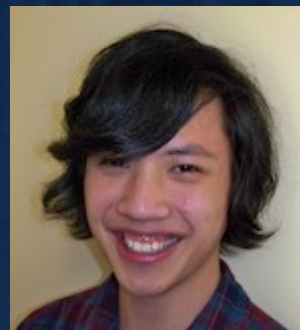




How does Endpoint Detection use the MITRE ATT&CK Framework?

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

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

65% more MITRE ATT&CK coverage than average

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

CrowdStrike Coverage Evaluation

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

on with 100%

MITRE Vectra 90%

Coverage maintained

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

Rapid7 Delivers Complete Kill Chain Coverage

MITRE ATT&CK



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (1)	Acquire Access (1)	Content Injection (1)	Cloud Administration Command (1)	Account Manipulation (1)	Abuse Elevation Control (1)	Abuse Elevation Control (1)	Adversary-In-the-Middle (1)	Account Discovery (1)	Exploitation of Remote Services (1)	Adversary-In-the-Middle (1)	Application Layer Protocol (1)	Automated Exfiltration (1)	Account Access Removal (1)
Information (1)	Compromise Accounts (1)	Exploit Public-Facing Application (1)	Interpreter (1)	Boot or Logon Autostart Execution (1)	Access Token Manipulation (1)	Access Token Manipulation (1)	Credentials from Password Stores (1)	Browser Information Discovery (1)	Lateral Tool Transfer (1)	Audio Capture (1)	Removable Media (1)	Exfiltration Over Alternative Protocol (1)	Data Encrypted for Impairment (1)
Gather Victim Identity Information (1)	Compromise Infrastructure (1)	External Remote Services (1)	Container Administration Command (1)	Boot or Logon Autostart Execution (1)	Account Manipulation (1)	BTS Jobs (1)	Exploitation for Credential Access (1)	Cloud Infrastructure Discovery (1)	Remote Service Session Hijacking (1)	Automated Collection (1)	Content Injection (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)
Gather Victim Network Information (1)	Develop Capabilities (1)	Hardware Additions (1)	Deploy Container (1)	Boot or Logon Initialization Scripts (1)	Debugger Evasion (1)	Build Image on Host (1)	Debugger Evasion (1)	Cloud Service Dashboard (1)	Remote Services (1)	Browser Session Hijacking (1)	Data Encoding (1)	Exfiltration Over Other Network Medium (1)	Device Placement (1)
Gather Victim Org Information (1)	Establish Accounts (1)	Phishing (1)	Exploitation for Client Execution (1)	Boot or Logon Initialization Scripts (1)	Browser Extensions (1)	Direct Volume Access (1)	Forced Authentication (1)	Cloud Storage Object Discovery (1)	Application Through Removable Media (1)	Clipboard Data (1)	Data Obfuscation (1)	Exfiltration Over Physical Medium (1)	Disk Wipe (1)
Obtain Capabilities (1)	Obtain Capabilities (1)	Replication Through Removable Media (1)	Inter-Process Communication (1)	Compromise Host Software Binary (1)	Browser Extensions (1)	Domain or Tenant Policy Modification (1)	Forge Web Credentials (1)	Cloud Storage Object Discovery (1)	Software Deployment Tools (1)	Data from Cloud Storage (1)	Dynamic Resolution (1)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (1)
Phishing for Information (1)	Stage Capabilities (1)	Supply Chain Compromise (1)	Native API (1)	Event Triggered Execution (1)	Domain or Tenant Policy Modification (1)	Escape to Host (1)	Input Capture (1)	Container and Resource Discovery (1)	Tainted Shared Content (1)	Data from Configuration Repository (1)	Encrypted Channel (1)	Exfiltration Over Physical Medium (1)	Financial Theft (1)
Search Closed Sources (1)	Search Open Technical Websites (1)	Trusted Relationship (1)	Scheduled Task/Job (1)	Event Triggered Execution (1)	Domain or Tenant Policy Modification (1)	Event Triggered Execution (1)	Modify Authentication Process (1)	Debugger Evasion (1)	Use Alternate Authentication Material (1)	Data from Information Repositories (1)	Fallback Channels (1)	Exfiltration Over Web Service (1)	Firmware Corruption (1)
Search Open Websites/Downloads (1)	Valid Accounts (1)	Shared Modules (1)	Serverless Execution (1)	Event Triggered Execution (1)	Execution Guardrails (1)	Event Triggered Execution (1)	Multi-Factor Authentication Interception (1)	Device Driver Discovery (1)	Data from Local System (1)	Transfer Data to Cloud Account (1)	Hide Infrastructure (1)	Exfiltration Over Web Service (1)	Inhibit System Recovery (1)
Search Victim-Owned Websites (1)	System Services (1)	Software Deployment Tools (1)	System Services (1)	Event Triggered Execution (1)	Exploitation for Defense Evasion (1)	Exploitation for Defense Evasion (1)	Request Generation (1)	Domain Trust Discovery (1)	Data from Network Storage Drive (1)	Multi-Stage Channels (1)	Ingress/Tools Transfer (1)	Transfer Data to Cloud Account (1)	Network Denial of Service (1)
	User Execution (1)	Windows Management Instrumentation (1)	User Execution (1)	External Remote Services (1)	Hijack Execution Flow (1)	Hijack Execution Flow (1)	File and Directory Permissions Modification (1)	File and Directory Discovery (1)	Data from Removable Media (1)	Non-Application Layer Protocol (1)	Impair Defenses (1)	Transfer Data to Cloud Account (1)	Resource Hijacking (1)
			Windows Management Instrumentation (1)	Hijack Execution Flow (1)	Process Injection (1)	Process Injection (1)	Hide Artifacts (1)	Network Sniffing (1)	Data from Staged (1)	Non-Standard Port (1)	OS Credential Dumping (1)	Transfer Data to Cloud Account (1)	Service Stop (1)
				Modify Authentication Process (1)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Hide Artifacts (1)	Log Enumeration (1)	Email Collection (1)	Protocol Tunneling (1)	Log Enumeration (1)	Transfer Data to Cloud Account (1)	System Shutdown/Reboot (1)
				Office Application Startup (1)	Valid Accounts (1)	Valid Accounts (1)	Impair Defenses (1)	Screen Capture (1)	Input Capture (1)	Remote Access Software (1)	Screen Capture (1)	Transfer Data to Cloud Account (1)	
								Video Capture (1)	Web Service (1)	Web Service (1)			

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

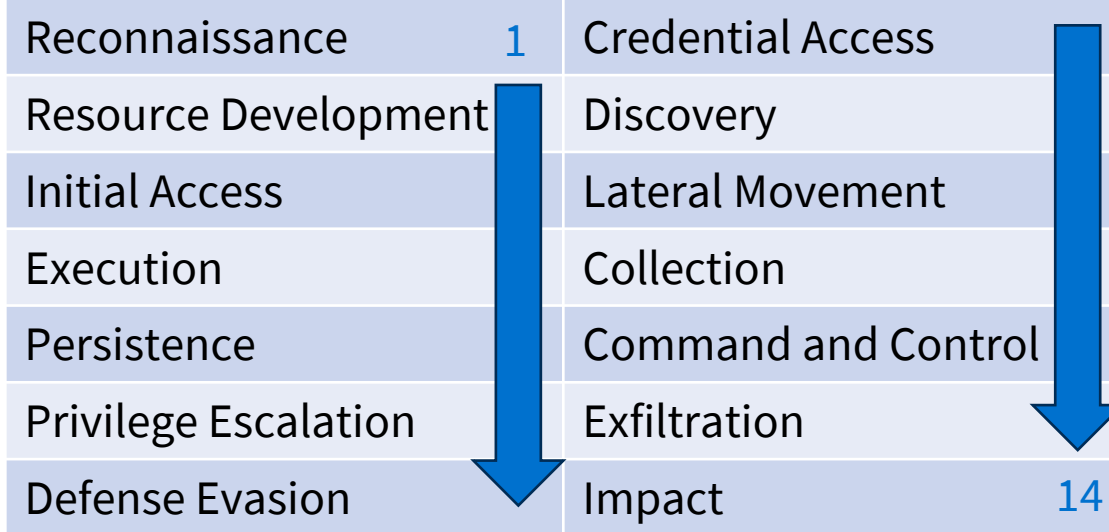
Virtualization Encryption (1)
XSL Script Processing (1)

MITRE ATT&CK



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (1)	Acquire Access (1)	Content Injection (1)	Cloud Administration Command (1)	Account Manipulation (1)	Abuse Elevation Control (1)	Abuse Elevation Control (1)	Adversary-In-the-Middle (1)	Account Discovery (1)	Exploitation of Remote Services (1)	Adversary-In-the-Middle (1)	Application Layer Protocol (1)	Automated Exfiltration (1)	Account Access Removal (1)
Information (1)	Compromise Accounts (1)	Exploit Public-Facing Application (1)	Interpreter (1)	Boot or Logon Autostart Execution (1)	Access Token Manipulation (1)	Access Token Manipulation (1)	Credentials from Password Stores (1)	Browser Information Discovery (1)	Lateral Tool Transfer (1)	Audio Capture (1)	Removable Media Content Injection (1)	Exfiltration Over Alternative Protocol (1)	Data Encrypted for Impairment (1)
Gather Victim Identity Information (1)	Compromise Infrastructure (1)	External Remote Services (1)	Container Administration Command (1)	Boot or Logon Autostart Scripts (1)	Account Manipulation (1)	BTS Jobs (1)	Exploitation for Credential Access (1)	Cloud Infrastructure Discovery (1)	Remote Service Session Hijacking (1)	Automated Collection (1)	Data Encoding (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)
Gather Victim Network Information (1)	Develop Capabilities (1)	Hardware Additions (1)	Deploy Container (1)	Boot or Logon Initialization Scripts (1)	Debugger Evasion (1)	Build Image on Host (1)	Forced Authentication (1)	Cloud Service Dashboard (1)	Remote Services (1)	Browser Session Hijacking (1)	Data Obfuscation (1)	Exfiltration Over Other Network Medium (1)	Device Placement (1)
Gather Victim Org Information (1)	Establish Accounts (1)	Phishing (1)	Exploitation for Client Execution (1)	Browser Extensions (1)	Boot or Logon Initialization Scripts (1)	Debuggers/Decode Files or Information (1)	Input Capture (1)	Cloud Storage Discovery (1)	Application Through Removable Media (1)	Clipboard Data (1)	Dynamic Resolution (1)	Exfiltration Over Physical Medium (1)	Disk Wipe (1)
Obtain Capabilities (1)	Stage Capabilities (1)	Replication Through Removable Media (1)	Inter-Process Communication (1)	Compromise Host Software Binary (1)	Drifts or Modify System Process (1)	Deploy Container (1)	Modify Authentication Process (1)	Cloud Storage Object Discovery (1)	Software Deployment Tools (1)	Data from Cloud Storage (1)	Encrypted Channel (1)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (1)
Search Closed Sources (1)	Supply Chain Compromise (1)	Scheduled Task/Job (1)	Native API (1)	Chaille Account (1)	Domain or Tenant Policy Modification (1)	Direct Volume Access (1)	Multi-Factor Authentication Interception (1)	Container and Resource Discovery (1)	Taint Shared Content (1)	Data from Configuration Repository (1)	Fallback Channels (1)	Exfiltration Over Web Service (1)	Financial Theft (1)
Search Open Technical Websites (1)	Trusted Relationship (1)	Serverless Execution (1)	Scheduled Task/Job (1)	Drifts or Modify System Process (1)	Escape to Host (1)	Domain or Tenant Policy Modification (1)	Multi-Factor Authentication Request Generation (1)	Debugger Evasion (1)	Use Alternate Authentication Material (1)	Data from Information Repositories (1)	Hide Infrastructure (1)	Scheduled Transfer (1)	Firmware Corruption (1)
Search Open Websites/Downloads (1)	Valid Accounts (1)	Software Deployment Tools (1)	System Services (1)	Event Triggered Execution (1)	Event Triggered Execution (1)	Execution Guardrails (1)	OS Credential Dumping (1)	Device Driver Discovery (1)	Data from Local System (1)	Ingress/Tools Transfer (1)	Ingress/Tools Transfer (1)	Transfer Data to Cloud Account (1)	Inhibit System Recovery (1)
Search Victim-Owned Websites (1)	Windows Management Instrumentation (1)	System Services (1)	External Remote Services (1)	Exploitation for Privilege Escalation (1)	Exploitation for Defense Evasion (1)	File and Directory Permissions Modification (1)	OS Credential Dumping (1)	Domain Trust Discovery (1)	Data from Network Shared Drives (1)	Multi-Stage Channels (1)	Non-Application Layer Protocol (1)	Network Denial of Service (1)	Network Denial of Service (1)
			Hijack Execution Flow (1)	Implant Internal Image (1)	Modify Authentication Process (1)	Hide Artifacts (1)	OS Credential Dumping (1)	File and Directory Discovery (1)	Data from Removable Media (1)	Non-Standard Port (1)	Protocol Tunneling (1)	Resource Hijacking (1)	Resource Hijacking (1)
			Windows Management Instrumentation (1)	Modify Authentication Process (1)	Scheduled Task/Job (1)	Hijack Execution Flow (1)	OS Credential Dumping (1)	Group Policy Discovery (1)	Data from System (1)	Non-Standard Port (1)	Protocol Tunneling (1)	Service Stop (1)	Service Stop (1)
				Office Application Startup (1)	Valid Accounts (1)	Impair Defenses (1)	OS Credential Dumping (1)	Log Enumeration (1)	Email Collection (1)	Non-Standard Port (1)	Protocol Tunneling (1)	System Shutdown/Reboot (1)	System Shutdown/Reboot (1)
							Steal Application Access Token (1)	Network Service Discovery (1)	Input Capture (1)	Remote Access Software (1)			
							Steal or Forge Authentication Certificates (1)	Network Share Discovery (1)	Screen Capture (1)	Traffic Signaling (1)			
									Video Capture (1)	Web Service (1)			

Approximately chronological order during an attack



- Tactics: high level goals

MITRE ATT&CK



	Initial Access 14 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 20 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Abuse Elevation Control Mechanism (6)	IM Host (1), IM Identity (1), IM Network (1), IM Org Information (1), IM Information (1), IM Webshell (1), IM Owned Webapps (1)	Acquire Access (1), Acquire Infrastructure (1), Drive-by Compromise (1), Exploit Public-Facing Application (1), External Remote Services (1), Hardware Additions (1), PHishing (1), Replication Through Removable Media (1), Stage Capabilities (1)	Cloud Administration Command (1), Command and Scripting Interpreter (1), Container Administration Command (1), Deploy Container (1), Exploitation for Client Execution (1), Inter-Process Communication (1), Native API (1), Scheduled Task/Job (1), Serverless Execution (1), Shared Modules (1), Software Deployment Tools (1), System Services (1), Trusted Relationship (1), Valid Accounts (1)	Abuse Elevation Control Mechanism (6), Access Token Manipulation (3), Account Manipulation (3), Boot or Logon Autostart Execution (1), Boot or Logon Initialization Scripts (1), Browser Extensions (1), Compromise Host Software Binary (1), Create or Modify System Process (1), Domain or Tenant Policy Modification (1), Escape to Host (1), Event Triggered Execution (1), External Remote Services (1), Hijack Execution Flow (1), Implant Internal Image (1), Modify Authentication Process (1), Office Application Startup (1), Power Settings (1), Pre-OS Boot (1), Scheduled Task/Job (1), Server Software Components (1), Traffic Signaling (1), Valid Accounts (1)	Abuse Elevation Control Mechanism (6), Bids Force (1), Credentials from Password Stores (1), Images on Host (1), Logger Evasion (1), Localizable/Decode Files or Folders (1), Native Container (1), Volume Access (1), Domain or Tenant Policy Modification (1), Domain Guardrails (1), Exploitation for Defense Evasion (1), File and Directory Permissions Modification (1), Hijack Execution Flow (1), Process Injection (1), Scheduled Task/Job (1), Valid Accounts (1)	Adversary-in-the-Middle (1), Bids Force (1), Credentials from Password Stores (1), Exploitation for Credential Access (1), Forced Authentication (1), Forge Web Credentials (1), Input Capture (1), Modify Authentication Process (1), Multi-Factor Authentication Interception (1), Multi-Factor Authentication Request Generation (1), Network Sniffing (1), OS Credential Dumping (1), Steal Application Access Token (1), Steal or Forge Authentication Certificates (1), Steal or Forge Hardware Tokens (1), Steal Web Session Cookie (1), Unsecured Credentials (1)	Account Discovery (1), Application Window Discovery (1), Browser Information Discovery (1), Cloud Infrastructure Discovery (1), Cloud Service Dashboard (1), Cloud Storage Object Discovery (1), Container and Resource Discovery (1), Debugger Evasion (1), Device Driver Discovery (1), Domain Trust Discovery (1), File and Directory Discovery (1), Group Policy Discovery (1), Log Enumeration (1), Network Service Discovery (1), Network Share Discovery (1), Network Sniffing (1), Password Policy Discovery (1), Peripheral Device Discovery (1), Permission Groups Discovery (1), Process Discovery (1), Query Registry (1), Remote System Discovery (1), Software Discovery (1), System Information Discovery (1), System Location Discovery (1), System Network Configuration Discovery (1), System Network Connections Discovery (1), System Owner/User Discovery (1), System Service Discovery (1), System Time Discovery (1), Virtualization/Sandbox Evasion (1)	Exploitation of Remote Services (1), Internal Spearphishing (1), Lateral Tool Transfer (1), Remote Service Session Hijacking (1), Remote Services (1), Replication Through Removable Media (1), Software Deployment Tools (1), Taint Shared Content (1), Use Alternate Authentication Material (1)	Adversary-in-the-Middle (1), Archive Collected Data (1), Communication Through Removable Media (1), Audio Capture (1), Automated Collection (1), Browser Session Hijacking (1), Clipboard Data (1), Data from Cloud Storage (1), Data from Configuration Repository (1), Data from Information Repositories (1), Data from Local System (1), Data from Network Shared Drive (1), Data from Removable Media (1), Data Staged (1), Email Collection (1), Input Capture (1), Screen Capture (1), Video Capture (1)	Application Layer Protocol (1), Automated Exfiltration (1), Data Transfer Size Limits (1), Communication Through Removable Media (1), Content Injection (1), Data Encoding (1), Data Obfuscation (1), Dynamic Resolution (1), Encrypted Channel (1), Fallback Channels (1), Hide Infrastructure (1), Ingress Tool Transfer (1), Multi-Stage Channels (1), Non-Application Layer Protocol (1), Non-Standard Port (1), Protocol Tunneling (1), Proxy (1), Remote Access Software (1), Traffic Signaling (1), Web Service (1)	Automated Exfiltration (1), Data Destruction (1), Data Encrypted for Impact (1), Data Manipulation (1), Defacement (1), Disk Wipe (1), Endpoint Denial of Service (1), Financial Theft (1), Firmware Corruption (1), Inhibit System Recovery (1), Network Denial of Service (1), Resource Hijacking (1), Service Stop (1), System Shutdown/Reboot (1)	

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

MITRE ATT&CK



	Initial Access 14 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 20 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Abuse Elevation Control Mechanism (6)	IM Host (14)	Cloud Administration Command (14)	Account Manipulation (20)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (17)	Account Discovery (32)	Exploitation of Remote Services (9)	Adversary-in-the-Middle (17)	Application Layer Protocol (18)	Automated Exfiltration (9)	Account Access Removal (14)
Access Token Manipulation (5)	IM Identity (14)	Command and Scripting Interpreter (14)	Account Manipulation (20)	Access Token Manipulation (5)	Access Token Manipulation (5)	Adversary-in-the-Middle (17)	Application Window Discovery (32)	Internal Spearphishing (9)	Archive Collected Data (17)	Communication Through Removable Media (18)	Data Transfer Size Limits (9)	Data Destruction (14)
Account Manipulation (6)	IM Network (14)	Container Administration Command (14)	Account Manipulation (20)	Account Manipulation (6)	Account Manipulation (6)	Adversary-in-the-Middle (17)	Browser Information Discovery (32)	Remote Service Session Hijacking (9)	Audio Capture (17)	Content Injection (18)	Exfiltration Over Alternative Protocol (9)	Data Encrypted for Impact (14)
Boot or Logon Autostart Execution (14)	IM Org Information (14)	Deploy Container (14)	Account Manipulation (20)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Adversary-in-the-Middle (17)	Cloud Infrastructure Discovery (32)	Remote Service Session Hijacking (9)	Automated Collection (17)	Data Obfuscation (18)	Exfiltration Over C2 Channel (9)	Data Manipulation (14)
Boot or Logon Initialization Scripts (5)	IM Information (14)	Exploitation for Client Execution (14)	Account Manipulation (20)	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Adversary-in-the-Middle (17)	Cloud Service Dashboard (32)	Remote Services (9)	Browser Session Hijacking (17)	Data Encoding (18)	Exfiltration Over Other Network Medium (9)	Defacement (14)
Create or Modify System Process (5)	IM Webshell (14)	Inter-Process Communication (14)	Account Manipulation (20)	Create or Modify System Process (5)	Create or Modify System Process (5)	Adversary-in-the-Middle (17)	Cloud Storage Object Discovery (32)	Replication Through Removable Media (9)	Clipboard Data (17)	Dynamic Resolution (18)	Exfiltration Over Physical Medium (9)	Disk Wipe (14)
Domain or Tenant Policy Modification (2)	Owned Webapps (14)	Native API (14)	Account Manipulation (20)	Domain or Tenant Policy Modification (2)	Domain or Tenant Policy Modification (2)	Adversary-in-the-Middle (17)	Container and Resource Discovery (32)	Software Deployment Tools (9)	Data from Cloud Storage (17)	Encrypted Channel (18)	Exfiltration Over Web Service (9)	Endpoint Denial of Service (14)
Escape to Host		Scheduled Task/Job (14)	Account Manipulation (20)	Escape to Host	Escape to Host	Adversary-in-the-Middle (17)	Debugger Evasion (32)	Taint Shared Content (9)	Data from Configuration Repository (17)	Fallback Channels (18)	Exfiltration Over Web Service (9)	Financial Theft (14)
Event Triggered Execution (16)		Serverless Execution (14)	Account Manipulation (20)	Event Triggered Execution (16)	Event Triggered Execution (16)	Adversary-in-the-Middle (17)	Device Driver Discovery (32)	Use Alternate Authentication Material (9)	Data from Information Repositories (17)	Hide Infrastructure (18)	Scheduled Transfer (9)	Firmware Corruption (14)
Exploitation for Privilege Escalation		Shared Modules (14)	Account Manipulation (20)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Adversary-in-the-Middle (17)	File and Directory Discovery (32)		Data from Local System Repositories (17)	Ingress Tool Transfer (18)	Scheduled Transfer to Cloud Account (9)	Inhibit System Recovery (14)
Hijack Execution Flow (12)		Software Deployment Tools (14)	Account Manipulation (20)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Adversary-in-the-Middle (17)	Group Policy Discovery (32)		Data from Network Shared Drive (17)	Multi-Stage Channels (18)	Transfer Data to Cloud Account (9)	Network Denial of Service (14)
Process Injection (12)		System Services (14)	Account Manipulation (20)	Process Injection (12)	Process Injection (12)	Adversary-in-the-Middle (17)	Log Enumeration (32)		Data from Removable Media (17)	Non-Application Layer Protocol (18)	Resource Hijacking (9)	Resource Hijacking (14)
Scheduled Task/Job (5)		Trusted Relationship (14)	Account Manipulation (20)	Scheduled Task/Job (5)	Scheduled Task/Job (5)	Adversary-in-the-Middle (17)	Network Service Discovery (32)		Data Staged (17)	Non-Standard Port (18)	Service Stop (9)	System Shutdown/Reboot (14)
Valid Accounts (4)		Valid Accounts (14)	Account Manipulation (20)	Valid Accounts (4)	Valid Accounts (4)	Adversary-in-the-Middle (17)	Network Share Discovery (32)		Email Collection (17)	Protocol Tunneling (18)	System Shutdown/Reboot (9)	

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



MITRE ATT&CK

Abuse Elevation Control Mechanism (1)
Access Token Manipulation (5)
Account Manipulation (6)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (5)
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)

Tactic: Privilege Escalation

Technique: Access Token Manipulation

Procedures: AppleSeed, BlackCat, SUNSPOT, ...

Initial Access	Discovery	Execution	Persistence	Privilege Escalation	Defense Evasion	Impact
17 techniques	17 techniques	17 techniques	17 techniques	17 techniques	17 techniques	14 techniques
...

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

Endpoint Detection



Carbon Black

```
1 process_name:wevtutil.exe
2 and process_cmdline:cl*
3 and -process_cmdline:clicktorun*
4 and -process_cmdline:AnyConnect\.evtx*
```

T1070 (Indicator Removal)
Defense Evasion

Splunk

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

T1021 (Remote Services)
Defense Evasion

Elastic

```
1 event.category : (network or network_traffic)
2 and network.transport:tcp
3 and (destination.port: 26
4   or (event.dataset:zeek.smtp
5     and destination.port: 26))
```

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

Endpoint Detection



Carbon Black

```
1 process_name:wevtutil.exe
2 and process_cmdline:cl*
3 and -process_cmdline:clicktorun*
4 and -process_cmdline:AnyConnect\.evtx*
```

T1070 (Indicator Removal)
Defense Evasion

Splunk

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

T1021 (Remote Services)
Defense Evasion

Elastic

```
1 event.category : (network or network_traffic)
2 and network.transport:tcp
3 and (destination.port: 26
4   or (event.dataset:zeek.smtp
5     and destination.port: 26))
```

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

Rules

Vendor tagged
techniques and tactics

Endpoint Detection



Carbon Black

```
1 process_name:wevtutil.exe
2 and process_cmdline:cl*
3 and -process_cmdline:clicktorun*
4 and -process_cmdline:AnyConnect\.evtx*
```

T1070 (Indicator Removal)
Defense Evasion

Splunk

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

T1021 (Remote Services)
Defense Evasion

Elastic

```
1 event.category : (network or network_traffic)
2 and network.transport:tcp
3 and (destination.port: 26
4   or (event.dataset:zeek.smtp
5     and destination.port: 26))
```

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

Rules

Vendor tagged
techniques and tactics

Endpoint Detection



Carbon Black

```
1 process_name:wevtutil.exe
2 and process_cmdline:cl*
3 and -process_cmdline:clicktorun*
4 and -process_cmdline:AnyConnect\.evtx*
```

T1070 (Indicator Removal)
Defense Evasion

Splunk

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

T1021 (Remote Services)
Defense Evasion

Elastic

```
1 event.category : (network or network_traffic)
2 and network.transport:tcp
3 and (destination.port: 26
4   or (event.dataset:zeek.smtp
5     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

```
1 process_name:wevtutil.exe
2 and process_cmdline:cl*
3 and -process_cmdline:clicktorun*
4 and -process_cmdline:AnyConnect\.evtx*
```

Splunk

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

Elastic

```
1 event.category : (network or network_traffic)
2 and network.transport:tcp
3 and (destination.port: 26
4   or (event.dataset:zeek.smtp
5     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

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

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

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

Rules



Exist on the Procedural level of ATT&CK!

90% coverage of ATT&CK

==

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

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	✓		✓	



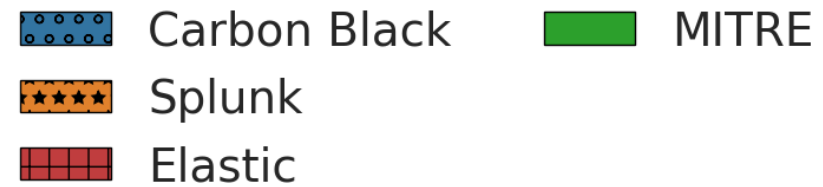
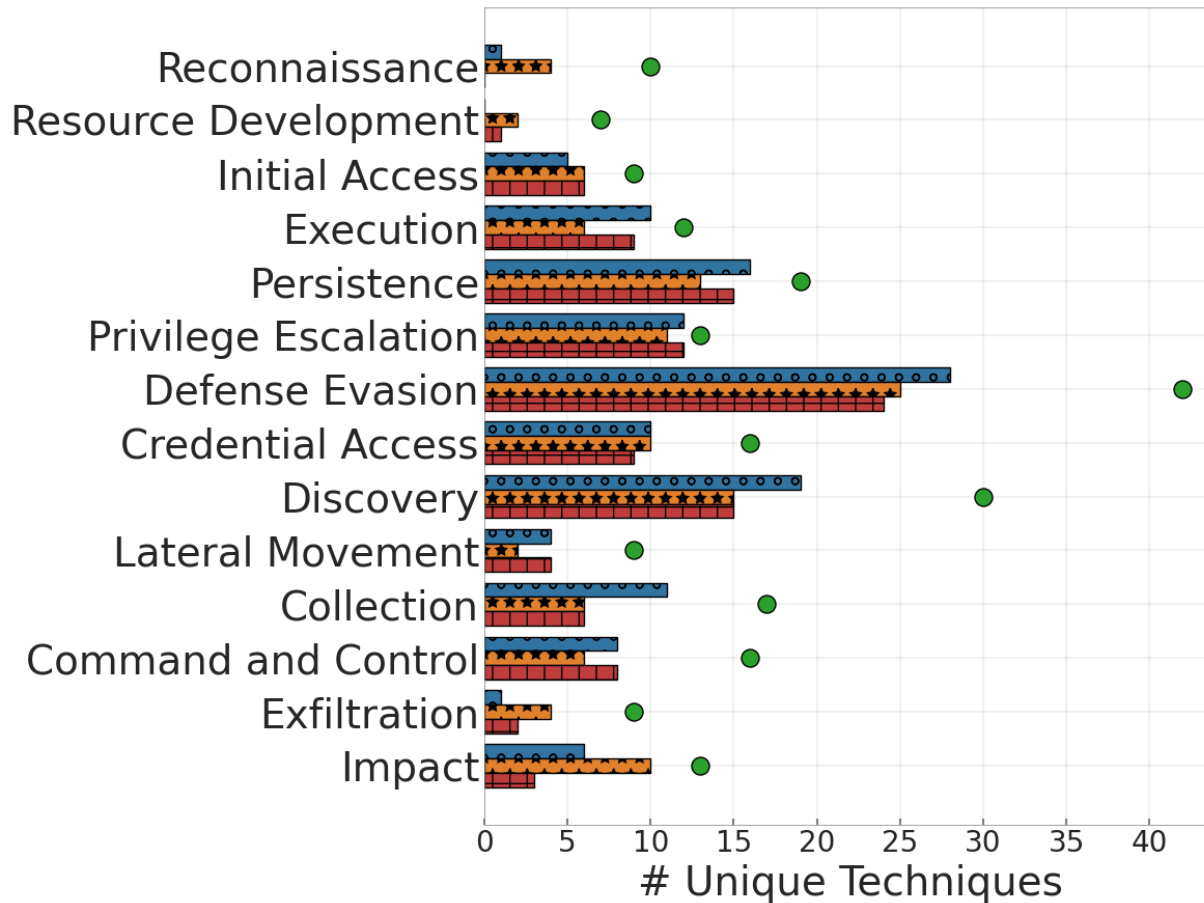
Research Questions



- 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

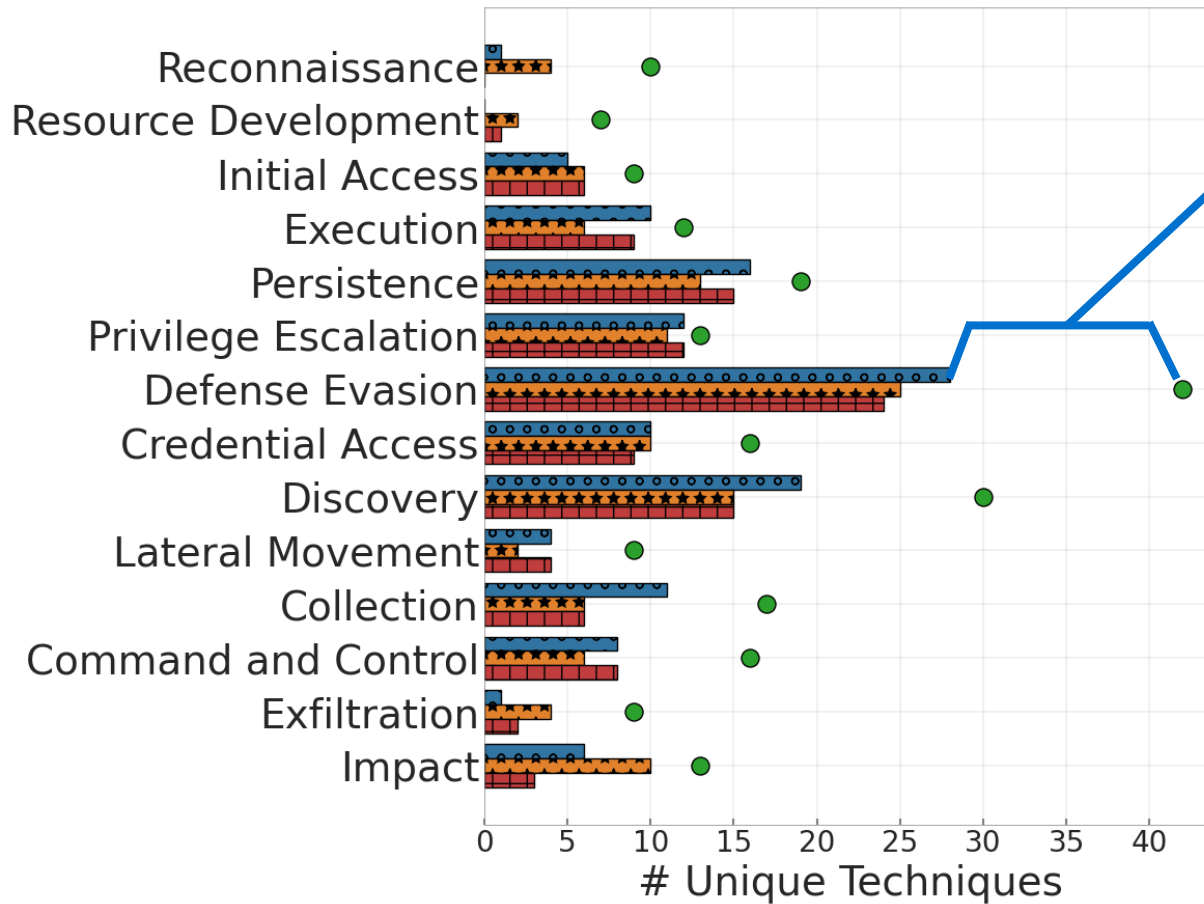


Findings:

- 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

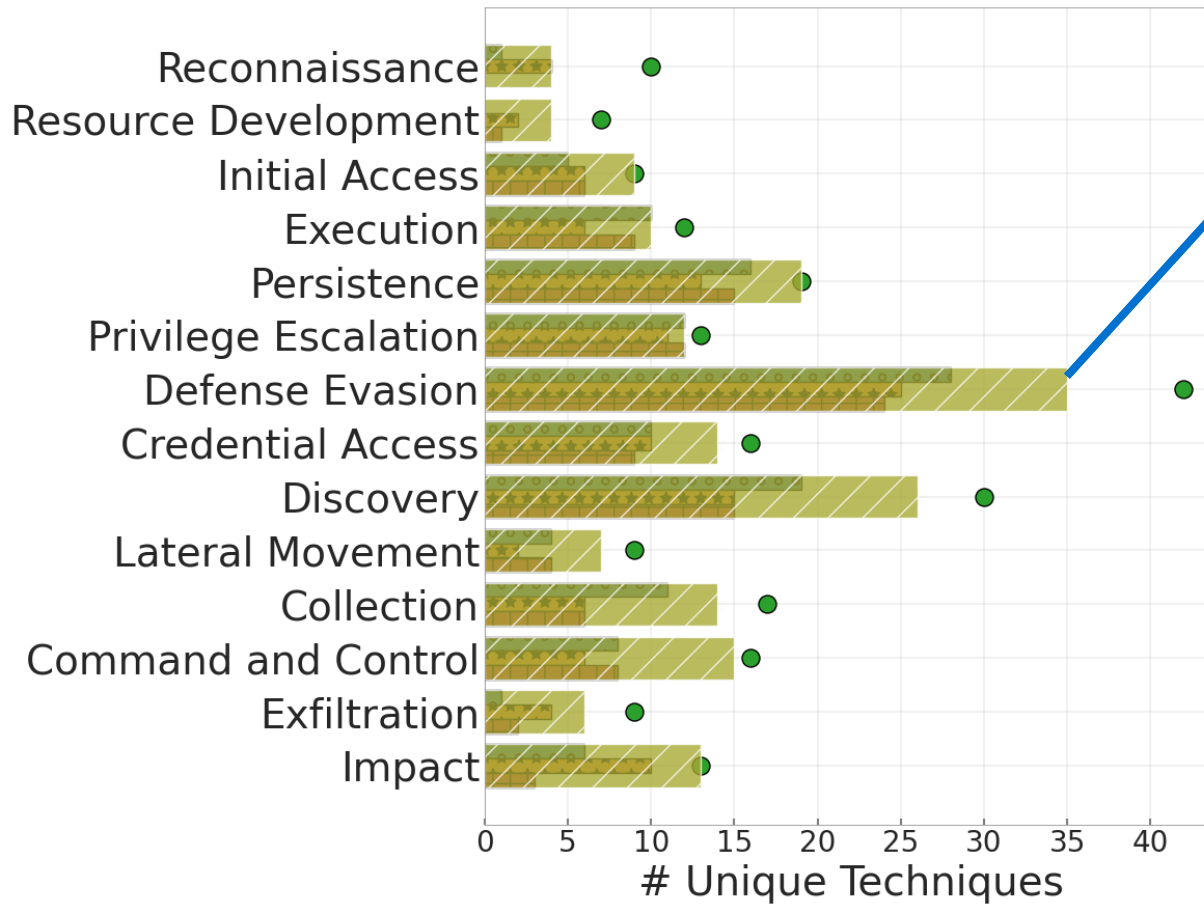
- Carbon Black
- Splunk
- Elastic
- MITRE

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.

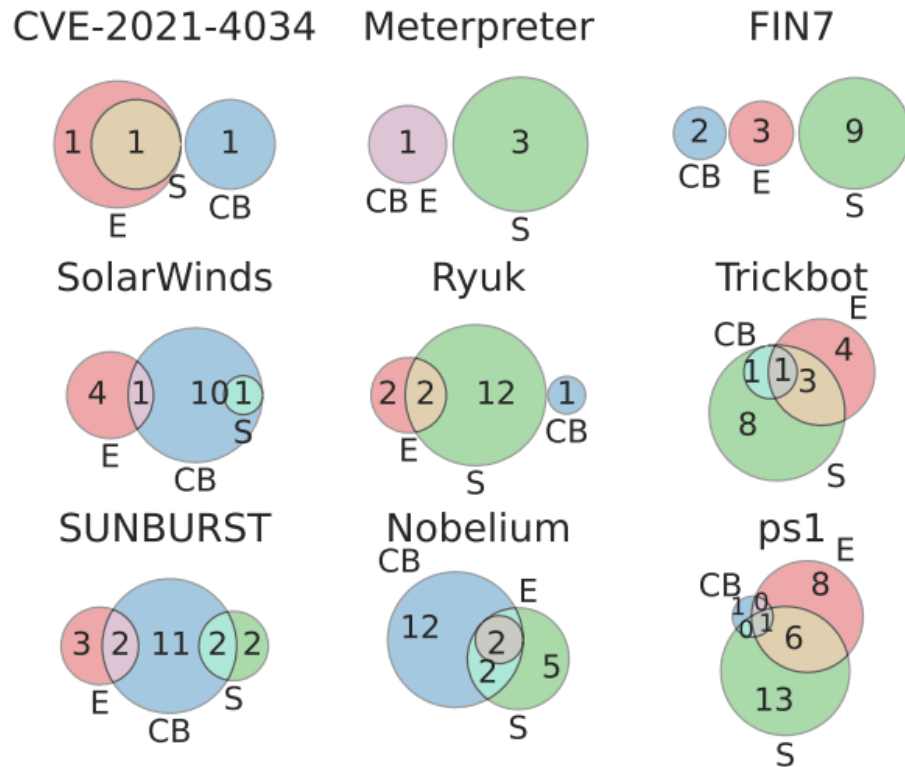
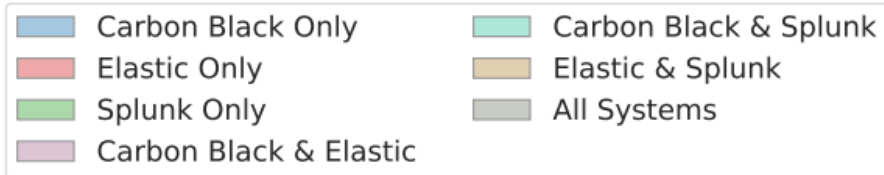
Research Questions



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



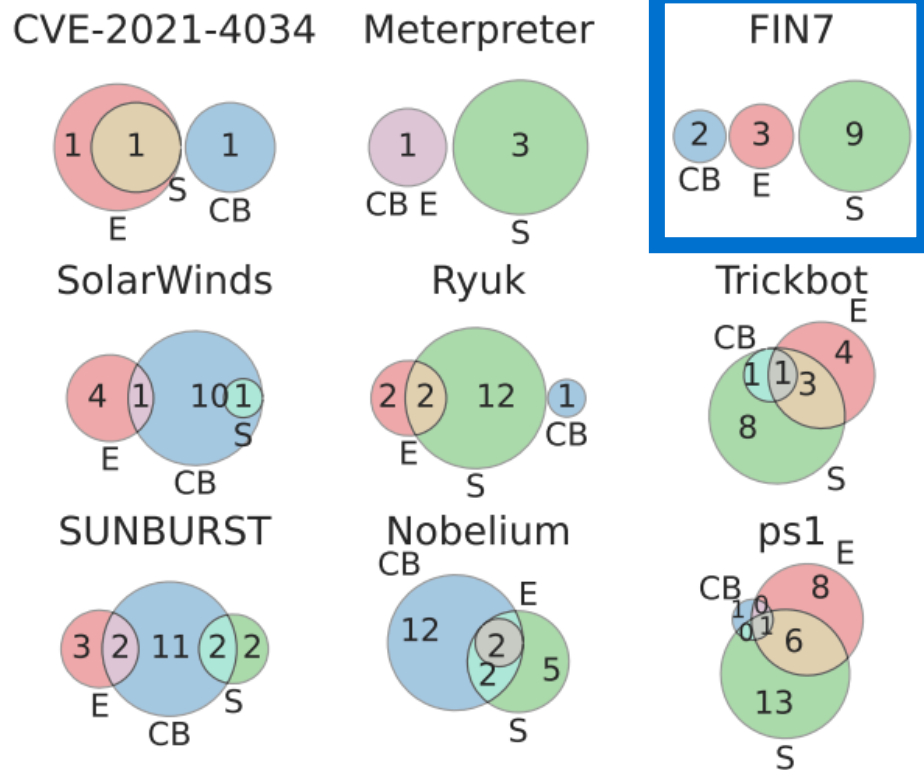
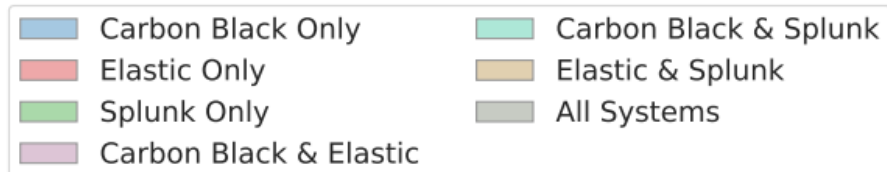
Identify rules are created to address a common malicious entity.

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

