



EMULATING ADVERSARIES FOR AUDITORS AND THE BUSINESS

September 16, 2022 • Alex Martirosyan

PS> whoami

- Senior Penetration Tester
- Started originally as an IT Auditor
- Background in mathematics
 - Substack: <https://almart.substack.com/>



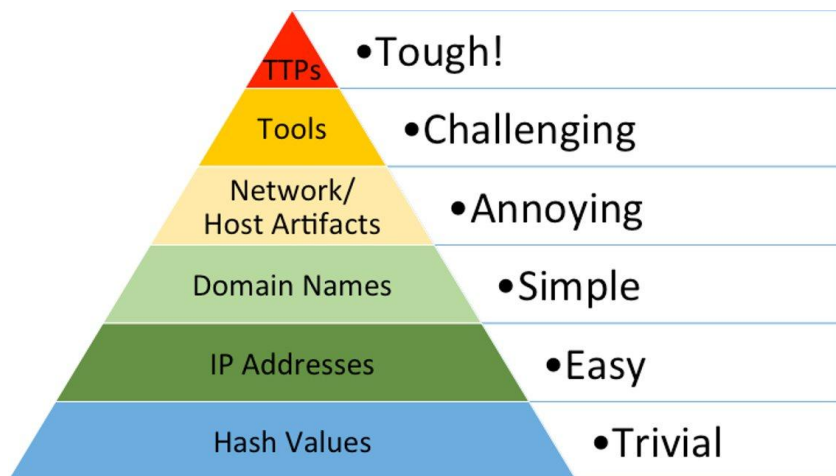
Twitter: @almartiros

Discord: almart#1785

Agenda

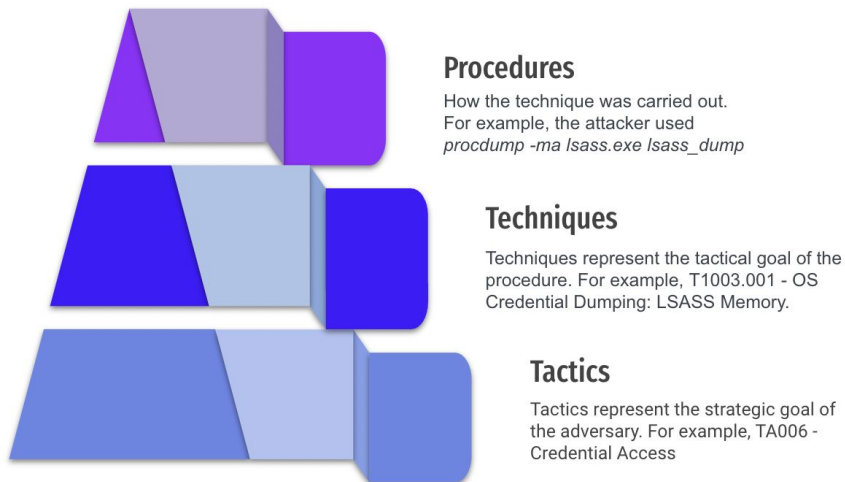
- The MITRE ATT&CK® problem
- Introduction to basic audit principles
- Understanding frameworks and the business
- Atomic Testing -> Micro Emulation -> Purple Teaming
- Tools to emulate realistic scenarios and create reports

Obligatory Pyramid Slide



Source:

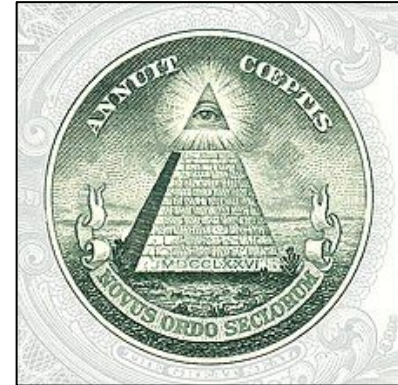
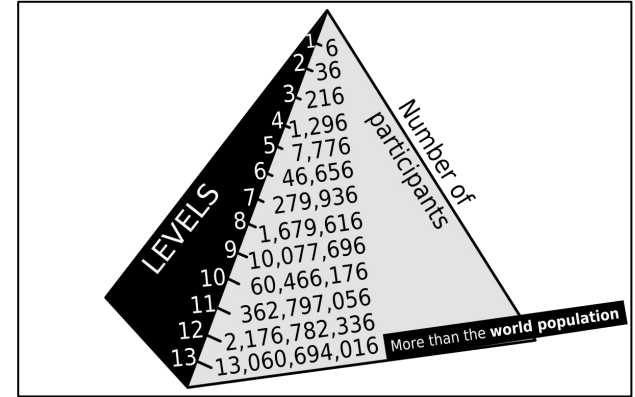
<https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>



Source:

<https://www.scythe.io/library/summitting-the-pyramid-of-pain-the-ttp-pyramid>

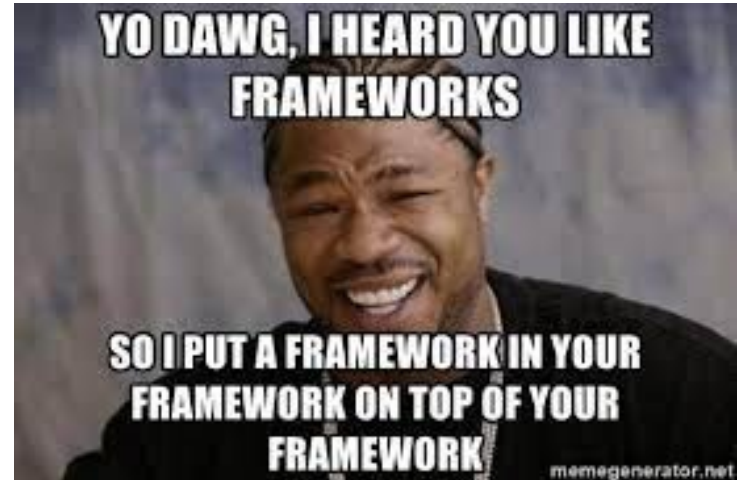
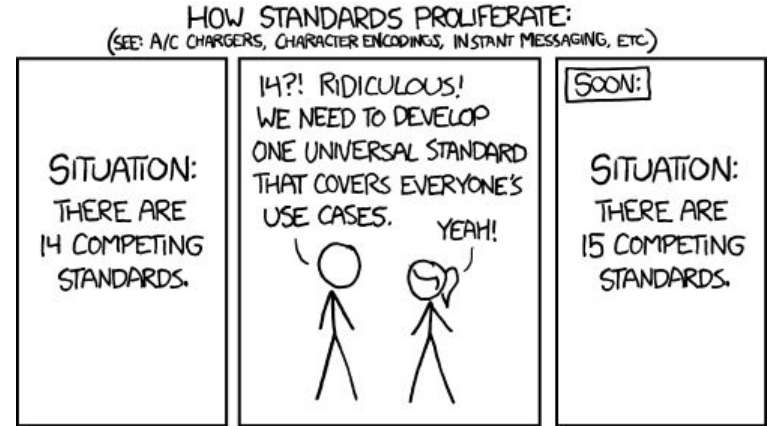
Pyramid Scheme?



Frameworks and Standards

Another framework/standard to follow!

- NIST 800-53 / NIST CSF / CIS Top 18
 - Mappings are great but can be overwhelming
- GLBA/PCI/HIPAA/SOC/SOX/etc.
- How does the business or management keep up?



Why Audit?

- Business already understands it
 - Offensive testing has not been uniformly accepted
- Measure effectiveness of control
- Create repeatable test cases
- Determine overall confidence



Auditing and QA

- Create testable and repeatable processes
- Validating assumptions against control environment
 - Systems have inputs and outputs...
- Everybody loves an auditor!

V. MODEL VALIDATION

Model validation is the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses. Effective validation helps ensure that models are sound. It also identifies potential limitations and assumptions, and assesses their possible impact. As with other aspects of effective challenge, model validation should be performed by staff with appropriate incentives, competence, and influence.

All model components, including input, processing, and reporting, should be subject to validation; this applies equally to models developed in-house and to those purchased from or developed by vendors or consultants. The rigor and sophistication of validation should be commensurate with the bank's overall use of models, the complexity and materiality of its models, and the size and complexity of the bank's operations.

ATT&CK Intro

MITRE ATT&CK Enterprise

- Tracks threat actors through **observable** data
- Tactics, Techniques, and Procedures (TTPs)
- Post compromise focus

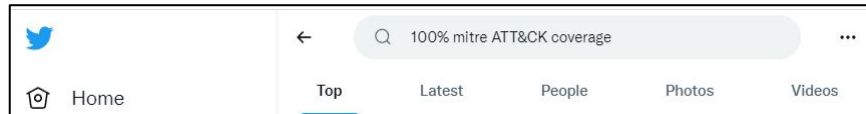
Can be overwhelming...

- 14 Tactics
- 191 Techniques (386 Sub-techniques)
- Procedures are key

Powerful classification framework → common language

ATT&CK Traps

- Offensive minded individuals don't think in TTP's
 - Threat actors certainly do not
- Emulating realism and being accurate is hard
- Misleading metrics creating false sense of security



Industry Issues

- Most security tools now map to ATT&CK
- Great for marketing and building a common language, needs to be actionable
- If it isn't in ATT&CK is it even real?

Multi-Factor Authentication Request Generation

Adversaries may attempt to bypass multi-factor authentication (MFA) mechanisms and gain access to accounts by generating MFA requests sent to users.

Adversaries in possession credentials to Valid Accounts may be unable to complete the login process if they lack access to the 2FA or MFA mechanisms required as an additional credential and security control. To circumvent this, adversaries may abuse the automatic generation of push notifications to MFA services such as Duo Push, Microsoft Authenticator, Okta, or similar services to have the user grant access to their account.

In some cases, adversaries may continuously repeat login attempts in order to bombard users with MFA push notifications, SMS messages, and phone calls, potentially resulting in the user finally accepting the authentication request in response to "MFA fatigue."^{[1][2][3]}

ID: T1621

Sub-techniques: No sub-techniques

① **Tactic:** [Credential Access](#)

② **Platforms:** Azure AD, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS

Contributors: Jon Sternstein, Stern Security, Pawel Partyka, Microsoft 365 Defender

Version: 1.0

Created: 01 April 2022

Last Modified: 20 April 2022

[Version](#) [Permalink](#)

Procedure Examples

ID	Name	Description
G0016	APT29	APT29 has used repeated MFA requests to gain access to victim accounts. ^[8]

Threat Model

The screenshot shows the MITRE ATT&CK search interface. The search term 'hospitals' is entered in the top search bar. The results are categorized into three sections: Software, Groups, and Techniques. The Software section lists BitPaymer, Software S0570. The Groups section lists Wizard Spider. The Techniques section is empty.

MITRE | ATT&CK

Matrices Tactics Techniques Data Sources Mitigations Groups Software Resources Blog Contribute Search

hospitals

Software

BitPaymer, Software S0570

BitPaymer BitPaymer is a ransomware variant first observed in August 2017 targeting hospitals in the U.K. BitPaymer uses a unique encryption key, ransom note, and contact information for each operation. BitPaymer has several indicators suggesting overlap with the Dridex malware and ...

Software

... ations in Russia, South Korea, and Japan since at least December 2010. S0570 BitPaymer wp_encrypt, FriedEx BitPaymer is a ransomware variant first observed in August 2017 targeting hospitals in the U.K. BitPaymer uses a unique encryption key, ransom note, and contact information for each operation. BitPaymer has several indicators suggesting overlap with the Dridex malware and ...

Groups

... ince at least 2016. Wizard Spider possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals. G0128 ZIRCONIUM APT31 ZIRCONIUM is a threat group operating out of China, active since at least 2017, that has targeted individuals associated with the 2020 US presidential election and pr...

The screenshot shows the MITRE ATT&CK page for the Wizard Spider threat group. The page includes a description of the group, a sidebar with metadata, and a table of associated group descriptions.

Wizard Spider

Wizard Spider is a Russia-based financially motivated threat group originally known for the creation and deployment of TrickBot since at least 2016. Wizard Spider possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals.^{[1][2][3]}

ID: G0102

Associated Groups: UNC1878, TEMPMixMaster, Grim Spider

Contributors: Edward Millington; Oleksiy Gayda

Version: 2.0

Created: 12 May 2020

Last Modified: 14 October 2021

Version Permalink

Associated Group Descriptions

Name	Description
UNC1878	[4]
TEMPMixMaster	[5]
Grim Spider	[1][6]

Techniques Used

Domain	ID	Name	Use
--------	----	------	-----

ATT&CK® Navigator Layers

Enterprise Layer

How It's Made

1. Penetration phase

The penetration vector in this attack was social engineering, specifically spear-phishing attacks against carefully selected, high-profile targets in the company. Two types payloads were found in the **spear-phishing emails**:

1. **Link to a malicious site that downloads a fake Flash Installer** delivering Cobalt Strike Beacon
2. **Word documents with malicious macros** downloading Cobalt Strike payloads

2. Initial Access - Spearphishing Attachment (T1193)

Fake Flash Installer delivering Cobalt Strike Beacon

1. Initial Access - Spearphishing Link (T1192)

3. Defense Evasion/
Execution -
Scripting (T1064)

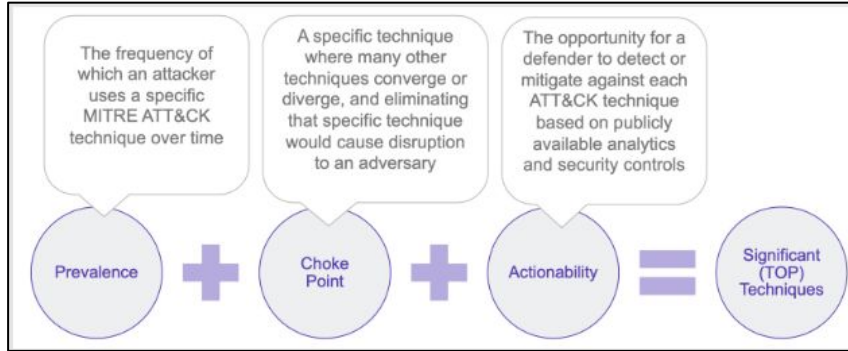
4. Execution - User
Execution (T1204)


The victims received a spear-phishing email using a pretext of applying to a position with the company. The email contained a link to a redirector site that led to a download link, containing a fake Flash installer. The fake Flash installer launches **a multi-stage fileless infection process**. This technique of infecting a target with an **fake Flash installer** is consistent with the OceanLotus Group and [has been documented in the past](#).

Source:

<https://attack.mitre.org/docs/training-cti/Cybereason%20Cobalt%20Kitty%20-%20original%20report.pdf>

Prioritization Using Math!





Center
for Threat
Informed
Defense

Filters

NIST 800-53 Controls

CIS Security Controls

☐ All CIS Controls

☐ 1.1

☐ 1.2

☐ 1.4

☐ 2.1

☐ 2.2

☐ 2.3

☐ 2.4

☐ 2.5

☐ 2.6

☐ 2.7

☐ 3.1

☐ 3.10

☐ 3.11

☐ 3.12

☐ 3.2

☐ 3.3

☐ 3.4

☐ 3.6

☐ 4.10

Detection Analytics

Operating Systems

Generate Results

Network Monitoring Components

None

Low

Medium

High

You have low network monitoring.

Process Monitoring Components

None

Low

Medium

High

You have medium process monitoring.

File Monitoring Components

None

Low

Medium

High

You have low file monitoring.

Cloud Monitoring Components

None

Low

Medium

High

You have medium cloud monitoring.

Hardware Monitoring Components

None

Low

Medium

High

You have no hardware monitoring.

X

1.

[T1047 - Windows Management Instrumentation](#)

X

2.

[T1059 - Command and Scripting Interpreter](#)

X

3.

[T1053 - Scheduled Task/Job](#)

X

4.

[T1562 - Impair Defenses](#)

X

5.

[T1574 - Hijack Execution Flow](#)

X

6.

[T1543 - Create or Modify System Process](#)

X

7.

[T1021 - Remote Services](#)

X

8.

[T1003 - OS Credential Dumping](#)

X

9.

[T1036 - Masquerading](#)

X

10.

[T1055 - Process Injection](#)

Conti Example

Cobalt strike MANUALS_V2 Active Directory

I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website

On Google : SITE + revenue (mycorporation.com + revenue) (
"mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

1.3 . **shell whoami** < ===== who am I

1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a
blue monik)

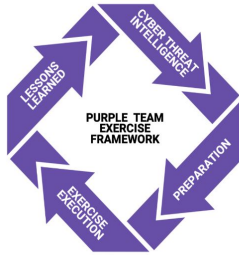
1.5 . 1 . **shell nltest / dclist:** <===== domain controllers

net dclist < ===== domain controllers

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip

Use Existing Resources

Purple Team Exercise Framework



Created and provided to the community by the team at



Source: <https://github.com/scythe-io/purple-team-exercise-framework/blob/master/PTEFv2.pdf>

Purple Team Lifecycle

Overall Status:

PB### - [Lifecycle Name]

Lifecycle Project Manager

Office: Office Phone
Mobile: Cell Phone
Email: Email

- Lifecycle Kickoff:
- Simulation Start:
- Simulation End:
- Configuration Identified:
- Change Management Referred
- Configuration Deployed:

Status Code Legend

- Attack Simulation
- Defense Simulation

- System Configuration Change
- Information

APT Lifecycle

Ingest and Research

- Lifecycle Type:
- Lifecycle Objective

● Ingest Source:

- Identify the ingest/intended attack and/or defense techniques. Define source of technique and type of ingest:

Attack methodology

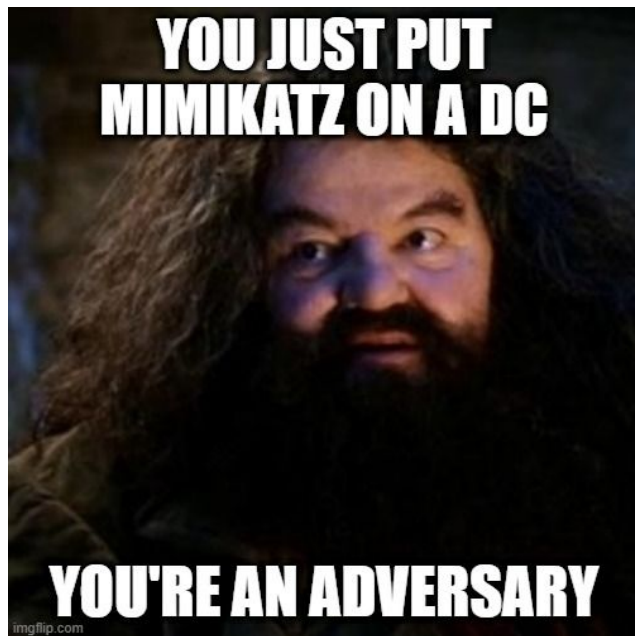
- Attack Methodology Test

Defense methodology

- Defense Methodology Test

Source: <https://github.com/DefensiveOrigins/AtomicPurpleTeam>

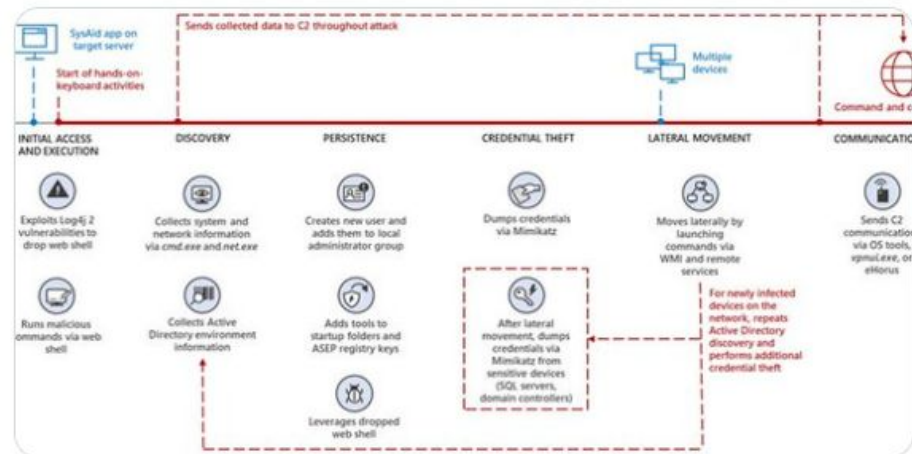
Sophisticated Cyber Attack



rvrsh3ll
@424f424f

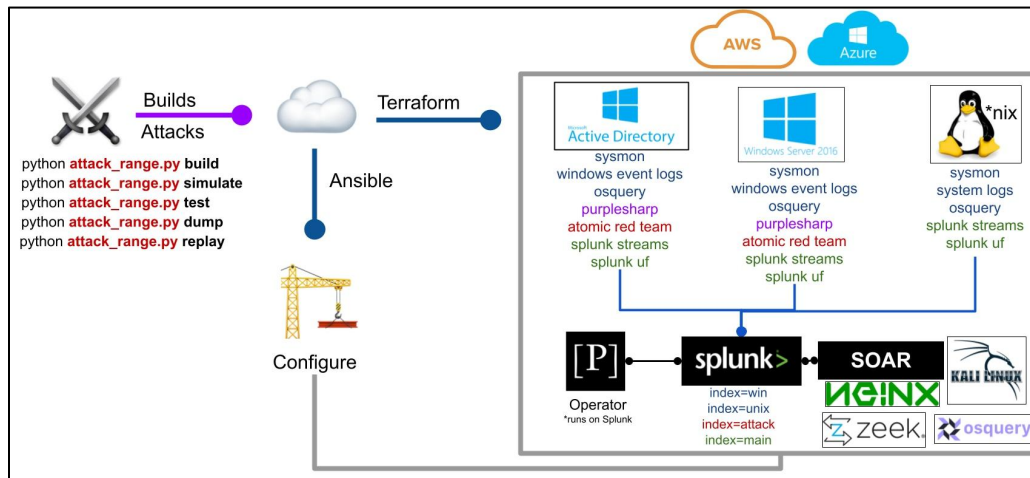
If I were to emulate these TTP's on engagement, I would get laughed at. Nation state my ass.

[microsoft.com/security/blog/...](https://microsoft.com/security/blog/)























Atomic Testing

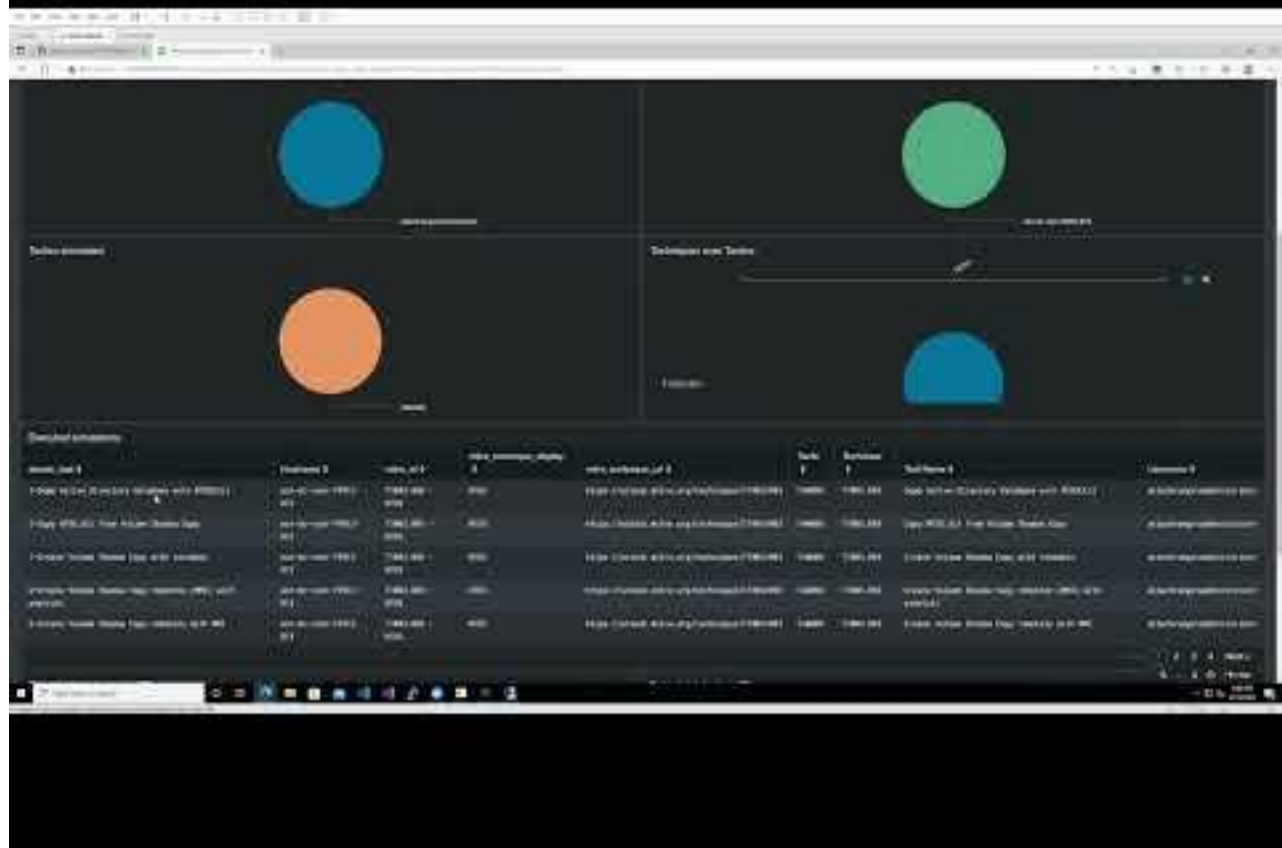


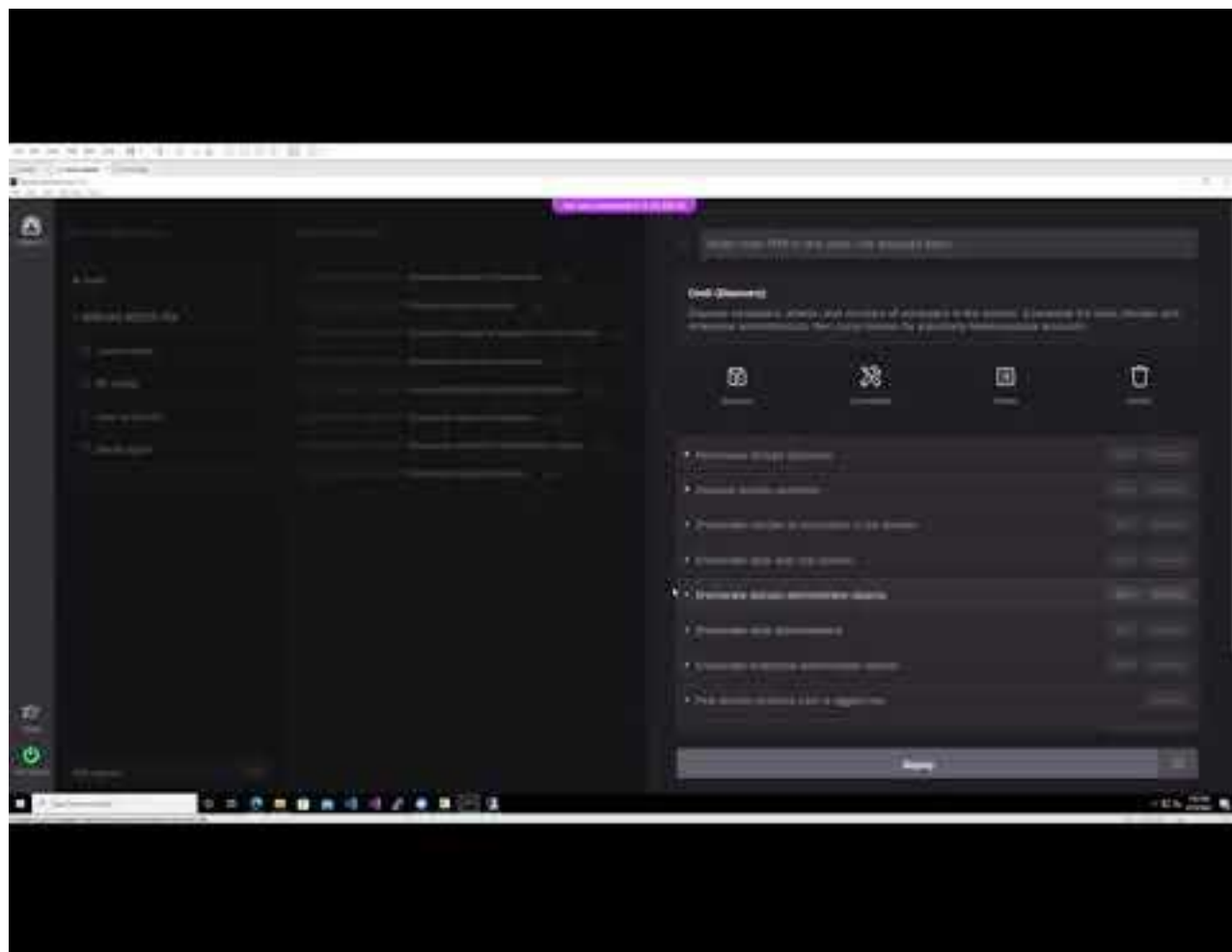
Source: https://www.splunk.com/en_us/blog/security/introducing-splunk-attack-range-v2-0.html

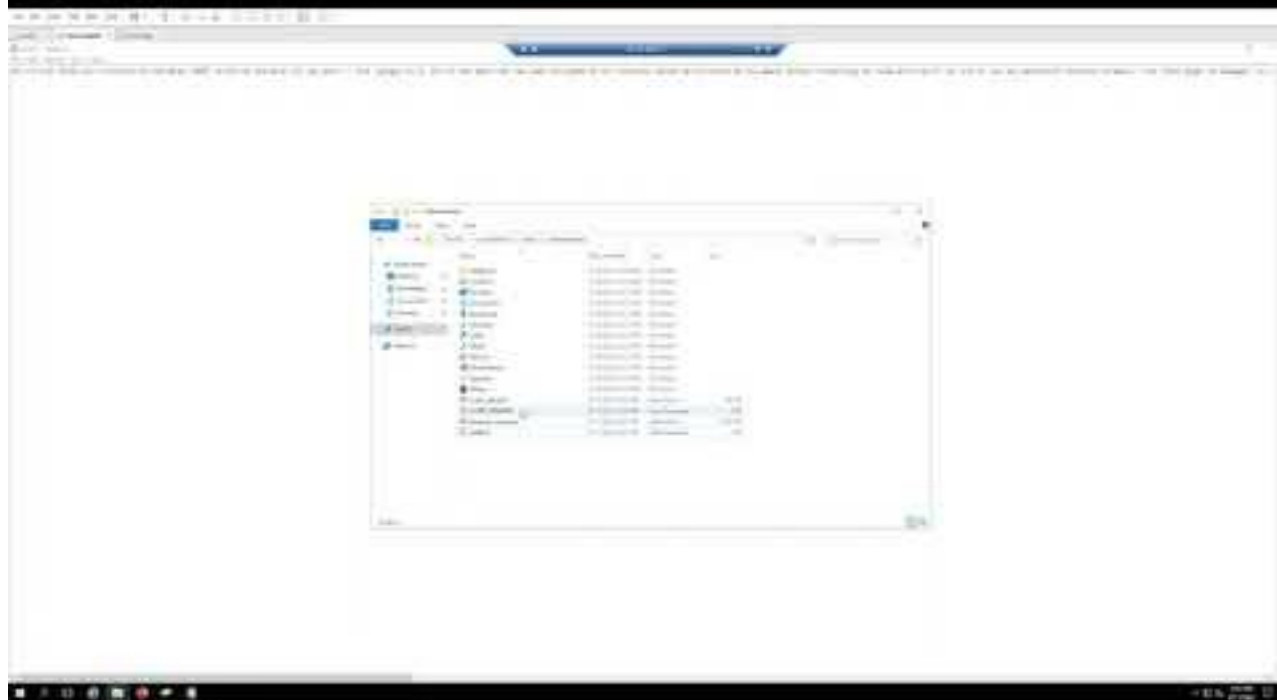


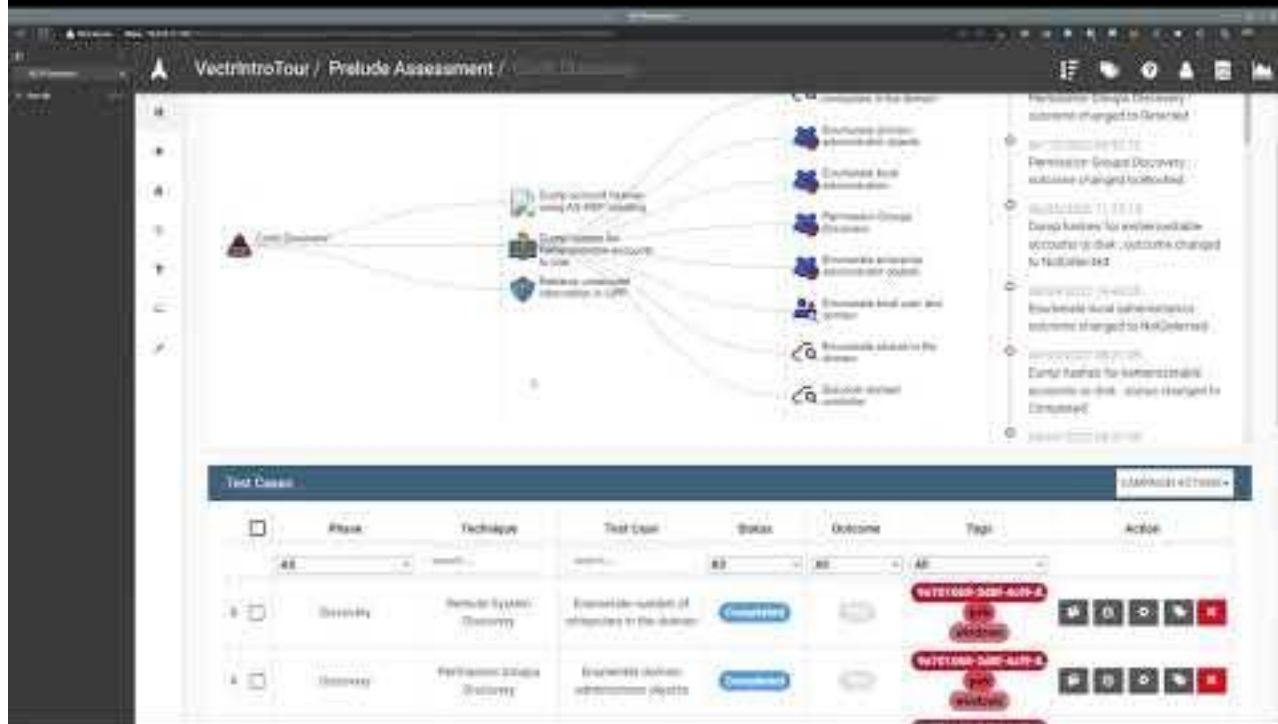
Emulation Plans

Atomic Testing	Micro Emulation	Full Emulation
Emulate single technique	Emulate compound behaviors across 2–3 techniques	Emulate adversary operation
 Executable in seconds	 Executable in seconds	 Executable in hours
<i>E.g., Atomic Red test for T1003.001 - LSASS Memory</i>	<i>E.g., Fork & Run Process Injection</i>	<i>E.g., FIN6 adversary emulation plan</i>
 Easy to automate	 Easy to automate	 Easy to automate
 Validate atomic analytics	 Validate atomic analytics	 Validate atomic analytics
 Validate chain analytics	 Validate chain analytics	 Validate chain analytics
 Evaluate SOC against a specific set of TTPs	 Evaluate SOC against a specific set of TTPs	 Evaluate SOC against a specific set of TTPs
 Evaluate SOC holistically against specific groups	 Evaluate SOC holistically against specific groups	 Evaluate SOC holistically against specific groups



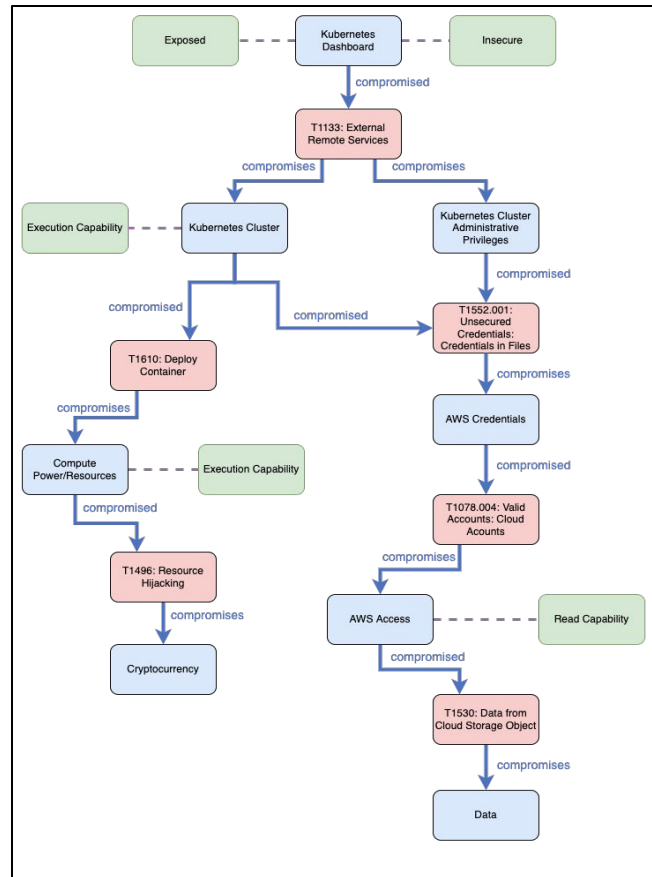




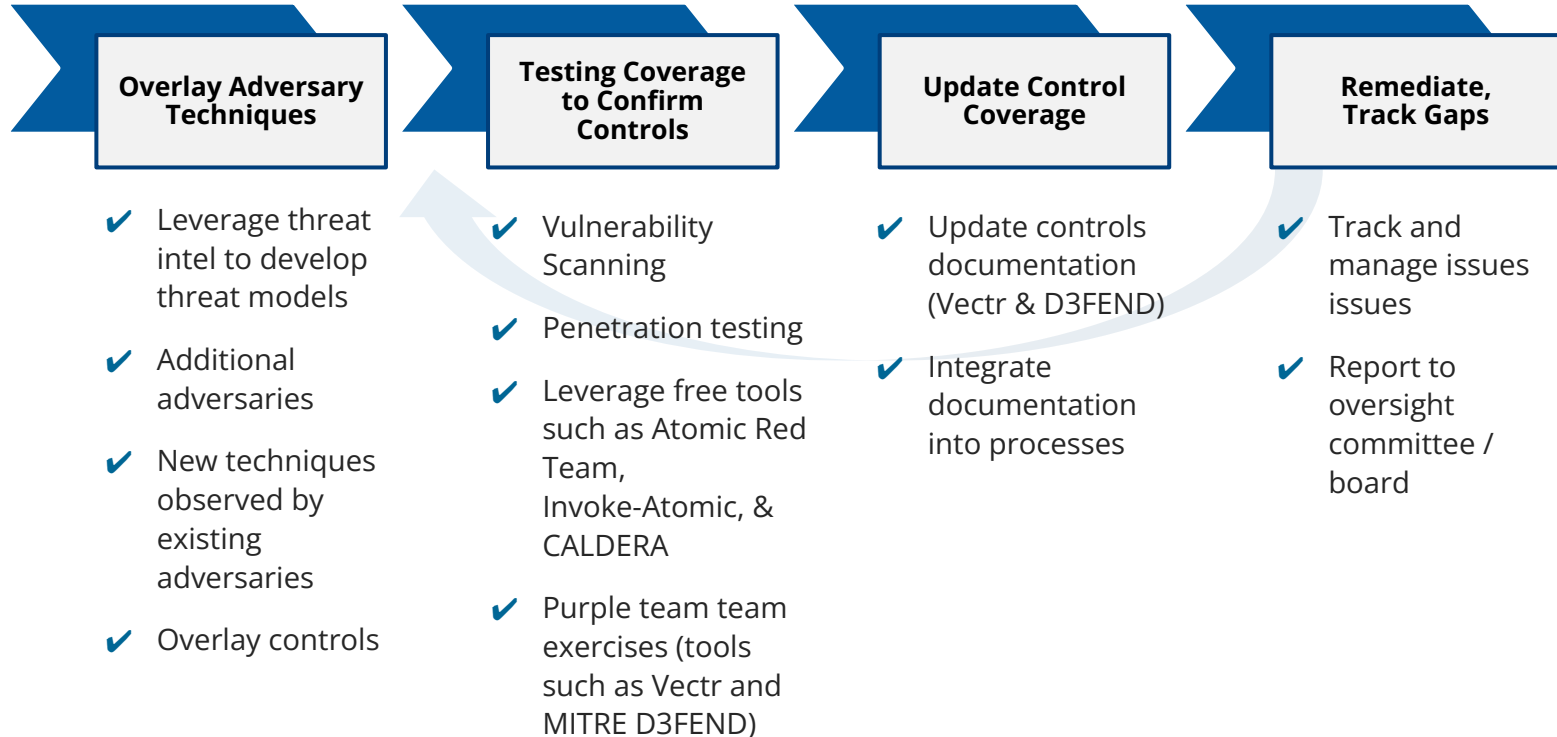


Future Thoughts

- Rich and detailed procedure level data from CTI isn't always available
- Making assumptions or a guess is OK in an emulation plan
- GOAL: Demonstrating high confidence in mitigating X threat



KEEP YOUR THREAT MODELS UP TO DATE





QUESTIONS