Check Point
SOFTWARE TECHNOLOGIES LTD

CPX 360

BEST PRACTICES TO PREVENT ATT&CKS

How to use Check Point to leverage MITRE ATT&CK Framework

Boaz Barzel | Advanced Threats Solutions Expert, WW

Yaelle Harel | Technical Product Marketing Manager

“Always Be yourself, unless you can Be Batman, then always Be Batman”

WELCOME TO THE FUTURE OF CYBER SECURITY

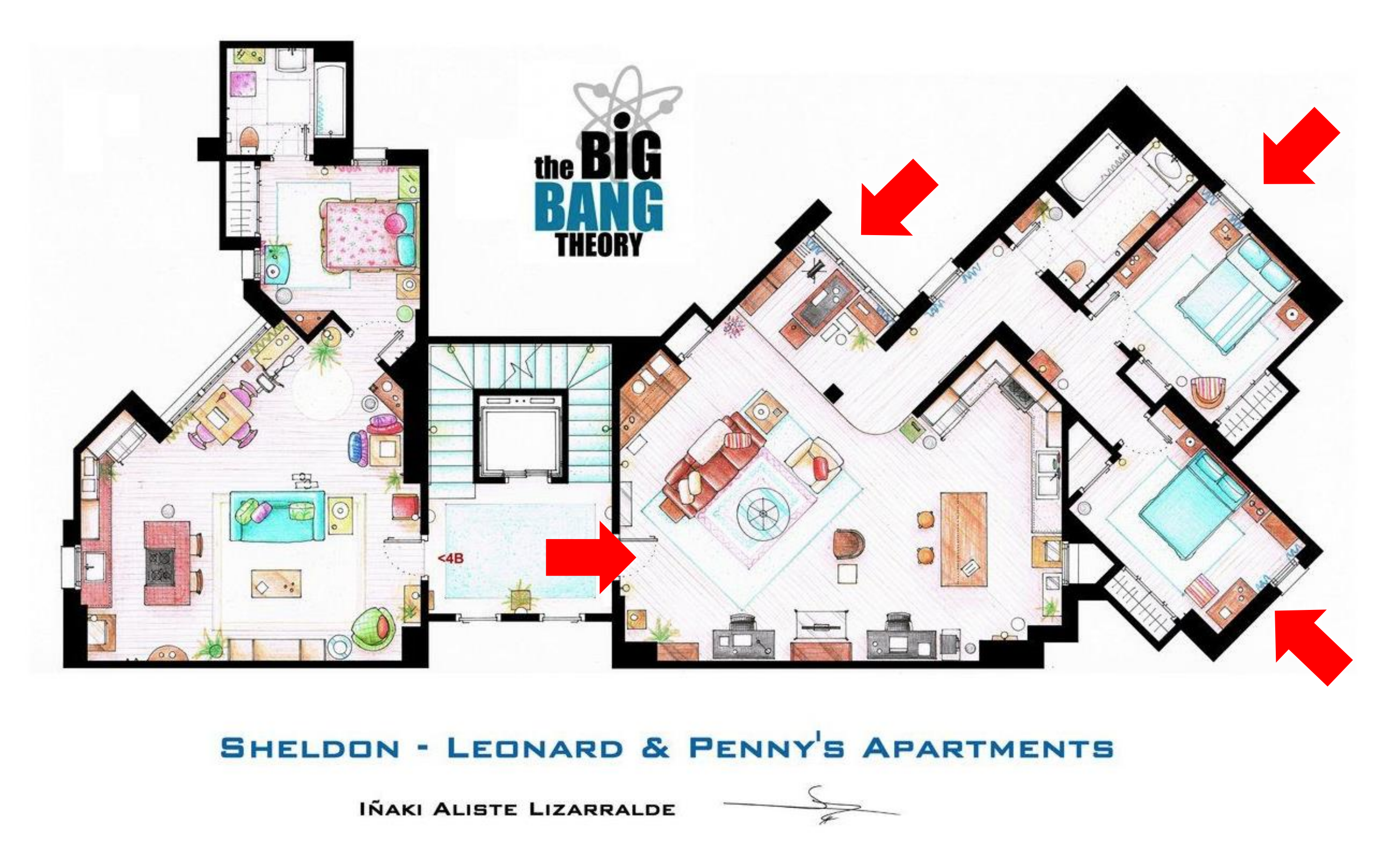
CAUTION

Why?

MARVEL BOY
JOURNEY INTO MYSTERY
CAPTAIN AMERICA
SUB-MARINER
JANN OF THE JUNGLE
STRANGE WORLDS
Fantastic Four
AMAZING FANTASY
SPIDER MAN
the X-MEN
TALES OF SUSPENSE
IRON MAN and CAPTAIN AMERICA
JOURNEY INTO MYSTERY WITH THE MIGHTY THOR
IN MY HAND THIS HAMMER!
Fantastic Four
"IF THIS BE DOOMSDAY!"
THE INCREDIBLE HULK
THE SILVER SURFER
the AMAZING SPIDER-MAN
GIANT-SIZE X-MEN
CAPTAIN AMERICA
MADBOMB
DAREDEVIL
THE MAN WITHOUT FEAR!

Who?

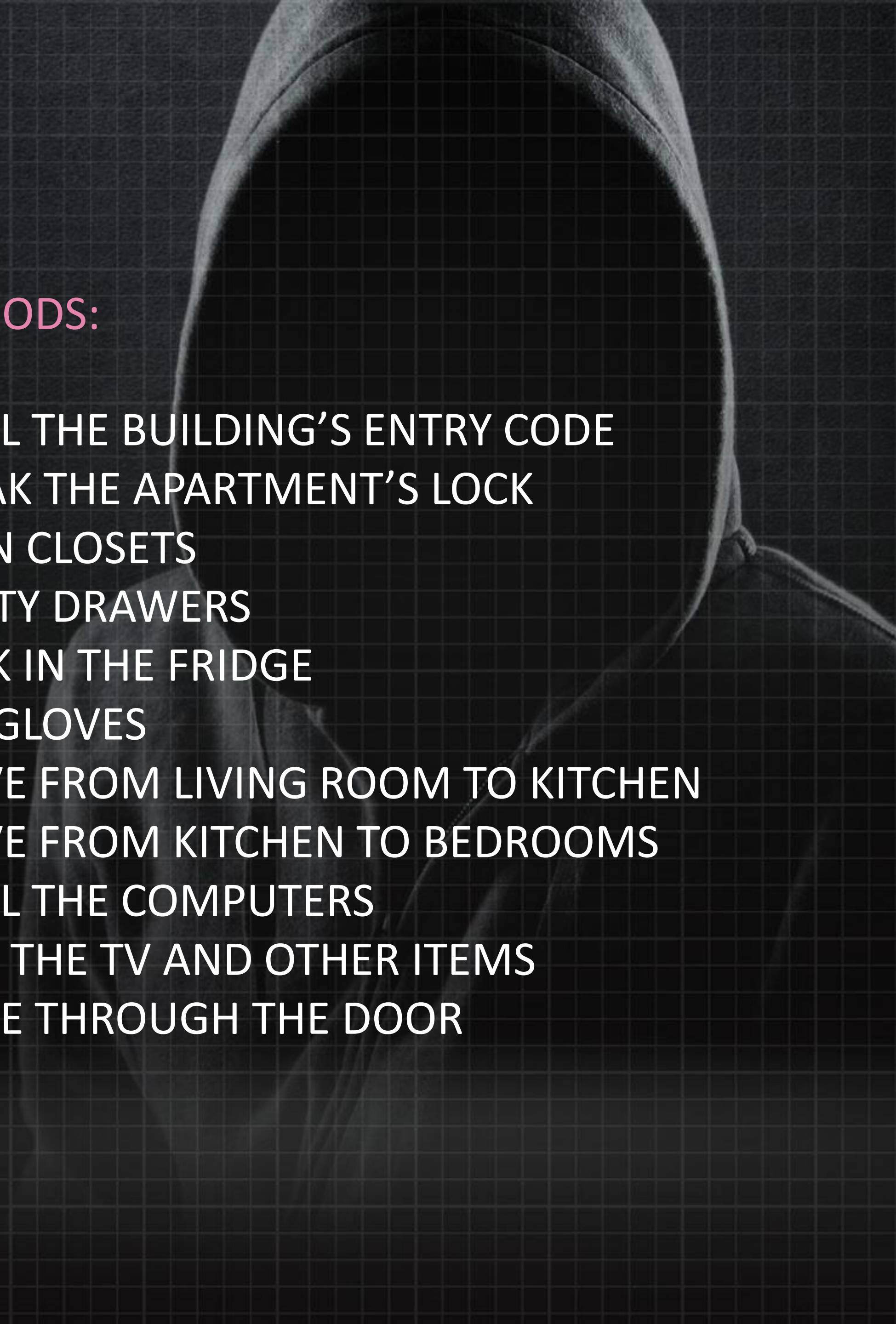
How?


the BIG BANG THEORY
<4B
SHELDON - LEONARD & PENNY'S APARTMENTS
IÑAKI ALISTE LIZARRALDE

PASADENA
POLICE

Attack Analysis

MOTIVATION:	MONEY
ATACKER:	ARBITRARY ROBBER
OBJECTIVES:	ENTER THE APARTMENT SCAN THE APARTMENT HIDE TRACKS STEAL FROM ALL ROOMS COLLECT DATA FROM COMPUTERS CARRY OUT STOLEN ITEMS RUNAWAY
TOOLS:	HAMMER GLOVES BAGS CAR



METHODS:

STEAL THE BUILDING’S ENTRY CODE
BREAK THE APARTMENT’S LOCK
OPEN CLOSETS
EMPTY DRAWERS
LOOK IN THE FRIDGE
USE GLOVES
MOVE FROM LIVING ROOM TO KITCHEN
MOVE FROM KITCHEN TO BEDROOMS
STEAL THE COMPUTERS
TAKE THE TV AND OTHER ITEMS
LEAVE THROUGH THE DOOR

Attack Analysis

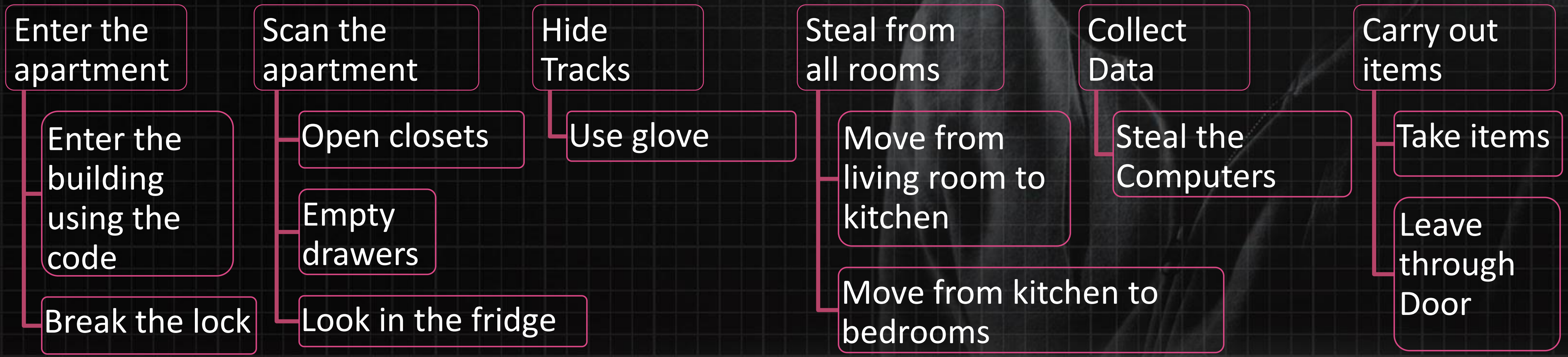
MOTIVATION: MONEY

ATACKER: ARBITRARY ROBBER

TOOLS:
HAMMER
GLOVES
BAGS
CAR

OBJECTIVES:

METHODS:



- Enter the apartment
  - Enter the building using the code
  - Break the lock
- Scan the apartment
  - Open closets
  - Empty drawers
  - Look in the fridge
- Hide Tracks
  - Use glove
- Steal from all rooms
  - Move from living room to kitchen
  - Move from kitchen to bedrooms
- Collect Data
  - Steal the Computers
- Carry out items
  - Take items
  - Leave through Door

Physical to Digital

Evolution of the Desk

In this workshop:

- ❑ MITRE ATT&CK overview
- ❑ Best Practices that will Boost your skills:
  - ❑ Visualize
  - ❑ Assess Risks
  - ❑ Map your Coverage
  - ❑ Investigate
  - ❑ Prevent
- ❑ Check Point’s solution value
- ❑ Takeaways you can apply

In this workshop:

- □ **MITRE ATT&CK overview**
- □ Best Practices that will Boost your skills:
  - □ Visualize
  - □ Assess Risks
  - □ Map your Coverage
  - □ Investigate
  - □ Prevent
- □ Check Point’s solution value
- □ Takeaways you can apply

Overview

MITRE ATT&CK Framework

Facts about MITRE

Mission: Solving Problems for a Safer World

- Nonprofit, federally-funded U.S. research organization.
- The very first company to register a .org domain name.
- Created the CVE – Common Vulnerabilities & Exposures (1999)
- Released CRITs - Collaborative Research Into Threats (2014)
- Launched MITRE ATT&CK framework (2015).

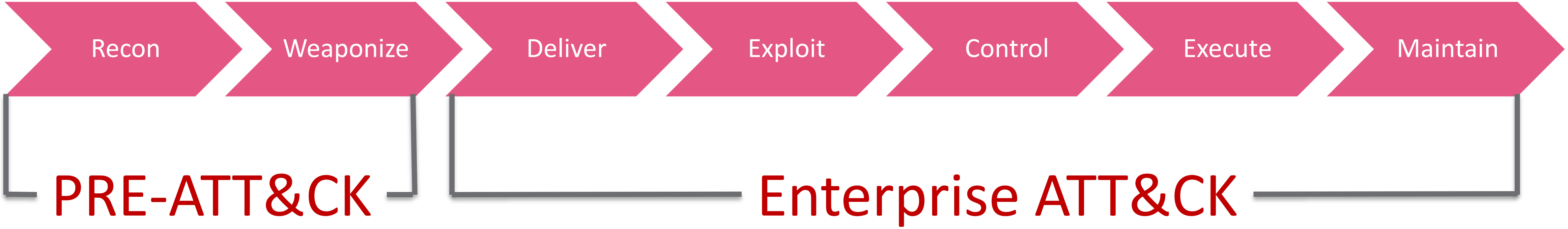
What is MITRE ATT&CK?

Adversaries **T**actics **T**echniques **&** **C**ommon **K**nowledge

- Common language knowledge base
- Real-world **visibility** into adversaries' behavior
- Free and Open community
- Adopted by Fortune 500 and government entities

Can be **leveraged** to **security Assessment** and **incident response**

Cyber Kill Chain vs. MITRE ATT&CK



Recon → Weaponize → Deliver → Exploit → Control → Execute → Maintain

PRE-ATT&CK

- Priority definition
  - Planning, Direction
- Target Selection
- Information Gathering
  - Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

Enterprise ATT&CK

1. Initial Access
2. Execution
3. Persistence
4. Privilege Escalation
5. Defense Evasion
6. Credential Access
7. Discovery
8. Lateral Movement
9. Collection
10. Exfiltration
11. Command and Control
12. Impact

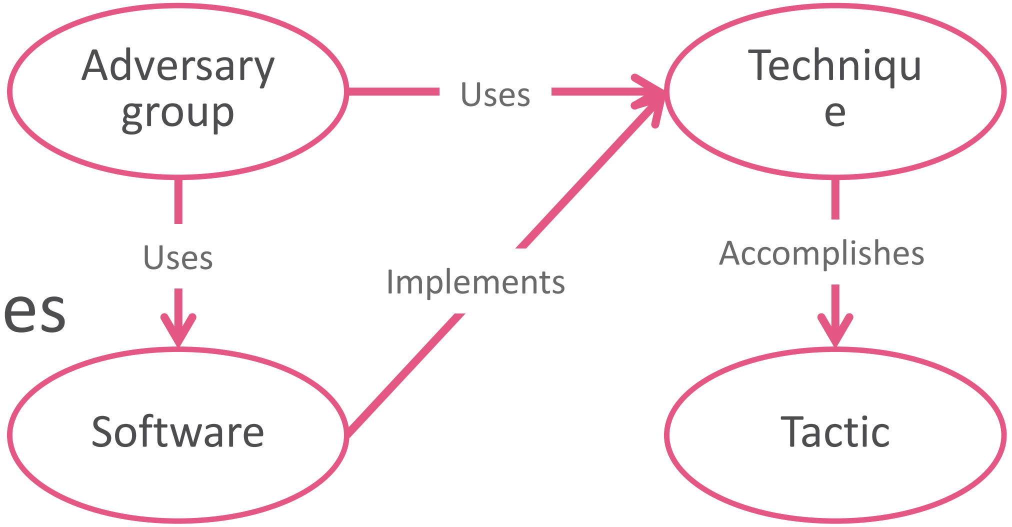
MITRE ATT&CK basics

Tactic The attacker’s tactical objective

Technique The way a tactic is achieved

Software Tools used to attack

Group Threat Actors - Known adversaries


Adversary group

Uses

Technique

Uses

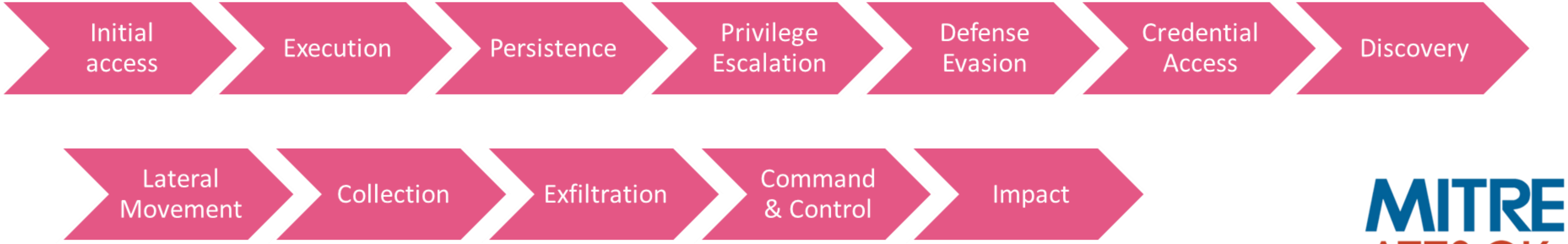
Implements

Accomplishes

Software

Tactic

MITRE ATT&CK Tactics:


Initial access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Exfiltration

Command & Control

Impact

Attack Analysis

MOTIVATION: MONEY

GROUP:

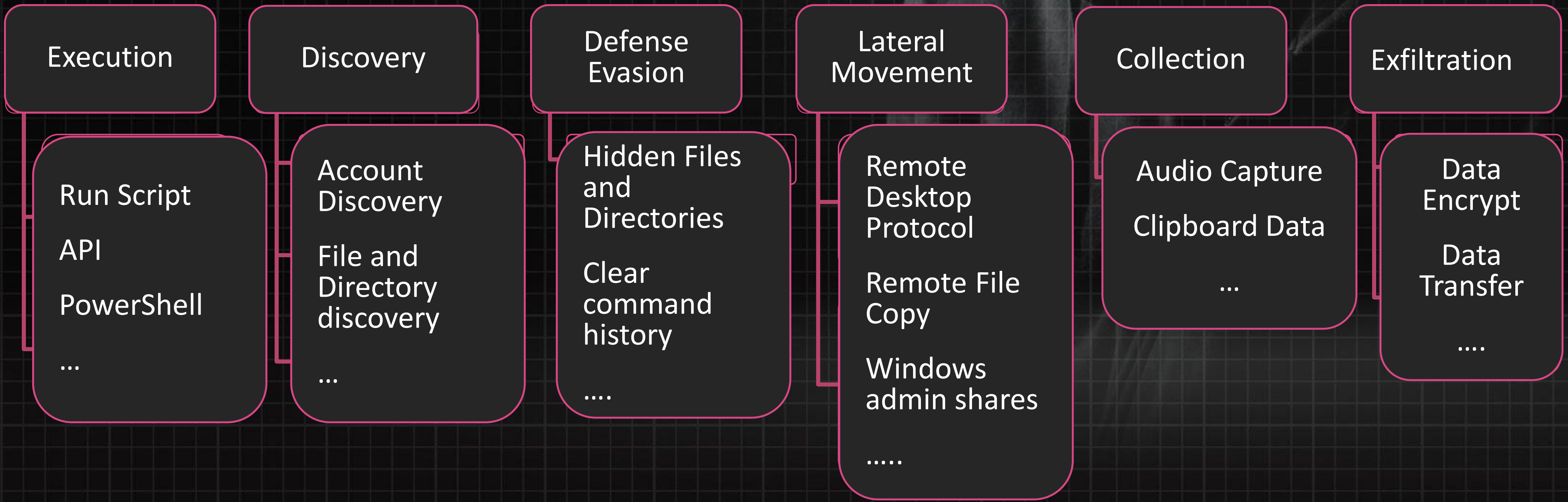
- APT 33
- DustDorm
- ….

SOFTWARE:

- WannaCry
- RobbinHood
- Agent Smith
- …..

TACTICS:

TECHNIQUES:



Execution
- Run Script
- API
- PowerShell
- …

Discovery
- Account Discovery
- File and Directory discovery
- …

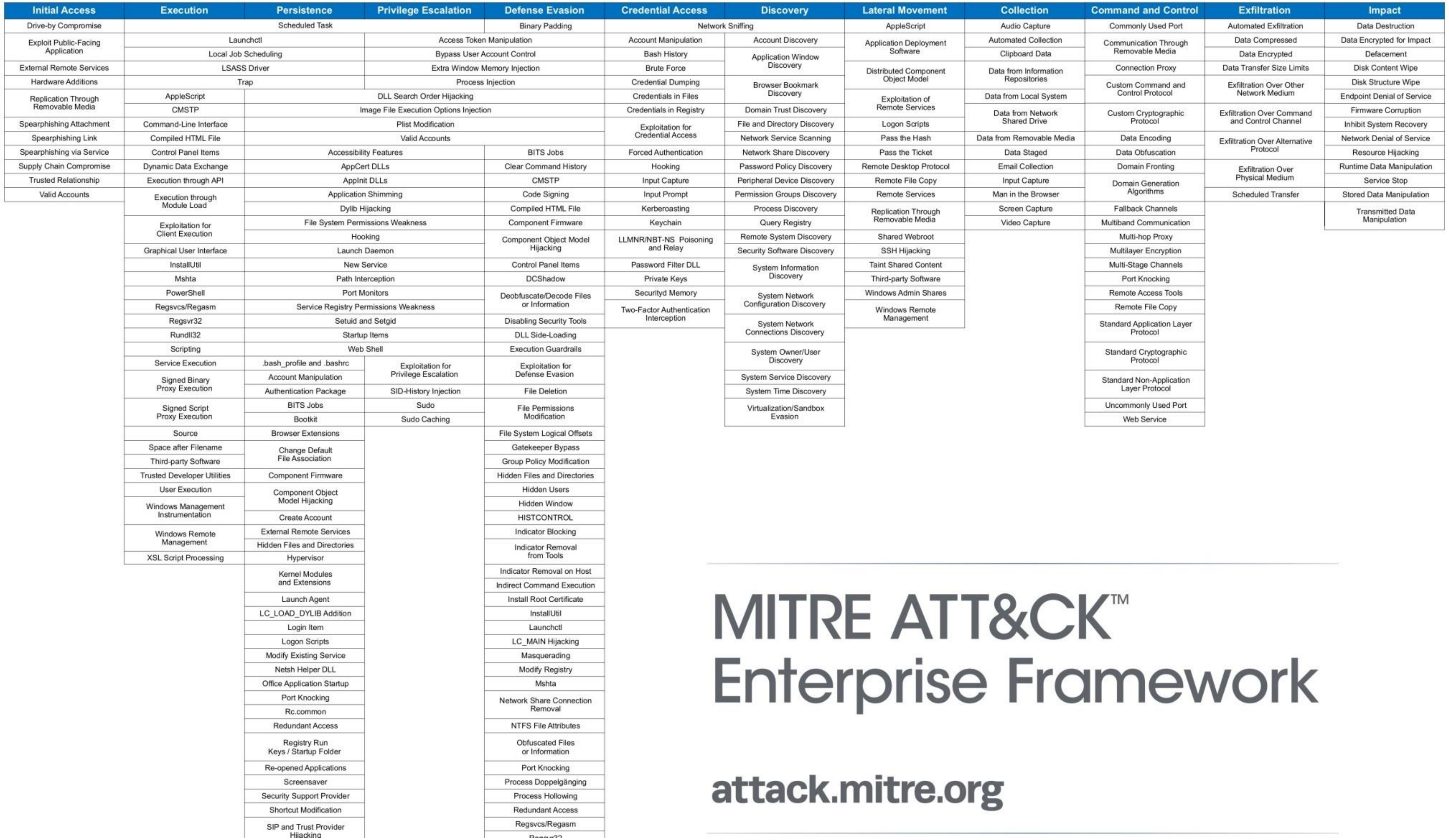
Defense Evasion
- Hidden Files and Directories
- Clear command history
- ….

Lateral Movement
- Remote Desktop Protocol
- Remote File Copy
- Windows admin shares
- …..

Collection
- Audio Capture
- Clipboard Data
- …

Exfiltration
- Data Encrypt
- Data Transfer
- ….

MITRE ATT&CK - Enterprise Matrix

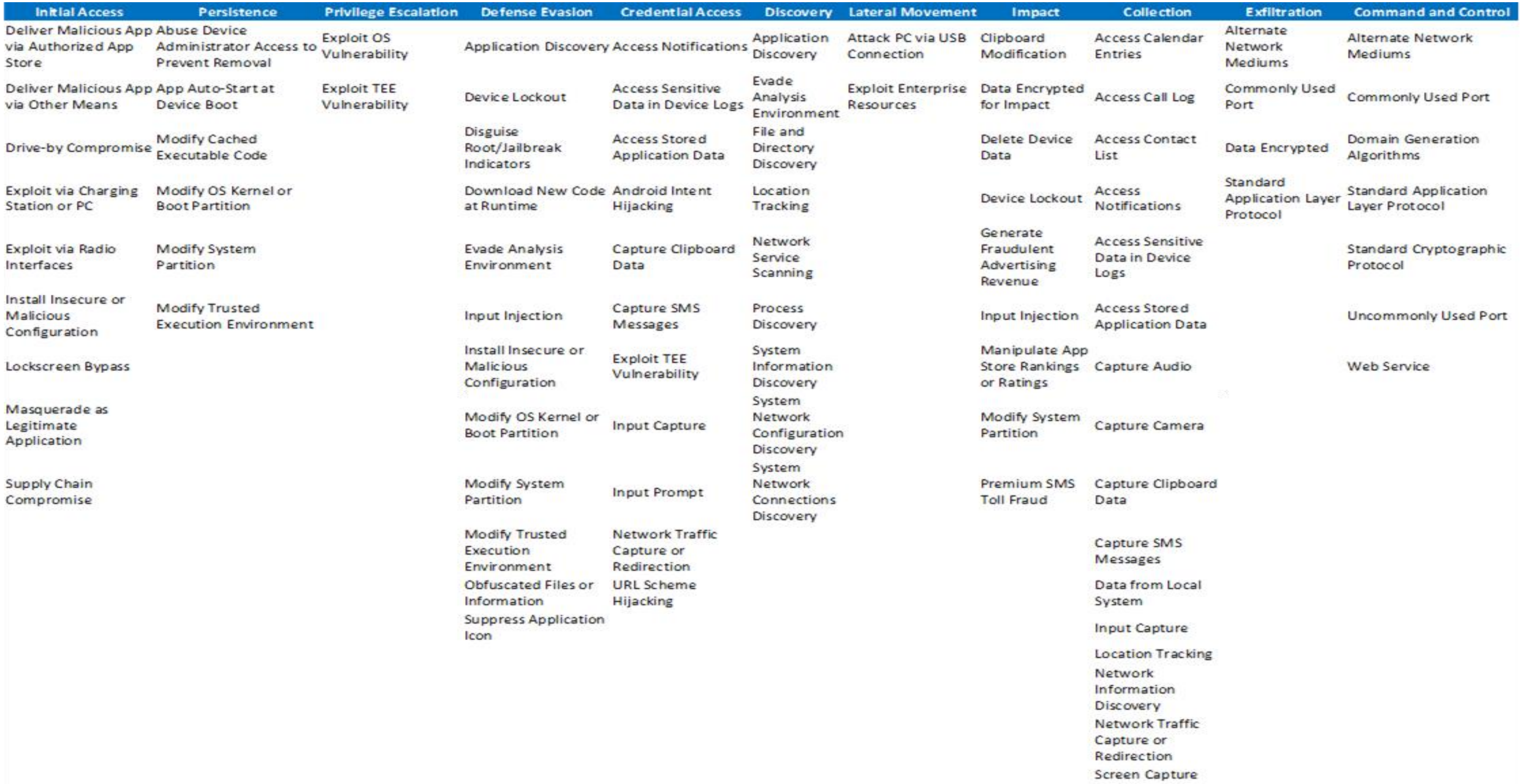


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery		Clipboard Data		Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force		Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping	Browser Bookmark Discovery			Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking			Credentials in Files		Exploitation of Remote Services	Data from Local System			Endpoint Denial of Service
	CMSTP	Image File Execution Options Injection			Credentials in Registry	Domain Trust Discovery		Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Attachment	Command-Line Interface	Plist Modification			Exploitation for Credential Access	File and Directory Discovery	Logon Scripts				Inhibit System Recovery
Spearphishing Link	Compiled HTML File	Valid Accounts				Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service
Spearphishing via Service	Control Panel Items	Accessibility Features		BITS Jobs	Forced Authentication	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation		Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Execution through API	AppInit DLLs		CMSTP	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms		Service Stop
Valid Accounts	Execution through Module Load	Application Shimming		Code Signing	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser		Scheduled Transfer	Stored Data Manipulation
		Dylib Hijacking		Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Fallback Channels		Transmitted Data Manipulation
	Exploitation for Client Execution	File System Permissions Weakness		Component Firmware	Keychain	Query Registry		Video Capture	Multiband Communication		
		Hooking		Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Shared Webroot		Multi-hop Proxy		
	Graphical User Interface	Launch Daemon				Security Software Discovery	SSH Hijacking		Multilayer Encryption		
	InstallUtil	New Service		Control Panel Items	Password Filter DLL	System Information Discovery	Taint Shared Content		Multi-Stage Channels		
	Mshta	Path Interception		DCShadow	Private Keys		Third-party Software		Port Knocking		
	PowerShell	Port Monitors		Deobfuscate/Decode Files or Information	Securityd Memory	System Network Configuration Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	Service Registry Permissions Weakness			Two-Factor Authentication Interception		Windows Remote Management		Remote File Copy		
	Regsvr32	Setuid and Setgid		Disabling Security Tools		System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Startup Items		DLL Side-Loading							
	Scripting	Web Shell		Execution Guardrails		System Owner/User Discovery			Standard Cryptographic Protocol		
	Service Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Exploitation for Defense Evasion							
	Signed Binary Proxy Execution	Account Manipulation				System Service Discovery			Standard Non-Application Layer Protocol		
		Authentication Package	SID-History Injection	File Deletion		System Time Discovery					
	Signed Script Proxy Execution	BITS Jobs	Sudo	File Permissions Modification		Virtualization/Sandbox Evasion			Uncommonly Used Port		
		Bootkit	Sudo Caching						Web Service		
	Source	Browser Extensions		File System Logical Offsets							
	Space after Filename	Change Default File Association		Gatekeeper Bypass							
	Third-party Software			Group Policy Modification							
	Trusted Developer Utilities	Component Firmware		Hidden Files and Directories							
	User Execution	Component Object Model Hijacking		Hidden Users							
	Windows Management Instrumentation			Hidden Window							
		Create Account		HISTCONTROL							
	Windows Remote Management	External Remote Services		Indicator Blocking							
		Hidden Files and Directories		Indicator Removal from Tools							
	XSL Script Processing	Hypervisor									
		Kernel Modules and Extensions		Indicator Removal on Host							
				Indirect Command Execution							
		Launch Agent		Install Root Certificate							
		LC_LOAD_DYLIB Addition		InstallUtil							
		Login Item		Launchctl							
		Logon Scripts		LC_MAIN Hijacking							
		Modify Existing Service		Masquerading							
		Netsh Helper DLL		Modify Registry							
		Office Application Startup		Mshta							
		Port Knocking		Network Share Connection Removal							
		Rc.common									
		Redundant Access		NTFS File Attributes							
		Registry Run Keys / Startup Folder		Obfuscated Files or Information							
		Re-opened Applications		Port Knocking							
		Screensaver		Process Doppelgänging							
		Security Support Provider		Process Hollowing							
		Shortcut Modification		Redundant Access							
		SIP and Trust Provider Hijacking		Regsvcs/Regasm							
				Regsvr32							

MITRE ATT&CK™
Enterprise Framework

attack.mitre.org

MITRE ATT&CK - Mobile Matrix



Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command and Control
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection	Clipboard Modification	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Device Lockout	Access Sensitive Data in Device Logs	Evade Analysis Environment	Exploit Enterprise Resources	Data Encrypted for Impact	Access Call Log	Commonly Used Port	Commonly Used Port
Drive-by Compromise	Modify Cached Executable Code		Disguise Root/Jailbreak Indicators	Access Stored Application Data	File and Directory Discovery		Delete Device Data	Access Contact List	Data Encrypted	Domain Generation Algorithms
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Download New Code at Runtime	Android Intent Hijacking	Location Tracking		Device Lockout	Access Notifications	Standard Application Layer Protocol	Standard Application Layer Protocol
Exploit via Radio Interfaces	Modify System Partition		Evade Analysis Environment	Capture Clipboard Data	Network Service Scanning		Generate Fraudulent Advertising Revenue	Access Sensitive Data in Device Logs		Standard Cryptographic Protocol
Install Insecure or Malicious Configuration	Modify Trusted Execution Environment		Input Injection	Capture SMS Messages	Process Discovery		Input Injection	Access Stored Application Data		Uncommonly Used Port
Lockscreen Bypass			Install Insecure or Malicious Configuration	Exploit TEE Vulnerability	System Information Discovery		Manipulate App Store Rankings or Ratings	Capture Audio		Web Service
Masquerade as Legitimate Application			Modify OS Kernel or Boot Partition	Input Capture	System Network Configuration Discovery		Modify System Partition	Capture Camera		
Supply Chain Compromise			Modify System Partition	Input Prompt	System Network Connections Discovery		Premium SMS Toll Fraud	Capture Clipboard Data		
			Modify Trusted Execution Environment	Network Traffic Capture or Redirection				Capture SMS Messages		
			Obfuscated Files or Information	URL Scheme Hijacking				Data from Local System		
			Suppress Application Icon					Input Capture		
								Location Tracking		
								Network Information Discovery		
								Network Traffic Capture or Redirection		
								Screen Capture		

A Few Questions to Ask Yourself

- How Effective are my Defenses?
- How do I Measure it?
- Do I have a Chance of detecting APTs?
- How Useful is the Data I am collecting?

MITRE ATT&CK Use Cases

Threat Intelligence

Detect & Analyze

Red Team & Adversary Emulation

Assessment & Response

Attack Navigator

In this workshop:

- ☑ MITRE ATT&CK overview
- □ **Best Practices that will Boost your skills:**
  - □ Visualize
  - □ Assess Risks
  - □ Map your Coverage
  - □ Investigate
  - □ Prevent
- □ Check Point’s solution value
- □ Takeaways you can apply

Best Practices

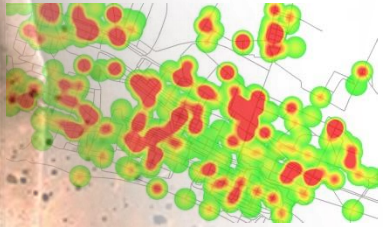
Boost your SECURITY capabilities

ATT&CK Best Practices

Visuali

Attacks, Advers

PREVENT

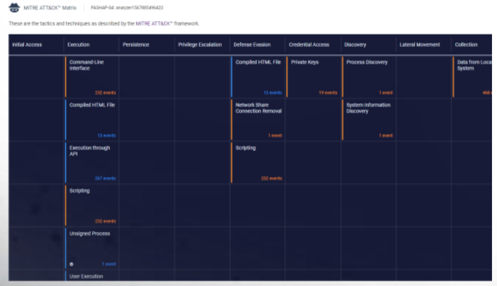


Map

Risks, Defense Gaps

Investigate

Attacks, Incidents



MITRE ATT&CK™ Matrix | PASHAP-04: analyzer1567885496423

These are the tactics and techniques as described by the MITRE ATT&CK™ framework.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
	Command-Line Interface 232 events			Compiled HTML File 13 events	Private Keys 19 events	Process Discovery 1 event		Data from Loca System 468
	Compiled HTML File 13 events			Network Share Connection Removal 1 event		System Information Discovery 1 event		
	Execution through API 267 events			Scripting 232 events				
	Scripting 232 events							
	Unsigned Process 1 event							
	User Execution							

In this workshop:

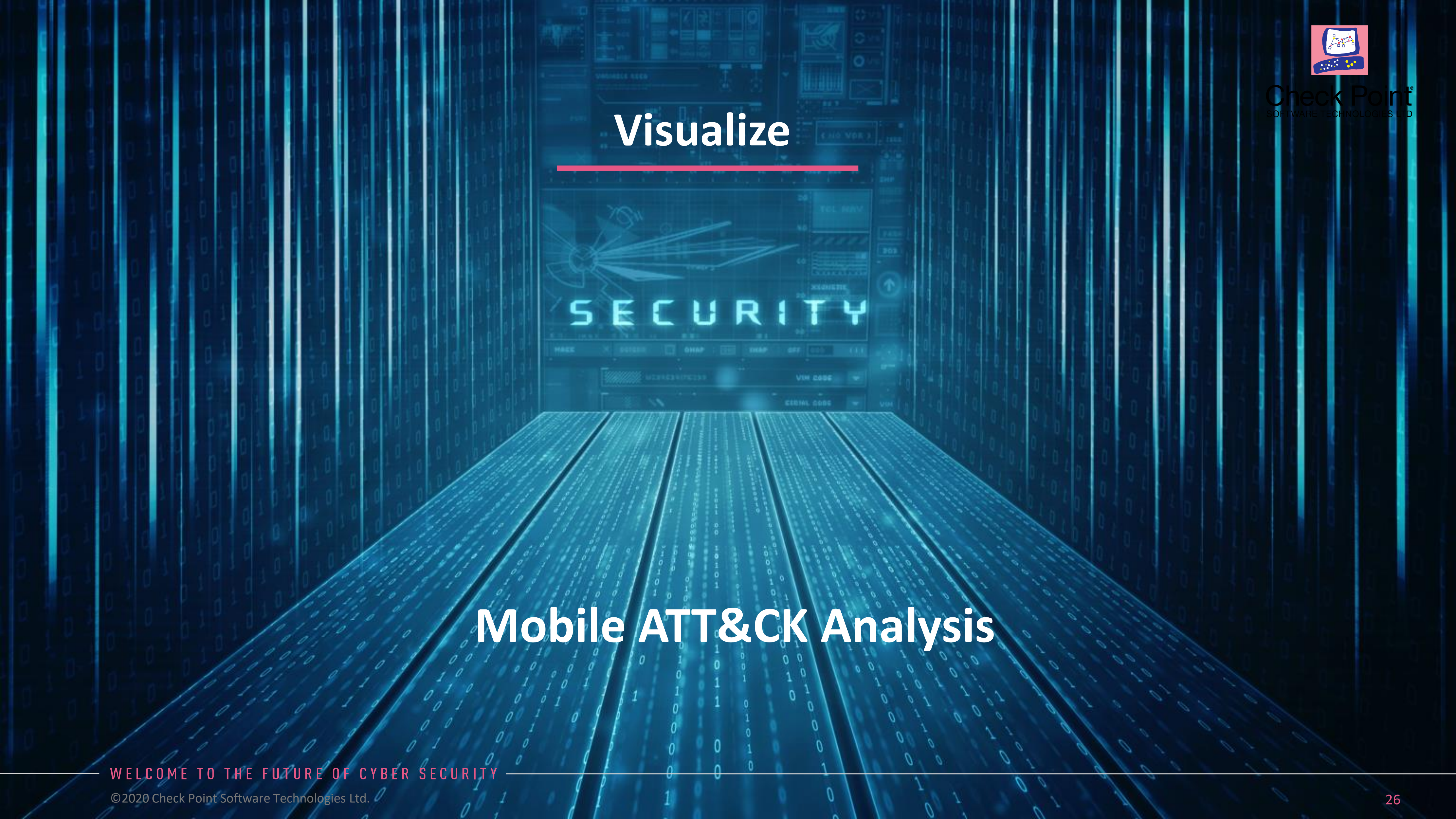
☑ MITRE ATT&CK overview

□ Best Practices that will Boost your skills:

- □ **Visualize**
- □ Assess Risks
- □ Map your Coverage
- □ Investigate
- □ Prevent

□ Check Point’s solution value

□ Takeaways you can apply

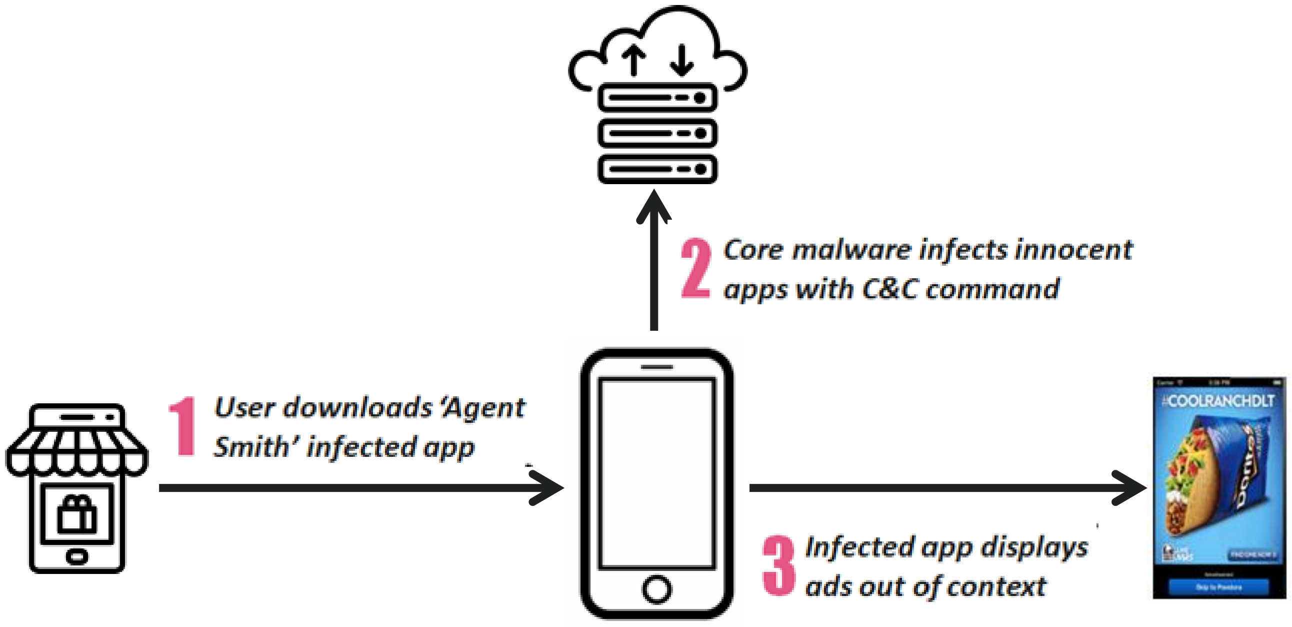


Visualize

Mobile ATT&CK Analysis

“Agent Smith” Mobile Malware

Discovered by Check Point’s research team



1 *User downloads ‘Agent Smith’ infected app*

2 *Core malware infects innocent apps with C&C command*

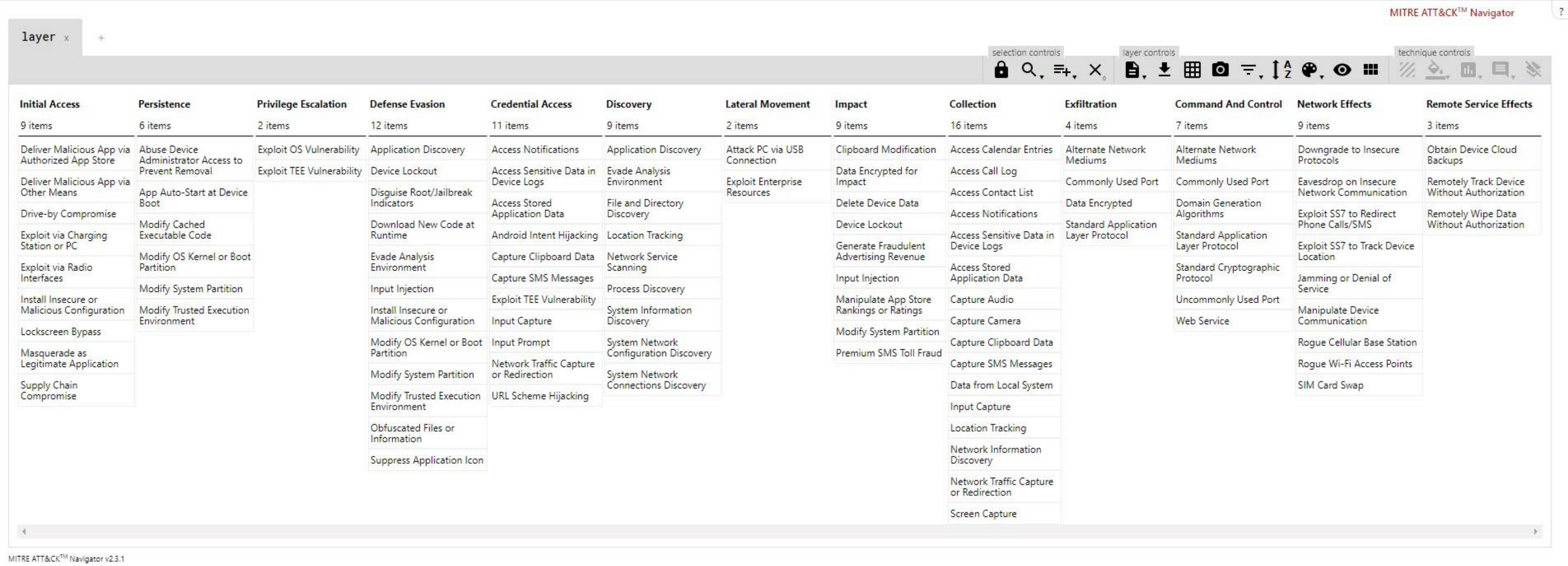
3 *Infected app displays ads out of context*

Agent Smith Attack Methods
Dormant versions on Play Store
Injected into legitimate apps
Listen on BOOT_COMPLETE
Exploit OS Vulnerability (Janus, Feng-Shui, Bundle)
Enumerate all apps
payload masked as JPG
Hide Icon
Man-in-the-Disk for specific apps
Calls ads for every intent of original app

Agent Smith – MITRE ATT&CK

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Agent Smith Attack Methods
Initial Access	Deliver Malicious App via Authorized App Store	Dormant versions on Play Store
	Masquerade as Legitimate Application	Injected into legitimate apps
Persistence	App Auto-Start at Device Boot	Listen on BOOT_COMPLETE
Privilege Escalation	Exploit OS Vulnerability	Janus, Feng-Shui, Bundle
Defense Evasion	Application Discovery	Enumerate all apps
	Obfuscated Files or Information	Payload masked as JPG
	Suppress Application Icon	Hide Icon
Credential Access	Access Stored Application Data	Man-in-the-Disk for specific apps
	Android Intent Hijacking	Calls ads for every intent of original app

ATT&CK Navigator Best Practices - Visualize



Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command And Control	Network Effects	Remote Service Effects
9 items	6 items	2 items	12 items	11 items	9 items	2 items	9 items	16 items	4 items	7 items	9 items	3 items
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection	Clipboard Modification	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums	Downgrade to Insecure Protocols	Obtain Device Cloud Backups
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Device Lockout	Access Sensitive Data in Device Logs	Evade Analysis Environment	Exploit Enterprise Resources	Data Encrypted for Impact	Access Call Log	Commonly Used Port	Commonly Used Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Drive-by Compromise	Modify Cached Executable Code		Disguise Root/Jailbreak Indicators	Access Stored Application Data	File and Directory Discovery		Delete Device Data	Access Contact List	Data Encrypted	Domain Generation Algorithms	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Download New Code at Runtime	Android Intent Hijacking	Location Tracking		Device Lockout	Access Notifications	Standard Application Layer Protocol	Standard Application Layer Protocol	Exploit SS7 to Track Device Location	
Exploit via Radio Interfaces	Modify System Partition		Evade Analysis Environment	Capture Clipboard Data	Network Service Scanning		Generate Fraudulent Advertising Revenue	Access Sensitive Data in Device Logs		Standard Cryptographic Protocol	Jamming or Denial of Service	
Install Insecure or Malicious Configuration	Modify Trusted Execution Environment		Input Injection	Capture SMS Messages	Process Discovery		Input Injection	Access Stored Application Data		Uncommonly Used Port	Manipulate Device Communication	
Lockscreen Bypass			Install Insecure or Malicious Configuration	Exploit TEE Vulnerability	System Information Discovery		Manipulate App Store Rankings or Ratings	Capture Audio		Web Service	Rogue Cellular Base Station	
Masquerade as Legitimate Application			Modify OS Kernel or Boot Partition	Input Capture	System Network Configuration Discovery		Modify System Partition	Capture Camera			Rogue Wi-Fi Access Points	
Supply Chain Compromise			Modify System Partition	Input Prompt	System Network Connections Discovery		Premium SMS Toll Fraud	Capture Clipboard Data			SIM Card Swap	
			Modify Trusted Execution Environment	Network Traffic Capture or Redirection				Capture SMS Messages				
			Obfuscated Files or Information	URL Scheme Hijacking				Data from Local System				
			Suppress Application Icon					Input Capture				
								Location Tracking				
								Network Information Discovery				
								Network Traffic Capture or Redirection				
								Screen Capture				

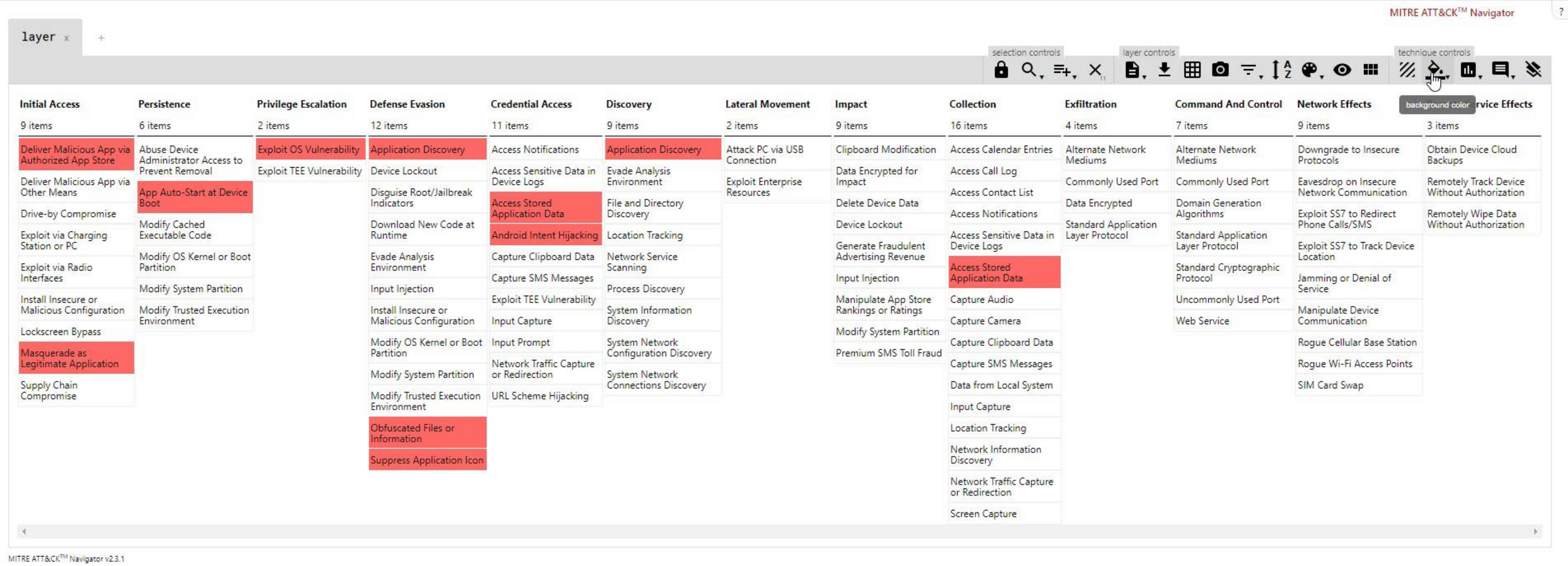
In this workshop:

- ☑ MITRE ATT&CK overview
- □ Best Practices that will Boost your skills:
  - ☑ Visualize
  - □ **Assess Risks**
  - □ Map your Coverage
  - □ Investigate
  - □ Prevent
- □ Check Point’s solution value
- □ Takeaways you can apply

Assess Risks

Know your Weak Points

ATT&CK Navigator Best Practices – Assess Risks

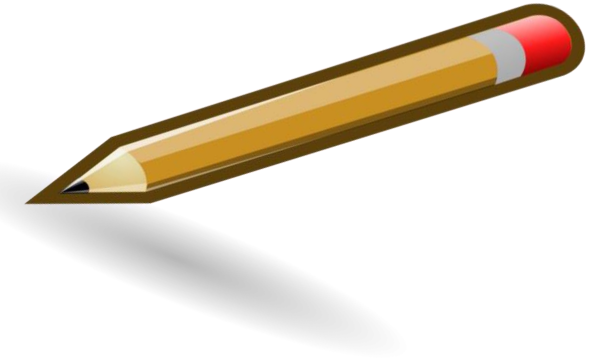


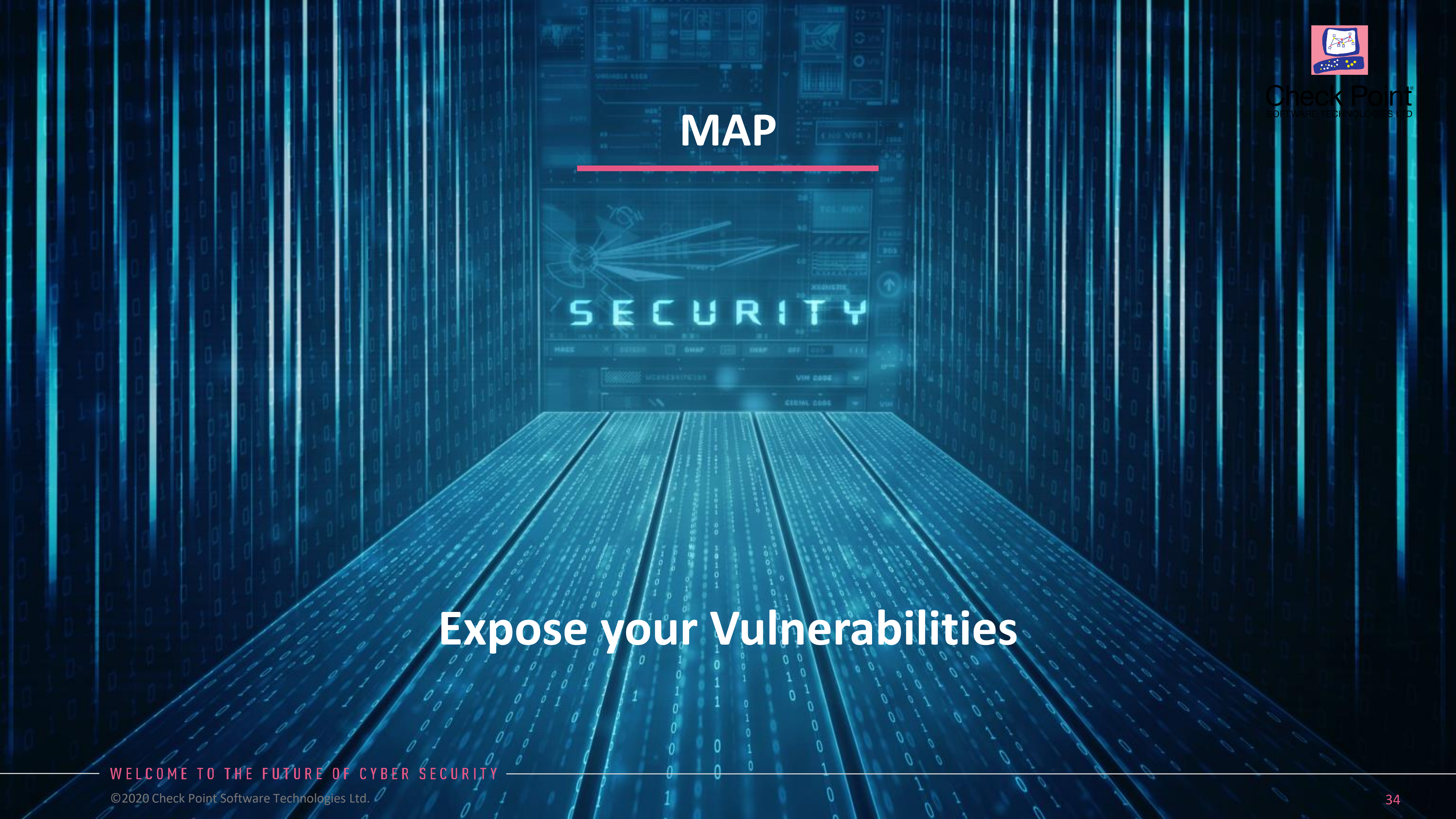
Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command And Control	Network Effects	rvice Effects
9 items	6 items	2 items	12 items	11 items	9 items	2 items	9 items	16 items	4 items	7 items	9 items	3 items
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection	Clipboard Modification	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums	Downgrade to Insecure Protocols	Obtain Device Cloud Backups
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Device Lockout	Access Sensitive Data in Device Logs	Evade Analysis Environment	Exploit Enterprise Resources	Data Encrypted for Impact	Access Call Log	Commonly Used Port	Commonly Used Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Drive-by Compromise	Modify Cached Executable Code		Disguise Root/Jailbreak Indicators	Access Stored Application Data	File and Directory Discovery		Delete Device Data	Access Contact List	Data Encrypted	Domain Generation Algorithms	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Download New Code at Runtime	Android Intent Hijacking	Location Tracking		Device Lockout	Access Notifications	Standard Application Layer Protocol	Standard Application Layer Protocol	Exploit SS7 to Track Device Location	
Exploit via Radio Interfaces	Modify System Partition		Evade Analysis Environment	Capture Clipboard Data	Network Service Scanning		Generate Fraudulent Advertising Revenue	Access Sensitive Data in Device Logs		Standard Cryptographic Protocol	Jamming or Denial of Service	
Install Insecure or Malicious Configuration	Modify Trusted Execution Environment		Input Injection	Capture SMS Messages	Process Discovery		Input Injection	Access Stored Application Data		Uncommonly Used Port	Manipulate Device Communication	
Lockscreen Bypass			Install Insecure or Malicious Configuration	Exploit TEE Vulnerability	System Information Discovery		Manipulate App Store Rankings or Ratings	Capture Audio		Web Service	Rogue Cellular Base Station	
Masquerade as Legitimate Application			Modify OS Kernel or Boot Partition	Input Capture	System Network Configuration Discovery		Modify System Partition	Capture Camera			Rogue Wi-Fi Access Points	
Supply Chain Compromise			Modify System Partition	Input Prompt	System Network Connections Discovery		Premium SMS Toll Fraud	Capture Clipboard Data			SIM Card Swap	
			Modify Trusted Execution Environment	Network Traffic Capture or Redirection				Capture SMS Messages				
			Obfuscated Files or Information	URL Scheme Hijacking				Data from Local System				
			Suppress Application Icon					Input Capture				
								Location Tracking				
								Network Information Discovery				
								Network Traffic Capture or Redirection				
								Screen Capture				

MITRE ATT&CK™ Navigator v2.3.1

In this workshop:

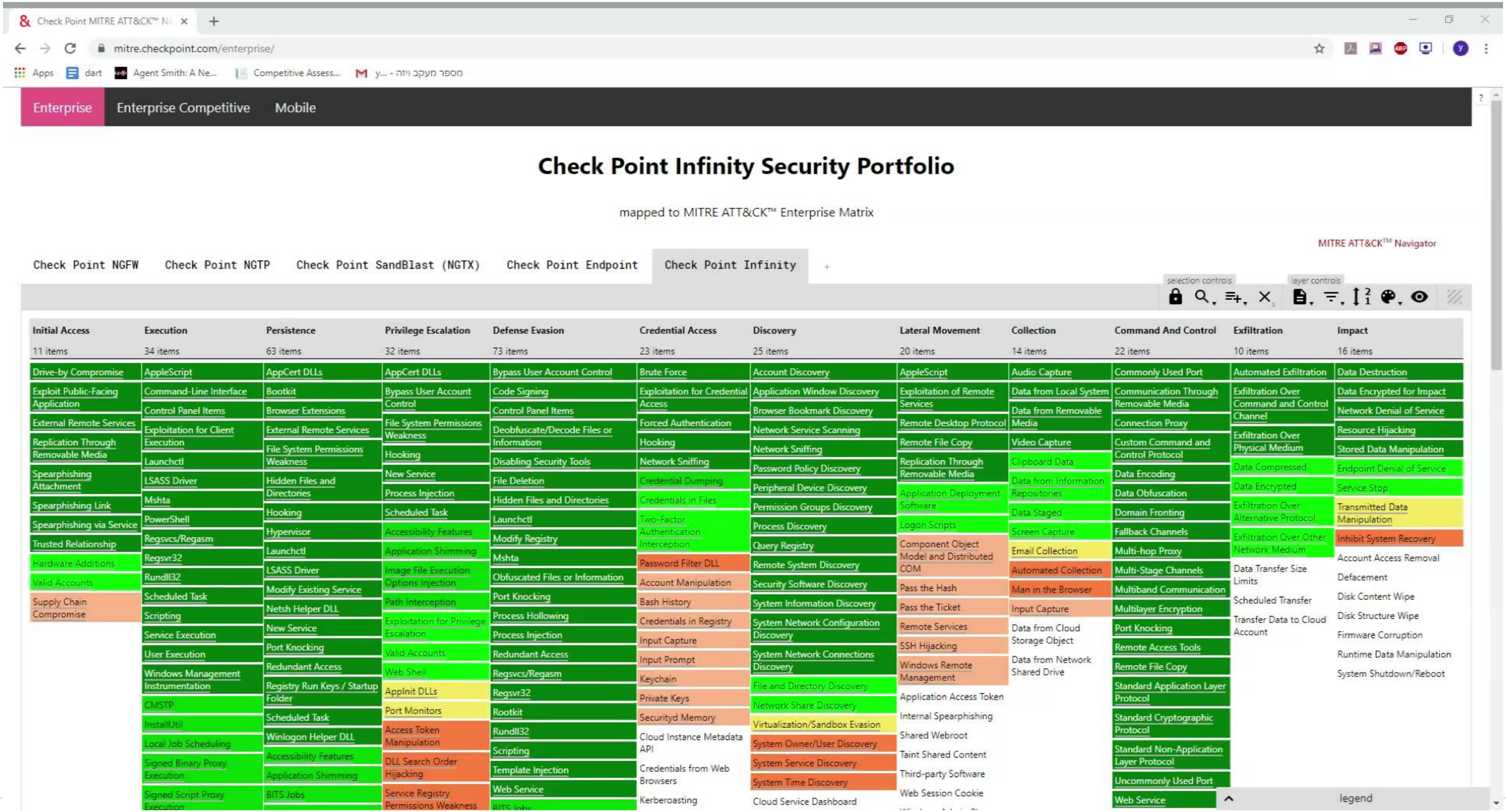
- ☑ MITRE ATT&CK overview
- □ Best Practices that will Boost your skills:
  - ☑ Visualize
  - ☑ Assess Risks
  - □ **Map your Coverage**
  - □ Investigate
  - □ Prevent
- □ Check Point’s solution value
- □ Takeaways you can apply





MAP

Expose your Vulnerabilities



Enterprise | Enterprise Competitive | Mobile

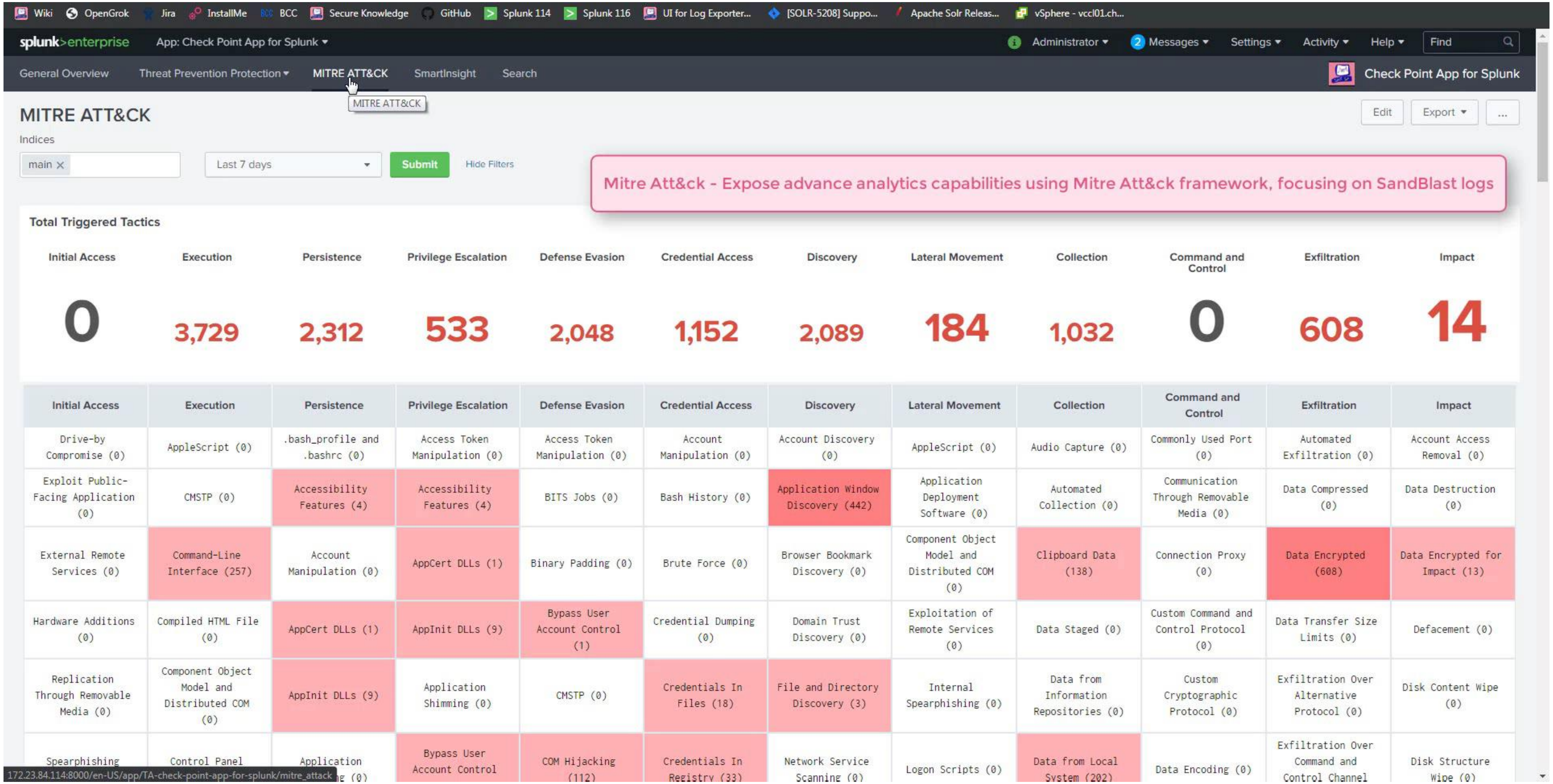
Check Point Infinity Security Portfolio

mapped to MITRE ATT&CK™ Enterprise Matrix

Check Point NGFW | Check Point NGTP | Check Point SandBlast (NGTX) | Check Point Endpoint | Check Point Infinity | +

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	63 items	32 items	73 items	23 items	25 items	20 items	14 items	22 items	10 items	16 items
Drive-by Compromise	AppleScript	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Bootkit	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Application Window Discovery	Exploitation of Remote Services	Data from Local System	Communication Through Removable Media	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
External Remote Services	Control Panel Items	Browser Extensions	File System Permissions Weakness	Control Panel Items	Forced Authentication	Browser Bookmark Discovery	Remote Desktop Protocol	Data from Removable Media	Connection Proxy	Exfiltration Over Physical Medium	Network Denial of Service
Replication Through Removable Media	Exploitation for Client Execution	External Remote Services	Hooking	Deobfuscate/Decode Files or Information	Hooking	Network Service Scanning	Remote File Copy	Video Capture	Custom Command and Control Protocol	Data Compressed	Resource Hijacking
Spearphishing Attachment	Launchctl	File System Permissions Weakness	New Service	Disabling Security Tools	Network Sniffing	Network Sniffing	Replication Through Removable Media	Clipboard Data	Data Encoding	Data Encrypted	Stored Data Manipulation
Spearphishing Link	LSASS Driver	Hidden Files and Directories	Process Injection	File Deletion	Credential Dumping	Password Policy Discovery	Application Deployment Software	Data from Information Repositories	Data Obfuscation	Exfiltration Over Alternative Protocol	Endpoint Denial of Service
Spearphishing via Service	Mshta	Hooking	Scheduled Task	Hidden Files and Directories	Credentials in Files	Peripheral Device Discovery	Logon Scripts	Data Staged	Domain Fronting	Exfiltration Over Other Network Medium	Service Stop
Trusted Relationship	PowerShell	Hypervisor	Accessibility Features	Launchctl	Two-Factor Authentication Interception	Permission Groups Discovery	Component Object Model and Distributed COM	Screen Capture	Fallback Channels	Data Transfer Size Limits	Transmitted Data Manipulation
Hardware Additions	Regsvcs/Regasm	Launchctl	Application Shimming	Modify Registry	Password Filter DLL	Process Discovery	Pass the Hash	Email Collection	Multi-hop Proxy	Scheduled Transfer	Inhibit System Recovery
Valid Accounts	Regsvr32	LSASS Driver	Image File Execution Options Injection	Mshta	Account Manipulation	Query Registry	Pass the Ticket	Automated Collection	Multi-Stage Channels	Transfer Data to Cloud Account	Account Access Removal
Supply Chain Compromise	Rundll32	Modify Existing Service	Path Interception	Obfuscated Files or Information	Bash History	Remote System Discovery	Remote Services	Man in the Browser	Multiband Communication		Defacement
	Scheduled Task	Netsh Helper DLL	Exploitation for Privilege Escalation	Port Knocking	Credentials in Registry	Security Software Discovery	SSH Hijacking	Input Capture	Multilayer Encryption		Disk Content Wipe
	Scripting	New Service	Valid Accounts	Process Hollowing	Input Capture	System Information Discovery	Windows Remote Management	Data from Cloud Storage Object	Port Knocking		Disk Structure Wipe
	Service Execution	Port Knocking	Web Shell	Process Injection	Input Prompt	System Network Configuration Discovery	Application Access Token	Data from Network Shared Drive	Remote Access Tools		Firmware Corruption
	User Execution	Redundant Access	AppInit DLLs	Redundant Access	Keychain	System Network Connections Discovery	Internal Spearphishing		Remote File Copy		Runtime Data Manipulation
	Windows Management Instrumentation	Registry Run Keys / Startup Folder	Port Monitors	Regsvcs/Regasm	Private Keys	File and Directory Discovery	Shared Webroot		Standard Application Layer Protocol		System Shutdown/Reboot
	CMSTP	Scheduled Task	Access Token Manipulation	Regsvr32	Securityd Memory	Network Share Discovery	Taint Shared Content		Standard Cryptographic Protocol		
	InstallUtil	Winlogon Helper DLL	DLL Search Order Hijacking	Rootkit	Cloud Instance Metadata API	Virtualization/Sandbox Evasion	Third-party Software		Standard Non-Application Layer Protocol		
	Local Job Scheduling	Accessibility Features	Service Registry Permissions Weakness	Rundll32	Credentials from Web Browsers	System Owner/User Discovery	Web Session Cookie		Uncommonly Used Port		
	Signed Binary Proxy Execution	Application Shimming		Scripting	Kerberoasting	System Service Discovery			Web Service		
	Signed Script Proxy Execution	BITS Jobs		Template Injection		System Time Discovery					
				Web Service		Cloud Service Dashboard					
				BITS Jobs							

ATT&CK Navigator Best Practices – Map – CP Splunk app



MITRE ATT&CK

Indices: main ×

Last 7 days

Submit

Hide Filters

Mitre Att&ck - Expose advance analytics capabilities using Mitre Att&ck framework, focusing on SandBlast logs

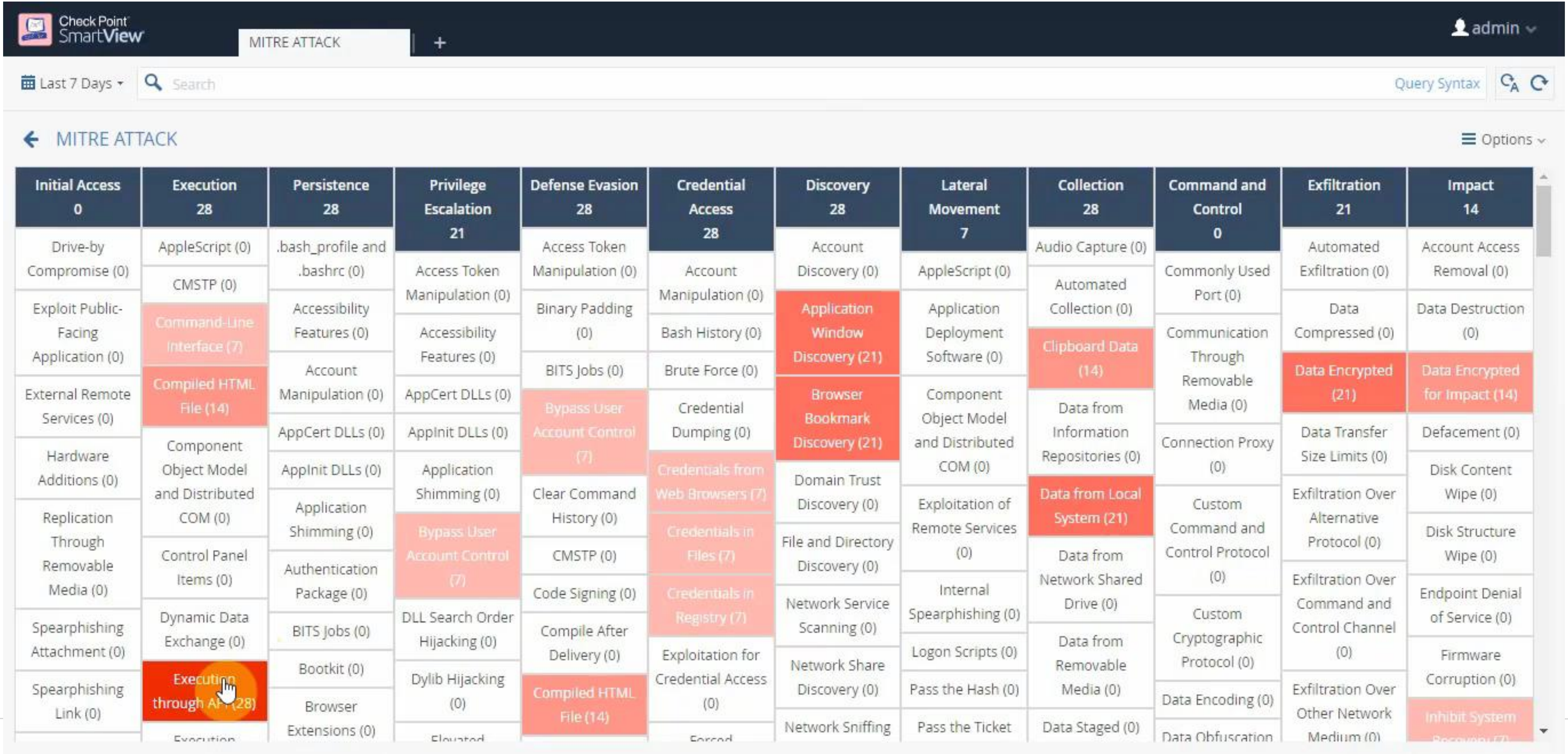
Total Triggered Tactics

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
0	3,729	2,312	533	2,048	1,152	2,089	184	1,032	0	608	14

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise (0)	AppleScript (0)	.bash_profile and .bashrc (0)	Access Token Manipulation (0)	Access Token Manipulation (0)	Account Manipulation (0)	Account Discovery (0)	AppleScript (0)	Audio Capture (0)	Commonly Used Port (0)	Automated Exfiltration (0)	Account Access Removal (0)
Exploit Public-Facing Application (0)	CMSTP (0)	Accessibility Features (4)	Accessibility Features (4)	BITS Jobs (0)	Bash History (0)	Application Window Discovery (442)	Application Deployment Software (0)	Automated Collection (0)	Communication Through Removable Media (0)	Data Compressed (0)	Data Destruction (0)
External Remote Services (0)	Command-Line Interface (257)	Account Manipulation (0)	AppCert DLLs (1)	Binary Padding (0)	Brute Force (0)	Browser Bookmark Discovery (0)	Component Object Model and Distributed COM (0)	Clipboard Data (138)	Connection Proxy (0)	Data Encrypted (608)	Data Encrypted for Impact (13)
Hardware Additions (0)	Compiled HTML File (0)	AppCert DLLs (1)	AppInit DLLs (9)	Bypass User Account Control (1)	Credential Dumping (0)	Domain Trust Discovery (0)	Exploitation of Remote Services (0)	Data Staged (0)	Custom Command and Control Protocol (0)	Data Transfer Size Limits (0)	Defacement (0)
Replication Through Removable Media (0)	Component Object Model and Distributed COM (0)	AppInit DLLs (9)	Application Shimming (0)	CMSTP (0)	Credentials In Files (18)	File and Directory Discovery (3)	Internal Spearphishing (0)	Data from Information Repositories (0)	Custom Cryptographic Protocol (0)	Exfiltration Over Alternative Protocol (0)	Disk Content Wipe (0)
Spearphishing	Control Panel	Application g (0)	Bypass User Account Control	COM Hijacking (112)	Credentials In Registry (33)	Network Service Scanning (0)	Logon Scripts (0)	Data from Local System (202)	Data Encoding (0)	Exfiltration Over Command and Control Channel	Disk Structure Wipe (0)

172.23.84.114:8000/en-US/app/TA-check-point-app-for-splunk/mitre_attack

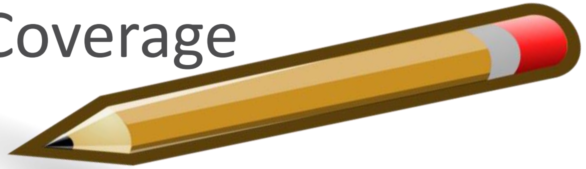
ATT&CK Navigator Best Practices – Map – SmartEvent



Initial Access 0	Execution 28	Persistence 28	Privilege Escalation 21	Defense Evasion 28	Credential Access 28	Discovery 28	Lateral Movement 7	Collection 28	Command and Control 0	Exfiltration 21	Impact 14
Drive-by Compromise (0)	AppleScript (0)	.bash_profile and .bashrc (0)	Access Token Manipulation (0)	Access Token Manipulation (0)	Account Manipulation (0)	Account Discovery (0)	AppleScript (0)	Audio Capture (0)	Commonly Used Port (0)	Automated Exfiltration (0)	Account Access Removal (0)
Exploit Public-Facing Application (0)	CMSTP (0)	Accessibility Features (0)	Accessibility Features (0)	Binary Padding (0)	Bash History (0)	Application Window Discovery (21)	Application Deployment Software (0)	Automated Collection (0)	Communication Through Removable Media (0)	Data Compressed (0)	Data Destruction (0)
External Remote Services (0)	Command-Line Interface (7)	Account Manipulation (0)	AppCert DLLs (0)	BITS Jobs (0)	Brute Force (0)	Browser Bookmark Discovery (21)	Component Object Model and Distributed COM (0)	Clipboard Data (14)	Connection Proxy (0)	Data Encrypted (21)	Data Encrypted for Impact (14)
Hardware Additions (0)	Compiled HTML File (14)	AppCert DLLs (0)	AppInit DLLs (0)	Bypass User Account Control (7)	Credential Dumping (0)	Domain Trust Discovery (0)	Exploitation of Remote Services (0)	Data from Information Repositories (0)	Custom Command and Control Protocol (0)	Data Transfer Size Limits (0)	Defacement (0)
Replication Through Removable Media (0)	Component Object Model and Distributed COM (0)	AppInit DLLs (0)	Application Shimming (0)	Clear Command History (0)	Credentials from Web Browsers (7)	File and Directory Discovery (0)	Internal Spearphishing (0)	Data from Local System (21)	Custom Cryptographic Protocol (0)	Exfiltration Over Alternative Protocol (0)	Disk Content Wipe (0)
Spearphishing Attachment (0)	Control Panel Items (0)	Application Shimming (0)	Bypass User Account Control (7)	CMSTP (0)	Credentials in Files (7)	Network Service Scanning (0)	Logon Scripts (0)	Data from Network Shared Drive (0)	Data Encoding (0)	Exfiltration Over Command and Control Channel (0)	Disk Structure Wipe (0)
Spearphishing Link (0)	Dynamic Data Exchange (0)	Authentication Package (0)	DLL Search Order Hijacking (0)	Code Signing (0)	Credentials in Registry (7)	Network Share Discovery (0)	Pass the Hash (0)	Data from Removable Media (0)	Data Obfuscation	Exfiltration Over Other Network Medium (0)	Endpoint Denial of Service (0)
	Execution through API (28)	BITS Jobs (0)	Dylib Hijacking (0)	Compile After Delivery (0)	Exploitation for Credential Access (0)	Network Sniffing	Pass the Ticket	Data Staged (0)			Firmware Corruption (0)
	Execution	Bootkit (0)	Elevated	Compiled HTML File (14)	Forced						Inhibit System Recovery (7)
		Browser Extensions (0)									

In this workshop:

- ☑ MITRE ATT&CK overview
- □ Best Practices that will Boost your skills:
  - ☑ Visualize
  - ☑ Assess Risks
  - ☑ Map your Coverage
  - □ **Investigate**
  - □ Prevent



- □ Check Point’s solution value
- □ Takeaways you can apply

Investigate

RobbinHood ATT&CK Analysis

“RobbinHood” Ransomware

Demands payment in exchange for decryption

The New York Times

Hackers Are Holding Baltimore Hostage: How They Struck and What’s Next

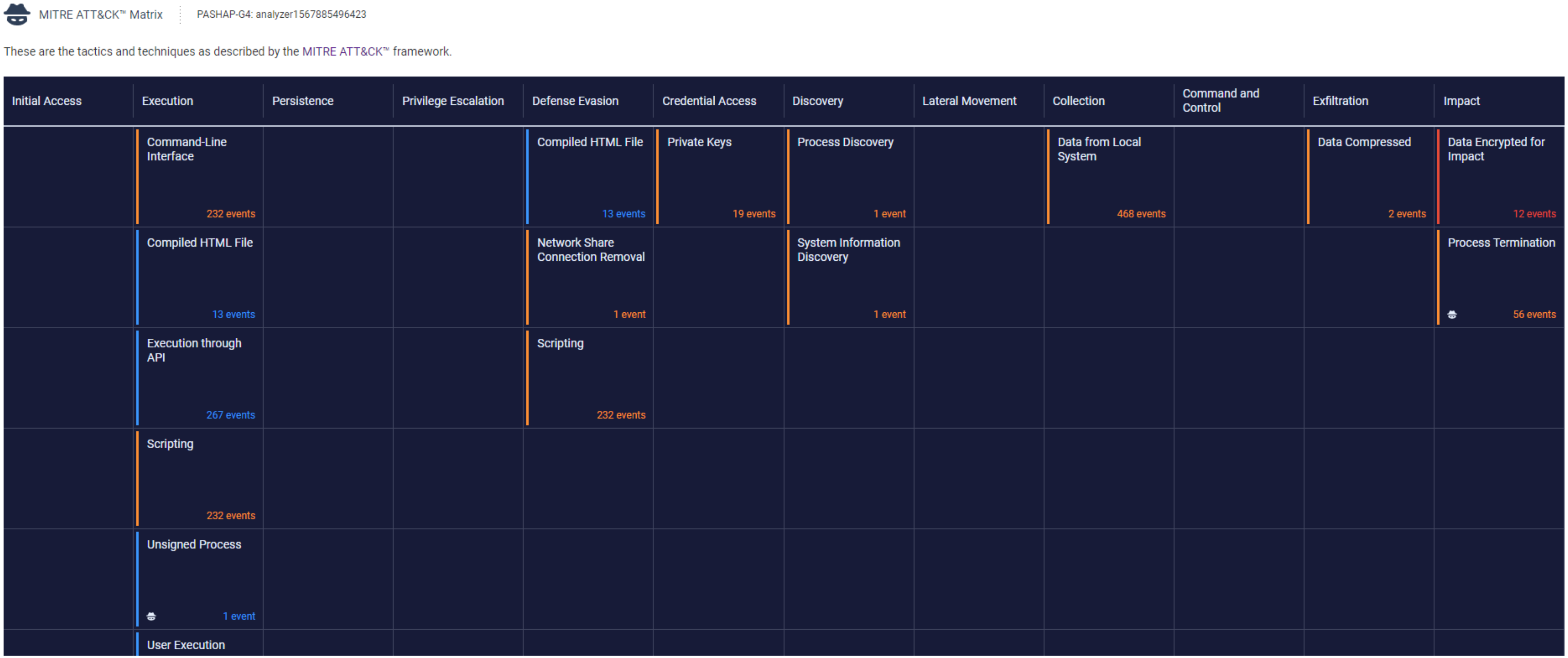
After it was hit by a ransomware attack, Baltimore immediately notified the F.B.I. and took systems offline, but not before several of them were affected. Gabriella Demczuk for The New York Times

RobbinHood – Tactics

➢ Execution	Command-line, API’s and other techniques.
➢ Defense Evasion	Removed share connections.
➢ Credential Access	Accessed encryption keys.
➢ Discovery	Gathered OS and processes information.
➢ Collection	Collected information from the system.
➢ Exfiltration	Data was compressed.
➢ Impact	Encrypted data and stopped services.

“RobbinHood” Phishing + RDP Attack

Sandblast Agent “RobbinHood” Full Forensics Report



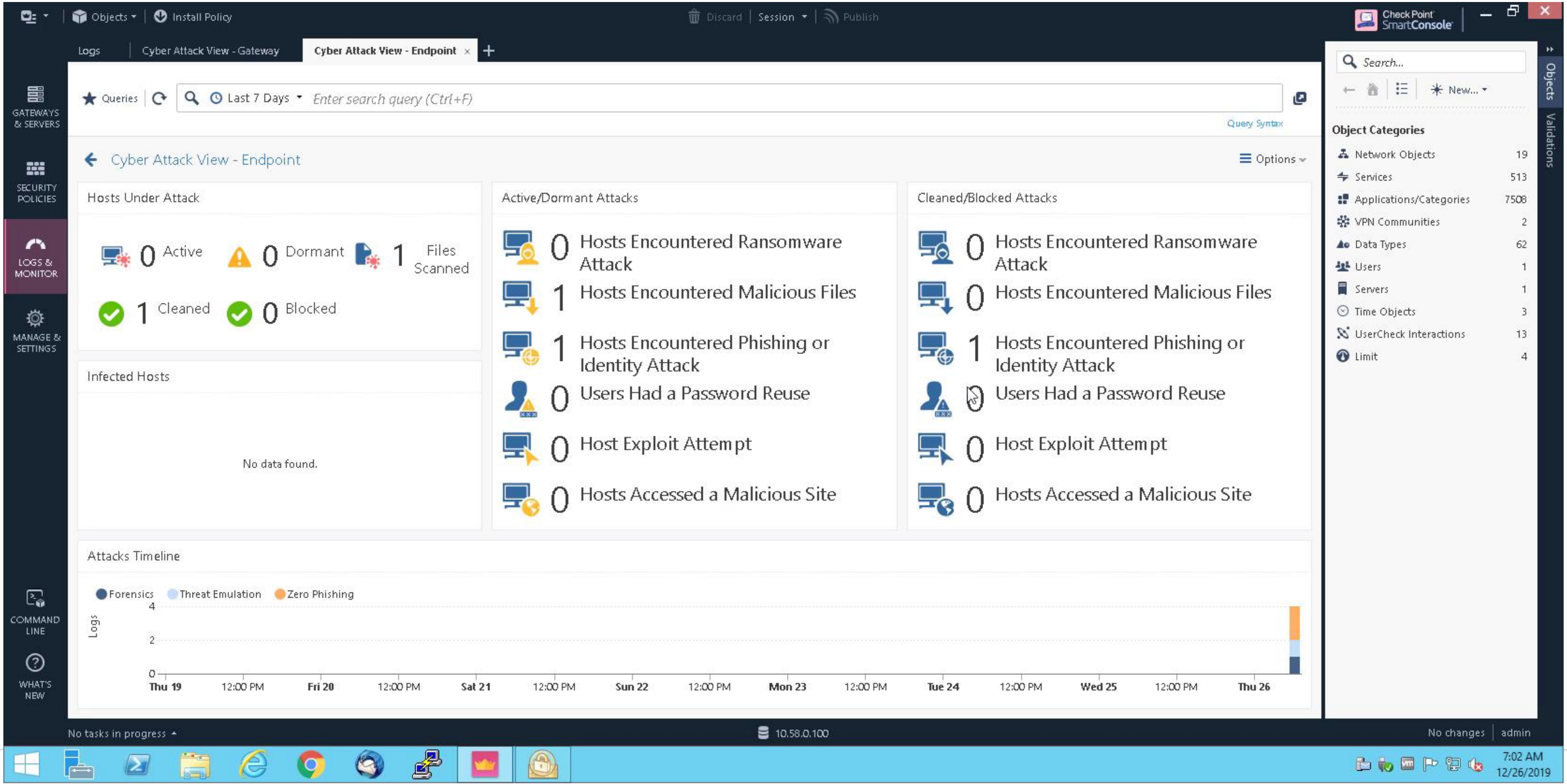
MITRE ATT&CK™ Matrix PASHAP-G4: analyzer1567885496423

These are the tactics and techniques as described by the MITRE ATT&CK™ framework.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Command-Line Interface 232 events			Compiled HTML File 13 events	Private Keys 19 events	Process Discovery 1 event		Data from Local System 468 events		Data Compressed 2 events	Data Encrypted for Impact 12 events
	Compiled HTML File 13 events			Network Share Connection Removal 1 event		System Information Discovery 1 event					Process Termination 56 events
	Execution through API 267 events			Scripting 232 events							
	Scripting 232 events										
	Unsigned Process 1 event										
	User Execution										

https://forensics.checkpoint.com/robinhood/

Sandblast Agent
“RobbinHood” Attack Prevention and Analysis



Cyber Attack View - Endpoint

Hosts Under Attack

0 Active · 0 Dormant · 1 Files Scanned

1 Cleaned · 0 Blocked

Active/Dormant Attacks

0	Hosts Encountered Ransomware Attack
1	Hosts Encountered Malicious Files
1	Hosts Encountered Phishing or Identity Attack
0	Users Had a Password Reuse
0	Host Exploit Attempt
0	Hosts Accessed a Malicious Site

Cleaned/Blocked Attacks

0	Hosts Encountered Ransomware Attack
0	Hosts Encountered Malicious Files
1	Hosts Encountered Phishing or Identity Attack
0	Users Had a Password Reuse
0	Host Exploit Attempt
0	Hosts Accessed a Malicious Site

Infected Hosts

No data found.

Attacks Timeline

Object Categories

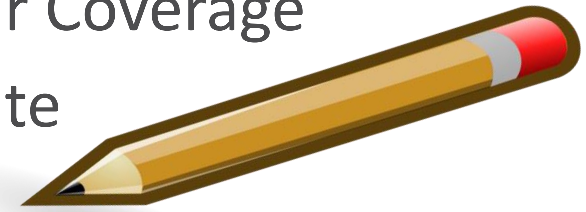
Network Objects	19
Services	513
Applications/Categories	7508
VPN Communities	2
Data Types	62
Users	1
Servers	1
Time Objects	3
UserCheck Interactions	13
Limit	4

No tasks in progress · 10.58.0.100 · No changes · admin

7:02 AM 12/26/2019

In this workshop:

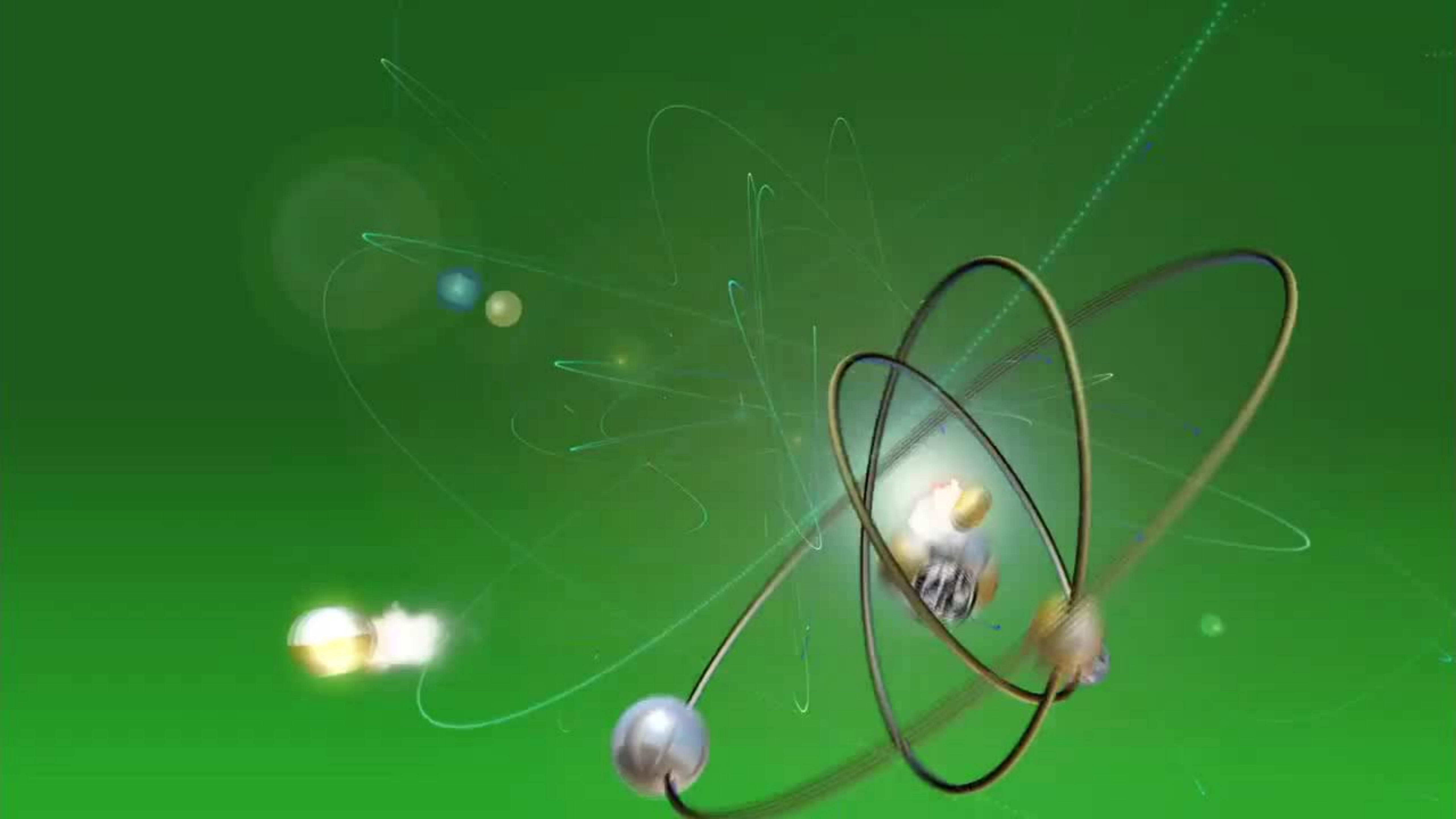
- ☑ MITRE ATT&CK overview
- □ Best Practices that will Boost your skills:
  - ☑ Visualize
  - ☑ Assess Risks
  - ☑ Map your Coverage
  - ☑ Investigate
  - □ **Prevent**



- □ Check Point's solution value
- □ Takeaways you can apply

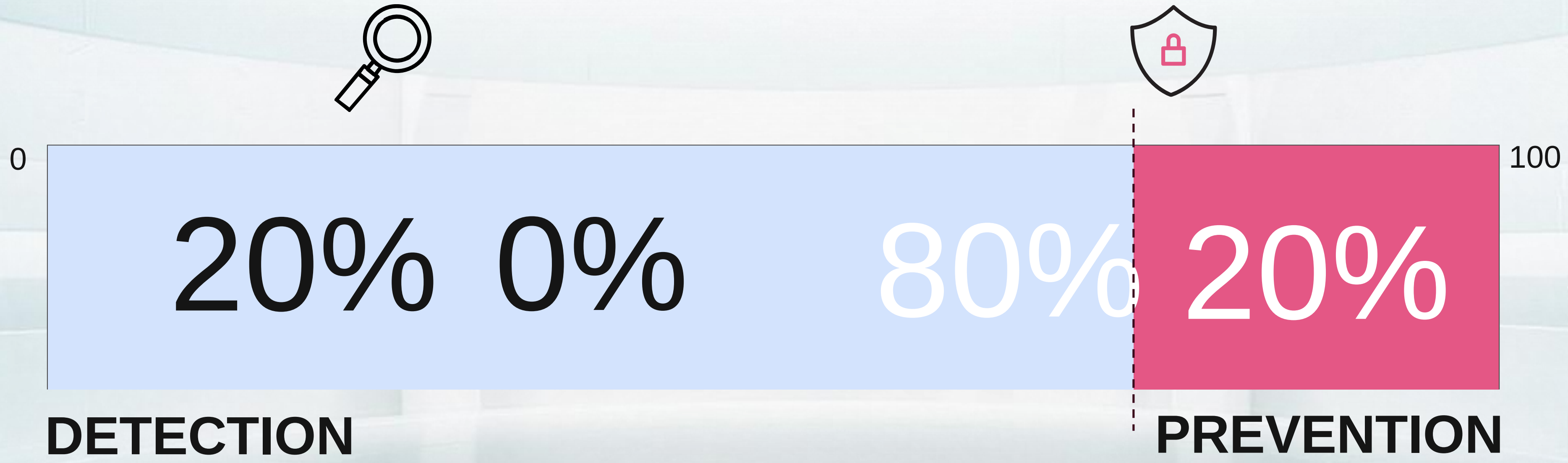
Prevent

ATT&CK Prevention



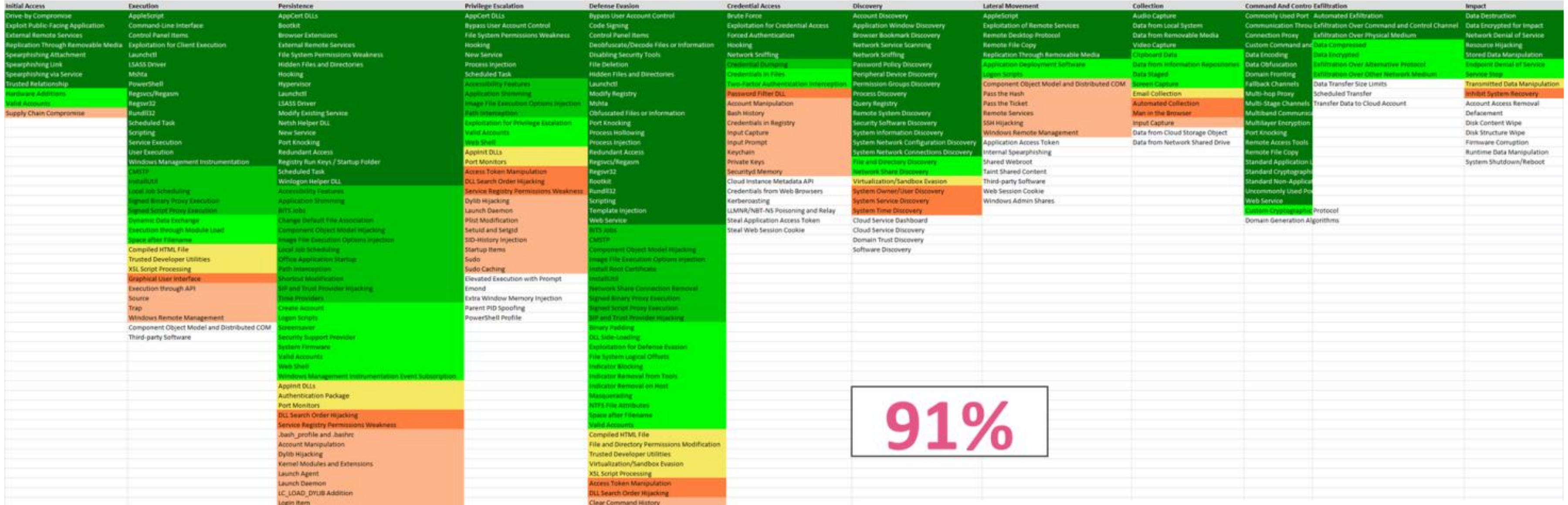
ATT&CK Navigator Best Practices - Prevent

Check Point
SOFTWARE TECHNOLOGIES LTD



- ✓ Stop Attacks before they cause more damage
- ✓ Reduce TCO (Total Cost of Ownership)
- ✓ Increase ROI (Return on Investment)

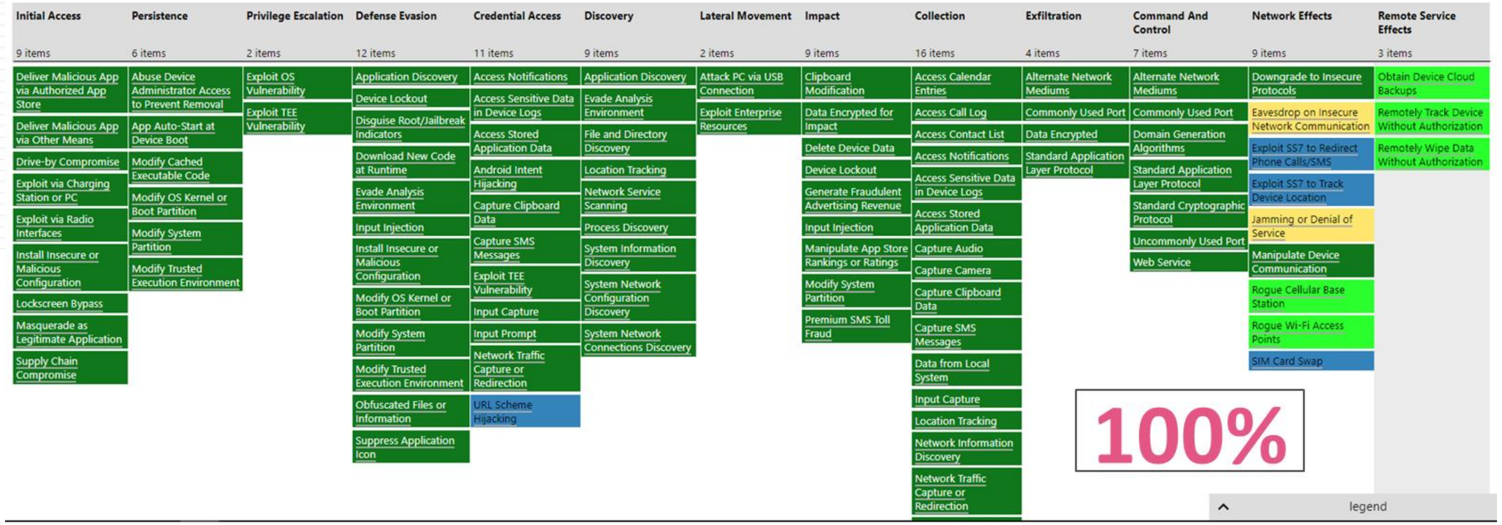
Check Point’s coverage



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Drive-by Compromise	AppleScript	AppCert DLLs	AppCert DLLs	Bypass User Account Control
Exploit Public-Facing Application	Command-Line Interface	Bootkit	Bypass User Account Control	Code Signing
External Remote Services	Control Panel Items	Browser Extensions	File System Permissions Weakness	Control Panel Items
Replication Through Removable Media	Exploitation for Client Execution	External Remote Services	Hooking	Deobfuscate/Decode Files or Information
Spearphishing Attachment	Launchctl	File System Permissions Weakness	New Service	Disabling Security Tools
Spearphishing Link	LSASS Driver	Hidden Files and Directories	Process Injection	File Deletion
Spearphishing via Service	Mshta	Hooking	Scheduled Task	Hidden Files and Directories
Trusted Relationship	PowerShell	Hypervisor	Accessibility Features	Launchctl
Hardware Additions	Regsvcs/Regasm	Launchctl	Application Shimming	Modify Registry
Valid Accounts	Regsvr32	LSASS Driver	Image File Execution Options Injection	Mshta
Supply Chain Compromise	Rundll32	Modify Existing Service	Path Interception	Obfuscated Files or Information
	Scheduled Task	Netsh Helper DLL	Exploitation for Privilege Escalation	Port Knocking
	Scripting	New Service	Valid Accounts	Process Hollowing
	Service Execution	Port Knocking	Web Shell	Process Injection
	User Execution	Redundant Access	AppInit DLLs	Redundant Access
	Windows Management Instrumentation	Registry Run Keys / Startup Folder	Port Monitors	Regsvcs/Regasm
	CMSTP	Scheduled Task	Access Token Manipulation	Regsvr32
	InstallUtil	Winlogon Helper DLL	DLL Search Order Hijacking	Rootkit
	Local Job Scheduling	Accessibility Features	Service Registry Permissions Weakness	Rundll32
	Signed Binary Proxy Execution	Application Shimming	Dylib Hijacking	Scripting
	Signed Script Proxy Execution	BITS Jobs	Launch Daemon	Template Injection
	Dynamic Data Exchange	Change Default File Association	Plist Modification	Web Service
	Execution through Module Load	Component Object Model Hijacking	Setuid and Setgid	BITS Jobs
	Space after Filename	Image File Execution Options Injection	SID-History Injection	CMSTP
	Compiled HTML File	Local Job Scheduling	Startup Items	Component Object Model Hijacking
	Trusted Developer Utilities	Office Application Startup	Sudo	Image File Execution Options Injection
	XSL Script Processing	Path Interception	Sudo Caching	Install Root Certificate
	Graphical User Interface	Shortcut Modification	Elevated Execution with Prompt	InstallUtil
	Execution through API	SIP and Trust Provider Hijacking	Emond	Network Share Connection Removal
	Source	Time Providers	Extra Window Memory Injection	Signed Binary Proxy Execution
	Trap	Create Account	Parent PID Spoofing	Signed Script Proxy Execution
	Windows Remote Management	Logon Scripts	PowerShell Profile	SIP and Trust Provider Hijacking
	Component Object Model and Distributed COM	Screensaver		Binary Padding
	Third-party Software	Security Support Provider		DLL Side-Loading
		System Firmware		Exploitation for Defense Evasion
		Valid Accounts		File System Logical Offsets
		Web Shell		Indicator Blocking
		Windows Management Instrumentation Event Subscription		Indicator Removal from Tools
		AppInit DLLs		Indicator Removal on Host
		Authentication Package		Masquerading
		Port Monitors		NTFS File Attributes
		DLL Search Order Hijacking		Space after Filename
		Service Registry Permissions Weakness		Valid Accounts
		.bash_profile and .bashrc		Compiled HTML File
		Account Manipulation		File and Directory Permissions Modification
		Dylib Hijacking		Trusted Developer Utilities
		Kernel Modules and Extensions		Virtualization/Sandbox Evasion
		Launch Agent		XSL Script Processing
		Launch Daemon		Access Token Manipulation
		LC_LOAD_DYLIB Addition		DLL Search Order Hijacking
		Login Item		Clear Command History
		Plist Modification		DCShadow
		Rc.common		Gatekeeper Bypass
		Re-opened Applications		Indirect Command Execution
		Setuid and Setgid		LC_MAIN Hijacking
		Startup Items		Plist Modification
		Trap		Process Doppelgänging
		Component Firmware		Application Access Token
		Emond		Compile After Delivery
		Implant Container Image		Component Firmware
		PowerShell Profile		Connection Proxy
		Server Software Component		Execution Guardrails
		Systemd Service		Extra Window Memory Injection
				Group Policy Modification
				Hidden Users
				Hidden Window
				HISTCONTROL
				Parent PID Spoofing
				Revert Cloud Instance
				Software Packing
				Timestomp
				Unused/Unsupported Cloud Regions
				Web Session Cookie

Credential Access	Discovery	Lateral Movement	Collection	Command And Contro	Exfiltration	Impact
Brute Force	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploitation for Credential Access	Application Window Discovery	Exploitation of Remote Services	Data from Local System	Communication Throu	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
Forced Authentication	Browser Bookmark Discovery	Remote Desktop Protocol	Data from Removable Media	Connection Proxy	Exfiltration Over Physical Medium	Network Denial of Service
Hooking	Network Service Scanning	Remote File Copy	Video Capture	Custom Command and	Data Compressed	Resource Hijacking
Network Sniffing	Network Sniffing	Replication Through Removable Media	Clipboard Data	Data Encoding	Data Encrypted	Stored Data Manipulation
Credential Dumping	Password Policy Discovery	Application Deployment Software	Data from Information Repositories	Data Obfuscation	Exfiltration Over Alternative Protocol	Endpoint Denial of Service
Credentials in Files	Peripheral Device Discovery	Logon Scripts	Data Staged	Domain Fronting	Exfiltration Over Other Network Medium	Service Stop
Two-Factor Authentication Interception	Permission Groups Discovery	Component Object Model and Distributed COM	Screen Capture	Fallback Channels	Data Transfer Size Limits	Transmitted Data Manipulation
Password Filter DLL	Process Discovery	Pass the Hash	Email Collection	Multi-hop Proxy	Scheduled Transfer	Inhibit System Recovery
Account Manipulation	Query Registry	Pass the Ticket	Automated Collection	Multi-Stage Channels	Transfer Data to Cloud Account	Account Access Removal
Bash History	Remote System Discovery	Remote Services	Man in the Browser	Multiband Communic		Defacement
Credentials in Registry	Security Software Discovery	SSH Hijacking	Input Capture	Multilayer Encryption		Disk Content Wipe
Input Capture	System Information Discovery	Windows Remote Management	Data from Cloud Storage Object	Port Knocking		Disk Structure Wipe
Input Prompt	System Network Configuration Discovery	Application Access Token	Data from Network Shared Drive	Remote Access Tools		Firmware Corruption
Keychain	System Network Connections Discovery	Internal Spearphishing		Remote File Copy		Runtime Data Manipulation
Private Keys	File and Directory Discovery	Shared Webroot		Standard Application L		System Shutdown/Reboot
Securityd Memory	Network Share Discovery	Taint Shared Content		Standard Cryptographi		
Cloud Instance Metadata API	Virtualization/Sandbox Evasion	Third-party Software		Standard Non-Applica		
Credentials from Web Browsers	System Owner/User Discovery	Web Session Cookie		Uncommonly Used Po		
Kerberoasting	System Service Discovery	Windows Admin Shares		Web Service		
LLMNR/NBT-NS Poisoning and Relay	System Time Discovery			Custom Cryptographic Protocol		
Steal Application Access Token	Cloud Service Dashboard			Domain Generation Algorithms		
Steal Web Session Cookie	Cloud Service Discovery					
	Domain Trust Discovery					
	Software Discovery					

91%



Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
9 items	6 items	2 items	12 items	11 items	9 items	2 items
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Device Lockout	Access Sensitive Data in Device Logs	Evade Analysis Environment	Exploit Enterprise Resources
Drive-by Compromise	Modify Cached Executable Code		Disguise Root/Jailbreak Indicators	Access Stored Application Data	File and Directory Discovery	
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Download New Code at Runtime	Android Intent Hijacking	Location Tracking	
Exploit via Radio Interfaces	Modify System Partition		Evade Analysis Environment	Capture Clipboard Data	Network Service Scanning	
Install Insecure or Malicious Configuration	Modify Trusted Execution Environment		Input Injection	Capture SMS Messages	Process Discovery	
Lockscreen Bypass			Install Insecure or Malicious Configuration	Exploit TEE Vulnerability	System Information Discovery	
Masquerade as Legitimate Application			Modify OS Kernel or Boot Partition	Input Capture	System Network Configuration Discovery	
Supply Chain Compromise			Modify System Partition	Input Prompt	System Network Connections Discovery	
			Modify Trusted Execution Environment	Network Traffic Capture or Redirection		
			Obfuscated Files or Information	URL Scheme Hijacking		
			Suppress Application Icon			

Impact	Collection	Exfiltration	Command And Control	Network Effects	Remote Service Effects
9 items	16 items	4 items	7 items	9 items	3 items
Clipboard Modification	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums	Downgrade to Insecure Protocols	Obtain Device Cloud Backups
Data Encrypted for Impact	Access Call Log	Commonly Used Port	Commonly Used Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Delete Device Data	Access Contact List	Data Encrypted	Domain Generation Algorithms	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Device Lockout	Access Notifications	Standard Application Layer Protocol	Standard Application Layer Protocol	Exploit SS7 to Track Device Location	
Generate Fraudulent Advertising Revenue	Access Sensitive Data in Device Logs		Standard Cryptographic Protocol	Jamming or Denial of Service	
Input Injection	Access Stored Application Data		Uncommonly Used Port	Manipulate Device Communication	
Manipulate App Store Rankings or Ratings	Capture Audio		Web Service	Rogue Cellular Base Station	
Modify System Partition	Capture Camera			Rogue Wi-Fi Access Points	
Premium SMS Toll Fraud	Capture Clipboard Data			SIM Card Swap	
	Capture SMS Messages				
	Data from Local System				
	Input Capture				
	Location Tracking				
	Network Information Discovery				
	Network Traffic Capture or Redirection				

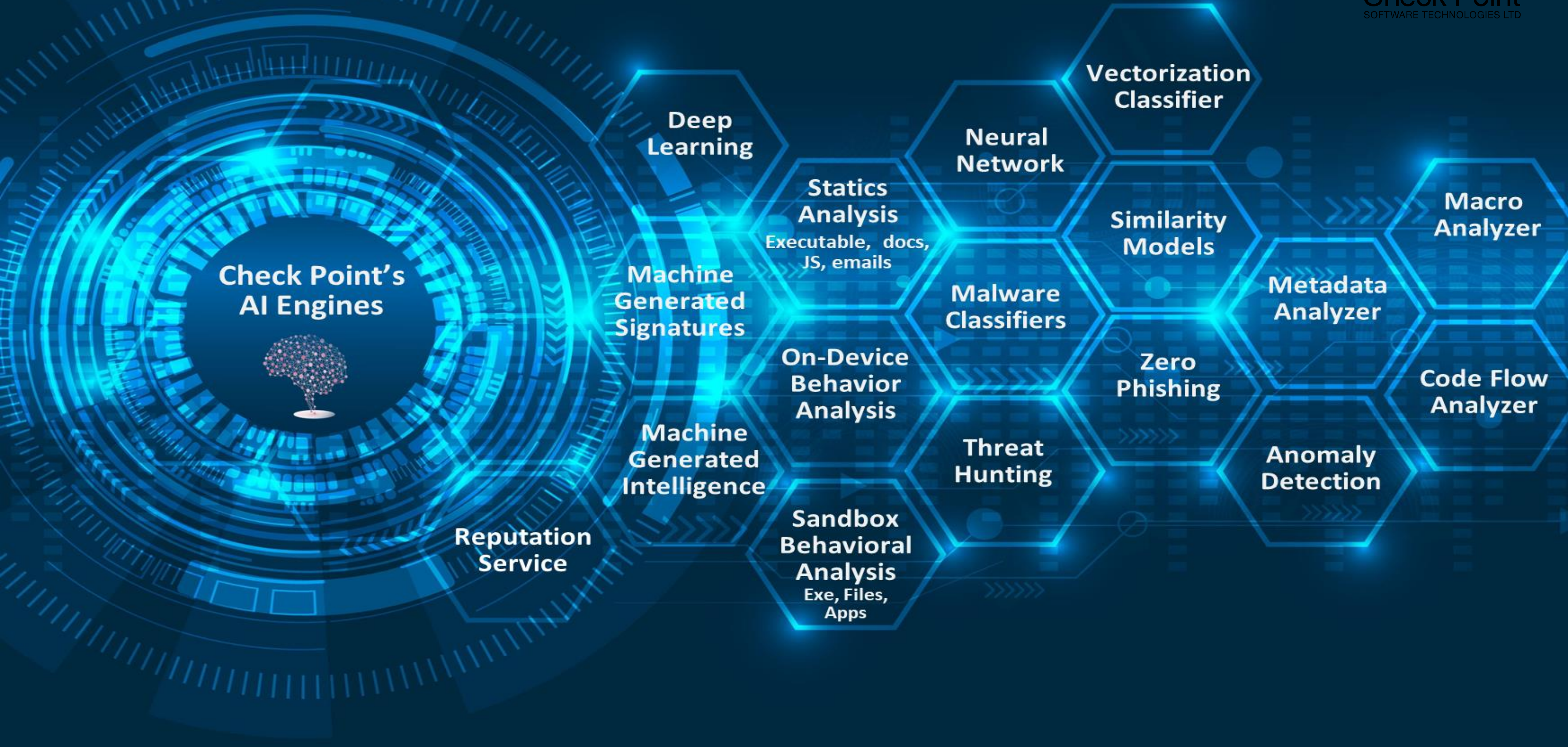
100%

Enterprise matrix coverage by Check Point Infinity

Mobile matrix coverage by Check Point SBM + UEM

Best Prevention by leveraging AI

Check Point
SOFTWARE TECHNOLOGIES LTD



Check Point's AI Engines

Deep Learning

Machine Generated Signatures

Machine Generated Intelligence

Reputation Service

Statics Analysis
Executable, docs, JS, emails

On-Device Behavior Analysis

Sandbox Behavioral Analysis
Exe, Files, Apps

Neural Network

Malware Classifiers

Threat Hunting

Vectorization Classifier

Similarity Models

Zero Phishing

Metadata Analyzer

Anomaly Detection

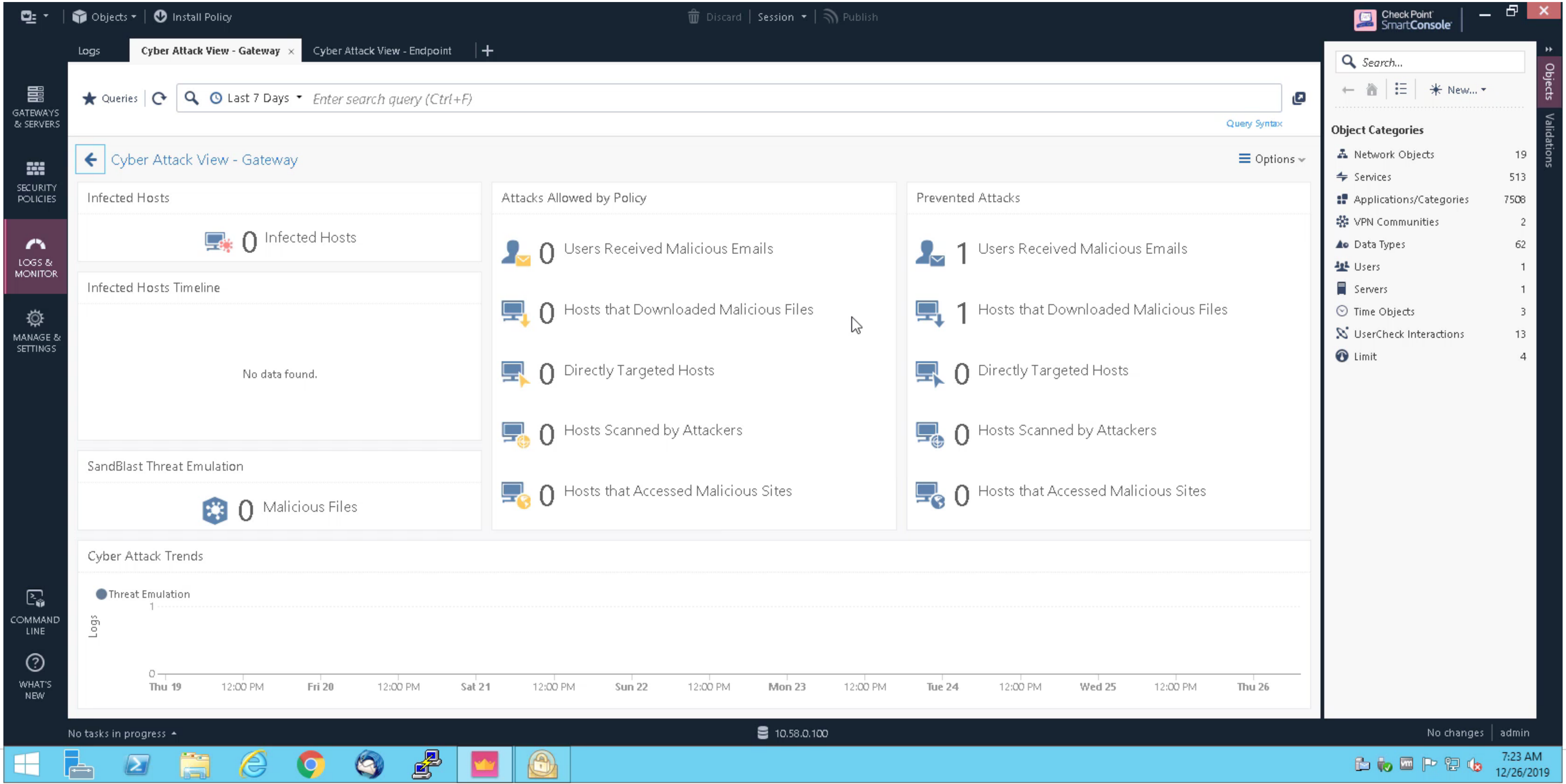
Macro Analyzer

Code Flow Analyzer

“RobbinHood” Mail Attack

SandBlast Network “RobbinHood” Attack Prevention and Analysis

Check Point
SOFTWARE TECHNOLOGIES LTD



Cyber Attack View - Gateway

Infected Hosts

0 Infected Hosts

Infected Hosts Timeline

No data found.

SandBlast Threat Emulation

0 Malicious Files

Attacks Allowed by Policy

0	Users Received Malicious Emails
0	Hosts that Downloaded Malicious Files
0	Directly Targeted Hosts
0	Hosts Scanned by Attackers
0	Hosts that Accessed Malicious Sites

Prevented Attacks

1	Users Received Malicious Emails
1	Hosts that Downloaded Malicious Files
0	Directly Targeted Hosts
0	Hosts Scanned by Attackers
0	Hosts that Accessed Malicious Sites

Cyber Attack Trends

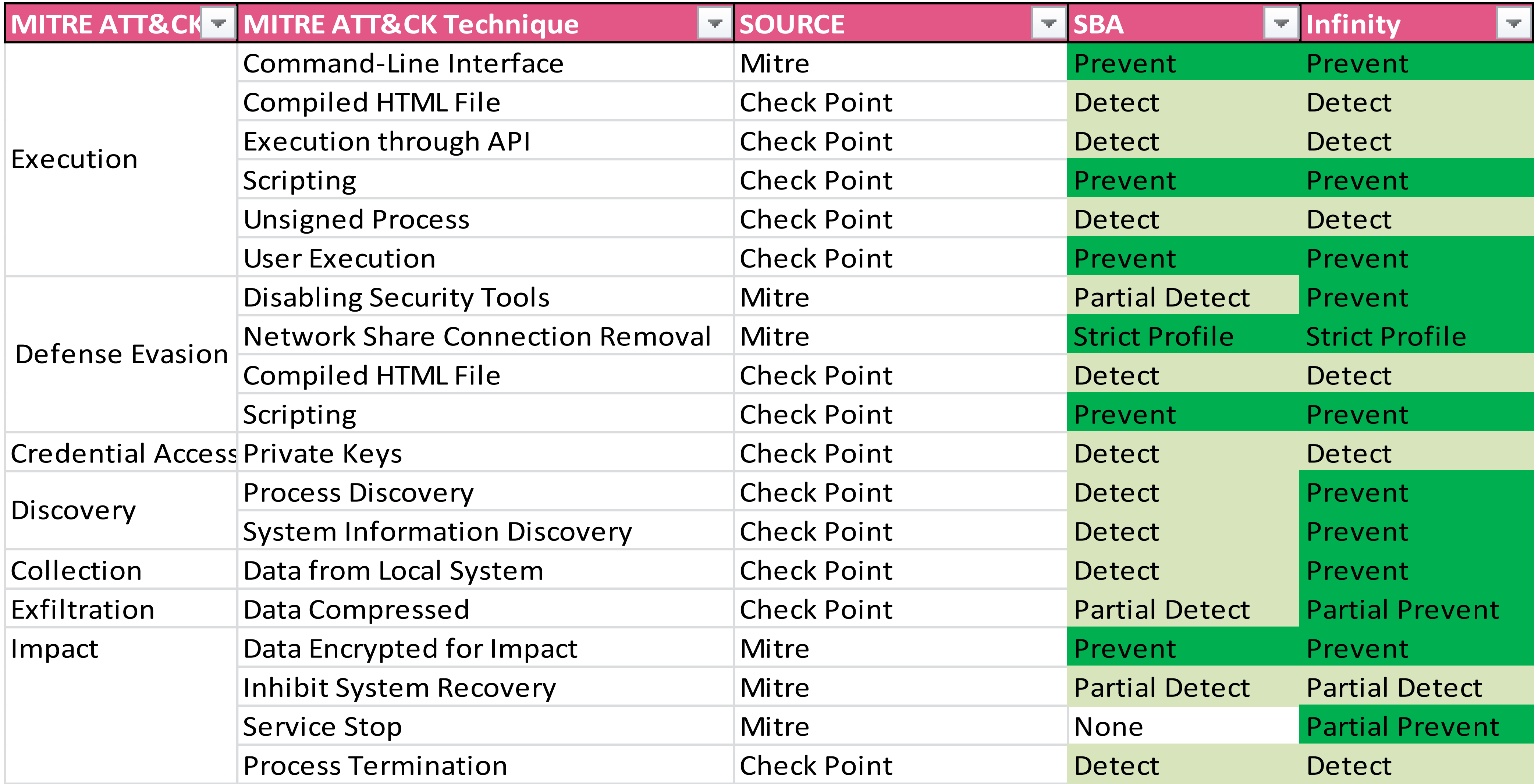
Object Categories

Network Objects	19
Services	513
Applications/Categories	7508
VPN Communities	2
Data Types	62
Users	1
Servers	1
Time Objects	3
UserCheck Interactions	13
Limit	4

No tasks in progress ▴ 10.58.0.100 No changes admin

7:23 AM
12/26/2019

RobbinHood – Mapping to MITRE ATT&CK Coverage

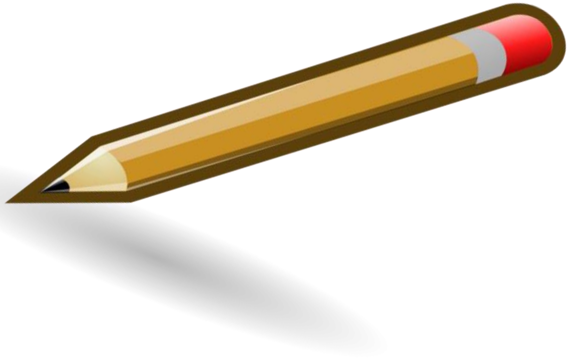


MITRE ATT&CK	MITRE ATT&CK Technique	SOURCE	SBA	Infinity
Execution	Command-Line Interface	Mitre	Prevent	Prevent
	Compiled HTML File	Check Point	Detect	Detect
	Execution through API	Check Point	Detect	Detect
	Scripting	Check Point	Prevent	Prevent
	Unsigned Process	Check Point	Detect	Detect
	User Execution	Check Point	Prevent	Prevent
Defense Evasion	Disabling Security Tools	Mitre	Partial Detect	Prevent
	Network Share Connection Removal	Mitre	Strict Profile	Strict Profile
	Compiled HTML File	Check Point	Detect	Detect
	Scripting	Check Point	Prevent	Prevent
Credential Access	Private Keys	Check Point	Detect	Detect
Discovery	Process Discovery	Check Point	Detect	Prevent
	System Information Discovery	Check Point	Detect	Prevent
Collection	Data from Local System	Check Point	Detect	Prevent
Exfiltration	Data Compressed	Check Point	Partial Detect	Partial Prevent
Impact	Data Encrypted for Impact	Mitre	Prevent	Prevent
	Inhibit System Recovery	Mitre	Partial Detect	Partial Detect
	Service Stop	Mitre	None	Partial Prevent
	Process Termination	Check Point	Detect	Detect

In this workshop:

Check Point
SOFTWARE TECHNOLOGIES LTD

- ☑ MITRE ATT&CK overview
- ☑ Best Practices that will Boost your skills:
  - ☑ Visualize
  - ☑ Assess Risks
  - ☑ Map your Coverage
  - ☑ Investigate
  - ☑ Prevent
- □ **Check Point's solution value**
- □ Takeaways you can apply

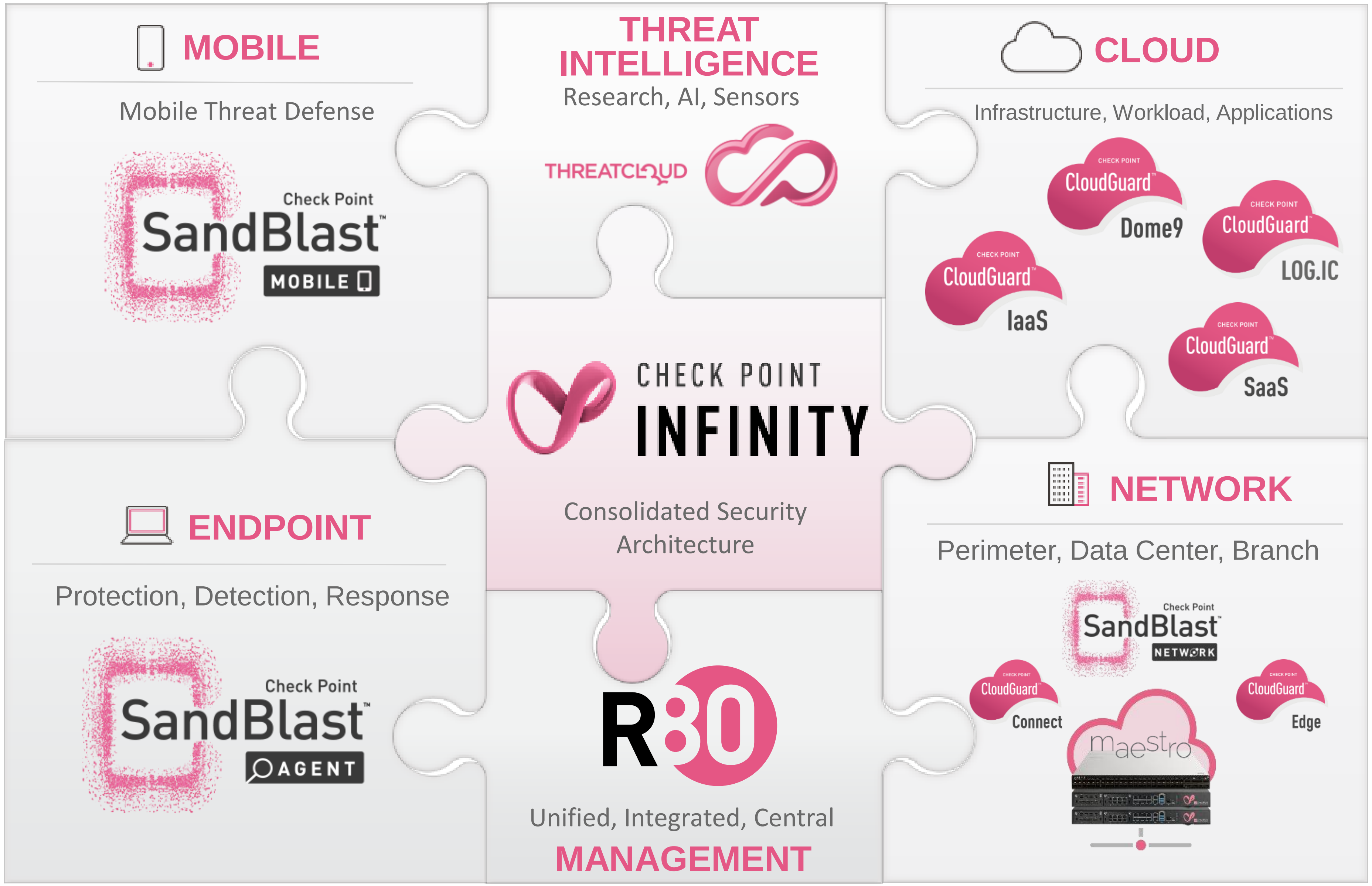


INFINITY

Check Point’s solution for ATT&CKs

Comprehensive

One consolidated architecture to cover the MITRE ATT&CK



MOBILE

Mobile Threat Defense

Check Point
SandBlast
MOBILE

THREAT INTELLIGENCE

Research, AI, Sensors

CLOUD

Infrastructure, Workload, Applications

CHECK POINT CloudGuard Dome9
CHECK POINT CloudGuard LOG.IC
CHECK POINT CloudGuard IaaS
CHECK POINT CloudGuard SaaS

CHECK POINT INFINITY

Consolidated Security Architecture

ENDPOINT

Protection, Detection, Response

Check Point
SandBlast
AGENT

Unified, Integrated, Central

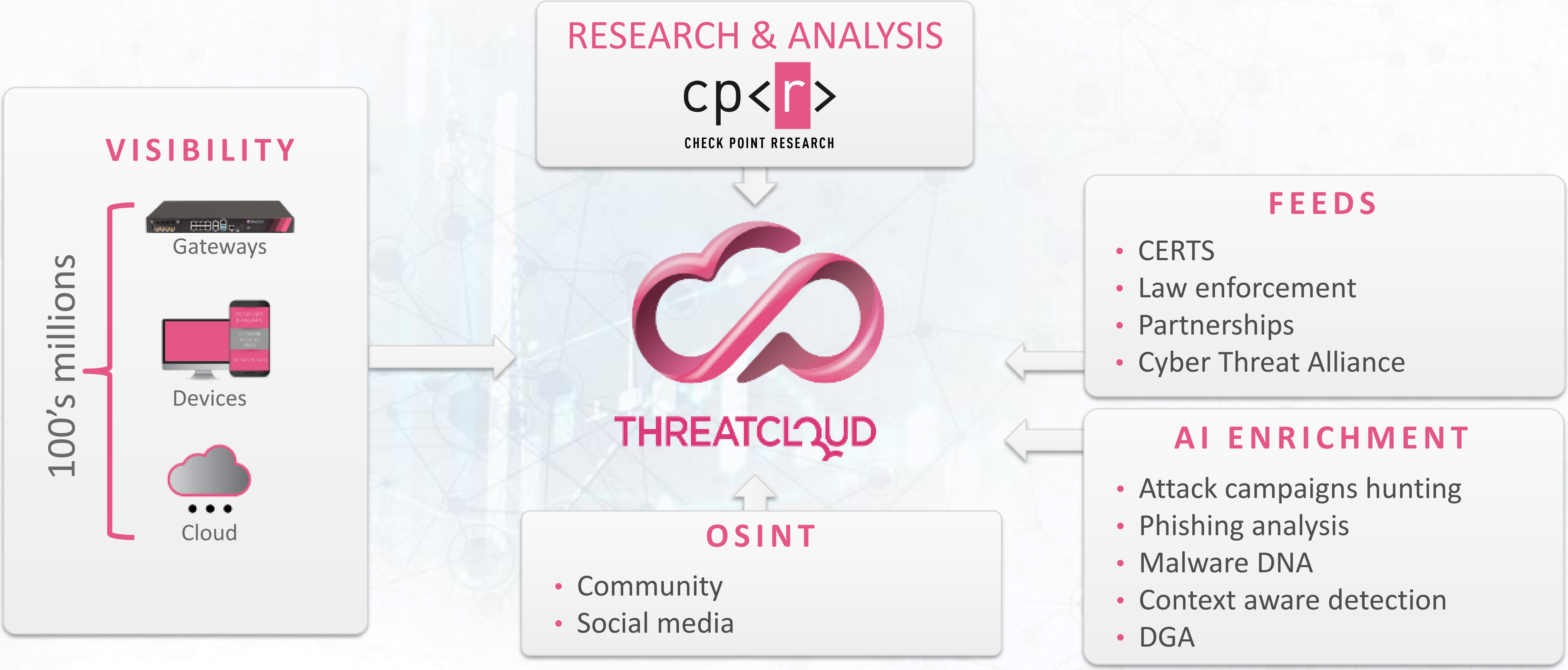
MANAGEMENT

NETWORK

Perimeter, Data Center, Branch

Check Point
SandBlast
NETWORK
CHECK POINT CloudGuard Connect
CHECK POINT CloudGuard Edge
maestro

ThreatCloud



RESEARCH & ANALYSIS

cp<r>
CHECK POINT RESEARCH

VISIBILITY

100's millions

- Gateways
- Devices
- Cloud

THREATCLOUD

FEEDS

- CERTS
- Law enforcement
- Partnerships
- Cyber Threat Alliance

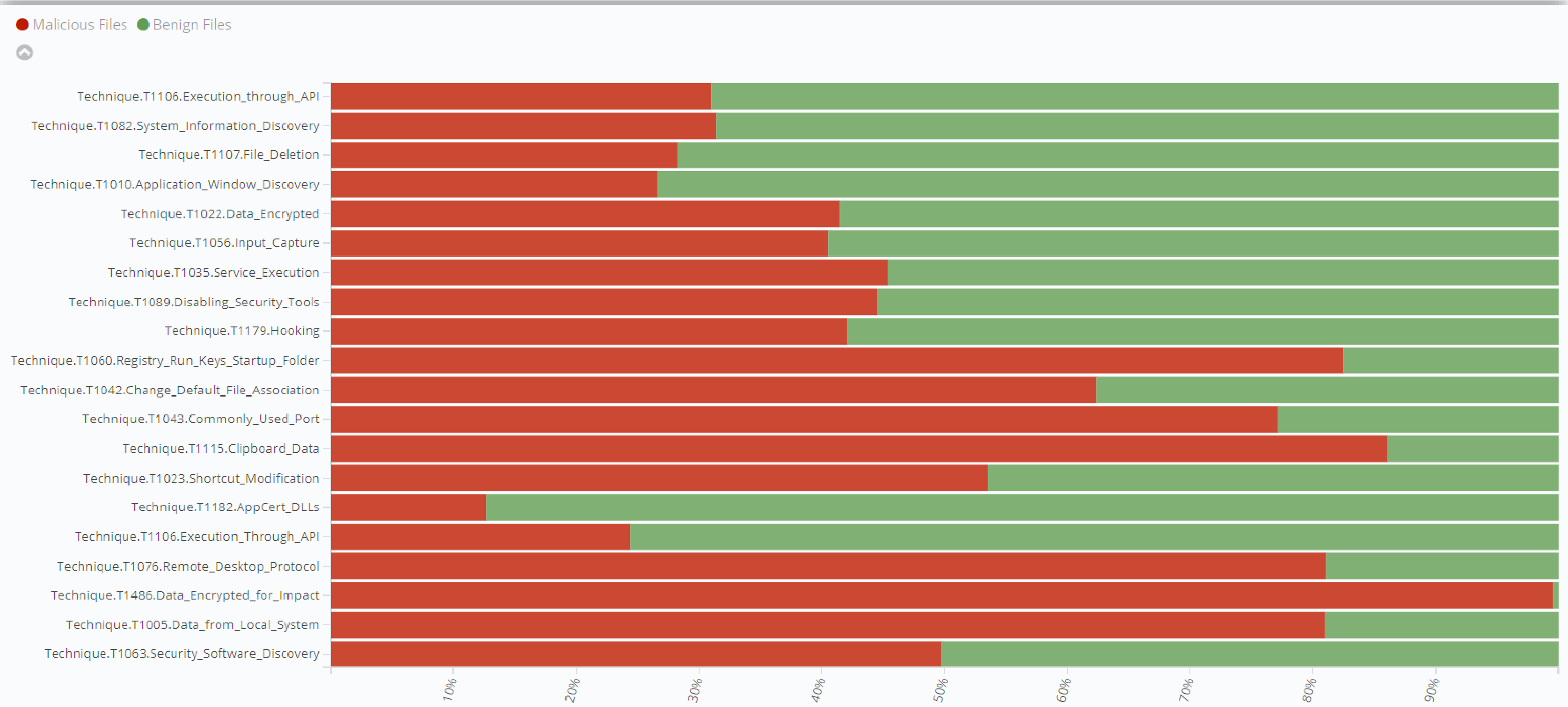
AI ENRICHMENT

- Attack campaigns hunting
- Phishing analysis
- Malware DNA
- Context aware detection
- DGA

OSINT

- Community
- Social media

ThreatCloud Automatic Technique Analysis



WELCOME TO THE FUTURE OF CYBER SECURITY

ThreatCloud Portal – Infinity SOC

Check Point Research insights

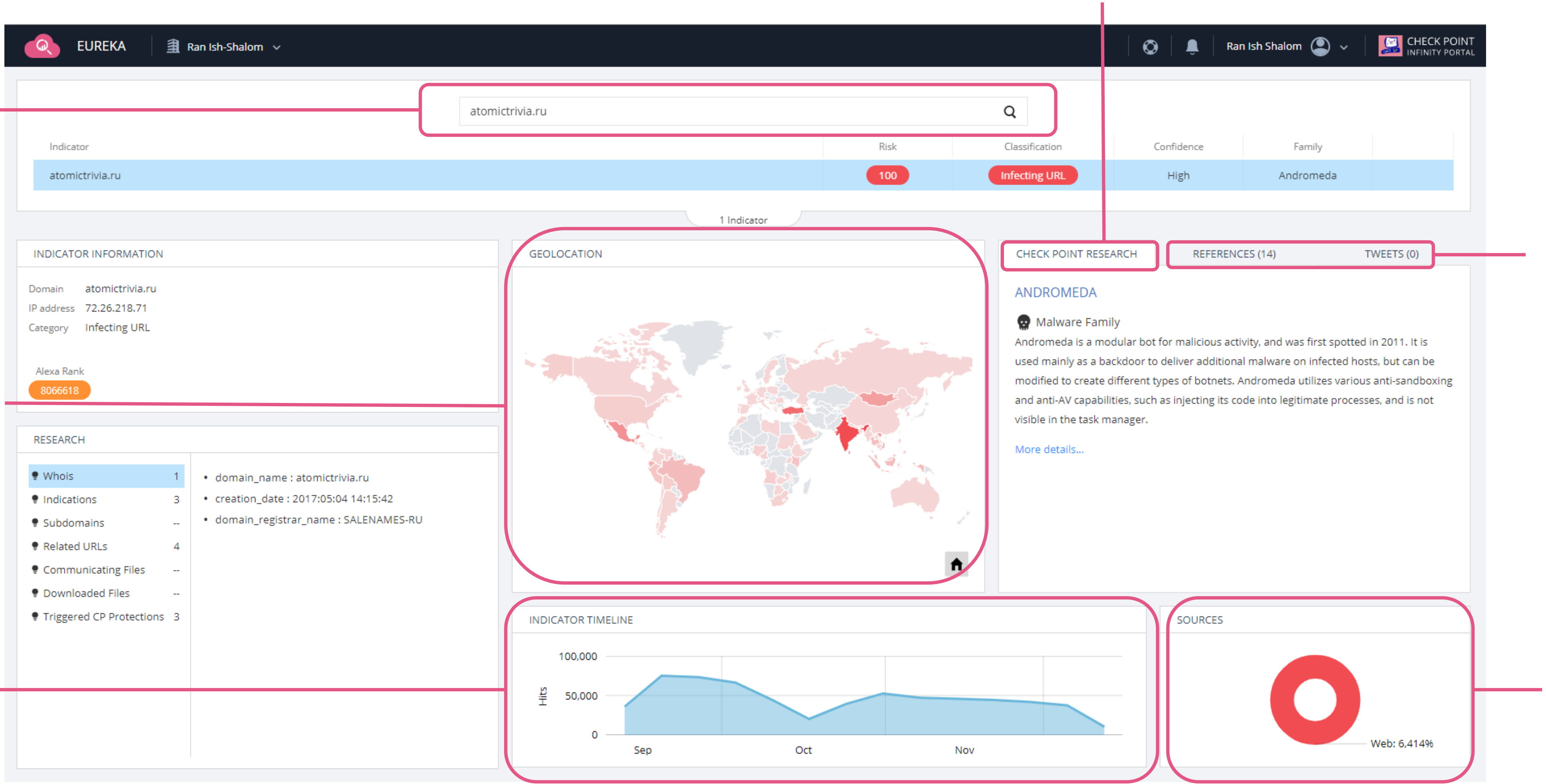
Search for any indicator

OSINT

Geographical spread

Activity timeline

Known attack surfaces



atomictrivia.ru

Indicator	Risk	Classification	Confidence	Family
atomictrivia.ru	100	Infecting URL	High	Andromeda

1 Indicator

INDICATOR INFORMATION

Domain	atomictrivia.ru
IP address	72.26.218.71
Category	Infecting URL

Alexa Rank
8066618

RESEARCH

Whois	1
Indications	3
Subdomains	--
Related URLs	4
Communicating Files	--
Downloaded Files	--
Triggered CP Protections	3

- domain_name : atomictrivia.ru
- creation_date : 2017:05:04 14:15:42
- domain_registrar_name : SALENAMES-RU

CHECK POINT RESEARCH | REFERENCES (14) | TWEETS (0)

ANDROMEDA

Malware Family

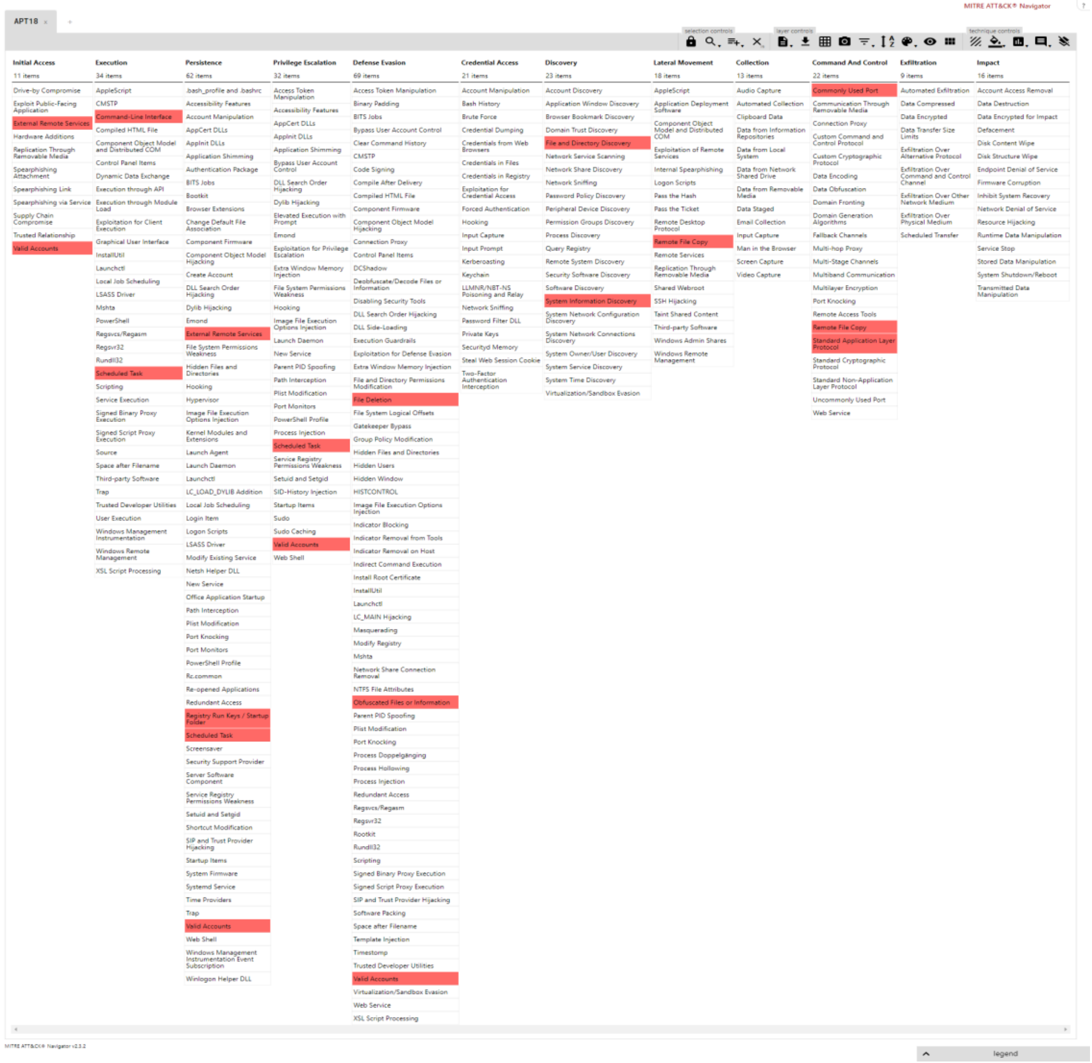
Andromeda is a modular bot for malicious activity, and was first spotted in 2011. It is used mainly as a backdoor to deliver additional malware on infected hosts, but can be modified to create different types of botnets. Andromeda utilizes various anti-sandboxing and anti-AV capabilities, such as injecting its code into legitimate processes, and is not visible in the task manager.

More details...

Investigation with contextualized threat intelligence from Threat Cloud

Let’s Analyze a Threat Group coverage

- Let’s analyze a Threat Group coverage
- For Example, you can see the MITRE ATT&CK mapping for APT 18
- APT 18 is a threat group that has operated since 2009
- Targets a range of industries, including technology, manufacturing, human rights groups, government, and medical



Initial Access
11 items

- Drive-by Compromise
- Exploit Public-Facing Application
- **External Remote Services**
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- **Valid Accounts**

Execution
34 items

- AppleScript
- CMSTP
- **Command-Line Interface**
- Compiled HTML File
- Component Object Model and Distributed COM
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- **Scheduled Task**
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence
62 items

- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- Emond
- **External Remote Services**
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition
- Local Job Scheduling
- Login Item
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Plist Modification
- Port Knocking
- Port Monitors
- PowerShell Profile
- Rc.common
- Re-opened Applications
- Redundant Access
- **Registry Run Keys / Startup Folder**
- **Scheduled Task**
- Screensaver
- Security Support Provider
- Server Software Component
- Service Registry Permissions Weakness
- Setuid and Setgid
- Shortcut Modification
- SIP and Trust Provider Hijacking
- Startup Items
- System Firmware
- Systemd Service
- Time Providers
- Trap
- **Valid Accounts**
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation
32 items

- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Elevated Execution with Prompt
- Emond
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Parent PID Spoofing
- Path Interception
- Plist Modification
- Port Monitors
- PowerShell Profile
- Process Injection
- **Scheduled Task**
- Service Registry Permissions Weakness
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo
- Sudo Caching
- **Valid Accounts**
- Web Shell

Defense Evasion
69 items

- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Connection Proxy
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File and Directory Permissions Modification
- **File Deletion**
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- **Obfuscated Files or Information**
- Parent PID Spoofing
- Plist Modification
- Port Knocking
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Space after Filename
- Template Injection
- Timestomp
- Trusted Developer Utilities
- **Valid Accounts**
- Virtualization/Sandbox Evasion
- Web Service
- XSL Script Processing

Credential Access
21 items

- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Steal Web Session Cookie
- Two-Factor Authentication Interception

Discovery
23 items

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- **File and Directory Discovery**
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- Software Discovery
- **System Information Discovery**
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
18 items

- AppleScript
- Application Deployment Software
- Component Object Model and Distributed COM
- Exploitation of Remote Services
- Internal Spearphishing
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- **Remote File Copy**
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection
13 items

- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control
22 items

- **Commonly Used Port**
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- **Remote File Copy**
- **Standard Application Layer Protocol**
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration
9 items

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact
16 items

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- System Shutdown/Reboot
- Transmitted Data Manipulation

APT 18 ATT&CK Coverage - NGTP

Check Point
SOFTWARE TECHNOLOGIES LTD

Tactics	Techniques	NGTP
Initial Access	External Remote Services	
Execution	Command line interface	
	Schedule task	
Persistence	Registry run keys	
Privilege escalation	Valid accounts	
Defense evasion	File deletion	
	Obfuscated files or information	
Discovery	File and Directory discovery	PARTIAL PREVENT
	System information discovery	
Lateral movement	Remote file copy	PREVENT
Command and control	Commonly used port	PREVENT
	Standard application layered protocol	PREVENT

APT 18 ATT&CK Coverage - NGTX

Tactics	Techniques	NGTP	NGTX
Initial Access	External Remote Services		ROADMAP
Execution	Command line interface		PREVENT
	Schedule task		PREVENT
Persistence	Registry run keys		PREVENT
Privilege escalation	Valid accounts		PARTIAL PREVENT
Defense evasion	File deletion		
	Obfuscated files or information		
Discovery	File and Directory discovery	PARTIAL PREVENT	PARTIAL PREVENT
	System information discovery		PREVENT
Lateral movement	Remote file copy	PREVENT	PREVENT
Command and control	Commonly used port	PREVENT	PREVENT
	Standard application layered protocol	PREVENT	PREVENT

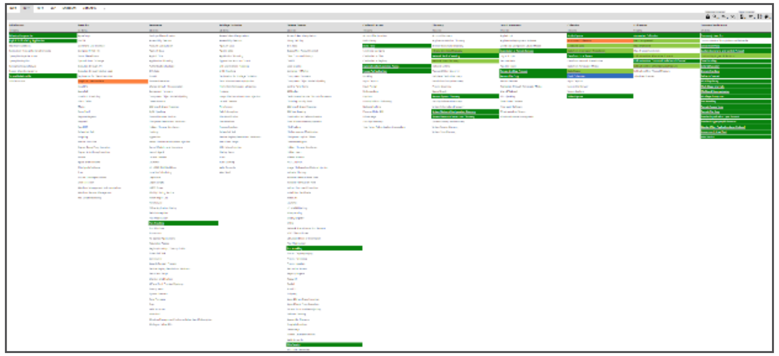
APT 18 ATT&CK Coverage – Sandblast Agent

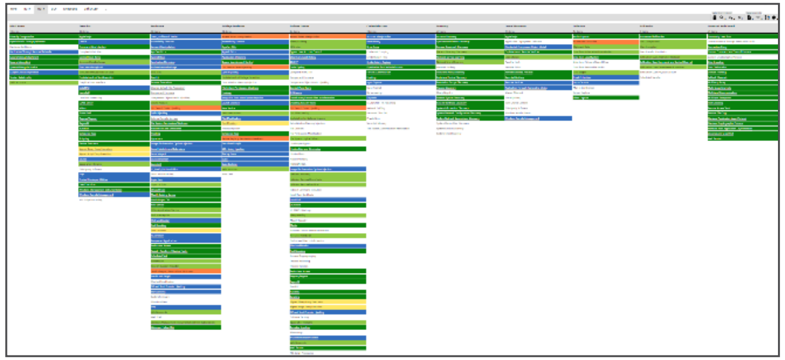
Tactics	Techniques	NGTP	NGTX	SBA
Initial Access	External Remote Services		ROADMAP	
Execution	Command line interface		PREVENT	PARTIAL PREVENT
	Schedule task		PREVENT	DETECT
Persistence	Registry run keys		PREVENT	PARTIAL PREVENT
Privilege escalation	Valid accounts		PARTIAL PREVENT	ROADMAP
Defense evasion	File deletion			PREVENT
	Obfuscated files or information			PREVENT
Discovery	File and Directory discovery	PARTIAL PREVENT	PARTIAL PREVENT	ROADMAP
	System information discovery		PREVENT	ROADMAP
Lateral movement	Remote file copy	PREVENT	PREVENT	DETECT
Command and control	Commonly used port	PREVENT	PREVENT	PARTIAL PREVENT
	Standard application layered protocol	PREVENT	PREVENT	ROADMAP

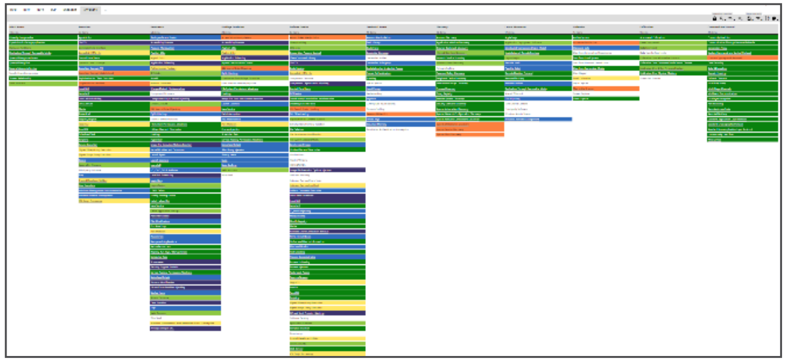
APT 18 ATT&CK Coverage - Infinity

Tactics	Techniques	NGTP	NGTX	SBA	INFINITY
Initial Access	External Remote Services		ROADMAP		PREVENT
Execution	Command line interface		PREVENT	PARTIAL PREVENT	PREVENT
	Schedule task		PREVENT	DETECT	PREVENT
Persistence	Registry run keys		PREVENT	PARTIAL PREVENT	PREVENT
Privilege escalation	Valid accounts		PARTIAL PREVENT	ROADMAP	PARTIAL PREVENT
Defense evasion	File deletion			PREVENT	PREVENT
	Obfuscated files or information			PREVENT	PREVENT
Discovery	File and Directory discovery	PARTIAL PREVENT	PARTIAL PREVENT	ROADMAP	PARTIAL PREVENT
	System information discovery		PREVENT	ROADMAP	PREVENT
Lateral movement	Remote file copy	PREVENT	PREVENT	DETECT	PREVENT
Command and control	Commonly used port	PREVENT	PREVENT	PARTIAL PREVENT	PREVENT
	Standard application layered protocol	PREVENT	PREVENT	ROADMAP	PREVENT

Check Point Infinity stands alone in addressing the entire MITRE ATT&CK Framework for the enterprise







NGTP → NGTX → INFINITY

Baseline network threat Prevention engines:

- Anti-Bot
- IPS
- Anti-Virus

Advanced network Threat Prevention engines:

- Threat Emulation
- Threat Extraction
- Artificial Intelligence

Additional security solutions:

- Endpoint: SandBlast Agent
- Mobile: SandBlast Mobile
- Cloud: CloudGuard family

Simple

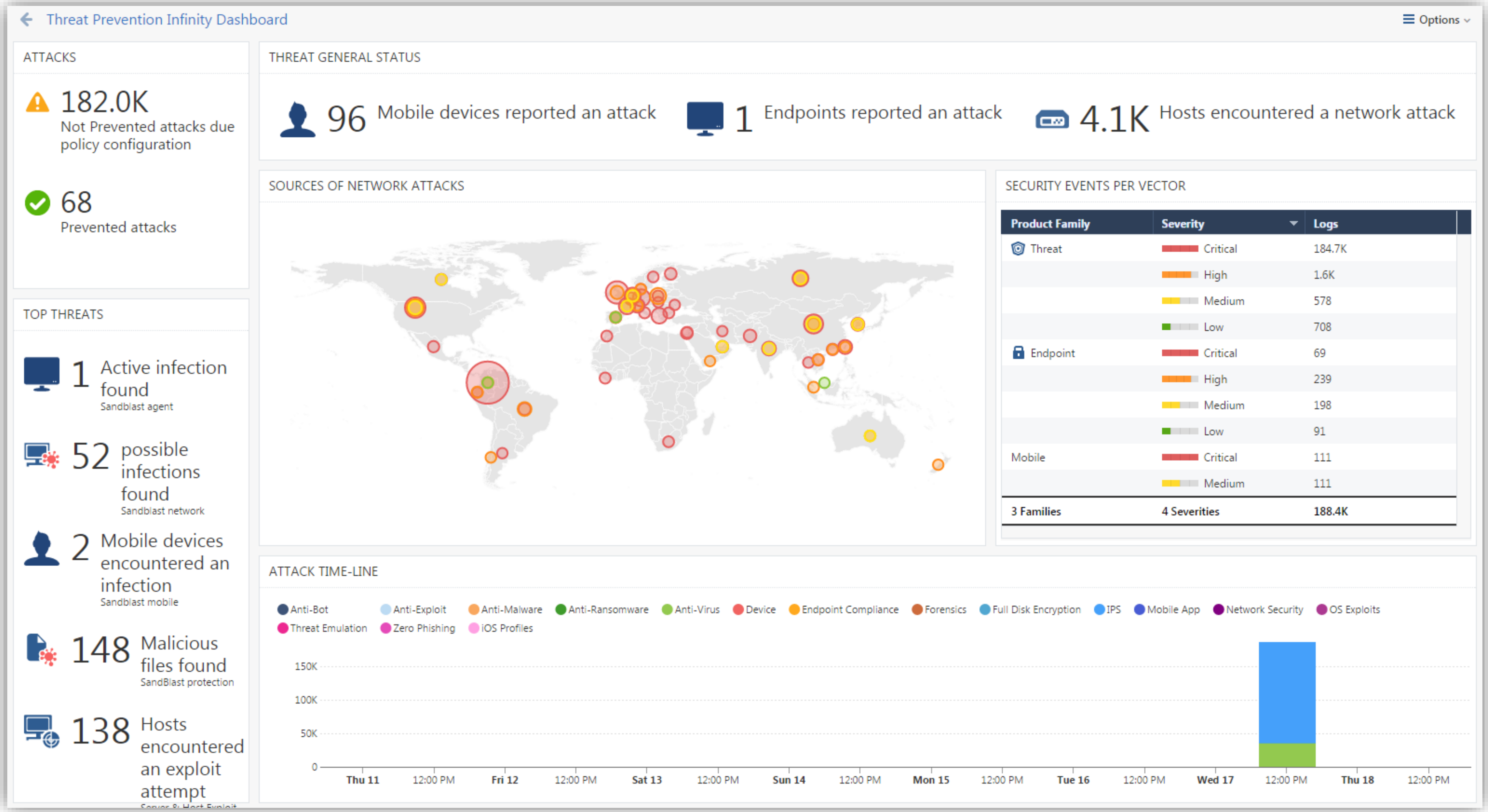
If it is not simple it will simply not happen

Learning mode to Best practice methodology

- **Sk15277-** Learning mode to Best practice methodology
  - Get ATT&CK visibility without impact to the organization
  - Simple to move to prevention
- **Threat Emulation**
  - Enable with Cloud Emulation
  - Background and Detect
- **SandBlast Agent**
  - Always Analyze
  - Don’t perform automatic remediation

Simple Operation and Analysis

Check Point
SOFTWARE TECHNOLOGIES LTD



Threat Prevention Infinity Dashboard

Options

ATTACKS

182.0K
Not Prevented attacks due policy configuration

68
Prevented attacks

TOP THREATS

1 Active infection found
Sandblast agent

52 possible infections found
Sandblast network

2 Mobile devices encountered an infection
Sandblast mobile

148 Malicious files found
SandBlast protection

138 Hosts encountered an exploit attempt
Server & Host Exploit

THREAT GENERAL STATUS

96 Mobile devices reported an attack

1 Endpoints reported an attack

4.1K Hosts encountered a network attack

SOURCES OF NETWORK ATTACKS

SECURITY EVENTS PER VECTOR

Product Family	Severity	Logs
Threat	Critical	184.7K
	High	1.6K
	Medium	578
	Low	708
Endpoint	Critical	69
	High	239
	Medium	198
	Low	91
Mobile	Critical	111
	Medium	111
3 Families	4 Severities	188.4K

ATTACK TIME-LINE

WELCOME TO THE FUTURE OF CYBER SECURITY

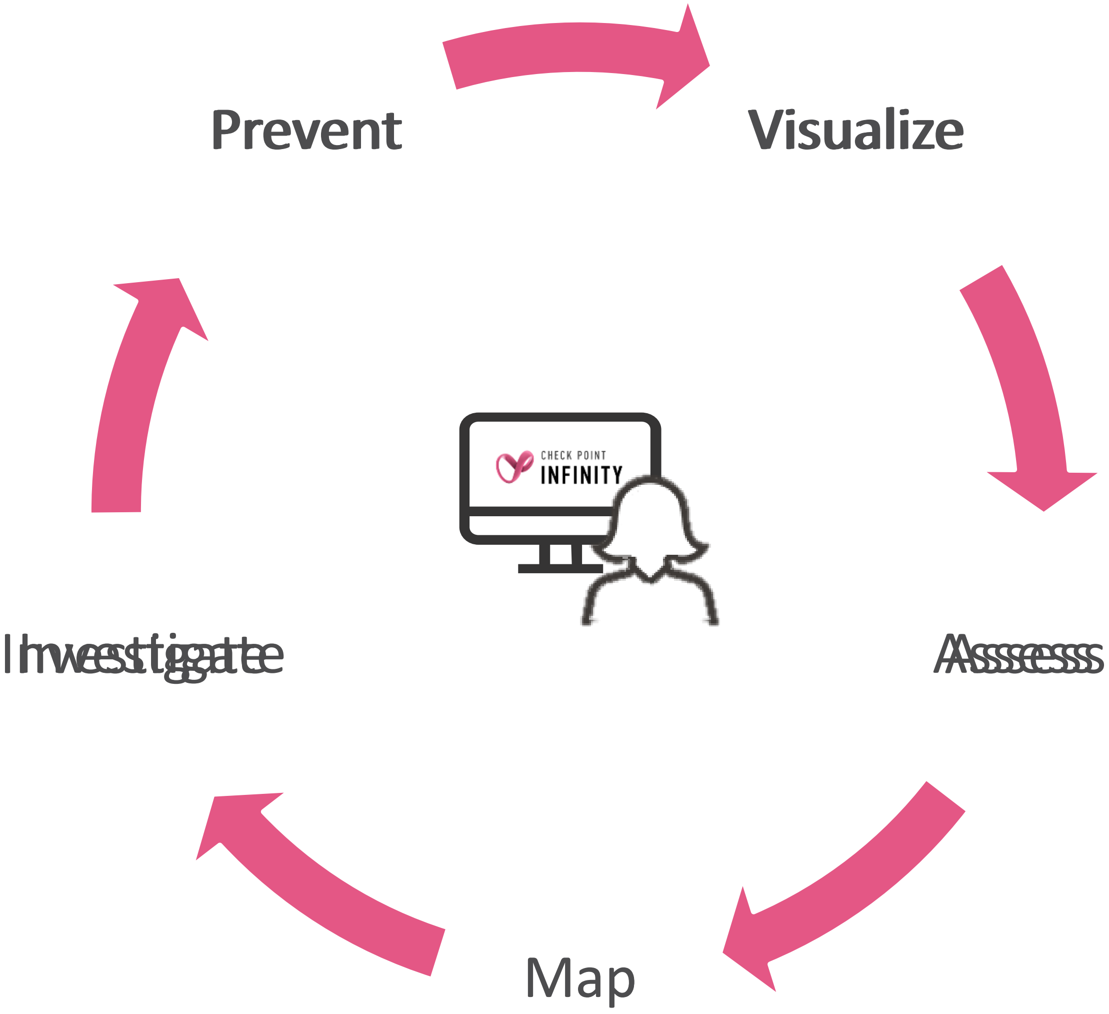
In this workshop:

- ☑ MITRE ATT&CK overview
- ☑ Best Practices that will Boost your skills:
  - ☑ Visualize
  - ☑ Assess Risks
  - ☑ Map your Coverage
  - ☑ Investigate
  - ☑ Prevent
- ☑ Check Point’s solution value
- □ **Takeaways you can apply**

Takeaways

Prevent, Assess, Investigate

ATT&CK Best Practices Summary



Prevent:
Assess:
Map:
Investigate:
Visualize:

- ✓ Apply **Prevention**, NOT Detection
- ✓ **Identify** your adversaries
- ✓ **Map** your security coverage
- ✓ Use **SmartEvent** to find incidents
- ✓ Implement Threat Prevention **Architecture**
- ✓ Use **Forensics Reports**
- ✓ Assess using Check Point **MITRE Matrix app**
- ✓ Use Checkpoint's navigator beta tool to map your Check Point's products coverage
- ✓ **Analyze** using **Forensic Reports** and **Threat Emulation Reports**
- ✓ Assess using Check Point **SmartEvent**
- ✓ Advanced **AI technologies**: **Predict**
- ✓ Leverage **ATT&CK navigator** for assessment
- ✓ **Respond** quickly to **ATT&CKs**
- ✓ Choose Solutions **Recommended** by independent, trusted 3d party evaluators
- ✓ **Plan** you security gaps closure

Useful links

Snap It!

Preventing Zero Day Attacks using MITRE ATT&CK Framework

ATT&CK Navigator

AI Technologies White Paper

Learning mode to Best Practice Methodology

Boaz (Batman) Barzel

Yaelle Harel