Entities



Identify rules are created to address a common malicious entity.

Discrete sets of techniques!

Findings:

- Even when products try to detect the same threat, they rarely use the same ATT&CK techniques to describe it!

Case Studies of Inconsistent Techniques

Named pipe impersonation– associated with **Meterpreter**

```
event.type == “start”
and process.pe.original_file_name in (“Cmd.exe”,
      “Powershell.EXE”)
and process.args : “echo”
and process.args : “>”
and process.args : “\\\\.\\pipe\\*”
```

Elastic: T1134 (Access Token Manipulation)

```
Processes.process_name= “cmd.exe”
OR Processes.original_file_name= Cmd.exe
OR Processes.process= *%comspec%*
(Processes.process=*echo* AND
Processes.process=*pipe*)
```

Splunk: T1059 (Command and Scripting Interpreter), T1543 (Create or Modify System Process)

cmd.exe /c echo 4 sgryt3436 > \\ .\ pipe \5 erg53

Both rules would fire!

Findings:

- Ambiguity and overlap between techniques at the procedural level leads to disagreement.

Disagreement in Tactics

Potentially malicious DNS activity with nslookup – associated with **FIN7** and **SUNBURST**

event.category:process
and **event.type**:start
and **process.name**:nslookup.exe
and **process.args**:
(-querytype= or* –qt=* *or* –q=* *or* type=*)

Elastic: Command and Control

Process.process_name = "nslookup.exe"
Process.process = "*-querytype=*" *OR*
Process.process = "*-qt=*" *OR*
Process.process = "*-q=*" *OR*
Process.process = "*-type=*" *OR*
Process.process = "*-retry=*"

Splunk: Exfiltration

Nslookup.exe –querytype=A usenix.org

Both rules would fire!

Findings:

- Security analysts may attribute the same system log activity to completely different motivations depending on which product they are using!

Takeaways

1. How do products use ATT&CK?

   Products prioritize similar tactics and techniques, but do not reach 100% technique coverage even if combined.

2. Why don’t products detect all of ATT&CK?

   A fraction of techniques are inherently difficult to detect!

3. How consistently do products apply ATT&CK?

   Products disagree on ATT&CK techniques for similar rules due to ambiguities and overlaps within ATT&CK itself.

Discussion with Stakeholders

- Vendors are aware of the tension between ATT&CK coverage metrics and effective detections.

- MITRE confirmed the importance of investigating the details of low-level detection behaviors.

- Practitioners from a cyber risk assessment company highlighted that the security community is not aligned about how tactics and techniques happen at an endpoint.

Recommendations

- MITRE: provide more extensive guidelines on how to interpret ATT&CK.
  - Formalize relationships between overlapping or connected techniques.
  - Ongoing efforts: Improved ATT&CK Evaluations, Summiting the Pyramid.

- Practitioners: take steps to support other methods of rule evaluation.
  - Systematize exchange of rule performance information across organizations.
  - Develop alternate heuristics to evaluate rules independent of environment.

Thank you!

How does Endpoint Detection use the MITRE ATT&CK Framework?

Apurva Virkud, Muhammad Adil Inam, Andy Riddle, Jason Liu,
Gang Wang, Adam Bates
University of Illinois Urbana-Champaign