Let's go

The bridge to possible

Evaluating and Improving Defenses with MITRE ATT&CK

A free and open approach!

Tim Snow, Cyber Architect, APJC
@TimSnowIT

BRKSEC-2227

Agenda

- Introduction
- CTI & ATT&CK Primer
- Know Your Enemy
- Know Yourself
- Trust but Verify
- Focus on Fixes & Iterate
- Conclusion

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Webex App

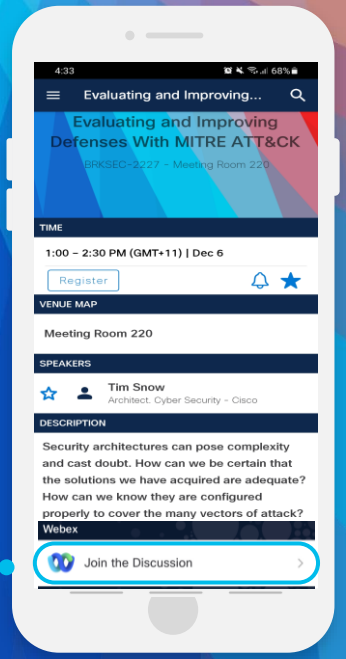
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2227

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Your Speaker

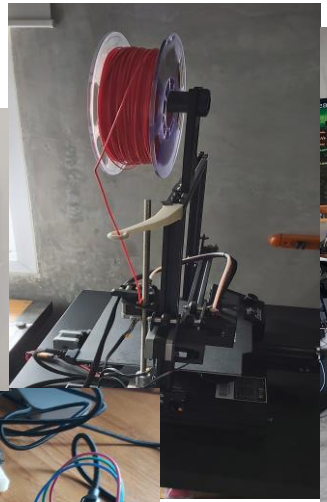
- IT Architect with domain experience in Enterprise Networks (Campus, WAN, DC), Security and Applications
- 20+ Year CCIE
- 18 Years at Cisco in multiple roles

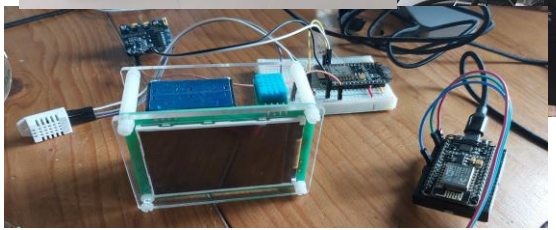
Prior to Cisco

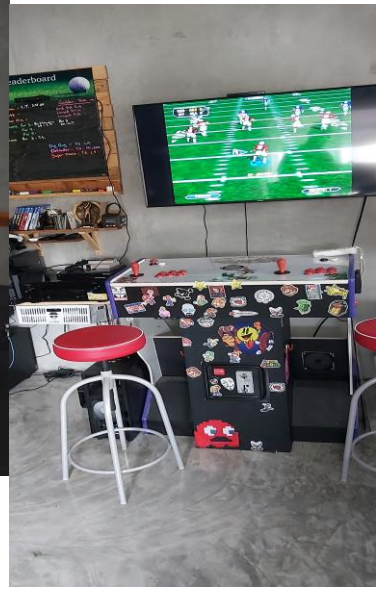
- Comp. Sci major – Michigan
- Developer
- TAC L3 and SecOps

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

About Me







- Canadian, Husband, Father
- Tinkerer – IOT systems
  (automate the things that don't need to be automated)
- 3D Printing and Robotics
  As a way to show my kids tech
- Retro Arcade gaming – growing up in the 80's
- Lifelong beginner at golf

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is this session about?

Background:

- Security through compliance == complex and disjointed
- Checking boxes rarely counters threats

Process:

- Using free vendor neutral ATT&CK framework to identify our threats
- Learn what you can already do (visibility & detection)
- Threat Picture – Security Coverage = Gaps to fill!

Benefit:

- Quick wins beat pain and suffering
- Unified vision for engineering, detections, protection, testing, & operations

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Important: Reference Materials along the way!

- This is a deep topic – they have their own Con!
  - https://www.mitre.org/attackcon
- We're here to discuss using ATT&CK to make your architecture more effective, not point fingers
- Download slides! Includes lots of references to expand on topic of gap assessment
- We will not cover:
  - How-to for red-team (penetration) testing
  - Competitive assessments of coverage
  - Who is good vs. bad – your judgement will vary

For Your Reference

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why do we need Cyber Threat Intelligence (& MITRE ATT&CK?)

Time for a little game. Can you guess?

1. Enterprise-class business and service provider
   - Full-service and turn-key
   - Considered a technical and strategy leader
2. Multi-national, multi-million-dollar org based in Eastern Europe
3. Specializes in Full-Service Data Encryption and Transport
   - Provides or outsources entire chain for customers, both commercial and government
4. Over 125k server environment, heavily “invested” in healthcare
   - Developed Conti, Ryuk, Trickbot

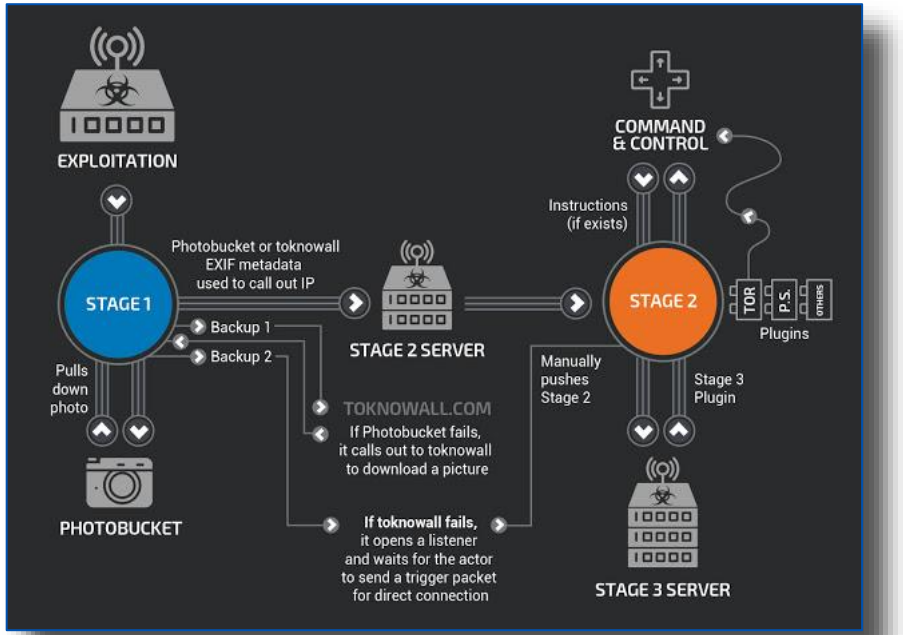
Any guesses???

Wizard Spider (a.k.a. UNC1878, Grim Spider, TempMisMaster, etc.
(https://attack.mitre.org/groups/G0102/)
(https://www.theregister.com/2022/05/18/wizard-spider-ransomware-conti/)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Should <insert APT here> scare you?

Exciting stuff makes the news…Effective practices and remediations do not



VPNFilter, borrowing from BlackEnergy
https://blog.talosintelligence.com/2018/05/VPNFilter.html

- BlackEnergy use limited to Sandworm APT (as far as we know)
  - Are you a former USSR republic's utility?
  - Wielded by skilled attackers – copycat unlikely for now
  - Not disclosed in "Shadow Brokers"–like leak – yet
- But there is always a "but"
  - So far, 23 Techniques attributed that are mimicked in your environments:
    - WMI use, Process injection, Daemon launch, New Services, Discovery, etc.
    - Other tools borrow techniques or overlap (VPNFilter)
  - Each new attack advances the state of the art.
- Bottom Line: *Learn from others, but use your own Threat Picture to prioritize*

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

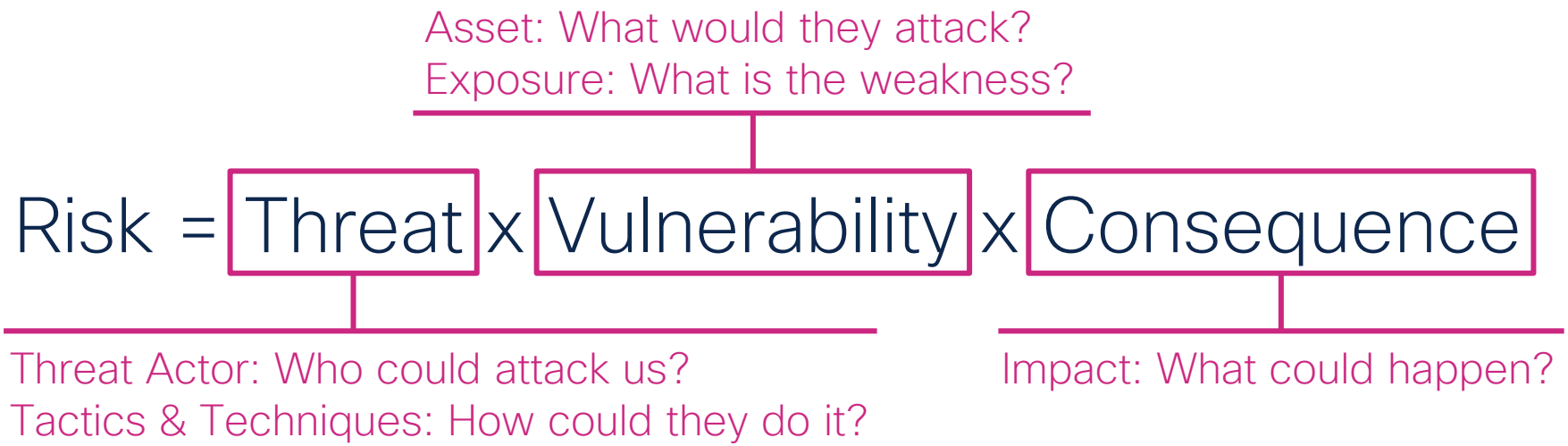
Don’t chase other peoples’ boogiemen

Are you driven by press or by your own threat picture?

- Likely tactics?
  - Everyone exposed to ransomware, phishing: the devil is in the details
  - Ex. Unlikely to see Quantum insert exploits on politically insignificant sites, Magecart in non-commerce, etc.
- Likely adversaries?
  - Threat actors usually concentrate on certain vertical/geography
  - Could be implicated by political affinity, downstream customers (e.g. ISPs for government, banks serving sector)
  - “Cui bono” = to whom will it benefit? Who can benefit from compromising you?
  - Don’t forget the wide-net aspect of threat actors (log4j/log4shell)
- Find and read up your most likely actors through incident reports and CTI

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

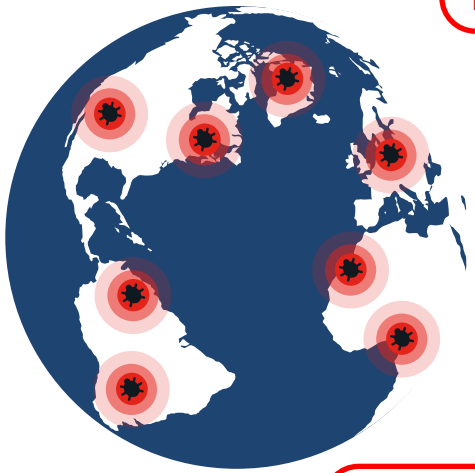
Cybersecurity Risk Formula



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

But where do we start?

Global Threat Picture is complex and overwhelming



Cryptojacking

Dual-Use Tools

Ransomware

Unpatched Software

Data/IP Theft

Spyware/Malware

Code Bugs

Malvertising

Wiper Attacks

Drive by Downloads

Phishing

Rogue Software

Man in the Middle

Botnets

Exposed Datastores

Credential compromise

Advanced Persistent Threats

DDoS

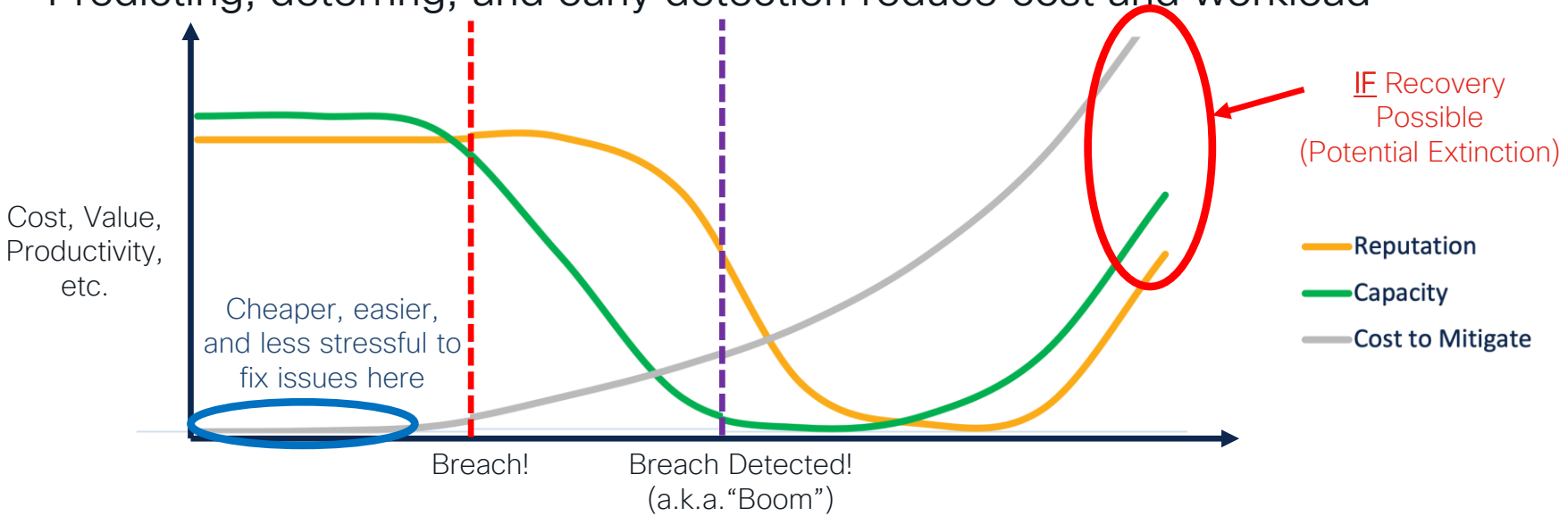
Supply chain attacks

We need to narrow our focus!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

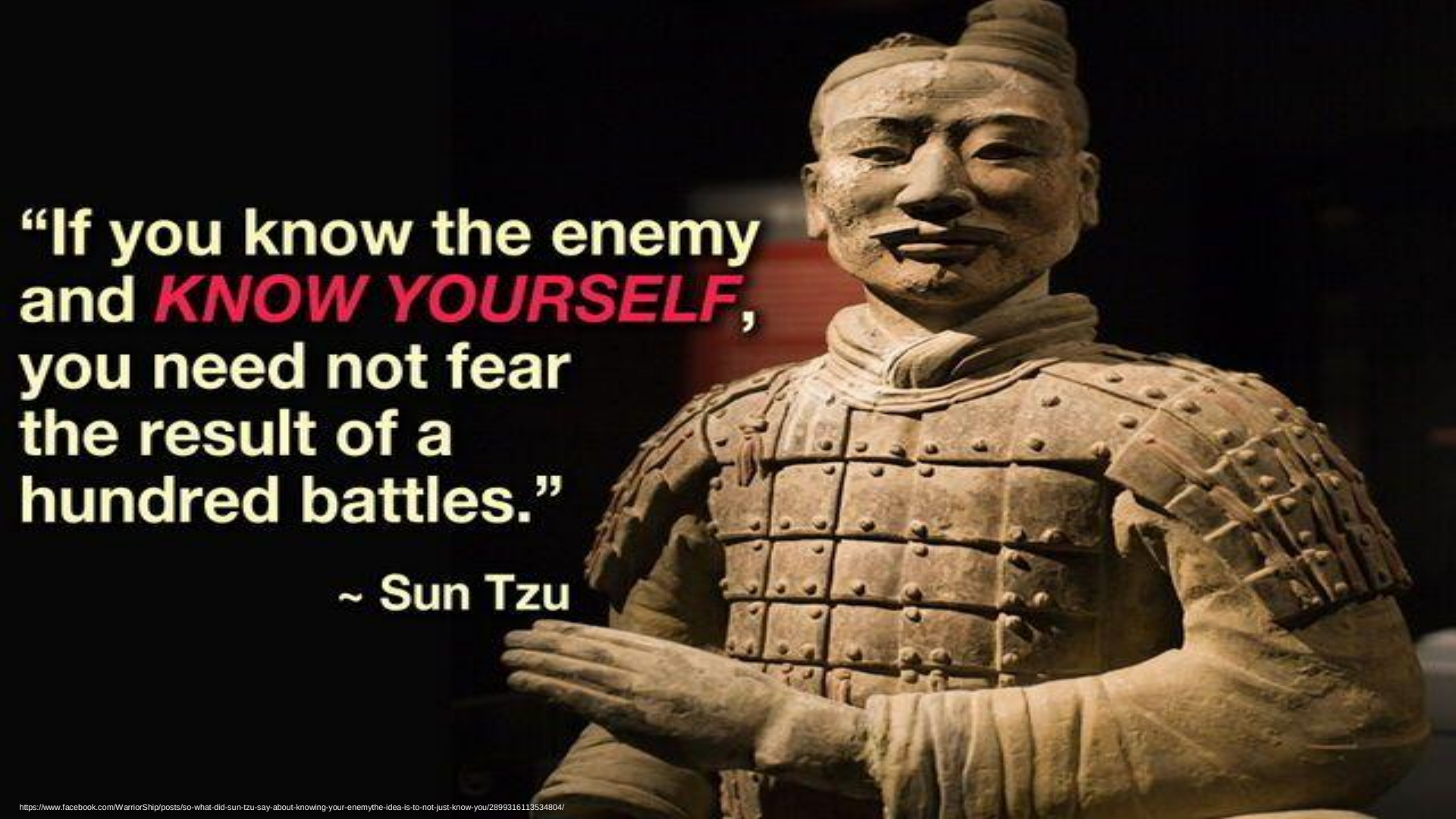
Earlier Detection == Cheaper Mitigation

Predicting, deterring, and early detection reduce cost and workload



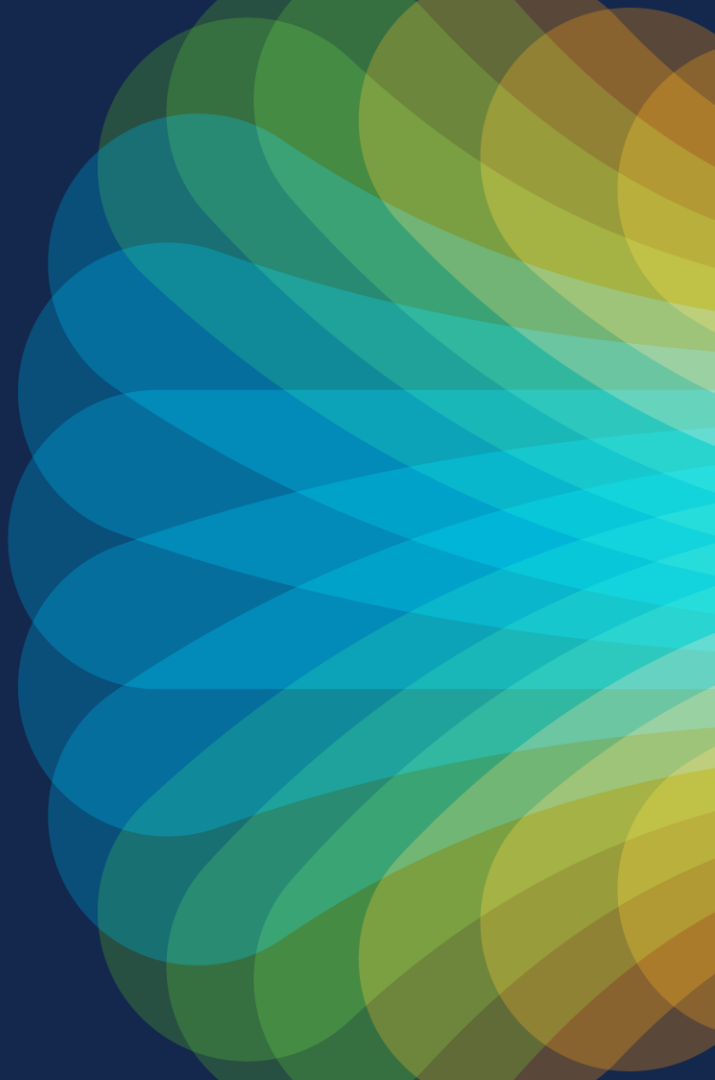
- Better to be "left of boom" – a period when you still have a chance to prepare and avert a crisis
- Earlier & effective controls = better performance, lower pressure/cost, preserved reputation
- CTI relieves pressure! Not just for Global corporations/governments…we all need it!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



https://www.facebook.com/WarriorShip/posts/so-what-did-sun-tzu-say-about-knowing-your-enemythe-idea-is-to-not-just-know-you/2899316113534804/

MITRE ATT&CK Crash Course



cisco Live!

Get to know your adversary with MITRE's ATT&CK

- Who is MITRE Corporation?
  - Not-for-profit, US company with multiple federally funded R&D centers (FFRDCs)
  - Public-private partnerships in many areas, including cybersecurity
  - Same folks who brought us CVE database/list
- What is ATT&CK
  - **A**dversarial **T**actics, **T**echniques, and **C**ommon **K**nowledge
  - Born in 2013 to document tactics, techniques, and procedures (TTPs) that APTs use on Windows networks
  - Globally-accessible knowledge base
  - Used for the development of specific threat models & methodologies in the private sector, in government, and in the cybersecurity product and service community.

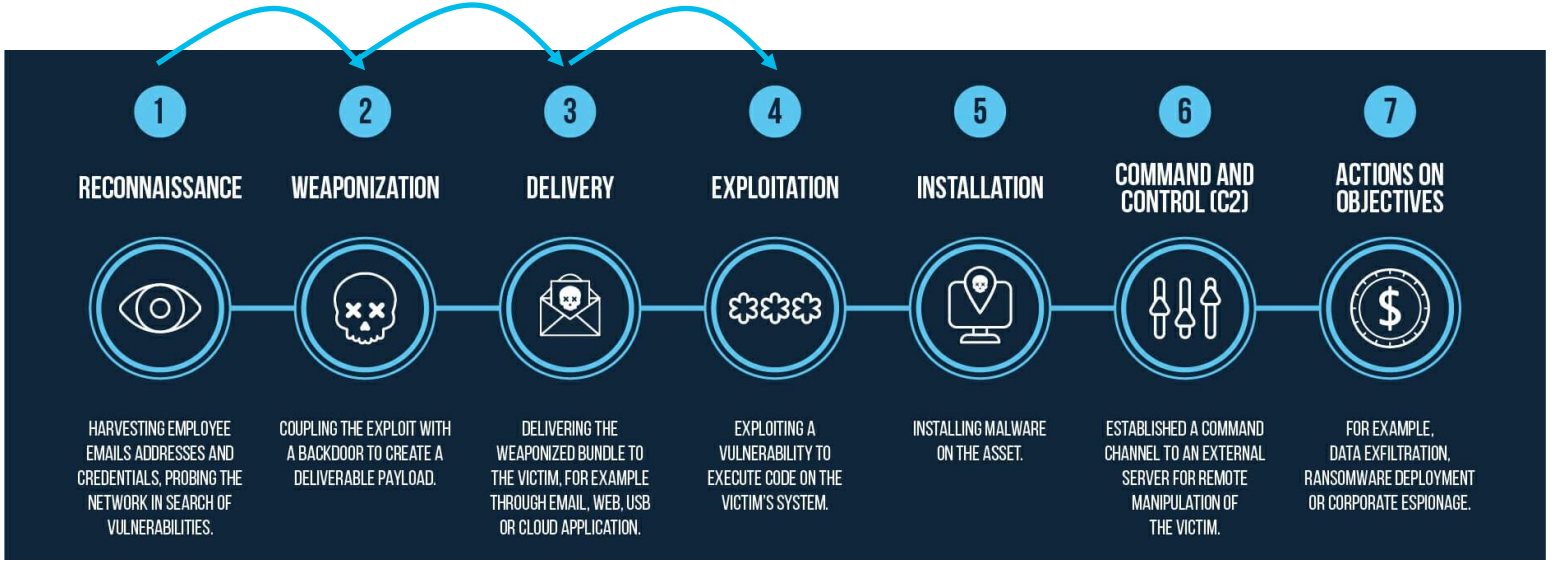
MITRE

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Visualizing the kill chain

CYBER KILL CHAIN VS. MITRE ATT&CK



Cyber Kill Chain focuses on the steps of a cyberattack, whereas MITRE ATT&CK focuses on the tactics and techniques employed by cyber attackers

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

MITRE ATT&CK – TTP's

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is a Tactic?

Tactics represent the "why" of an ATT&CK technique.

It is the adversary's tactical goal: the reason for performing an action.

For example, an adversary may want to achieve credential access.

There are currently 14 Enterprise Tactics

Credential Access

The adversary is trying to steal account names and passwords.

Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

ID: TA0006
Created: 17 October 2018
Last Modified: 19 July 2019

Version Permalink

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is a Technique?

Techniques represent 'how' an adversary achieves a tactical goal by performing an action.

For example, an adversary may dump credentials to achieve credential access.

There are currently 201 Enterprise Techniques

T1003 – Credential Dumping
T1040 – Network Sniffing
T1056 – Input Capture
T1110 – Brute Force

OS Credential Dumping

Sub-techniques (8)

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Sub-Techniques

Sub-techniques are a more specific description of the adversarial behavior used to achieve a goal. They describe behavior at a lower level than a technique.

For example, an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets

T1003 – Credential Dumping

001 LSAAS Memory

....

004 LSA Secrets

....

008 /etc/passwd

OS Credential Dumping: LSA Secrets

Other sub-techniques of OS Credential Dumping (8)

Adversaries with SYSTEM access to a host may attempt to access Local Security Authority (LSA) secrets, which can contain a variety of different credential materials, such as credentials for service accounts.[1][2][3] LSA secrets are stored in the registry at `HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets`. LSA secrets can also be dumped from memory.[4]

Reg can be used to extract from the Registry. Mimikatz can be used to extract secrets from memory.[4]

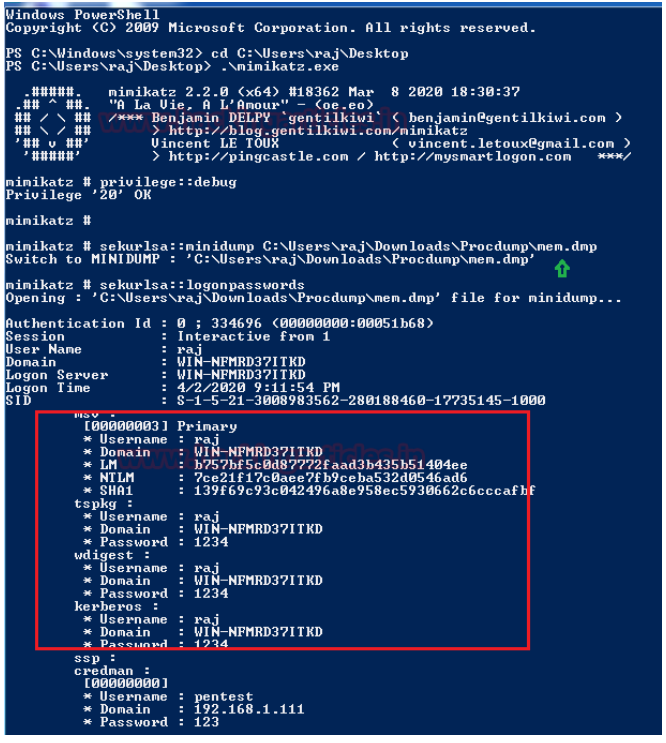
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is a Procedure?

Procedures are the specific implementation the adversary uses for techniques or sub-techniques.

For example, a procedure could be an adversary using a sysinternals tool to dump the local system policy, password hashes, etc and then run mimkatz to read the memory dump.

Procedures are categorized in ATT&CK as the observed “in the wild” use of techniques in the "Procedure Examples" section of technique pages



The Smash and Grab

https://media.yourobserver.com/img/photos/2022/04/28/photo-1-9672-20110110173546_t1100.jpg?31a214c4405663fd4bc7e33e8c8cedcc07d61559

https://as1.ftcdn.net/v2/jpg/02/77/16/52/1000_F_277165295_Qlw1TtYPPlu53uMHIii3klBb9zFxPePf.jpg

https://content.api.news/v3/images/bin/02143ab9e54077b712accad3fa3f612b?width=320

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Heist

https://www.theguardian.com/world/2017/oct/04/brazil-bank-robbery-sao-paulo-tunnel

eastnews.co.ug/blow-by-blow-account-of-how-police-tracked-nwsc-dressed-robbers&server=hkg1&prefs=&tagging=&nref

https://www.observerbd.com/news.php?id=416493

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

What MITRE ATT&CK is NOT!

(1)

- A Compliance Framework
- An Architecture
- A miracle cure or all-encompassing guide
- A guarantee of Efficacy or Success
  - Coverages is not always indicative of detections
  - Not all Techniques or Sub-techniques are equal in impact
  - Same technique may have vastly different risk depending on factors such as environment, host, threat etc.

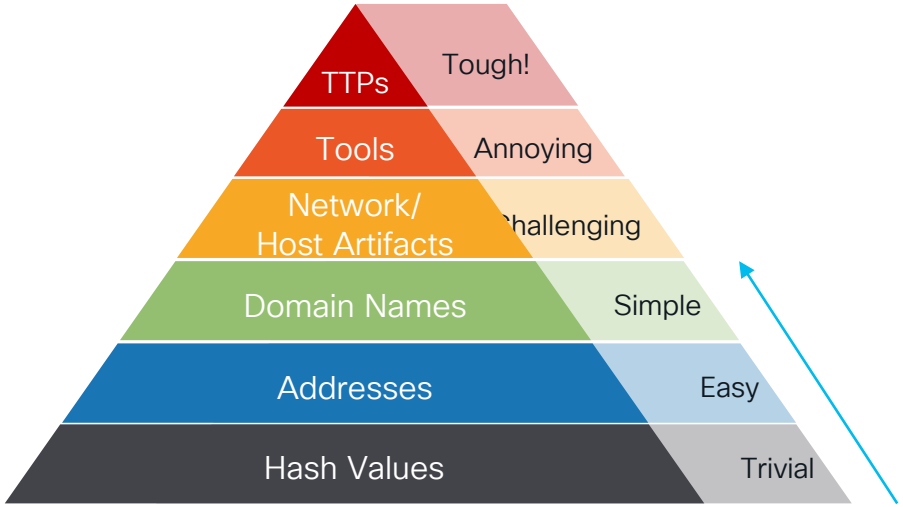
- Lastly – It is not Exhaustive.
  - ATT&CK draws on public knowledge
  - Many TTPs are not yet public or discovered

(1) https://www.istockphoto.com/vector/funny-stickman-gm1291051473-386274494

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

ATT&CK changes our focus

Concentrate on the root of the problem to achieve security enlightenment



From David Biacco:
https://www.eventtracker.com/blog/2015/february/the-pyramid-of-pain/

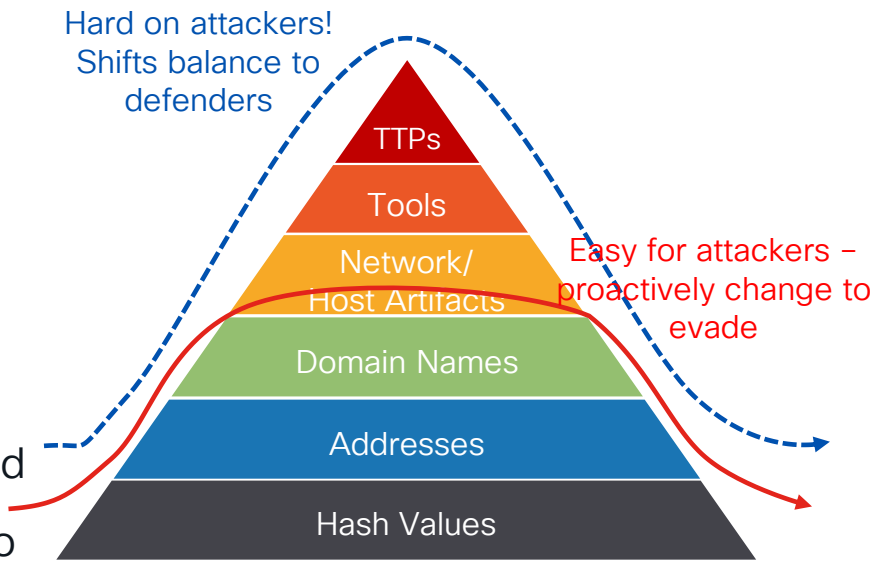
- TTPs, a.k.a. “The Problem”:
  - Good: TTPs behaviors ingrained in adversary – much harder to modify
  - Bad: Behavior defies checking boxes
  - HARD to tackle = conceptual, prone to false positives/negatives without good context
- IOCs, a.k.a. “The Symptom”:
  - Good: Generally, focus on are easily tracked attributes – “tangible”
  - Bad: easily tracked attributes are easily changed – Attacker advantage

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Push the adversary to change

Why should the defender always sweat it out?

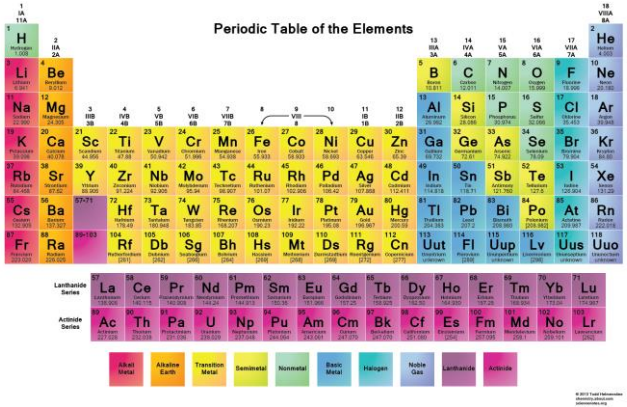
- Time-based security: protection buys time.
  - Will always fail – must detect and remediate before that happens
- Forcing TTP changes → harder on adversaries
  - Changing TTP (or tooling) takes time, depletes resources, and exhausts funds
  - Strategic shifts create more detectable events
- Adversaries may leave, or become frustrated
- Defenders can – with commitment – work to force the paradigm shift

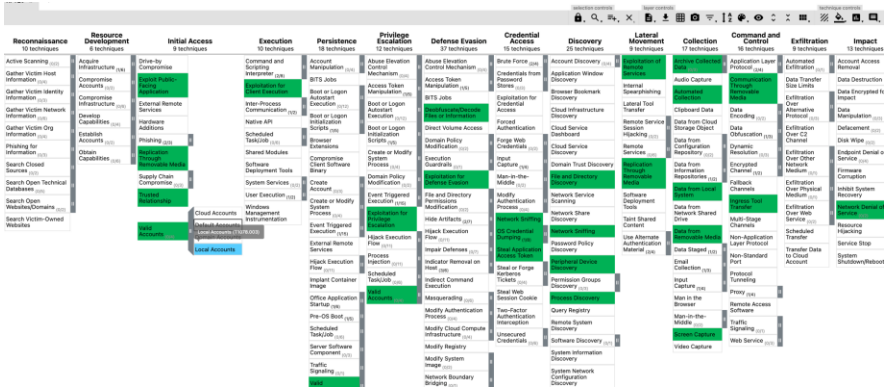


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Alchemy of Adversarial Behavior

Techniques are the Elements, bonded together to form APT patterns





- Groups (similar behavior/valence band)
- Elements and their oxidation states
- MSDS Sheets
- Molecules
- Compounds drastically different than elements that form them

- Tactics (base on similar adversarial goals)
- Techniques and their Sub-Techniques
- Mitigations
- Adversaries
- Adversaries drastically different despite using similar techniques but in different ways

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is inside ATT&CK?

Enterprise Matrix as an example...

Open-Source CTI
Blog Entries
MITRE R&D
Community Feeds

- Detection Tips
- STIX/TAXII Feeds
- Navigator Matrix
- Open-Source Tools

Key platforms:

- OS: Windows, macOS, Linux
- Cloud (IaaS & SaaS)
- O365, Google Workspaces
- Containers, Network, VMs
- iOS & Android

14 Tactics

201 Techniques &
424 Sub-techniques

Employed By

143 Groups

Implemented Thru

760 Software Applications

43 Mitigations

Enterprise | Mobile | ICS

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The 5 W's plus an H of Threat Modeling

My English teacher would be so proud...

• **Who** is threatening us?	Group
• **What** are they doing?	Technique
• **Why** are they doing it?	Tactic
• **How** are they doing it?	Procedure and/or Software
• **Where** can we prevent it?	Mitigation
• **When** are we going to notice?	Detection

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Understand your ATT&CK Model Relationships

MITRE's approach simplifies mapping goals to behaviors (a.k.a. TTPs)

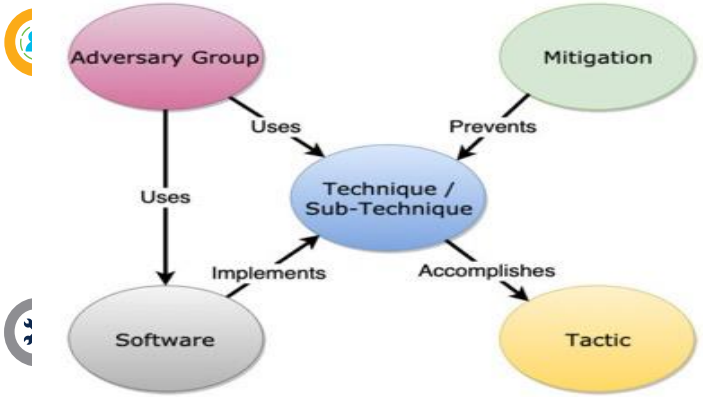
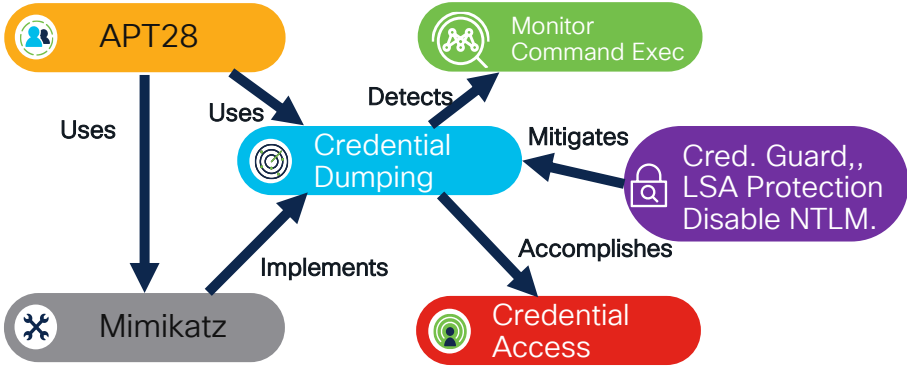


Figure 3. ATT&CK Model Relationships

- Detections or Mitigations can happen in Software, Technique, or Tactics
- https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy

MITRE Advice on Detection for T1003.001
(OS Credential Dumping: LSASS Memory)

- Monitor event IDs 10, 4104, 4633 and 4688
- Find process where target = "*lsass.exe" AND source is taskmgr.exe



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Before we start – let's understand our environment

We're a 30k employee healthcare network, based in APJC

- 6 hospital campuses, 50 out-patient clinics & urgent care facilities.
- Well architected infrastructure, but due for refresh
- Windows endpoints, Windows/Linux servers 80/20, with shift to Cloud (~30% of workloads and slowly increasing)

- Staffing: 15 FTEs dedicated to security (CISO, 3 Managers, 2 architects, 9 Engineer/Analysts)
- Training and operating – not enough time!
- ~50 vendors in or adjacent to Security

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Navigator Demo

Know your Enemy

ATT&CK v14 has been released! Check out the blog post or release notes for more information.

ATT&CK®

Getting Started | Take a Tour

Contribute | Blog

FAQ | Random Page

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

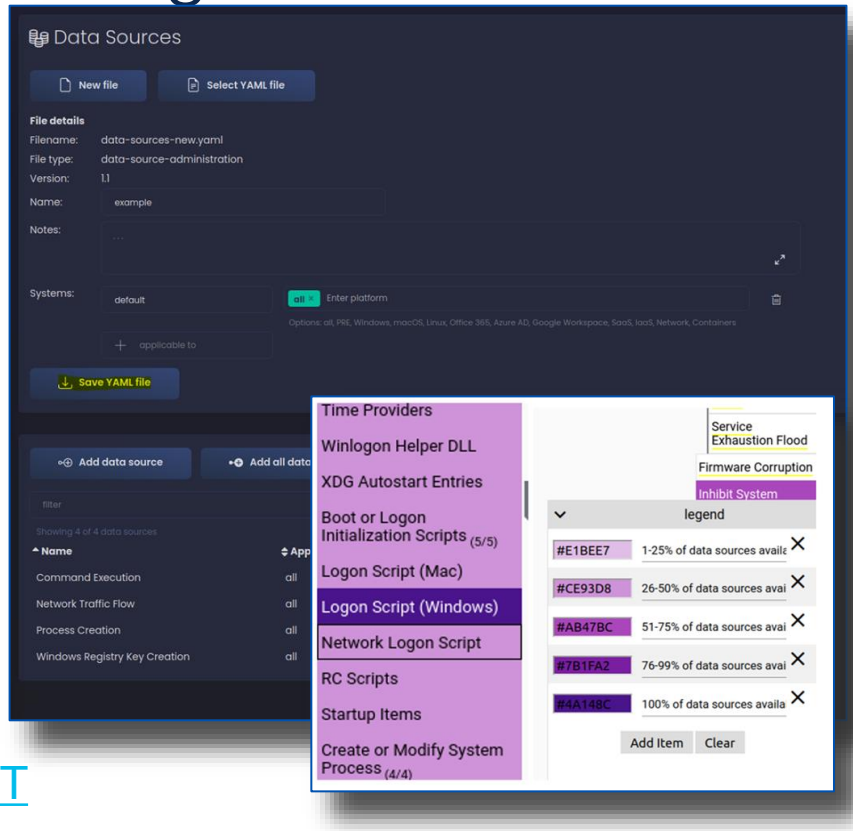
layout: flat | show sub-techniques | hide sub-techniques

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

Know Yourself

DeTT&CT helps provide coverage matrices

- Python tool that tailors YAML files to derive ATT&CK Navigator coverage matrices. (local or Docker)
- Quantitative analysis of logging and visibility coverage
  - OS-focused
  - Generic coverage for AV and tools – better using Enginuity or Vendor-validated
- Optimal coverage assumed – contingent on proper configuration



https://github.com/rabobank-cdc/DeTTECT

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

DeTT&CT Demo

Demo brought to you by

Mike McPhee
Architect. Cisco

Raiders of the lost ARP
https://raidersofthelostarp.tech/

Best Friends: What makes the Diamond Model a useful threat modeling tool for analysts?

A Retro Feast for the Family: The Cyber Kill Chain

NOVEMBER 22, 2023 · MIKE · 0 COMMENTS

Americans reading this may be like me and headed towards a food coma. My gift to you? I give you a crowd-pleasing topic for family banter. Rather than argue over controversial topics, avoiding Aunt Mildred's hugs, or snoozing through a futile Cowboys game, cook up a retro feast for the family with the Cyber Kill Chain! If you've seen the "Fishes" episode of The Bear, you know how bad things can get. So consider this your safe topic, one everybody can enjoy. Your kids will thank you. Your family will be prepared to defend against nation state threats while bickering over the wishbone. Relative peace AND security? You're welcome.

The Basics of the Cyber Kill Chain

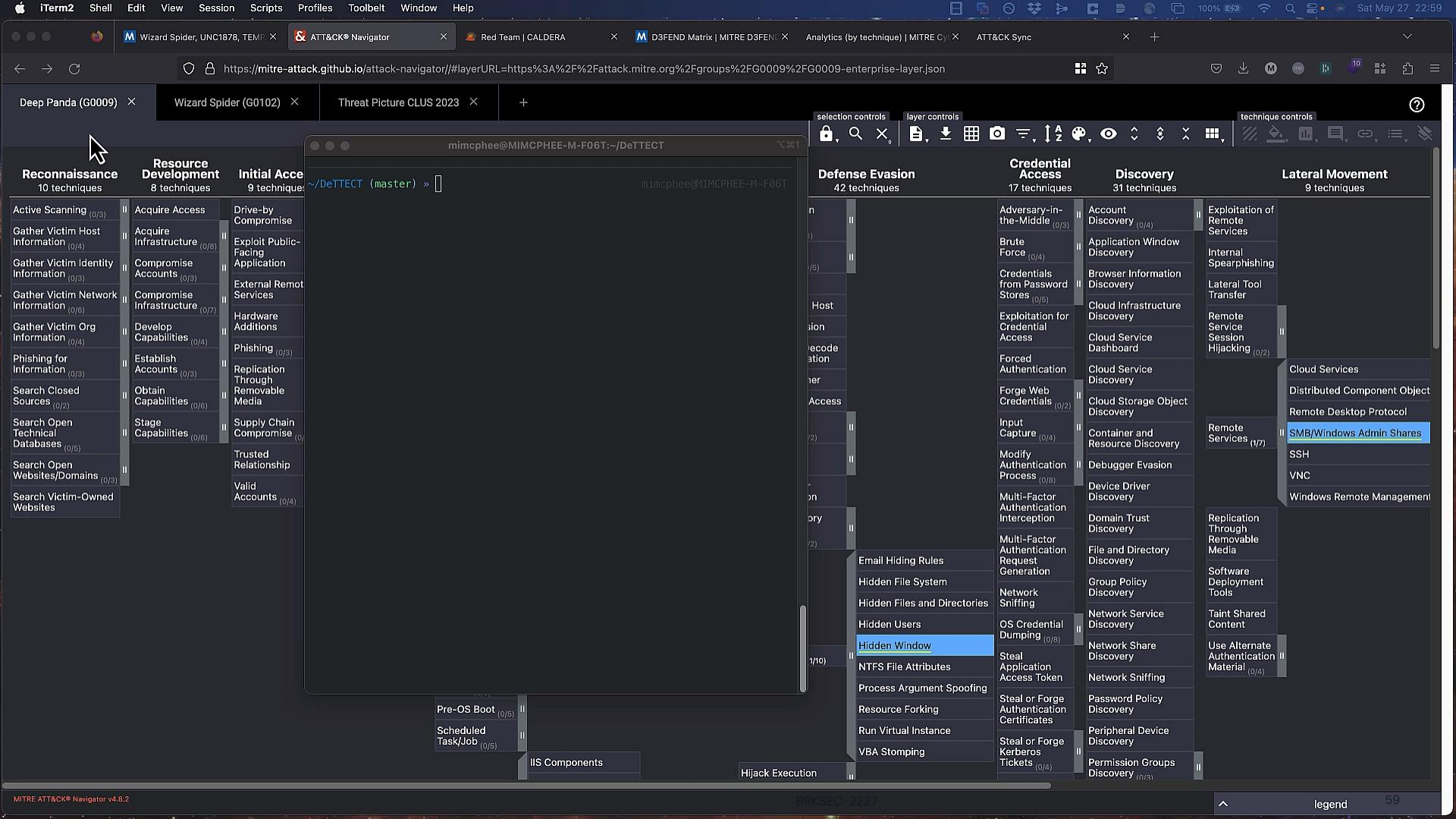
It's been a rough year for Stu. He just never was able to untangle his SOC's stack. AI drew him with 4 legs, and he missed a CISA bulletin about Thanksgiving scams...

Gap Analysis With ATT&CK: Fix Your Posture, Young Man!

NOVEMBER 19, 2023 · MIKE · 0 COMMENTS

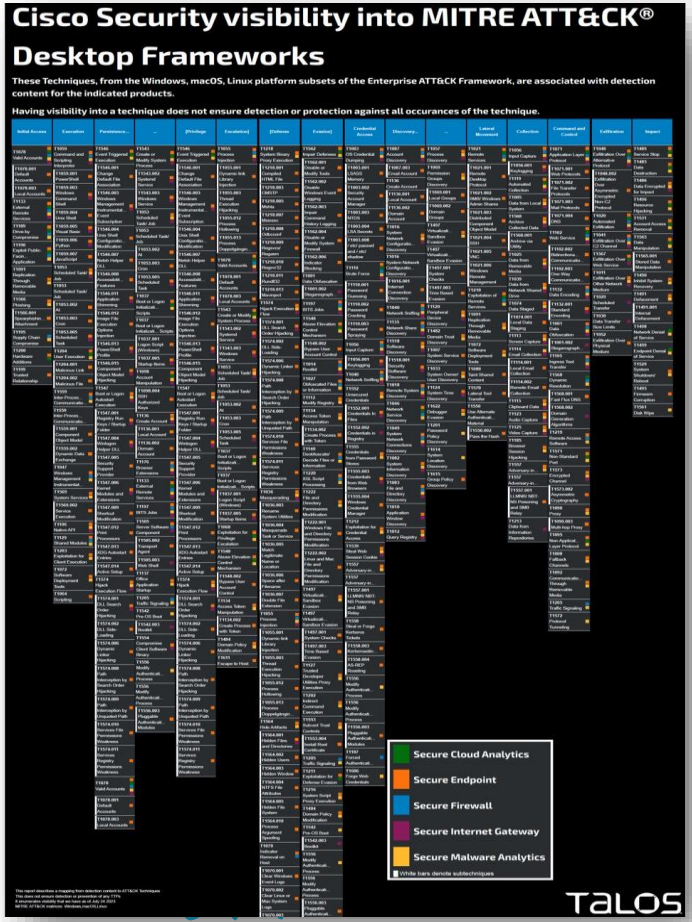
Early adopters certainly focused on using ATT&CK for glamorous use cases like Threat Intelligence and Adversary Emulation. Conducting gap analysis with ATT&CK to prioritize engineering efforts is a high-return effort for you and your organization. It's my favorite of the use cases because it can help any organization!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public


iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help
Wizard Spider, UNC1878, TEMP
ATT&CK® Navigator
Red Team | CALDERA
D3FEND Matrix | MITRE D3FEND
Analytics (by technique) | MITRE CV
ATT&CK Sync
https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0009%2FG0009-enterprise-layer.json
Deep Panda (G0009)
Wizard Spider (G0102)
Threat Picture CLUS 2023
selection controls
layer controls
technique controls
mimcphee@MIMCPHEE-M-F06T:~/DeTTECT
~/DeTTECT (master) »
Reconnaissance
10 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (0/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/7)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (0/6)
Stage Capabilities (0/6)
Initial Acce
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remot Services
Hardware Additions
Phishing (0/3)
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts (0/4)
Defense Evasion
42 techniques
Email Hiding Rules
Hidden File System
Hidden Files and Directories
Hidden Users
Hidden Window
NTFS File Attributes
Process Argument Spoofing
Resource Forking
Run Virtual Instance
VBA Stomping
Pre-OS Boot (0/5)
Scheduled Task/Job (0/5)
IIS Components
Hijack Execution
Credential Access
17 techniques
Adversary-in-the-Middle (0/3)
Brute Force (0/4)
Credentials from Password Stores (0/5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Modify Authentication Process (0/8)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/4)
Discovery
31 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (0/3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (1/7)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)
Cloud Services
Distributed Component Object
Remote Desktop Protocol
SMB/Windows Admin Shares
SSH
VNC
Windows Remote Management
MITRE ATT&CK® Navigator v4.8.2
BRKSEC-2227
legend
59

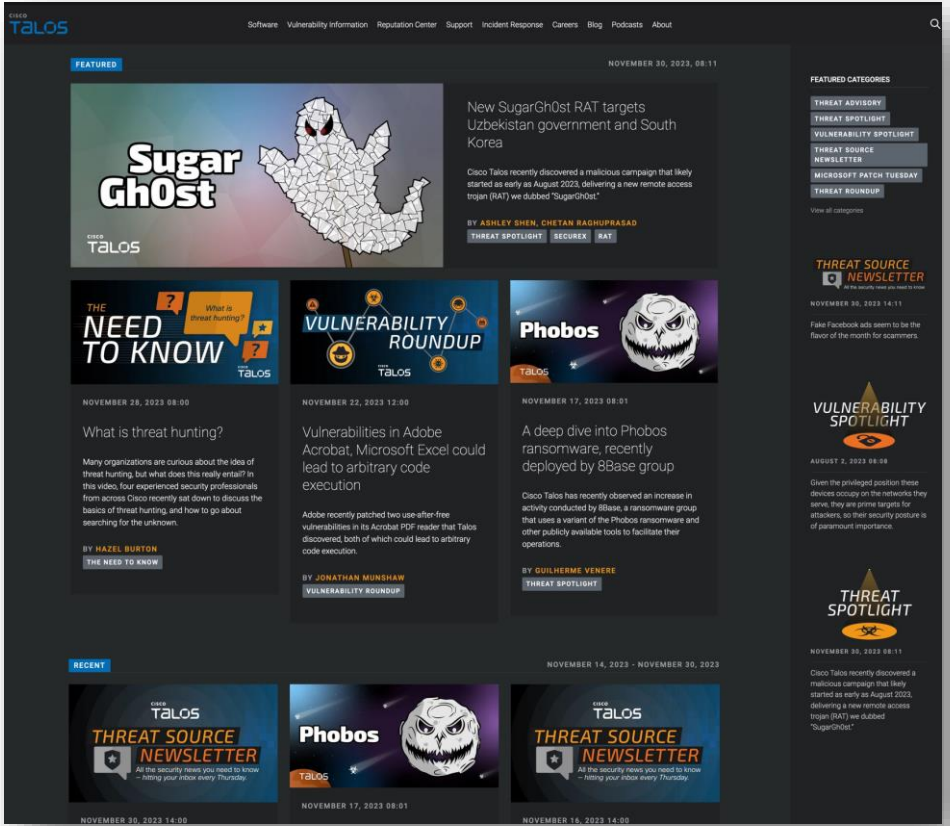
How do Cisco tools align with the framework?

Cisco Mapping to MITRE ATT&CK



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

TalosIntelligence.com



- Blogs
- Threat Spotlights
- Beers with Talos
- Software Tools
- Vulnerability Reports
- Searchable Reputation Database

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

TalosIntelligence.com

New SugarGh0st RAT targets Uzbekistan government and South Korea

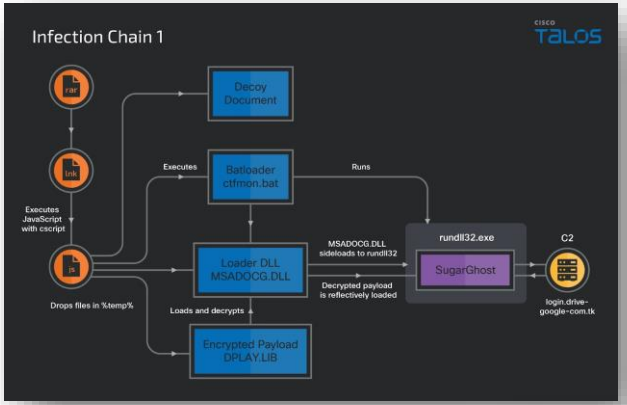
By Ashley Shen, Chetan Raghuprasad

THURSDAY, NOVEMBER 30, 2023 08:00

THREAT SPOTLIGHT | SECUREX | RAT

- Cisco Talos recently discovered a malicious campaign that likely started as early as August 2023, delivering a new remote access trojan (RAT) we dubbed "SugarGh0st."
- We found evidence suggesting the threat actor is targeting the Uzbekistan Ministry of Foreign Affairs and users in South Korea.
- We assess with high confidence that the SugarGh0st RAT is a new customized variant of Gh0st RAT, an infamous trojan that's been active for more than a decade, with customized commands to facilitate the remote administration tasks as directed by the C2 and modified communication protocol based on the similarity of the command structure and the strings used in the code.
- We observed two infection chains leveraging Windows Shortcut embedded with malicious JavaScript to deliver the components to drop and launch the SugarGh0st payload.
- In one infection chain, the actor leverages the DynamixWrapperX tool to enable Windows API function calls in malicious JavaScript for running the shellcode.
- Talos assesses with low confidence that a Chinese-speaking threat actor is operating this campaign based on the artifacts we found in the attack samples.

Suspected Chinese Actor targeting Uzbekistan and South Korea



Mitre ATT&CK mapping

All of the previously described TTPs that were observed in this attack are listed below based on the phase of the attack in which they occurred.

Initial Access

ATT&CK Technique : Phishing (T1566)

ATT&CK Technique : Valid Accounts (T1078)

Execution

ATT&CK Technique : System Services: Service Execution (T1569.002)

Persistence

ATT&CK Technique : Create Account: Local Account (T1136.001)

ATT&CK Technique : Account Manipulation: Device Registration (T1098.005)

Privilege Escalation

ATT&CK Technique : Event Triggered Execution: Image File Execution Options Injection (T1546.012)

Defense Evasion

ATT&CK Technique : Indicator Removal on Host (T1070)

ATT&CK Technique : Indicator Removal on Host: Clear Windows Event Logs (T1070.001)

ATT&CK Technique : Masquerading: Match Legitimate Name or Location (T1036.005)

ATT&CK Technique : Impair Defenses: Disable or Modify System Firewall (T1562.004)

ATT&CK Technique : Modify Registry (T1112)

IOCs

DOMAINS - COMMON:
windows[.]menu

IP'S - COMMON:
52.149.228[.]45

20.46.245[.]56

HASHES - COMMON:
Apply.ps1

D97088F9795F278B868732D57F42CBD725A6139AFE13E31AE832A5C947099676

defender.vbs

B54DD21019AD75047CE74FE0A0E608F56769933556AED22D25F4F8B01EE0DA15

HASHES - BLACKCAT:
Reverse-ssh (compiled with hardcoded domain):

47AFFAED55D85E1EBE29CF6784DA7E9CDBDB6020DF882E9162A0B1A67F092DCD

stealer:

65DBAFE9963CB15CE3406E50E007408DE7D12C98668DE5DA10386693AA6CD73

Blackcat ransomware:

060CA3F63F3887804420729CDE3FC30D126C2A0FFC0104B8E698F78EDAB96767

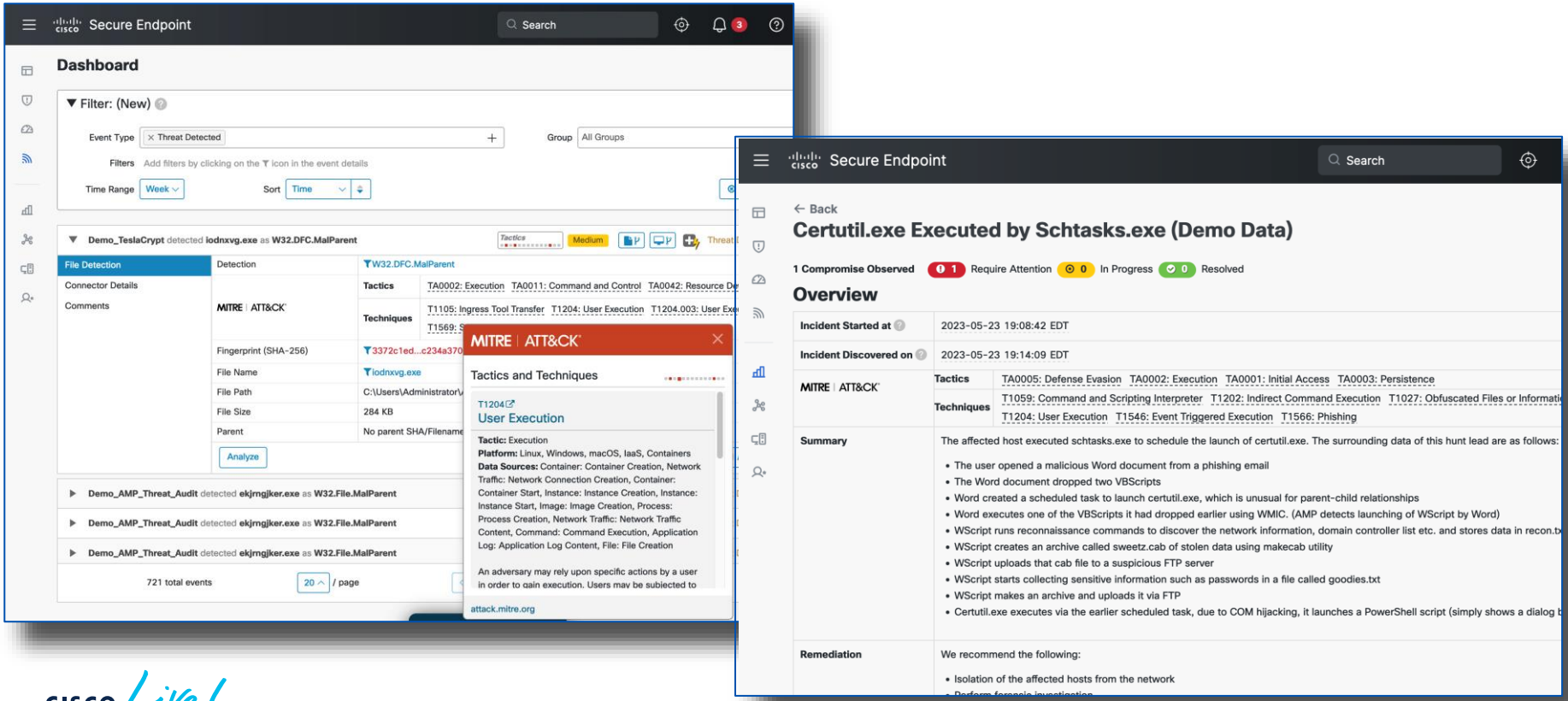
HASHES - BLACKMATTER:
BlackMatter ransomware:

706F3EEC328E91FF7F66C8F0A2FB9B556325C153A329A2062DCB5879C540839D

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Endpoint flags ATT&CK TTPs

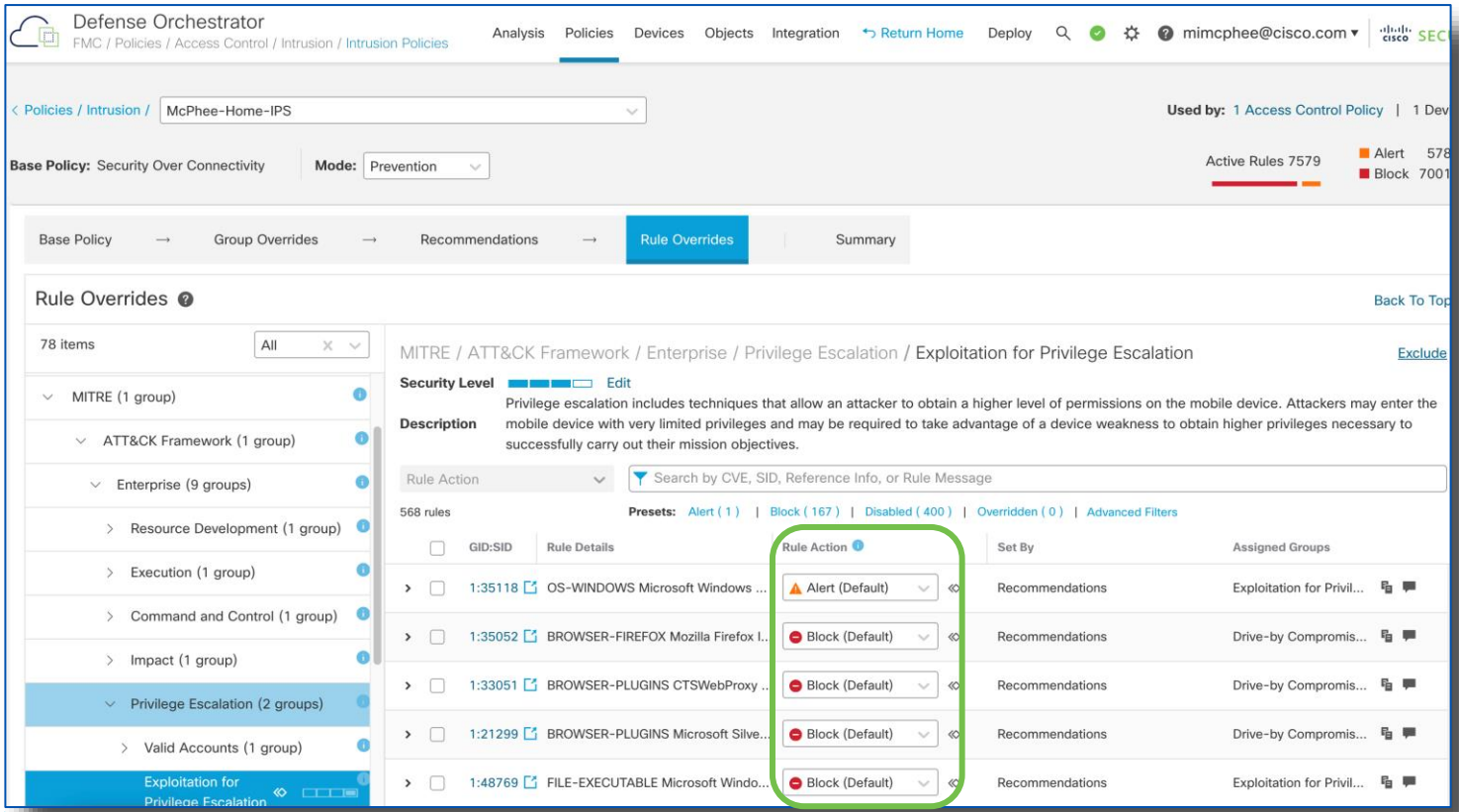
Enrichment available in Events, Threat Hunting, and Analysis portions of the tool



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Firewall Rules to cover TTPs

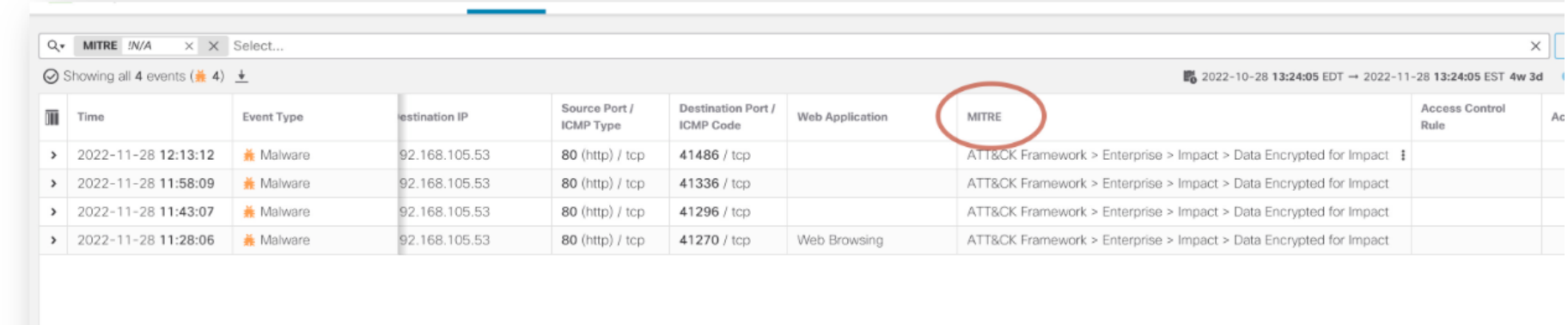
In FTD 7.3, IPS rules can be implemented per tactic or technique.



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Firewall

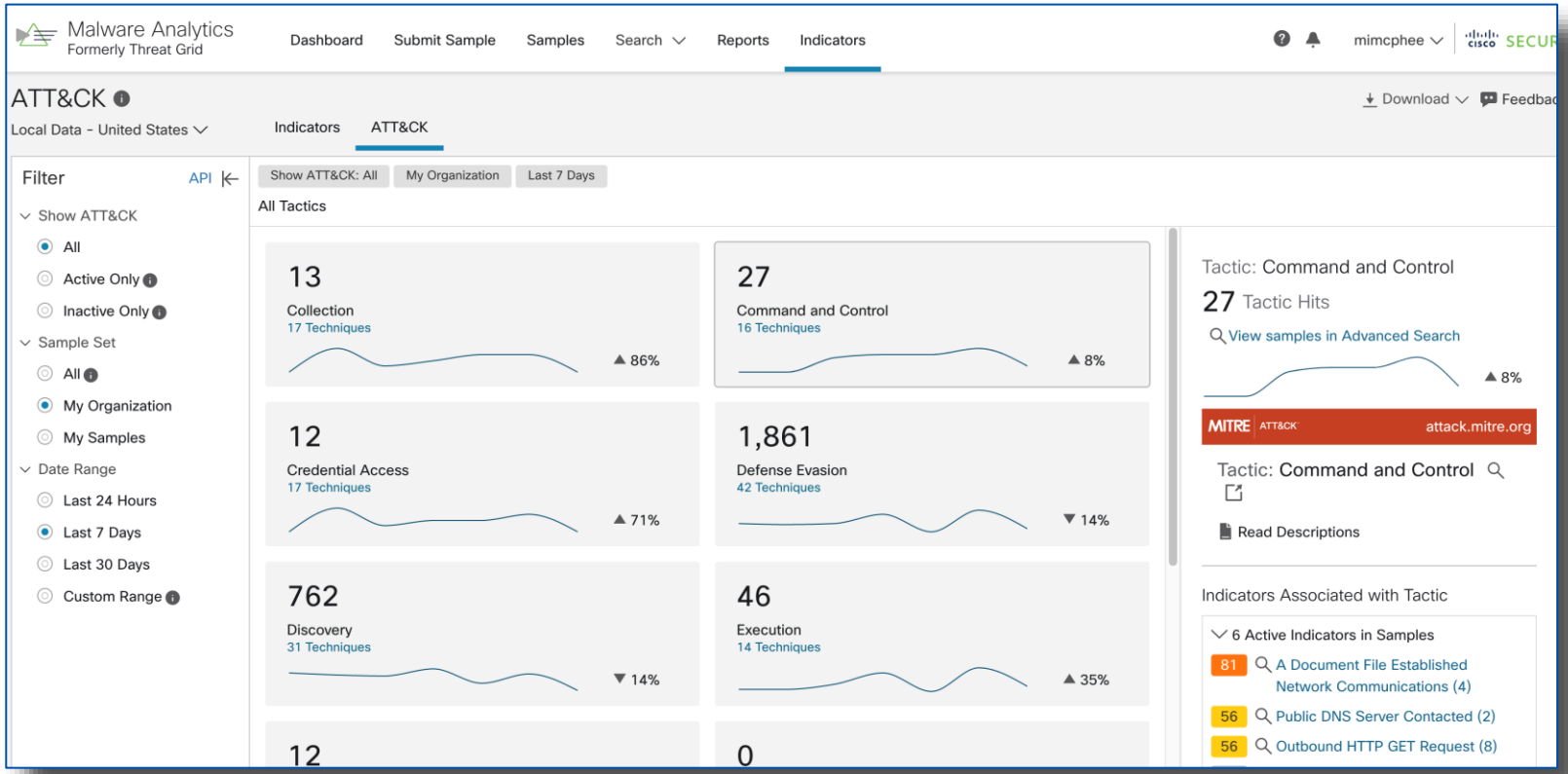
Unified event viewer. The MITRE column is new. It is hidden by default.



7.3 – Introduction of IPS Mappings
7.4 – Introduction of Malware Mappings to AV Signatures

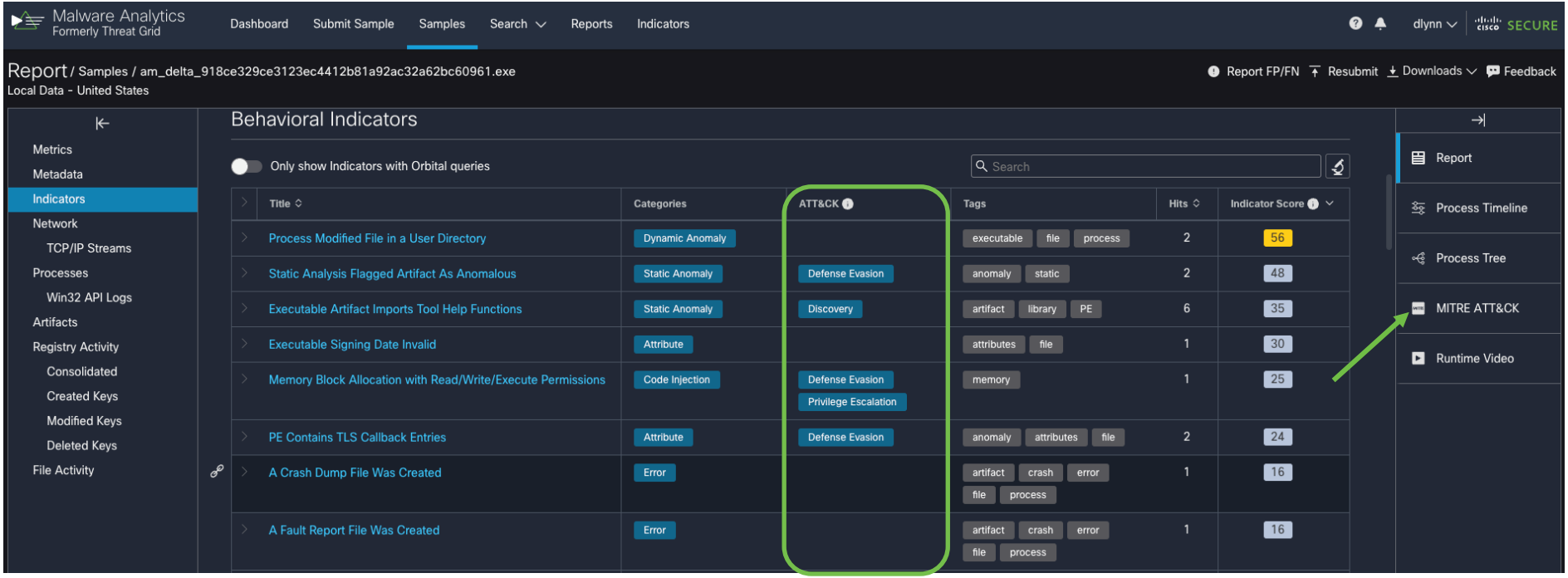
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Malware Analytics



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

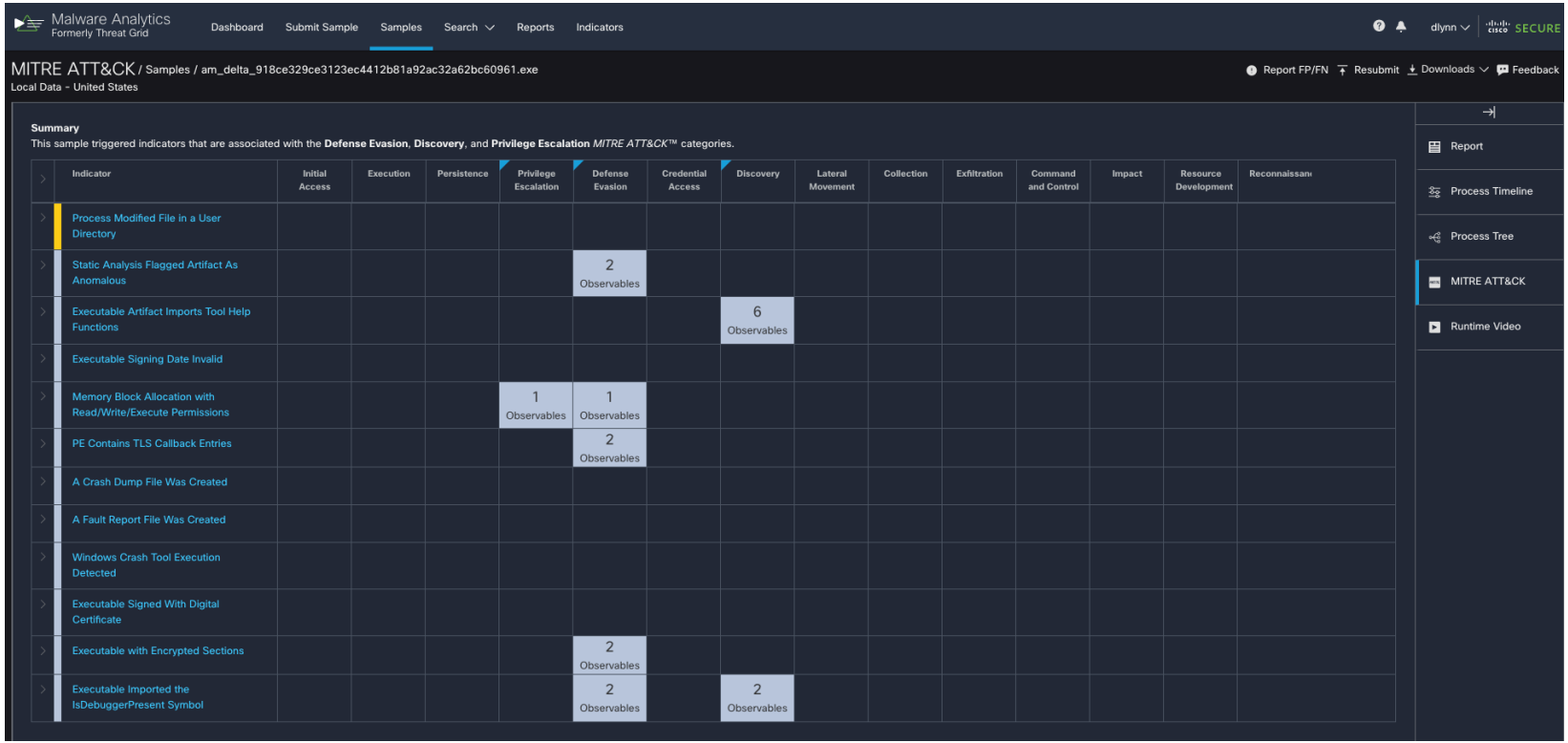
Cisco Secure Malware Analytics



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

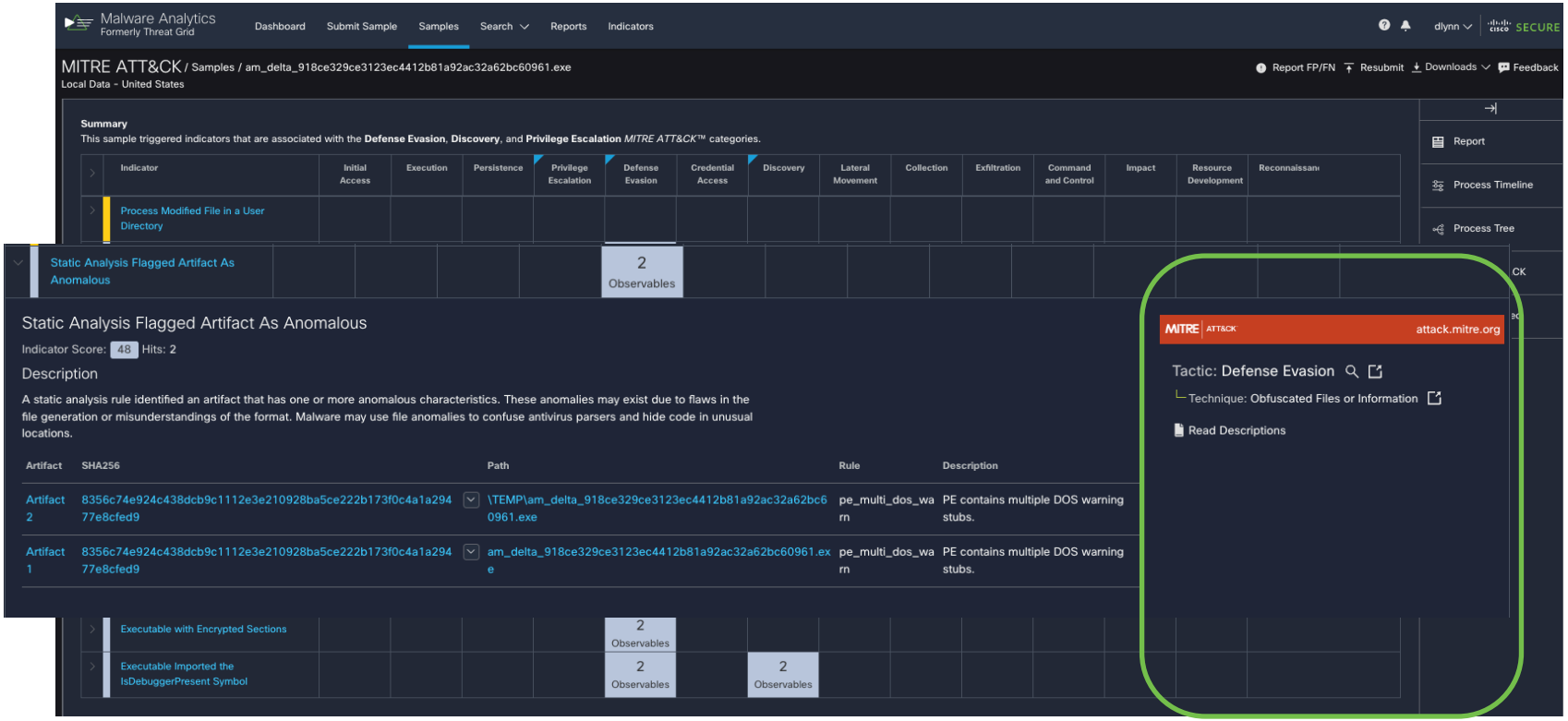
Cisco Secure Malware Analytics

Behaviours mapped to MITRE ATT&CK within a Sample Submission



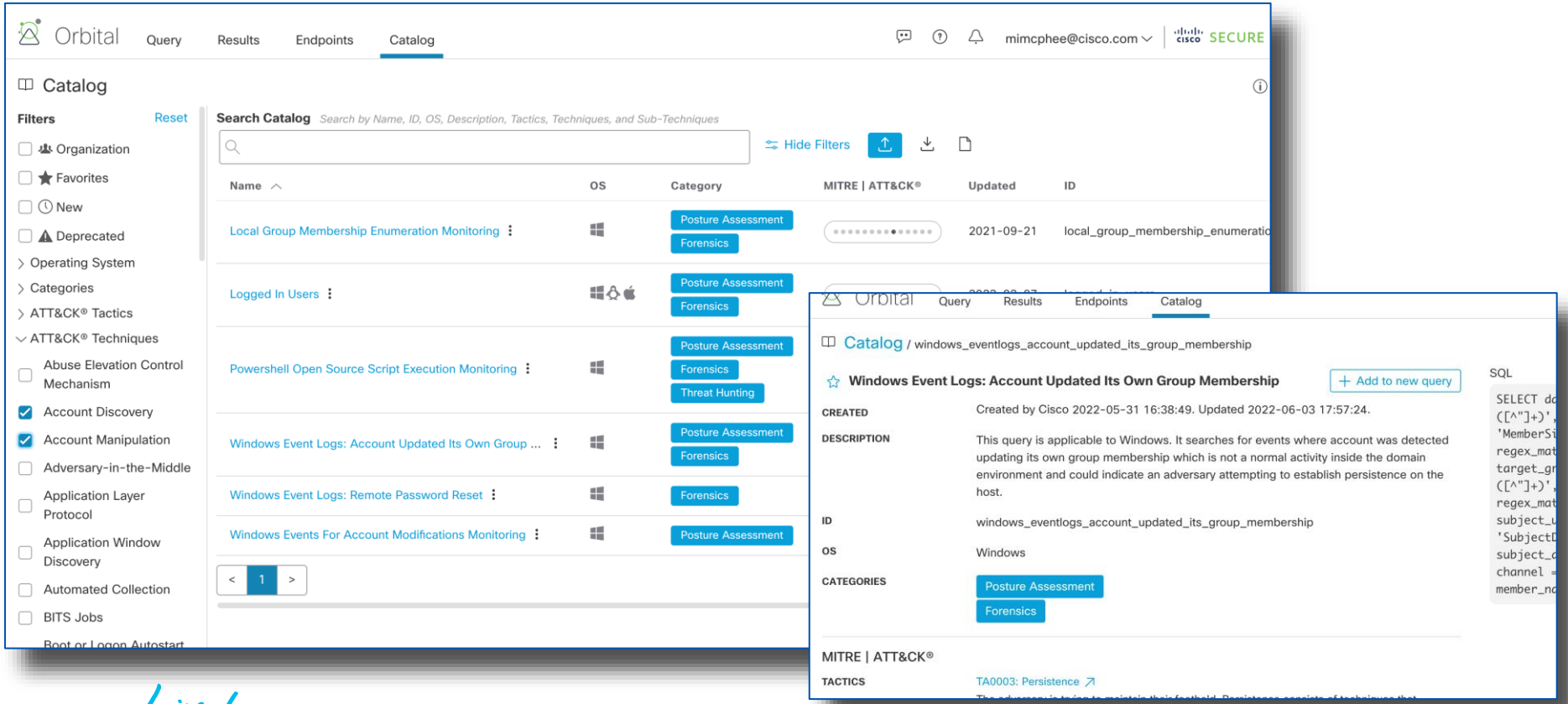
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Malware Analytics



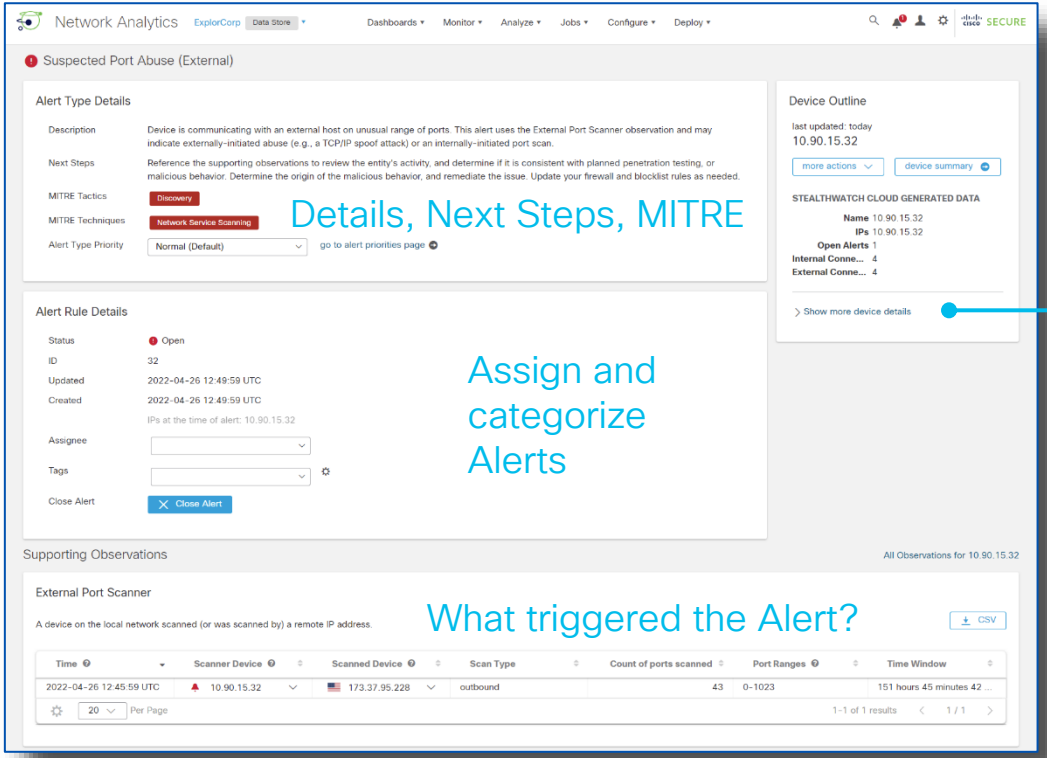
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

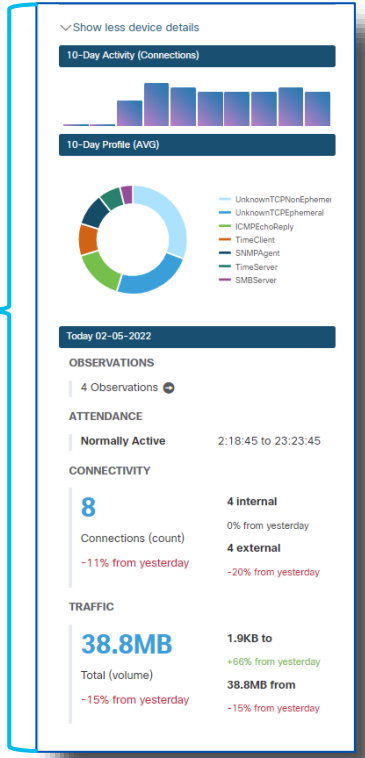
Orbital helps proactively query endpoints for TTPs



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Network Analytics





Device Details

- 10 Day Connection Graph
- 10 Day traffic profile
- Last 24hr Observations
- Activity comparison for connections and traffic bandwidth

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mapping to the MITRE ATT&CK Enterprise matrix

Reconnaissance
- Active Scanning
- Gather Victim Host Information
- Gather Victim Network Information

Credential Access
- Brute Force
- LLMNR/NBT-NS Poisoning and Relay

Resource Development
- Compromise Infrastructure

Discovery
- Account Discovery
- Network Service Scanning
- Network Share Discovery
- Remote System Discovery
- System Information Discovery
- System Network Connections Discovery
- System Service Discovery

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Spearphishing Attachment
- Spearphishing Link
- Trusted Relationship
- Valid Accounts

Lateral Movement
- Exploitation of Remote Services
- Remote Desktop Protocol
- Remote Services
- SMB/Windows Admin Shares
- Software Deployment Tools
- Windows Remote Management

Execution
- Exploitation for Client Execution
- PowerShell
- Windows Management Instrumentation

Collection
- Archive Collected Data
- Data from Information Repositories
- Data from Network Shared Drive
- Data Staged
- Email Collection

Persistence
- BITS Jobs
- External Remote Services
- Port Knocking
- Valid Accounts

Command and Control
- Commonly Used Port
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Enorypted Channel
- External Proxy
- Fallback Channels
- Internal Proxy
- Multi-hop Proxy
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Port Knocking
- Remote Access Software
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Uncommonly Used Port
- Web Service

Privilege Escalation
- Valid Accounts

Exfiltration
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Scheduled Transfer

Defense Evasion
- BITS Jobs
- Masquerading
- Network Boundary Bridging
- Port Knocking
- Rogue Domain Controller
- Valid Accounts

Impact
- Endpoint Denial of Service
- Network Denial of Service
- Resource Hijacking

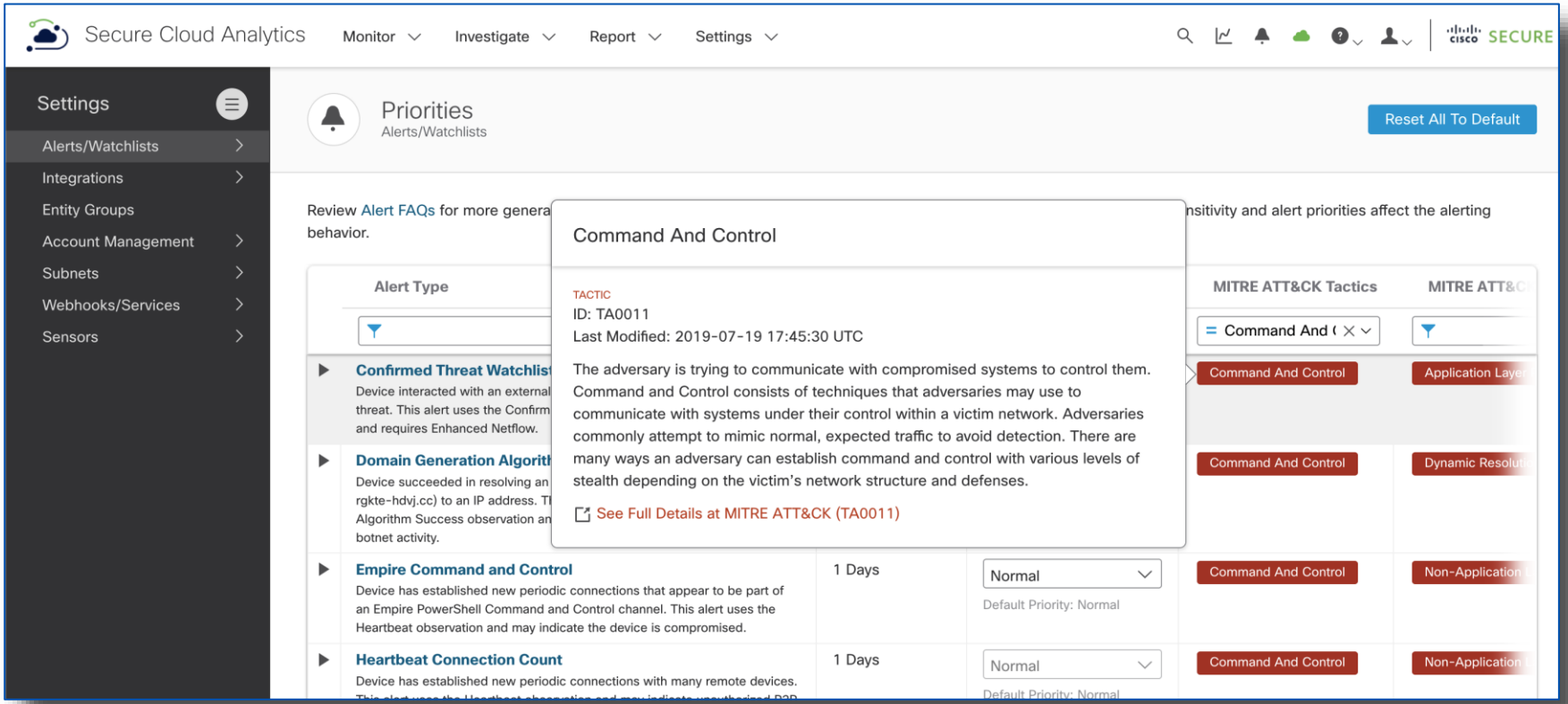
To learn more about Secure Network Analytics, please visit cisco.com/go/secure-network-analytics

Sign up for a free 2-week visibility assessment here

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 867164323 04/2022

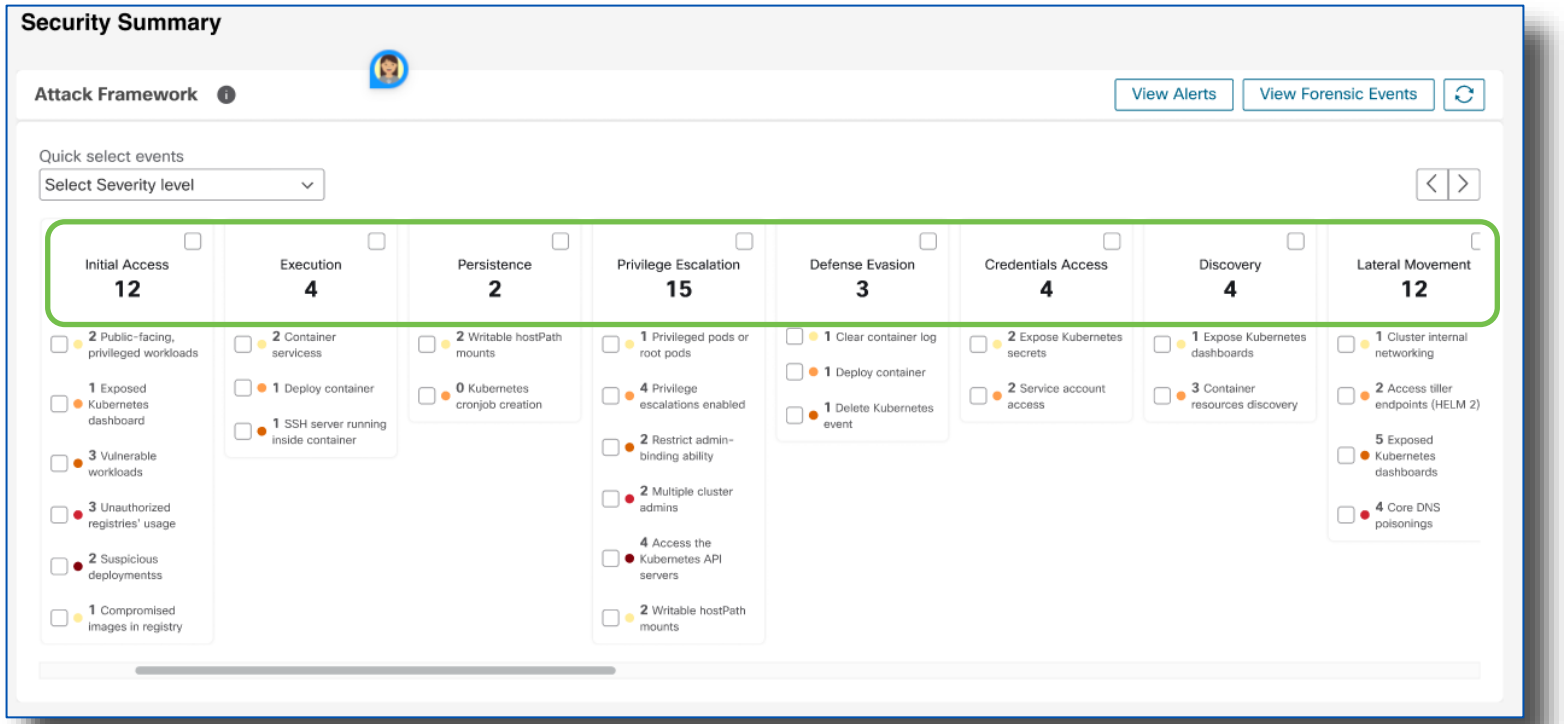
https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-mitre-use-case.pdf

Secure Cloud Analytics – full NDR TTP coverage



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Workload now sorts events by Tactic



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

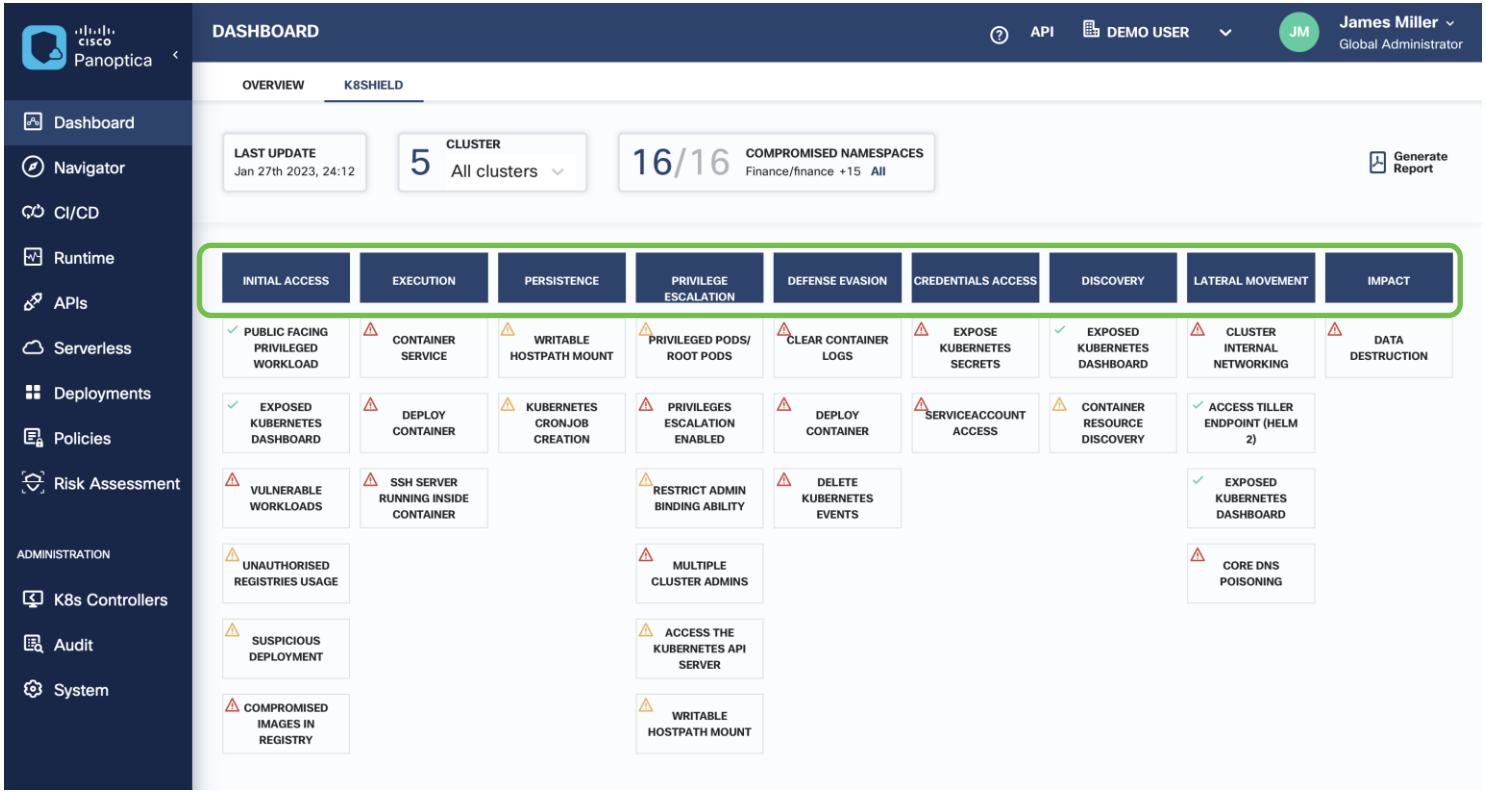
Secure Workload

Suspicious MS Office...	CL-215	A pre-defined rule that alerts and records if winword.exe or excel.exe or powerpnt.exe creates child processes.	ALERT, RECORD	HIGH	
T1003 - Credential D...	CL-215	A pre-defined rule that alerts if procdump.exe is used to dump lsass process Learn more	ALERT, RECORD	HIGH	
T1003 - Credential D...	CL-215	A pre-defined rule that alerts if reg.exe is used to save/export registry hives to a file Learn more	ALERT, RECORD	HIGH	
T1003 - Credential D...	CL-215	A pre-defined rule that alerts if vaultcmd.exe is used to dump credentials from windows credential vault Learn more	ALERT, RECORD	HIGH	
T1015 - Accessibilit...	CL-215	A pre-defined rule that alerts and records if child processes are created through accessibility features. This rule needs to be used with T1015 - Accessibility features 2. Learn more	ALERT, RECORD	HIGH	
T1015 - Accessibilit...	CL-215	A pre-defined rule that alerts and records if child processes are created through accessibility features. This rule needs to be used with T1015 - Accessibility features 1. Learn more	ALERT, RECORD	HIGH	
T1053 - Scheduled Ta...	CL-215	A pre-defined rule that alerts if schtasks.exe is used to create a new scheduled task Learn more	ALERT, RECORD	MEDIUM	
T1070 - Indicator Re...	CL-215	A pre-defined rule that alerts if wevtutil.exe is used to clear event logs Learn more	ALERT, RECORD	HIGH	
T1070 - Indicator Re...	CL-215	A pre-defined rule that alerts if fsutil.exe is used to delete USN journals Learn more	ALERT, RECORD	HIGH	
T1076 - Remote Deskt...	CL-215	A pre-defined rule that alerts if tscon.exe is executed Learn more	ALERT, RECORD	HIGH	
T1081 - Credentials...	CL-215	A pre-defined rule that alerts if the attacker is trying to search for the string "password" or trying to read the file /etc/passwd Learn more	ALERT, RECORD	HIGH	
T1081 - Credentials...	CL-215	A pre-defined rule that alerts if the attacker is trying to find the string "password" Learn more	ALERT, RECORD	HIGH	
T1085 - rundll32	CL-215	A pre-defined rule that alerts and records if rundll32.exe creates child processes. Learn more	ALERT, RECORD	HIGH	
T1089 - Disabling Se...	CL-215	A pre-defined rule that alerts if sysmon driver is unloaded Learn more	ALERT, RECORD	HIGH	
T1114 - Email Collec...	CL-215	A pre-defined rule that alerts if a .pst or .ost file is accessed by any application other than outlook.exe Learn more	ALERT, RECORD	MEDIUM	
T1118 - InstallUtil	CL-215	A pre-defined rule that alerts and records if InstallUtil.exe creates child processes. Learn more	ALERT, RECORD	HIGH	
T1121 - Regsvcs/Rega...	CL-215	A pre-defined rule that alerts and records if regsvcs.exe or regasm.exe create child processes. Learn more	ALERT, RECORD	HIGH	

Credential Access sub-techniques mapped to forensic rules

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Panoptica

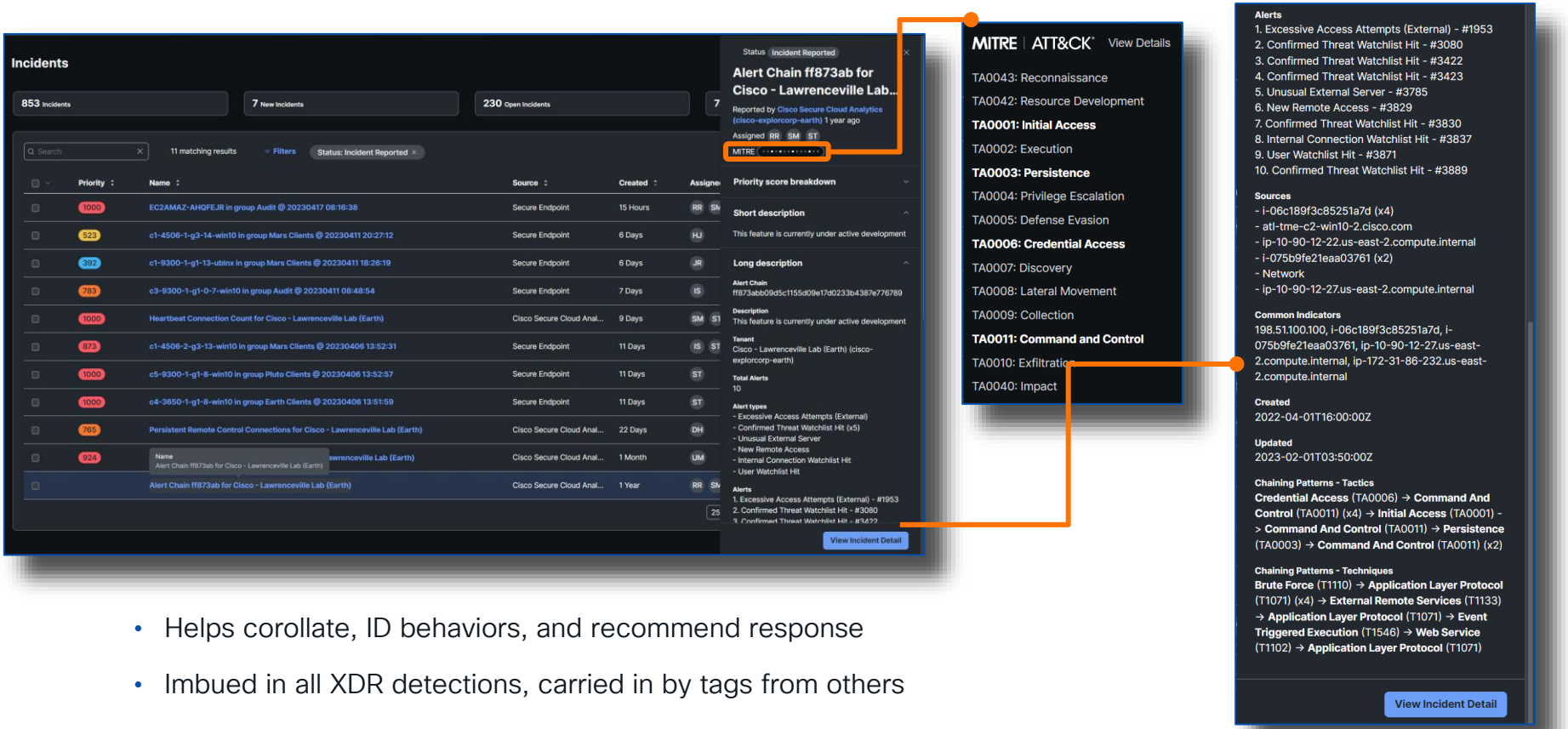


- Path Analysis
- Code Security
- CI/CD Security
- CSPM
- CWP

https://www.panoptica.app/blog/enhance-your-container-security-with-the-mitre-attck-framework

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Closing detection gaps and enriching events



- Helps corollate, ID behaviors, and recommend response
- Imbued in all XDR detections, carried in by tags from others

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Trust but Verify

But how can you be sure it works?

Verification & Validation is key to long-term success

1. Atomic Testing & Simulation – ex. Red Canary's Atomic Red Team (https://atomicredteam.io)
   - Running single step, isolated tests (like the atomic elements of an adversary)
   - More of a spot check than an exhaustive verification
2. Emulation – ex. MITRE's Caldera
   - Performing coordinated series of steps more representative of an APT's behavior – Red Teams, automated.
   - Often involves multiple subsystems (C2, delivery/implant, execution, etc.)
3. Breach & Attack Simulation (BAS) Tools – ex. Scythe, Cymulate, or AttackIQ
   - Combines both 1 & 2, while blending in Purple Teaming, Automation, mapping & analysis, and extensive reporting
   - Best leveraged with professional services to get full value

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Penetration Test versus Adversary Emulation

Penetration Testing

- Identify and exploit vulnerabilities on a system (or systems) to assess security
- Focused on a specific scope (app , system or a range to scan)
- Outcome is to test prevention, not on detection

Adversary Emulation

- Assess how resilient we are for a certain adversary group or type
- Focused on the execution of a scenario (can we go from host compromise to data exfil)
- Can be used for both prevention and detection

Both add extensive value in learning techniques used.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

No Red Team? Automate emulation w/ MITRE Caldera

Run entire Adversary campaigns against your environment and automate it all!

- Main project website: https://caldera.mitre.org/
- Includes plugins like Red Canary's Atomic Red Team & Emu(lation)
- Instructive in Training Red and Blue Teams alike
- Easily integrates with ATT&CK Navigator

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Caldera Definitions

- An Ability is at a similar level as an ATT&CK technique. Suite of actions achieving a goal
- Adversary describes an actor equipped with abilities
- Agents are software programs that connect back to Caldera at certain intervals to get instructions.
- Operations (like a playbook) run abilities on agent groups
- Jitter allows you to throttle the execution of operations (slow down to prevent detection)
- Caldera plugins can be customized to suite your environment, they also extended capabilities not native to Caldera

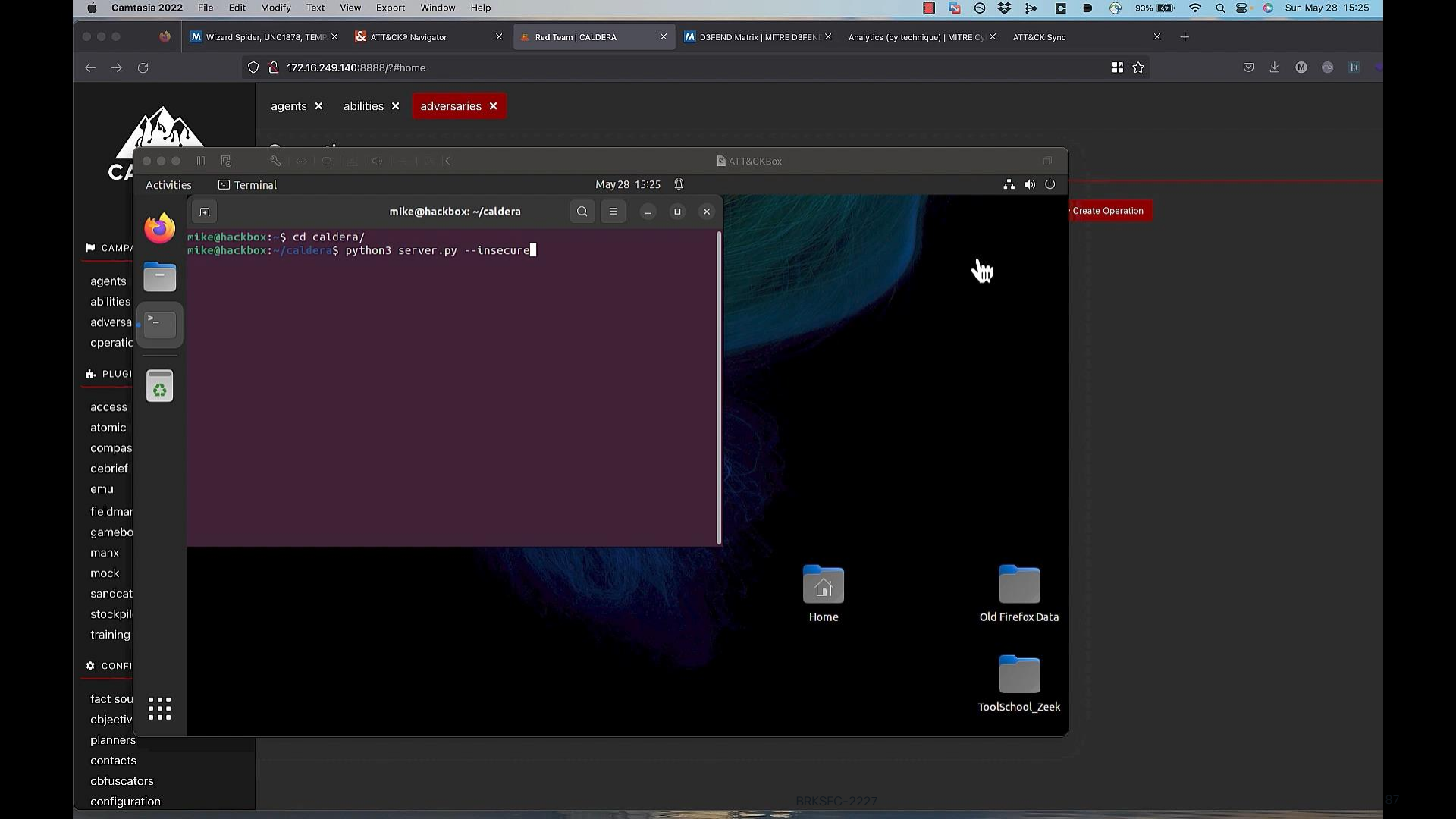
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Some of the cool plugins

- Mock – gives simulated agents to Caldera and allows you to run complete operations with just your laptop
- Sandcat – Caldera default agent. Written in GoLang (cross platform)
  Beacons back to C2 server for instructions, execution and sending results
- Response – Gives Incident Response capabilities to the system
- Gameboard – Self descriptive, gives a Red/Blue scoreboard.
- Human – Allows you to simulate a user at the console. Web browsing, create excel sheets, download files or custom commands.

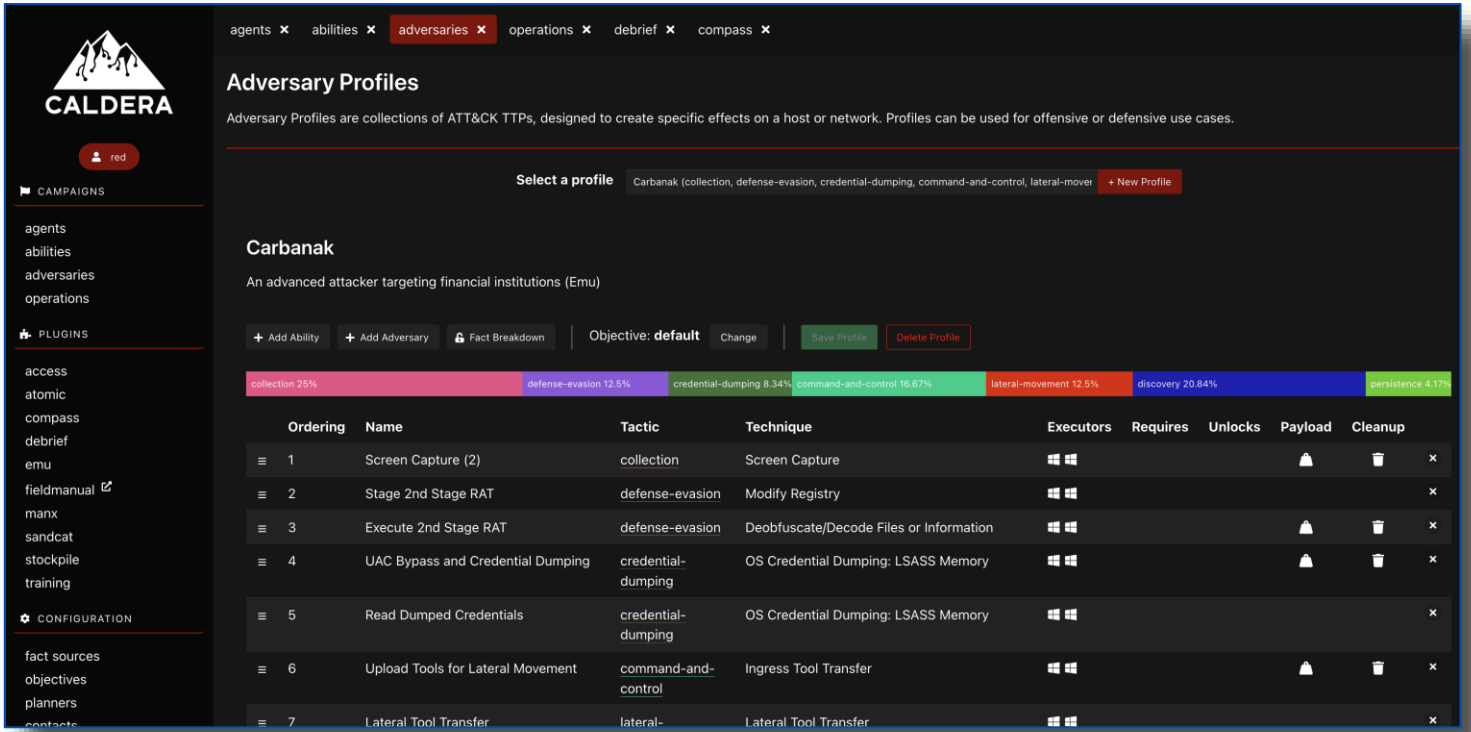
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Caldera Demo


Camtasia 2022
File
Edit
Modify
Text
View
Export
Window
Help
Sun May 28 15:25
Wizard Spider, UNC1878, TEMP
ATT&CK® Navigator
Red Team | CALDERA
D3FEND Matrix | MITRE D3FEND
Analytics (by technique) | MITRE Cy
ATT&CK Sync
172.16.249.140:8888/?#home
agents
abilities
adversaries
Create Operation
ATT&CKBox
Activities
Terminal
May 28 15:25
mike@hackbox: ~/caldera
mike@hackbox:~$ cd caldera/
mike@hackbox:~/caldera$ python3 server.py --insecure
Home
Old Firefox Data
ToolSchool_Zeek
agents
abilities
adversa
operatic
access
atomic
compas
debrief
emu
fieldmar
gamebo
manx
mock
sandcat
stockpil
training
fact sou
objectiv
planners
contacts
obfuscators
configuration
BRKSEC-2227

Adversary Profiles: which techniques are used, when?

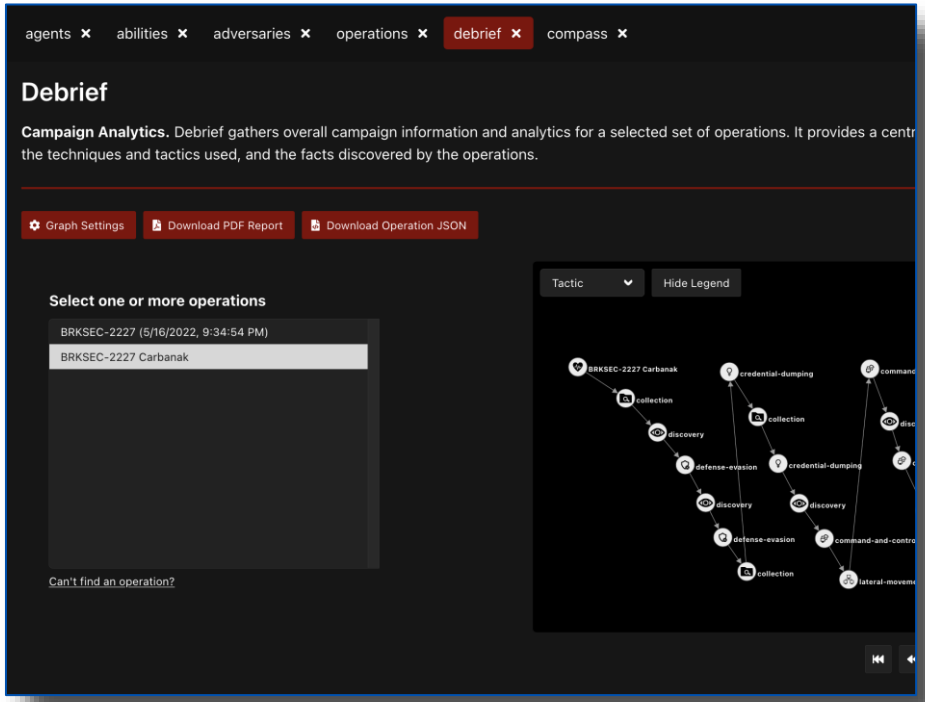
Easy to emulate your threat picture or pull from known emulation profiles

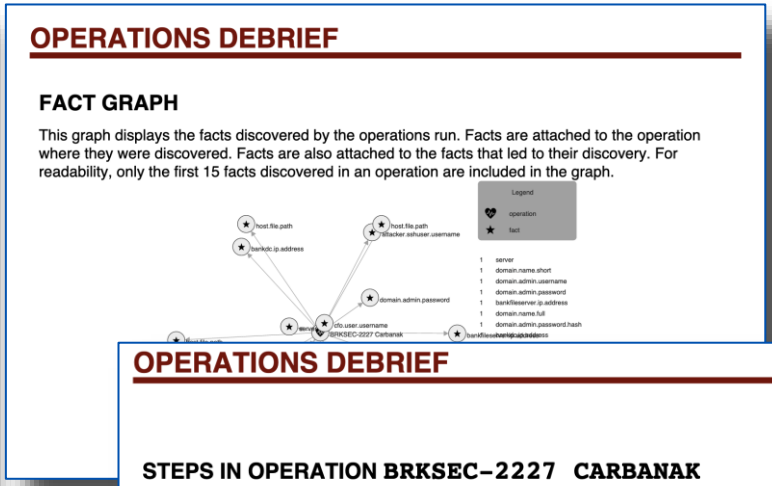


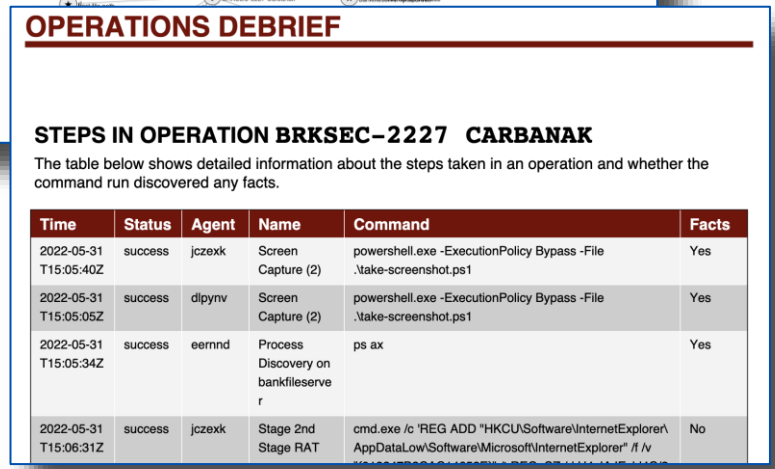
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Debrief: Useful reporting helps with take-aways

Extensive PDF and flexible JSON help make the results actionable



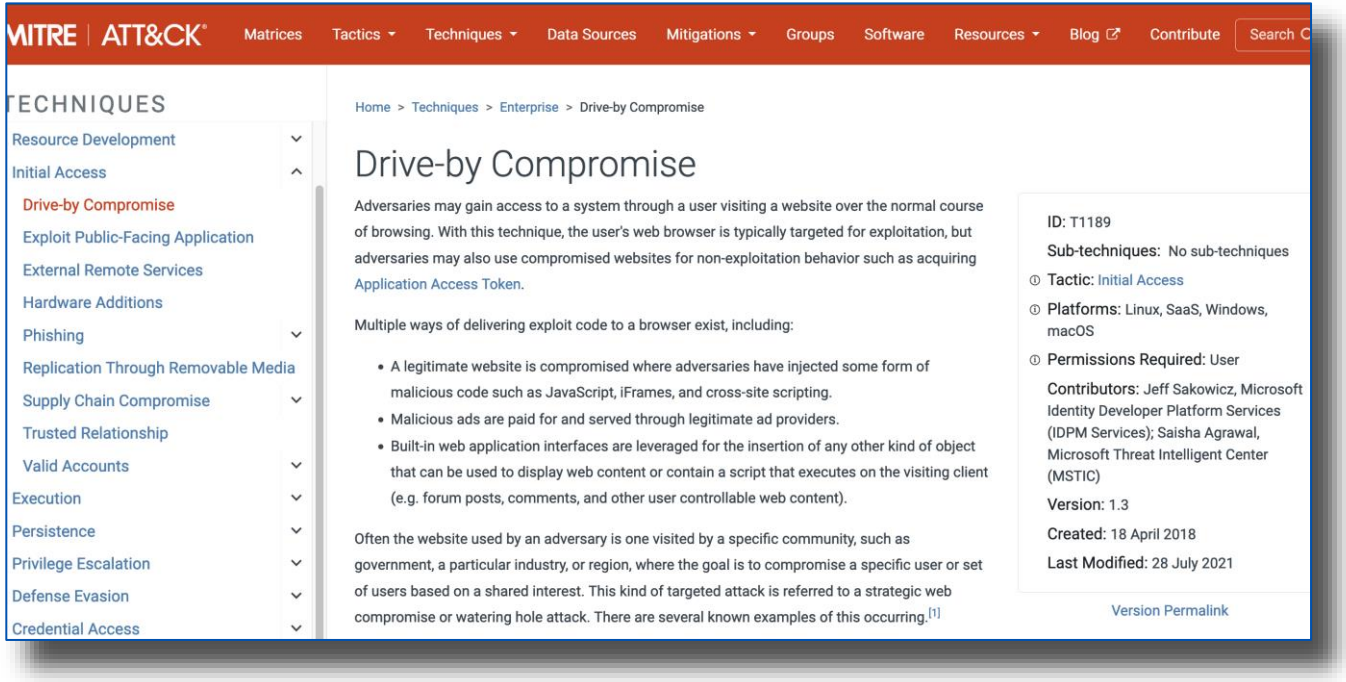




© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Focus on Fixes

High-level overview of each technique



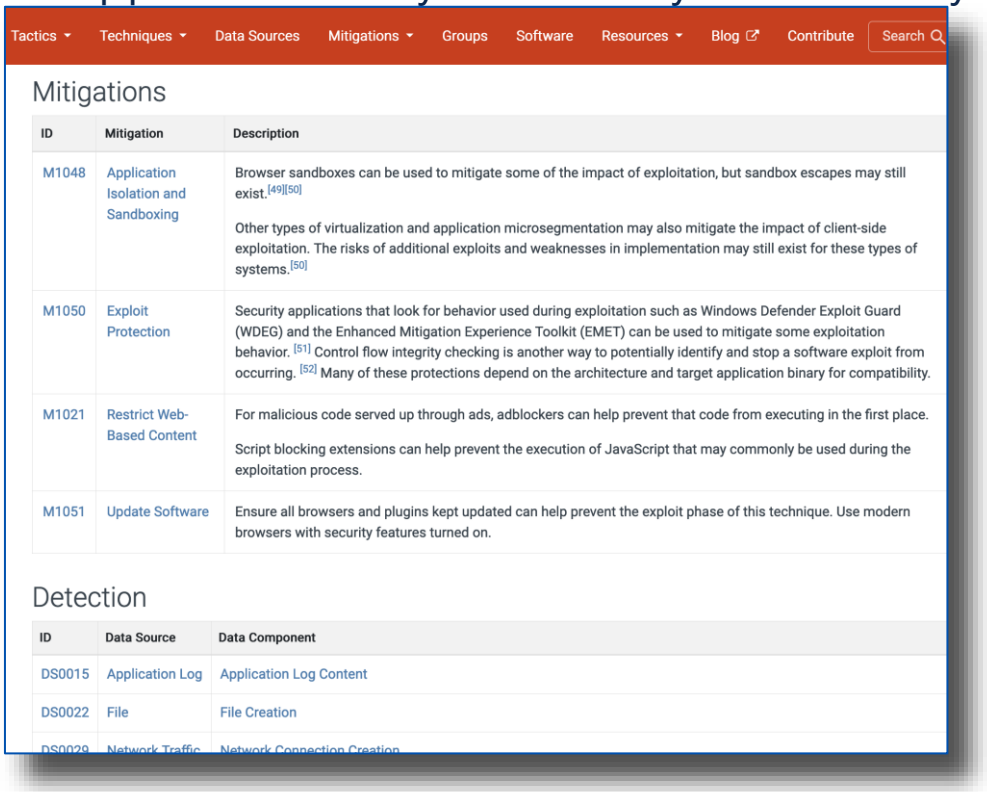
- Helps outline potential indicators
- Presents targets of technique
  - Platforms
  - Vectors
  - Permissions
- Helpful in education of InfoSec team *and* users

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Uncover mitigation and detection approaches

Some require multiple facets, other approaches may add fidelity or resiliency

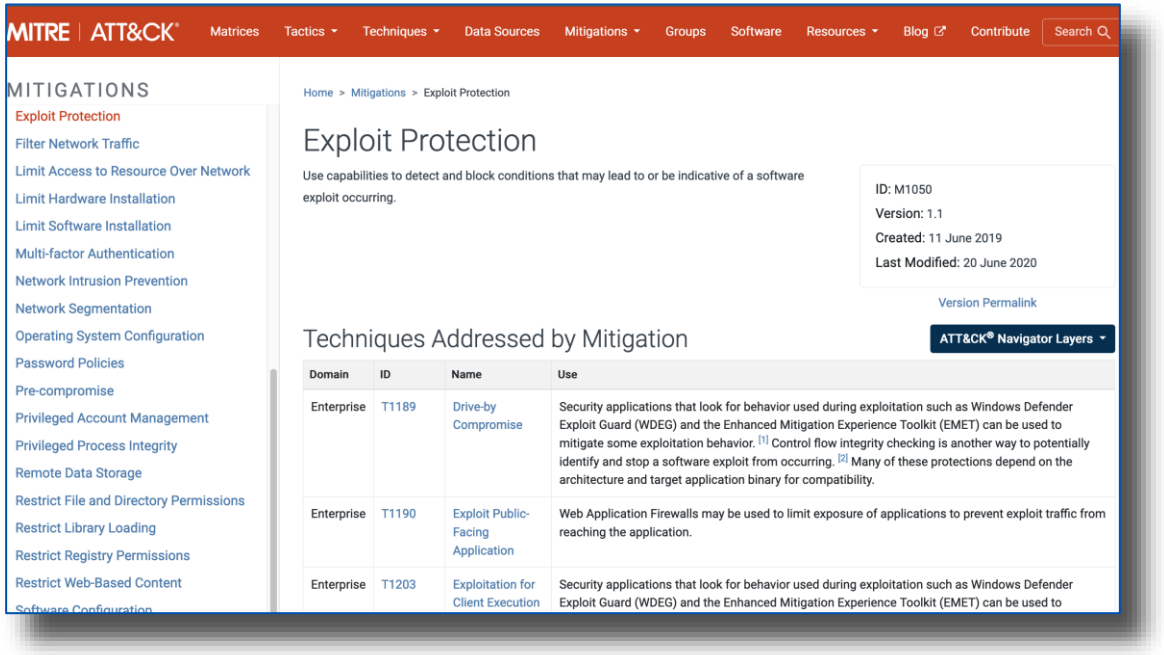
- Each Mitigation:
  - Covers many techniques
  - Includes controls for people, process, and product
  - BEST focus for gap coverage!
- Detections:
  - Generic but useful guidance:
    - Functions to enable
    - Features to license/purchase
    - Tools to use
  - Verification through testing



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Evaluate mitigation coverage for adjacent threats

Useful in helping business case for a new solution or feature



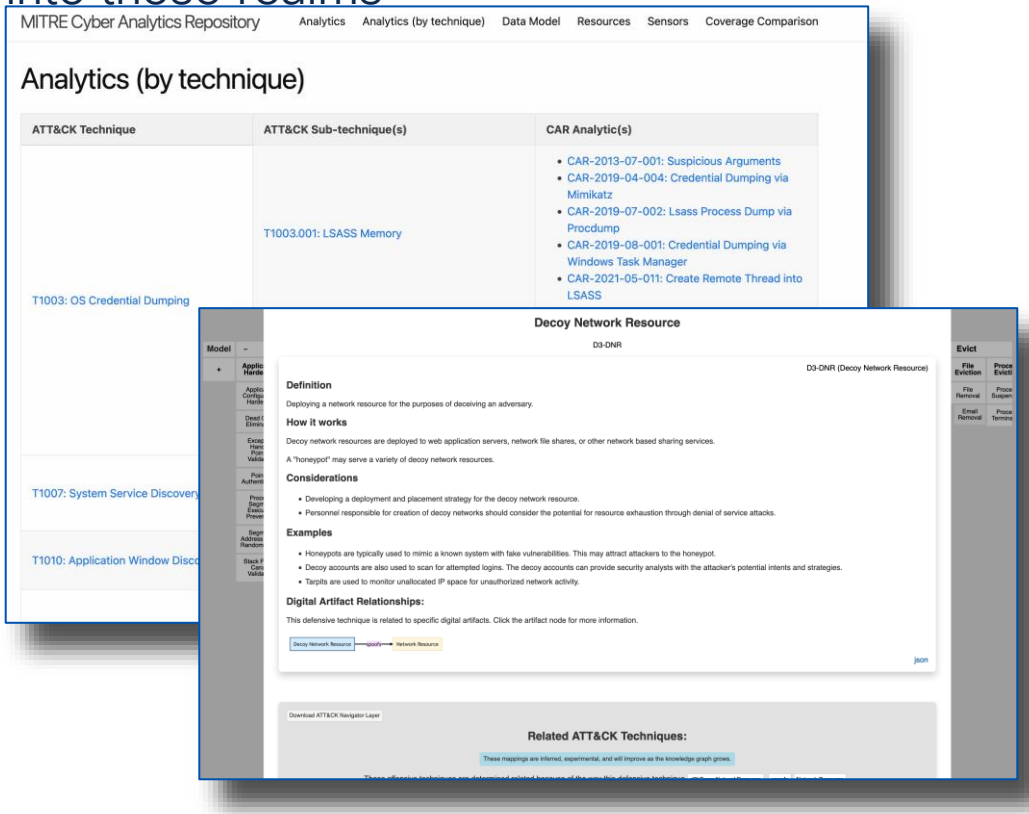
- Viewing from opposite side: what does 1 defensive measure do for the environment?
- Justify outages, prioritize implementation or purchase, etc.
- More products proving same mitigation:
  - Less opportunity for successful evasion
  - More tolerant of impairment or misconfiguration

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Building detections or engineering tools?

CAR and D3FEND extent ATT&CK into those realms

- Cyber Analytics Repository offers curated detections using SIEMs and related tools: https://car.mitre.org/analytics/by_technique
  - Psuedocode helpful for other products
  - Sigma project offers feed of supporting detections: https://github.com/SigmaHQ/sigma
- Engineering detection tools? D3FEND ties defensive tech to ATT&CK TTPs
  - https://d3fend.mitre.org/



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CAPEC: Hyber-focused on App and Web

Concentrate on the root of the problem to achieve security enlightenment

3000 - Domains of Attack

- Software - *(513)*
- Hardware - *(515)*
- Communications - *(512)*
- Supply Chain - *(437)*
- Social Engineering - *(403)*
  - Parameter Injection - *(137)*
  - Identity Spoofing - *(151)*
  - Resource Location Spoofing - *(154)*
  - Action Spoofing - *(173)*
  - Software Integrity Attack - *(184)*
  - Information Elicitation - *(410)*
  - Manipulate Human Behavior - *(416)*
  - Obstruction - *(607)*
- Physical Security - *(514)*

Common Attack Pattern Enumerations and Classifications (CAPEC)

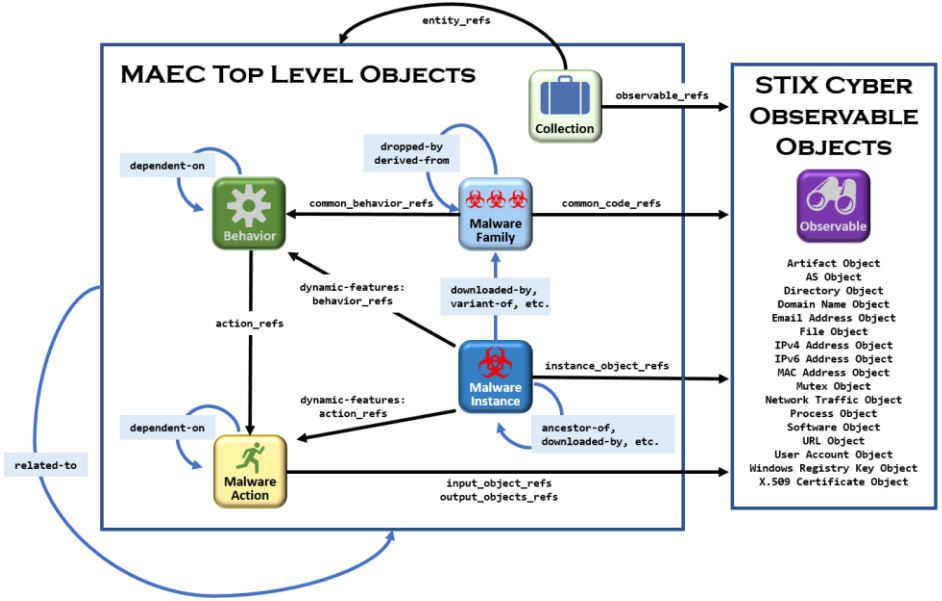
- Catalogues attack patterns used in exploiting an application
  - SQL Injection, XSS, Hijacking, etc.
  - Includes supply chain & social engineering
- Useful when dealing with a web-facing customer or SaaS provider
- Compliments ATT&CK, neither is a subset of the other

https://capec.mitre.org/index.html

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

MAEC: A Malware language

Concentrate on the root of the problem to achieve security enlightenment



Malware Attribute Enumeration and Characterization (MAEC)

- Community-driven
- Catalogues malware attributes
  - Behavior
  - Artifacts
  - Attack patterns
- Useful to malware researchers, IR teams and Cyber Threat Analysis

http://maecproject.github.io

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conclusion

What next? Baby Steps!

Build the habit – a little better every day is worth it

- Iterate
  - Repeat cycle and track improvement
  - Add APTs/threats as time permits
  - Continually test to validate progress
- Leverage tools that better support the SOC and engineering together!
- Educate and communicate across functions with Risk and ATT&CK
- Compel your partners and vendors to do the same

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

So what have we learned?

- ATT&CK can help us assess our gaps!
  - TTPs provide insight into adversarial behavior == know thy enemy!
- Cisco solutions support mapping to ATT&CK TTPs
  - Helps identity trends as they are happening
  - TTPs automatically linked in Cisco Secure Endpoint, Orbital Search Analytics, Malware Analytics, Workload, Cloud Analytics, and XDR
- Open-Source efforts from MITRE and others can help you test those defenses or learn about the adversaries
  - MITRE Caldera project as an automated framework
  - Atomic Red Team offering the tests we invoked in Caldera
- The Tools and process are there to help you improve your security posture in a measurable, tailored, and scalable manner.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lessons when self assessing

- Don't assume all techniques are equal – Some are specific, some are generic.
- Don't alert on every technique – Focus on the alerts in your environment that you MUST know. High fidelity = good
- Don't misunderstand your coverage. There are so many possibilities. Measure efficacy of the technique you can detect, not the unknown.
- Don't stay in the matrix. Adversaries move faster than models. Be proactive in how to research and detect emerging threats
- Don't forget the fundamentals – ATT&CK is a great repo but don't forget training, vulnerability and risk management, zero trust .

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional ATT&CK-related resources

Blogs & References

- MITRE's own ATT&CK materials are hard to beat: https://attack.mitre.org
- Getting Started Guide – useful for all 4 use cases: https://attack.mitre.org/resources/getting-started/
- Best blog on Medium: https://medium.com/mitre-attack/
- Pyramid of Pain: https://globalsecuresolutions.com/the-pyramid-of-pain/
- Orbital for ATT&CK: https://blogs.cisco.com/security/finding-the-malicious-needle-in-your-endpoint-haystacks
- Threat Grid use of ATT&CK TTPs in reports: https://blogs.cisco.com/security/black-hat-usa-2018-attck-in-the-noc
- MITRE ATT&CK Cisco Blog Series: https://blogs.cisco.com/security/mitre-attck-the-magic-of-mitigations

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional ATT&CK-related resources

Complimentary MITRE efforts

- Center for Threat-Informed Defense (CTID): group in MITRE Engenuity, leads ATT&CK, D3FEND, and related https://ctid.mitre-engenuity.org
- D3FEND: counter ATT&CKs TTPs by detailing how one can harden, detect, isolate, deceive, or evict the threat. https://d3fend.mitre.org
- Cyber Analytics Repository (CAR): validated analytical recipes for tools like Splunk, Elastic, etc. help detect TTPs in use https://car.mitre.org/
- ATT&CK Flow – a tool to assist in linking TTPs into an adversary's behavior (alchemy)
  - https://center-for-threat-informed-defense.github.io/attack-flow/
- ATT&CK Powered Suit: Browser plugin to link and research TTPs
  - https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/attack-powered-suit/
- Common Attack Pattern Enumeration and Classification (CAPEC): Like ATT&CK, but focused on applications https://capec.mitre.org/

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional ATT&CK-related resources

Software tools

- MITRE Caldera: provides a browser-driven automated emulation platform to test against ATT&CK TTPs for endpoints (Linux, Mac, Windows)
  - Main project website: https://caldera.mitre.org/
  - Awesome tutorial by Mohammed Alshaboti : https://medium.com/@alshaboti/getting-started-with-mitre-caldera-offensive-and-defensive-training-3ca9f693e0d7
- MITRE's ATT&CK Workbench: allows orgs to maintain a local repo of their own ATT&CK data and keep it in synch with global feeds
  - https://ctid.mitre-engenuity.org/our-work/attack-workbench/
- Red Canary's Atomic Red Team: https://atomicredteam.io
- D3TTECT: https://github.com/rabobank-cdc/DeTTECT/wiki
- BushidoUK's Open-Source Tools for CTI: https://github.com/BushidoUK/Open-source-tools-for-CTI

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional CTI-related resources

Blogs & References

- CIS Critical Security Controls, OS Benchmarks & Hardened Images a fantastic resource: https://www.cisecurity.org/cybersecurity-tools/
- OWASP Secure Software Development Lifecycle Project: https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project
- UK National Cybre Security Centre: https://www.ncsc.gov.uk/section/advice-guidance/all-topics
- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
- US-CERT Resources: https://www.us-cert.gov/resources
- CREST Resource page: https://www.crest-approved.org/knowledge-sharing/index.html
- SANS Cyber Defense Reading Room: https://cyber-defense.sans.org/resources/whitepapers

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

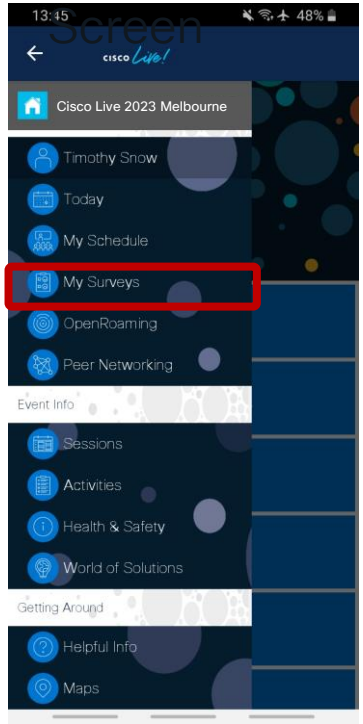
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

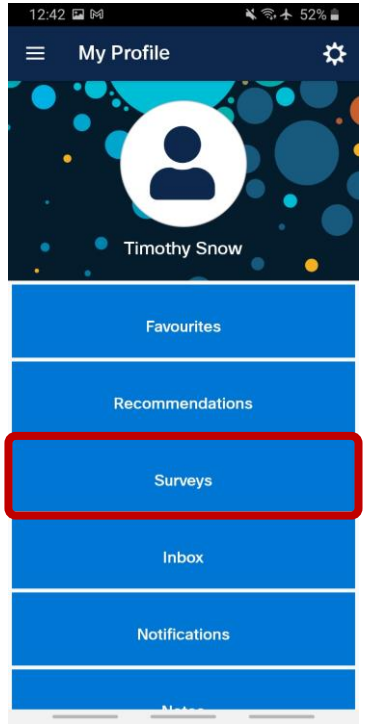
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Your feedback matters

Main Screen



Profile



- ○ Excellent
- ○ Above Average
- ○ Average
- ○ Below Average
- ○ Poor

Cisco Webex App

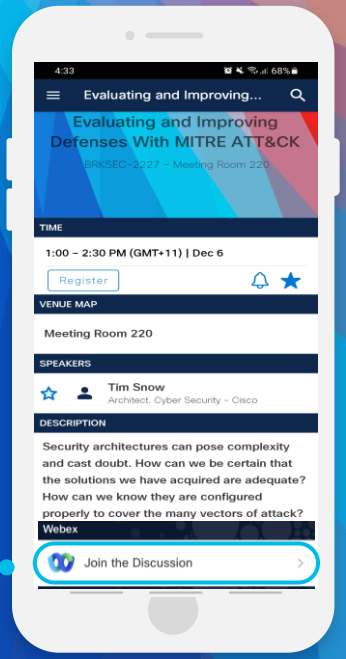
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

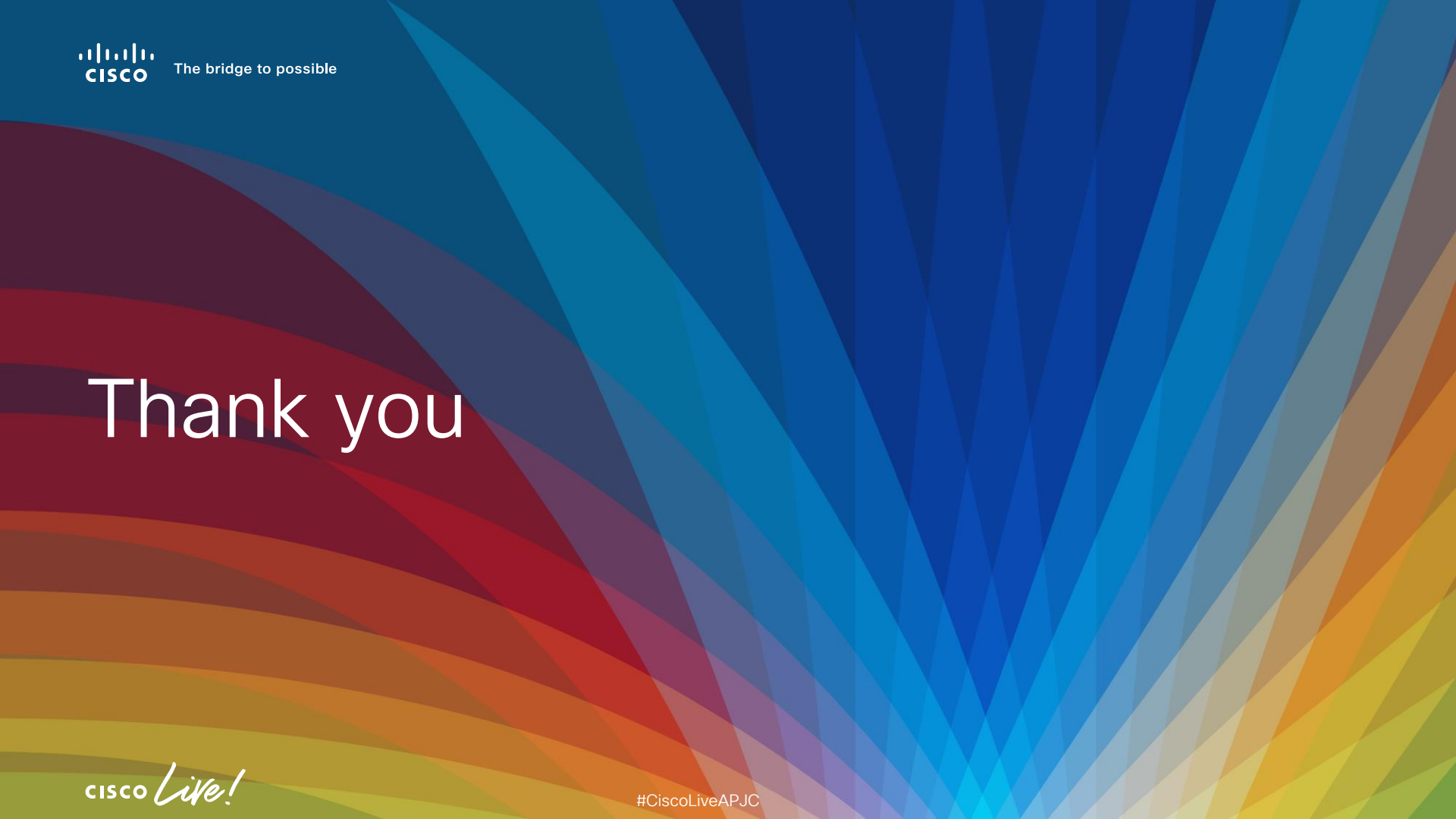
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2227

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLiveAPJC