WORKSHOP: AUTOMATING ATTACKS

October 20, 2023 • Alex Martirosyan, CRTO, OSCP, GPEN

WHOAMI

- 5+ years in offensive security
- IT Audit > Penetration Testing
- Interested in intersection of mathematics and security

Alex Martirosyan,
CRTO , OSCP, GPEN
Lead Penetration Tester, DenSecure
AMartirosyan@wolfandco.com
617.261.8138
https://www.linkedin.com/in/alex-martirosyan/
https://twitter.com/almartiros
https://www.wolfandco.com/services/densecure/

AGENDA

- Motivations and goals for the workshop
- Definitions, frameworks, and matrices
- Evolution of offensive security testing
- Introduction to Atomic Testing with ATR
- Introduction to Micro Emulations
- Introduction to Purple Team with Caldera
- Free time and exploration

SPECIAL THANKS

- Community Resources:
  - Atomic Red Team, Prelude, Scythe, MITRE ATT&CK®, etc.
- Infrastructure Deployment:
  - Jason Ostrom, GOAD, SnapLabs, Elastic Cloud, TailScale, Terraform, etc.
- Andy Robbins for template slides
  - https://bit.ly/3BE4zbj

MOTIVIATIONS

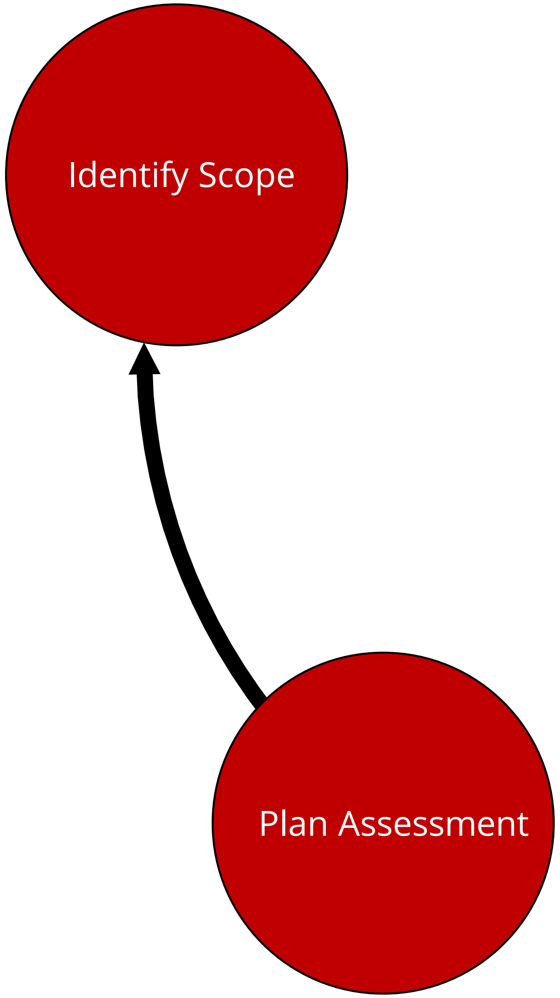
- Relatively new approach to security testing
  - Continuous vs Industry Standard
- Confusion behind varying testing methodologies
- Do our current approaches help solve cybersecurity challenges?
- Security controls are often times a black box

WORKSHOP GOALS AND LIMITATIONS

- **IDEA**: Relying on as many open-source tools as possible to building the environment
- **FOCUS**: Endpoint Detection & Response Solutions
- Lab != Production
- Understand the scale between accuracy and realism
- Windows endpoint focus (enterprise) with defaults

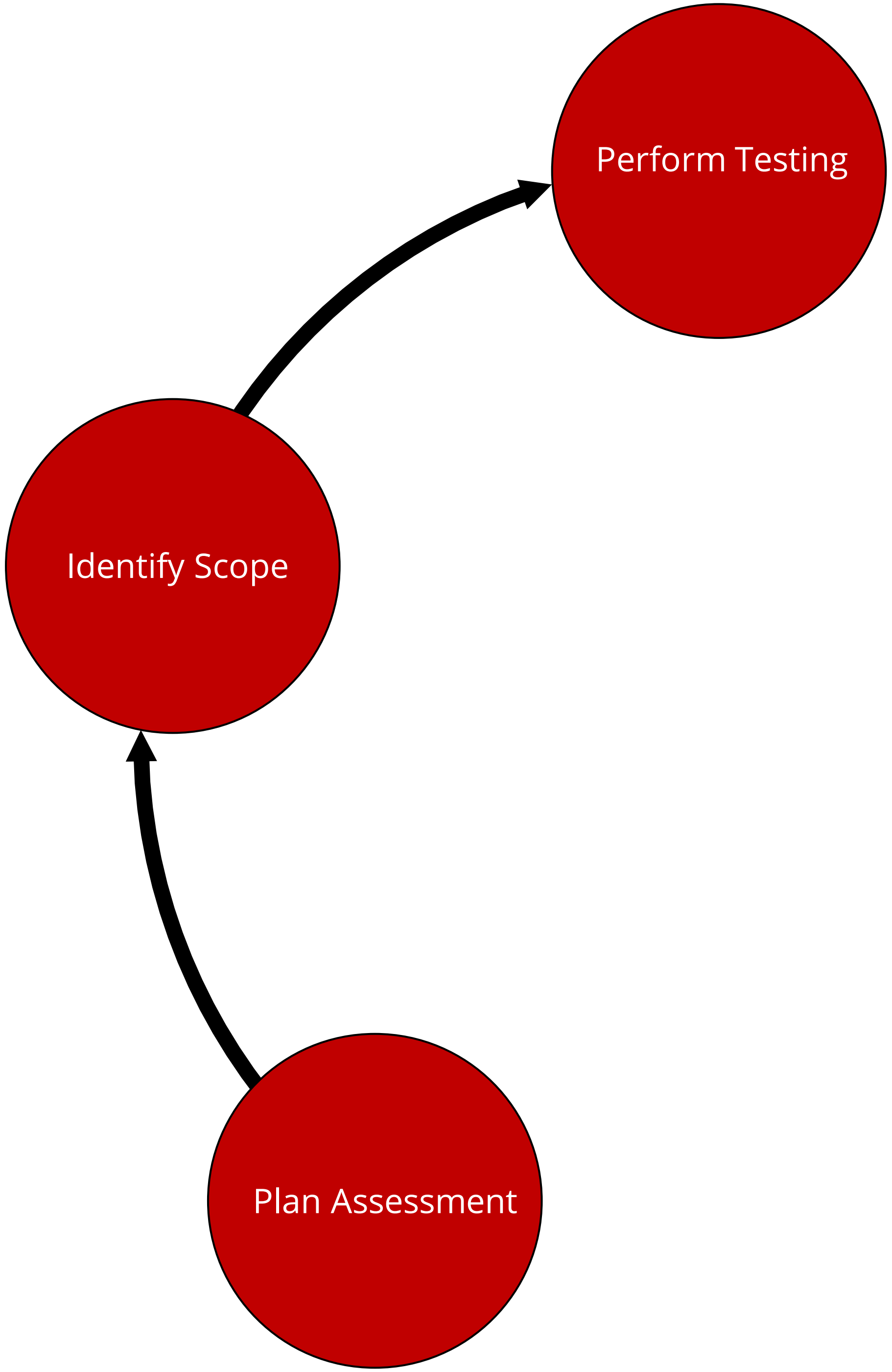
COMMON SECURITY TESTING MODEL

Plan Assessment



Identify Scope

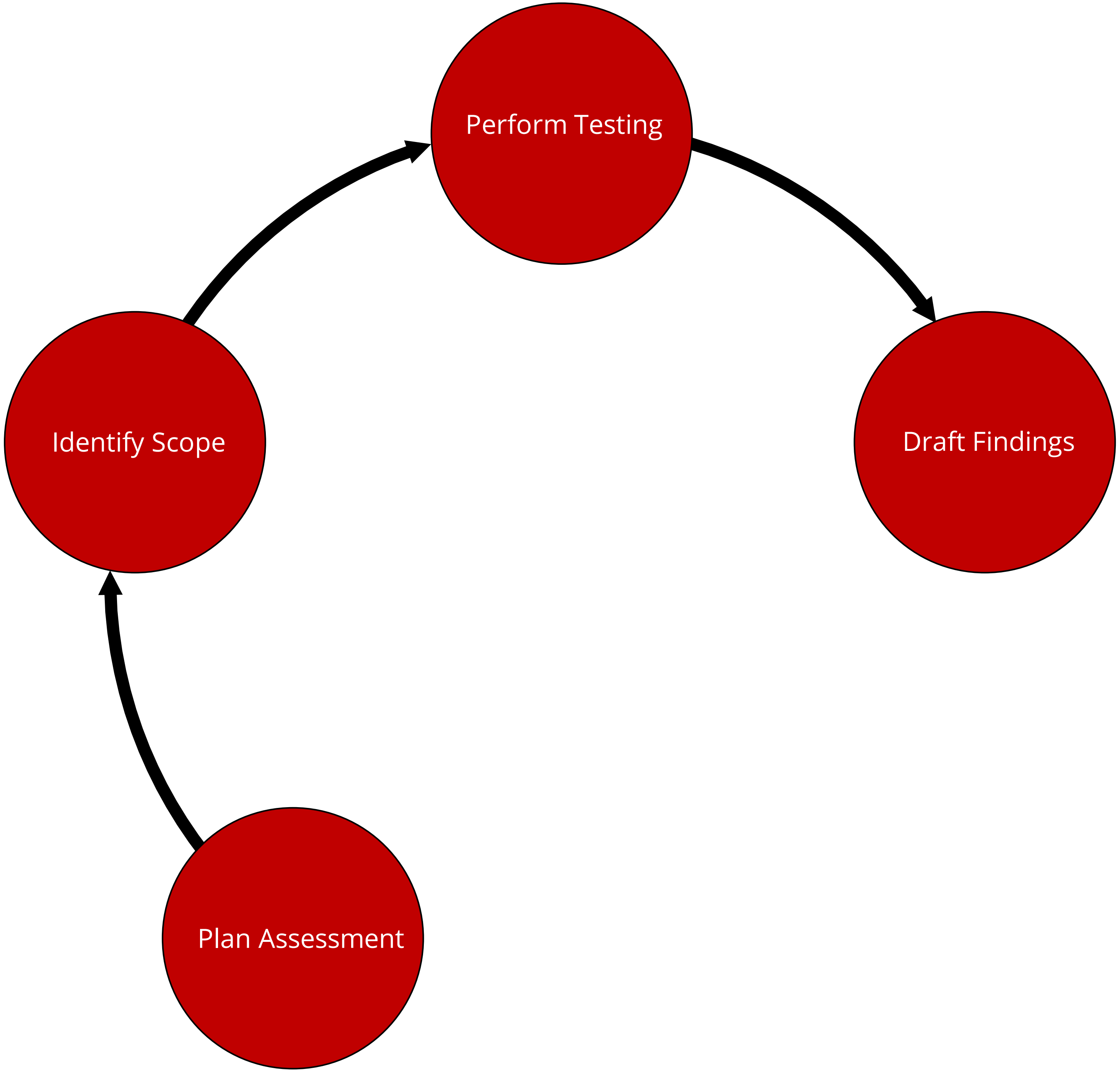
Plan Assessment



Plan Assessment

Identify Scope

Perform Testing

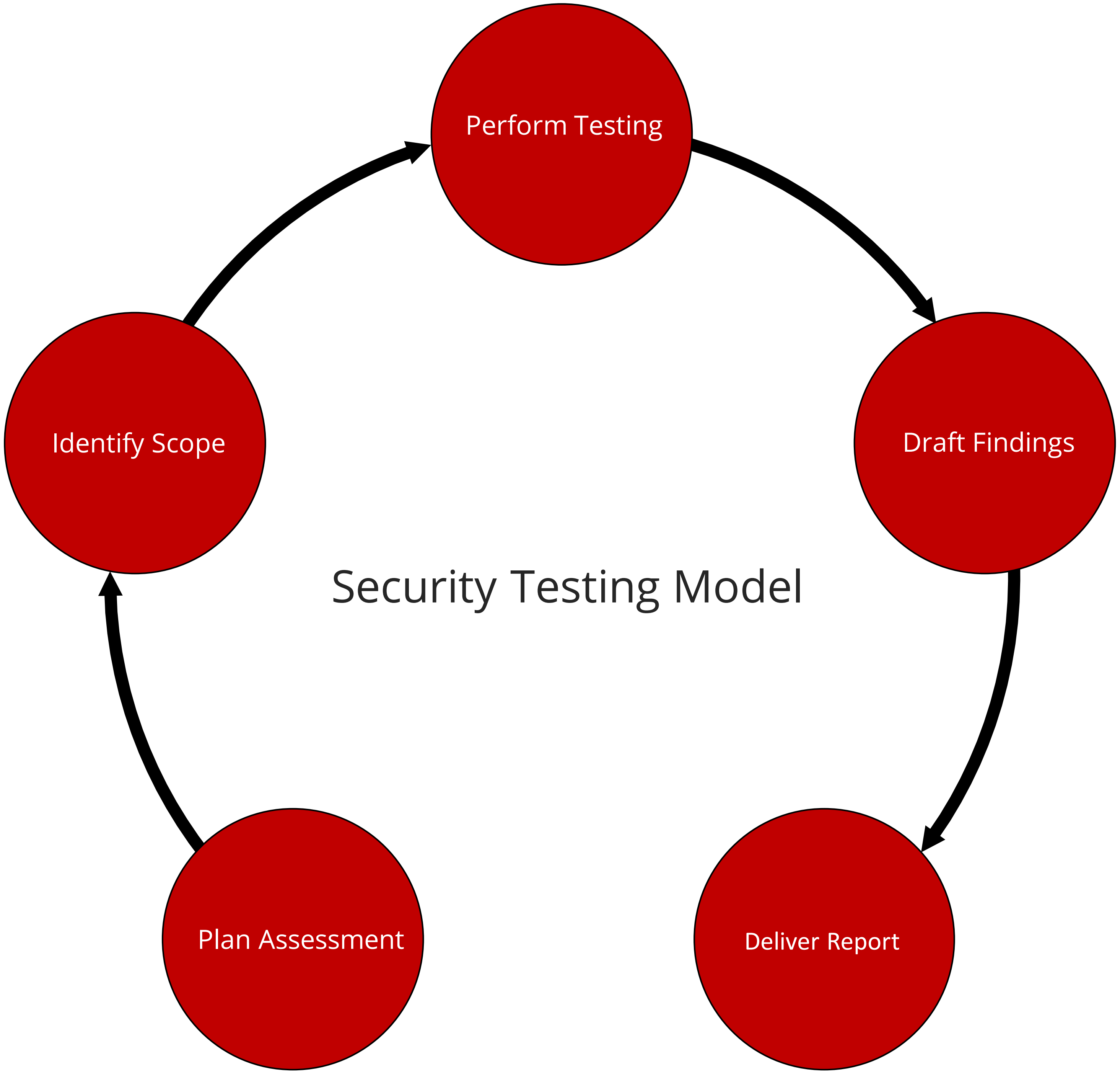


Plan Assessment

Identify Scope

Perform Testing

Draft Findings



Security Testing Model

Identify Scope

Perform Testing

Draft Findings

Deliver Report

Plan Assessment

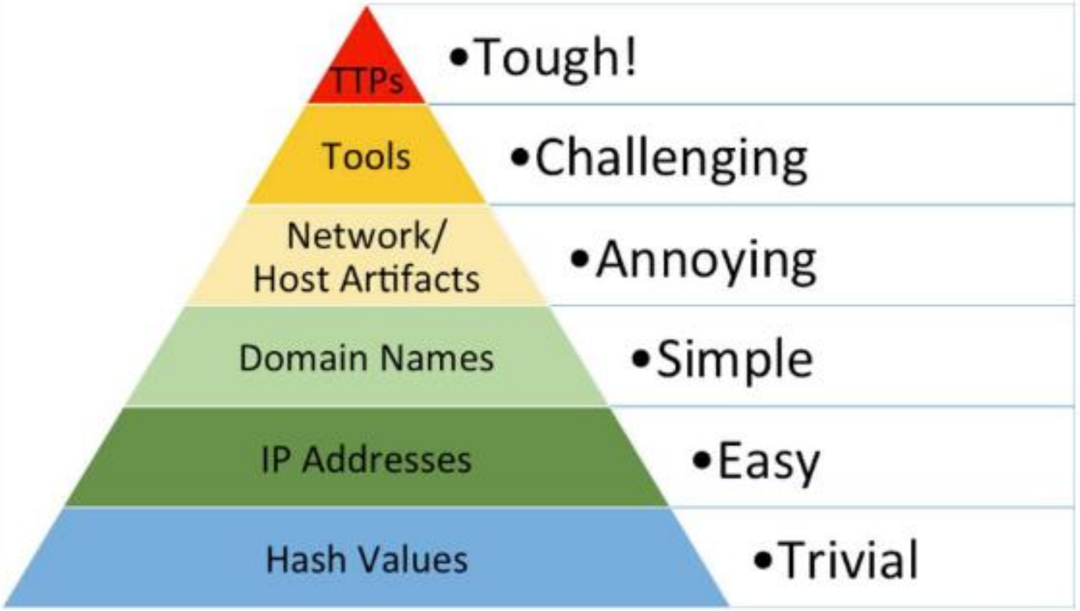
OFFENSIVE SECURITY THEORY

- Efforts in offensive security testing must align with defense

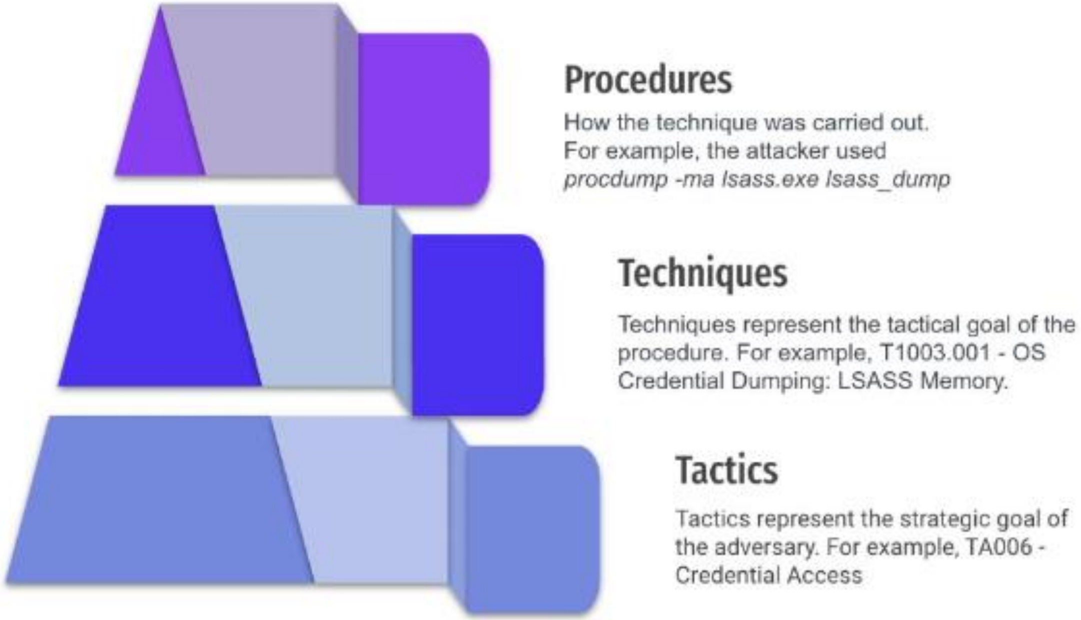
- How accurate and realistic can we be with our assessments?

- Traditional approach focus on point in time assessment

OFFENSIVE SECURITY THEORY



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


Procedures

How the technique was carried out. For example, the attacker used *procdump -ma lsass.exe lsass_dump*

Techniques

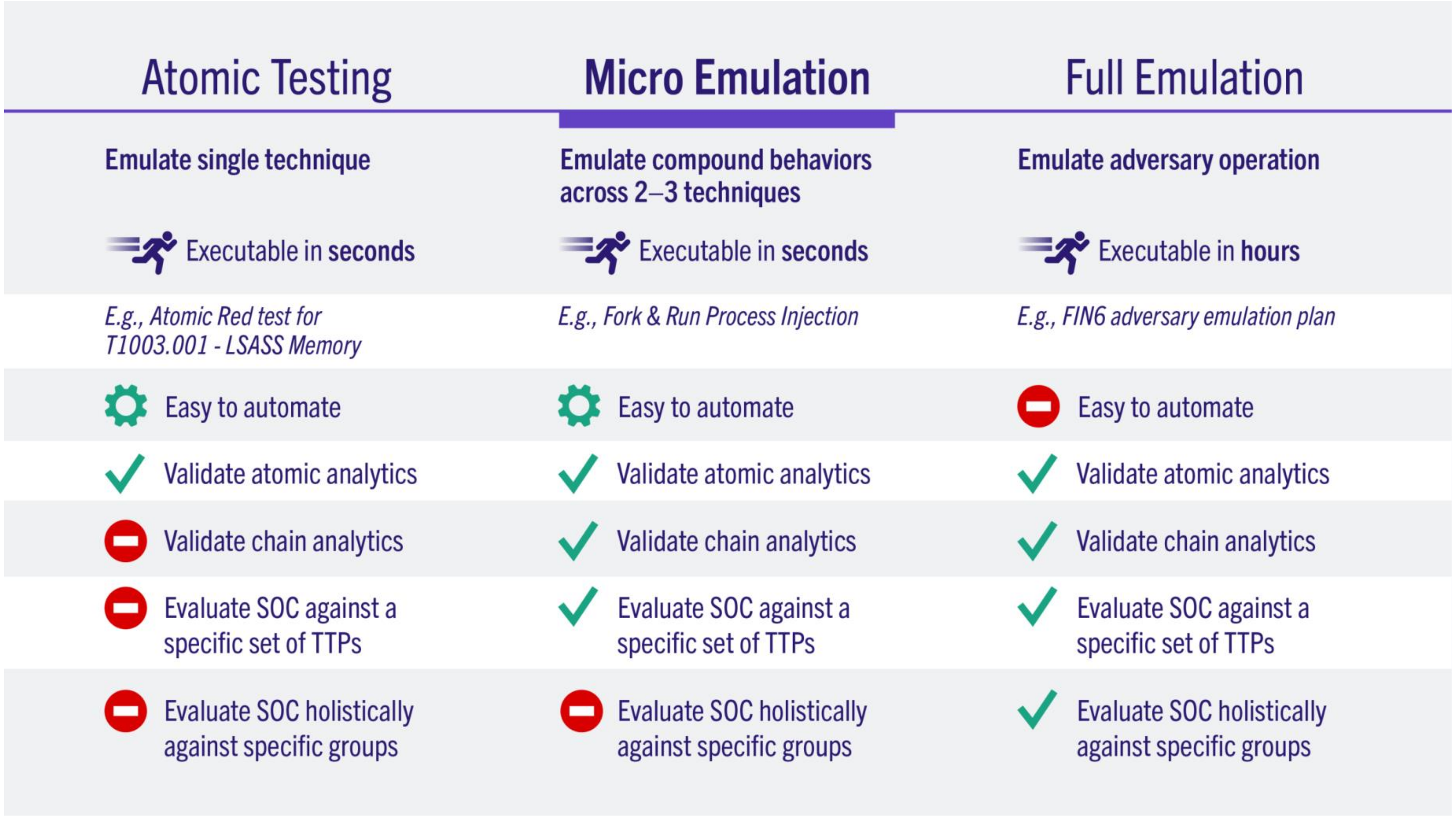
Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

Source:
https://www.scythe.io/library/summiting-the-pyramid-of-pain-the-ttp-pyramid

MICRO EMULATION



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**
E.g., Atomic Red test for T1003.001 - LSASS Memory	*E.g., Fork & Run Process Injection*	*E.g., FIN6 adversary emulation plan*
⚙ 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

https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/micro-emulation-plans/

ENDPOINT DETECTION & RESPONSE

- Acronym soup and misunderstandings:
  - EDR, XDR, MDR, etc.
- What are the main advantages of an EDR?
  - Protection
  - Detection
  - **Telemetry**

ENDPOINT DETECTION & RESPONSE

While all operating system vendors work to continuously improve the security of their products, two stand out as being "secure by design," specifically, Chromebooks and iOS devices like iPads.

Some organizations have migrated some or all their staff to use Chromebooks and iPads. As a result, they have removed a great deal of "attack surface," which in turn makes it much harder for attackers to get a foothold. Even if an attacker were able to find a foothold on those systems as part of a ransomware attack, the data primarily lives in a secure cloud service, reducing the severity of the attack.

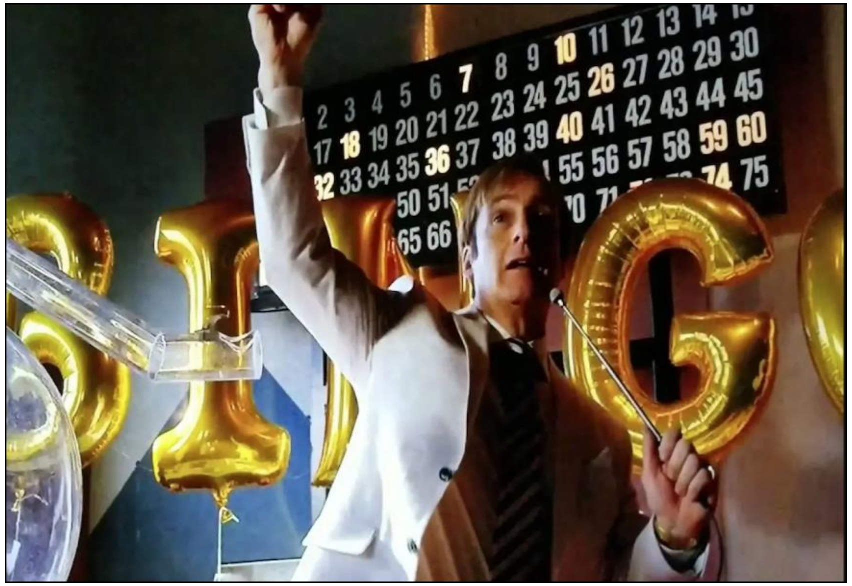
- https://docs.preludesecurity.com/docs/endpoints
- https://www.cisa.gov/cyber-guidance-small-businesses

MITRE ATT&CK® EVALUATIONS

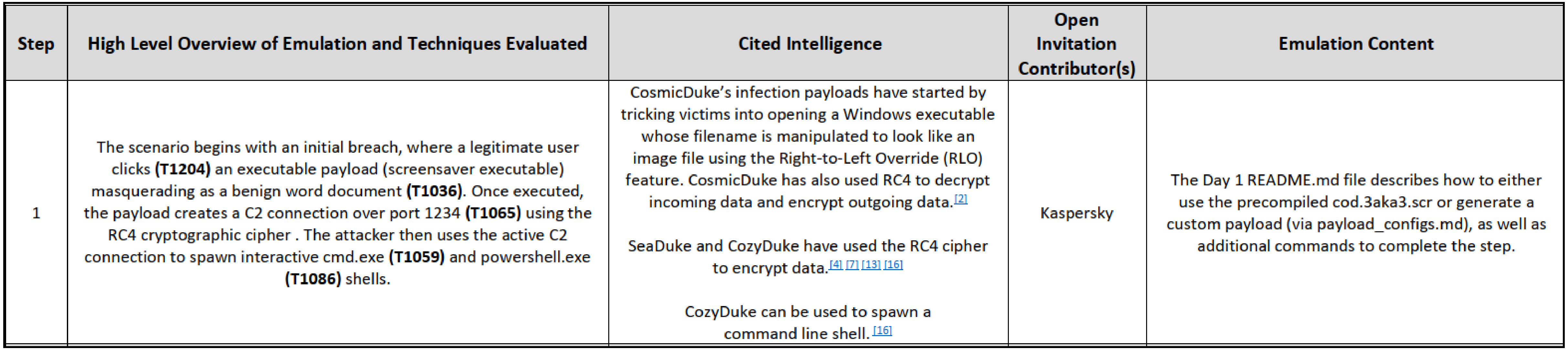
- Open evaluations against vendors using the ATT&CK matrix
  - Incredibly powerful resources worth investigating

- Everyone is a winner?

- Our industry likes checklists and pretty colors



MAPPING EXAMPLE



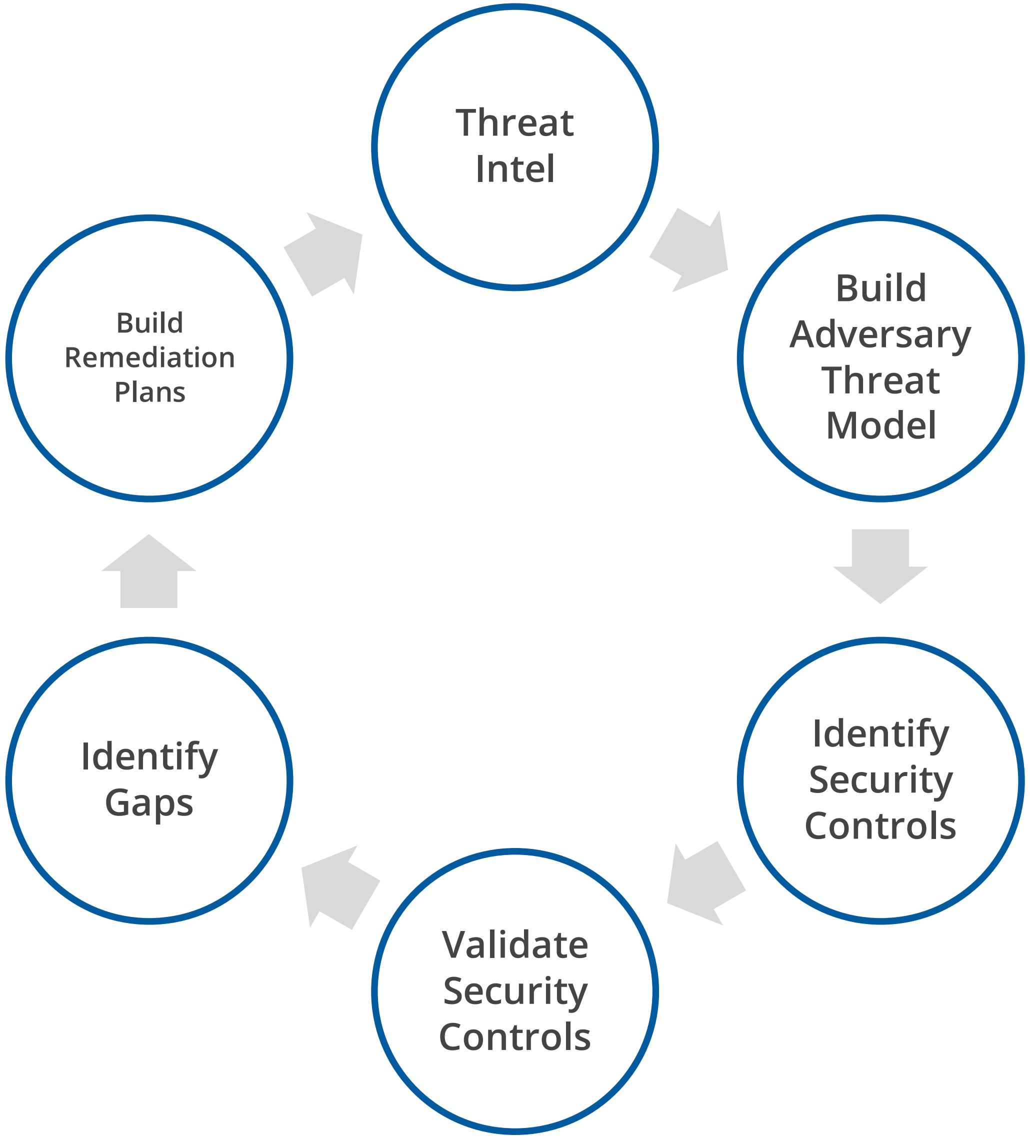
Step	High Level Overview of Emulation and Techniques Evaluated	Cited Intelligence	Open Invitation Contributor(s)	Emulation Content
1	The scenario begins with an initial breach, where a legitimate user clicks **(T1204)** an executable payload (screensaver executable) masquerading as a benign word document **(T1036)**. Once executed, the payload creates a C2 connection over port 1234 **(T1065)** using the RC4 cryptographic cipher . The attacker then uses the active C2 connection to spawn interactive cmd.exe **(T1059)** and powershell.exe **(T1086)** shells.	CosmicDuke's infection payloads have started by tricking victims into opening a Windows executable whose filename is manipulated to look like an image file using the Right-to-Left Override (RLO) feature. CosmicDuke has also used RC4 to decrypt incoming data and encrypt outgoing data.[2] SeaDuke and CozyDuke have used the RC4 cipher to encrypt data.[4] [7] [13] [16] CozyDuke can be used to spawn a command line shell. [16]	Kaspersky	The Day 1 README.md file describes how to either use the precompiled cod.3aka3.scr or generate a custom payload (via payload_configs.md), as well as additional commands to complete the step.

APT29 / Cozy Bear / The Dukes Emulation Plan – MITRE ATT&CK Evaluations

https://attackevals.mitre-engenuity.org/enterprise/participants/elastic

APPROACHES/PITFALLS WITH ATT&CK

- ATT&CK is not a check box
- ATT&CK is not the answer to all your security issues
- ATT&CK helps classify malicious actions


Threat Intel
Build Adversary Threat Model
Identify Security Controls
Validate Security Controls
Identify Gaps
Build Remediation Plans

EMULATION CHALLENGES

- Malicious actors do not care about the ATT&CK framework

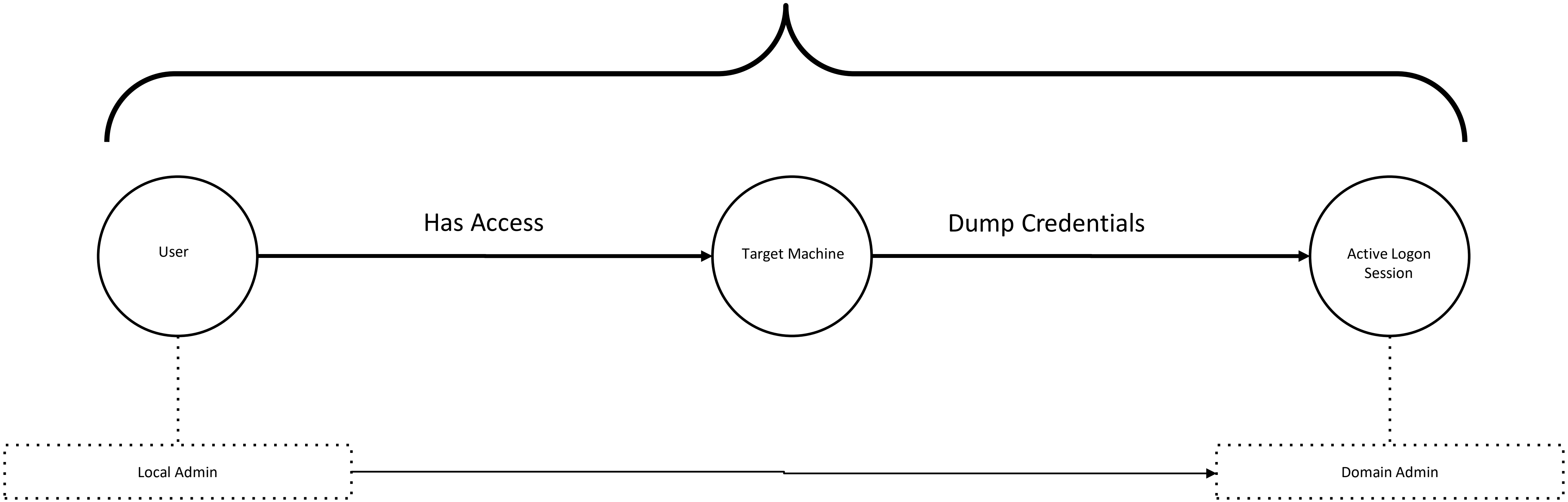
- We need actionable procedural data to ensure we are prioritizing threats

- Do we have the capabilities and resources to execute the same plan?

UNDERSTANDING THREATS

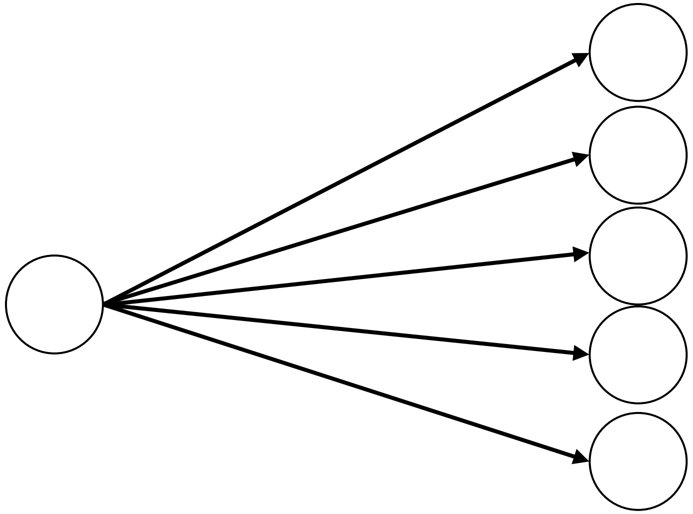
- Threats have intent
- Threats have a capability
- Threats have an opportunity (attacks are like water)

Escalation Plan



DEFENSIVE REALITY

- Detecting offensive outcomes is different for every procedure
- Offense has the luxury of a one-to-many mapping
- How many ways to perform Kerberoasting
  - PowerShell, C#, Mimikatz, etc.



Offensive Outcome One-to-Many

WALKTRHOUGH EVALUATIONS

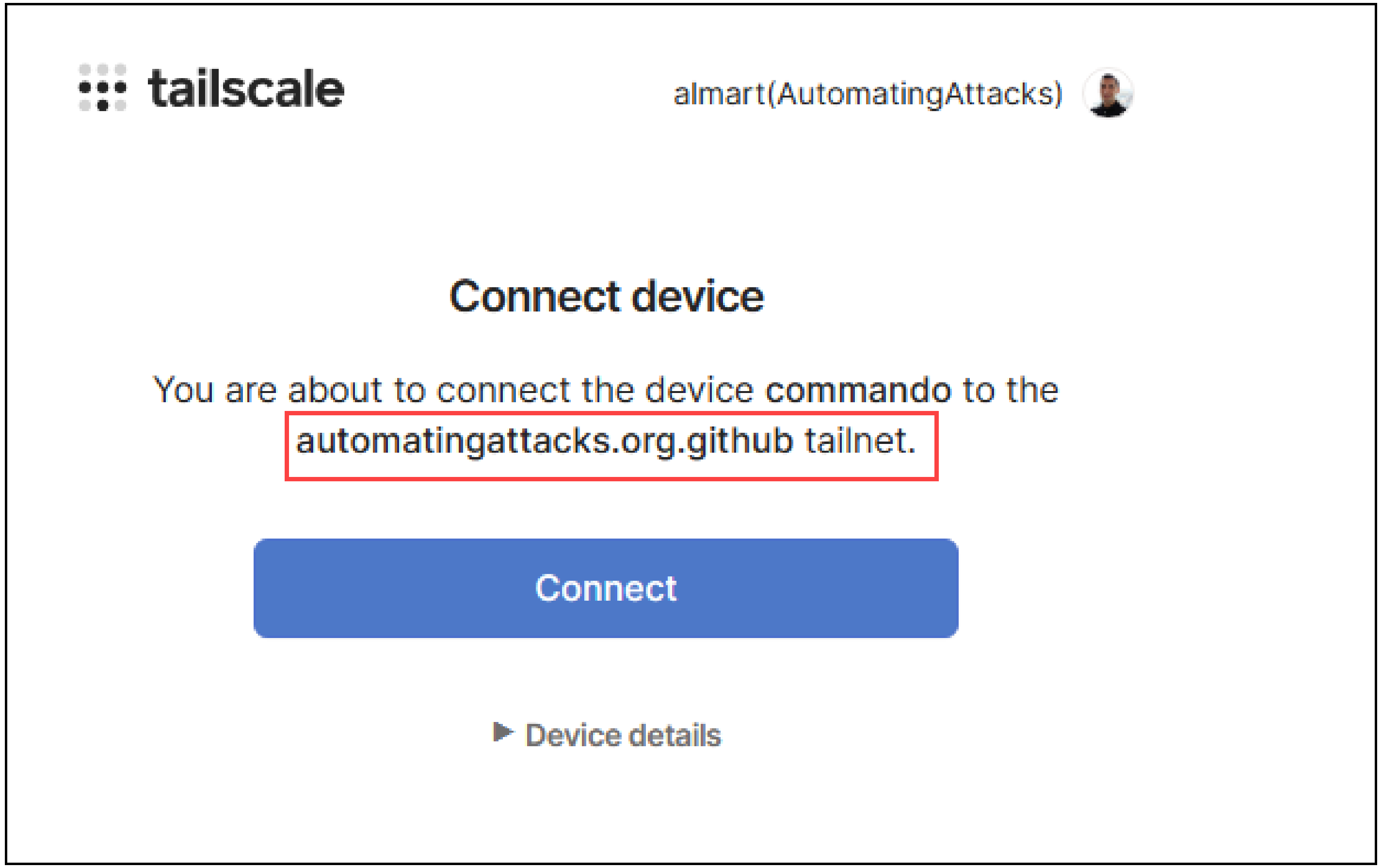
WORKSHOP STRUCTURE

- Access to the environment via GitHub/TailScale
  - https://github.com/AutomatingAttacks
- PurpleCloud used to automate deployment
- SnapLabs used to assist with deployment
  - https://www.purplecloud.network/ (Jason Ostrom)
  - Integrated with Elastic Cloud EDR
  - AD domain environment
  - https://github.com/warhorse

WORKSHOP STRUCTURE

- Lab environment will be online until 10/21
- Each workstation should be unique with same tools installed
  - Use a virtual machine and connect via TailScale
  - Information including IP’s, credentials, etc. distributed via Discord
    - @almart
    - https://github.com/DenSecure-Lab
    - Tailscale: densecure-lab.org.github

TailScale



Connect device

You are about to connect the device **commando** to the automatingattacks.org.github tailnet.

EDR INTEGRATION - ELASTIC

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.10.4-windows-x86_64.zip -OutFile elastic-agent-8.10.4-windows-x86_64.zip
Expand-Archive .\elastic-agent-8.10.4-windows-x86_64.zip -DestinationPath .
cd elastic-agent-8.10.4-windows-x86_64
.\elastic-agent.exe install --url=https://52ef142382ca4dcba71cbc10198b782c.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=MG56alM0c0JUSzFRSjBNcFpQeTk6Z2VwVWtxTkVScGVfd0FnbWdzSUV1dw==
```

- Policy on “detection” mode only

ATOMIC TESTING

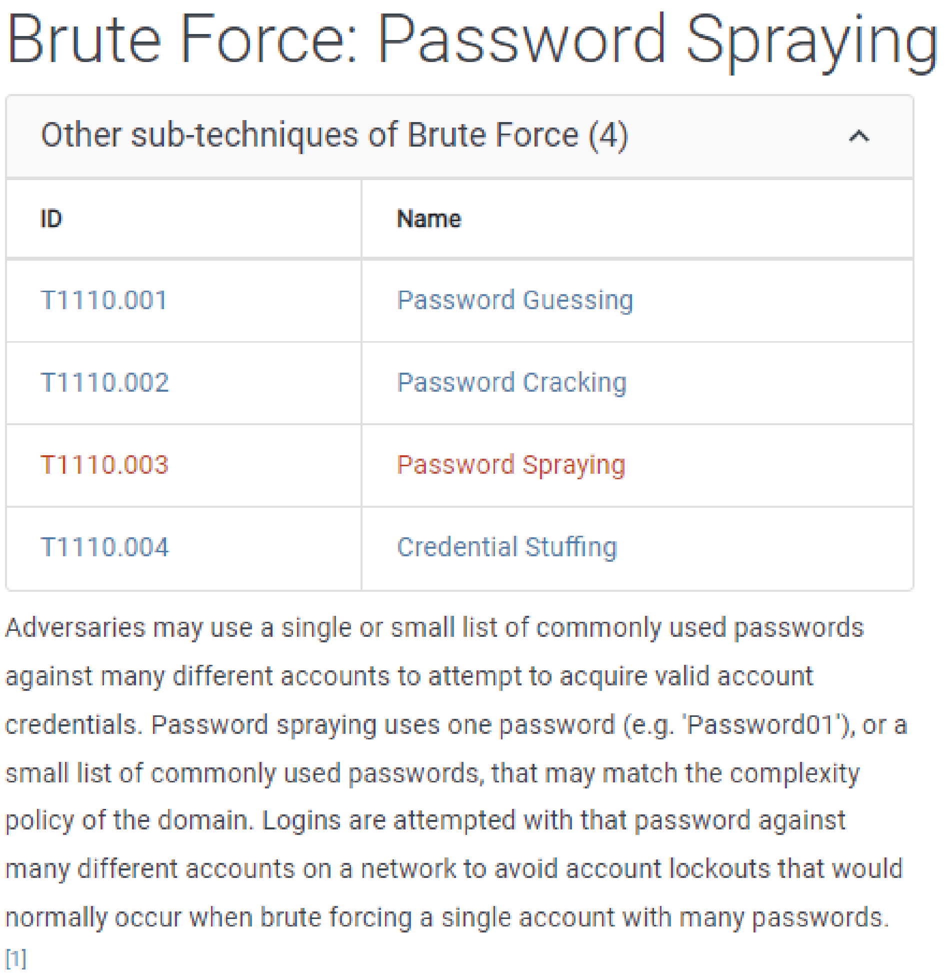
ATR OVERVIEW

```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-
atomicredteam.ps1'); Install-AtomicRedTeam –getAtomics -Force

Invoke-AtomicTest T1055 -TestNumbers 4
```

- ATR should be present on target workstation
  - Helps automate execution of procedures

- Run sample test using T1055 to verify

PASSWORD SPRAY

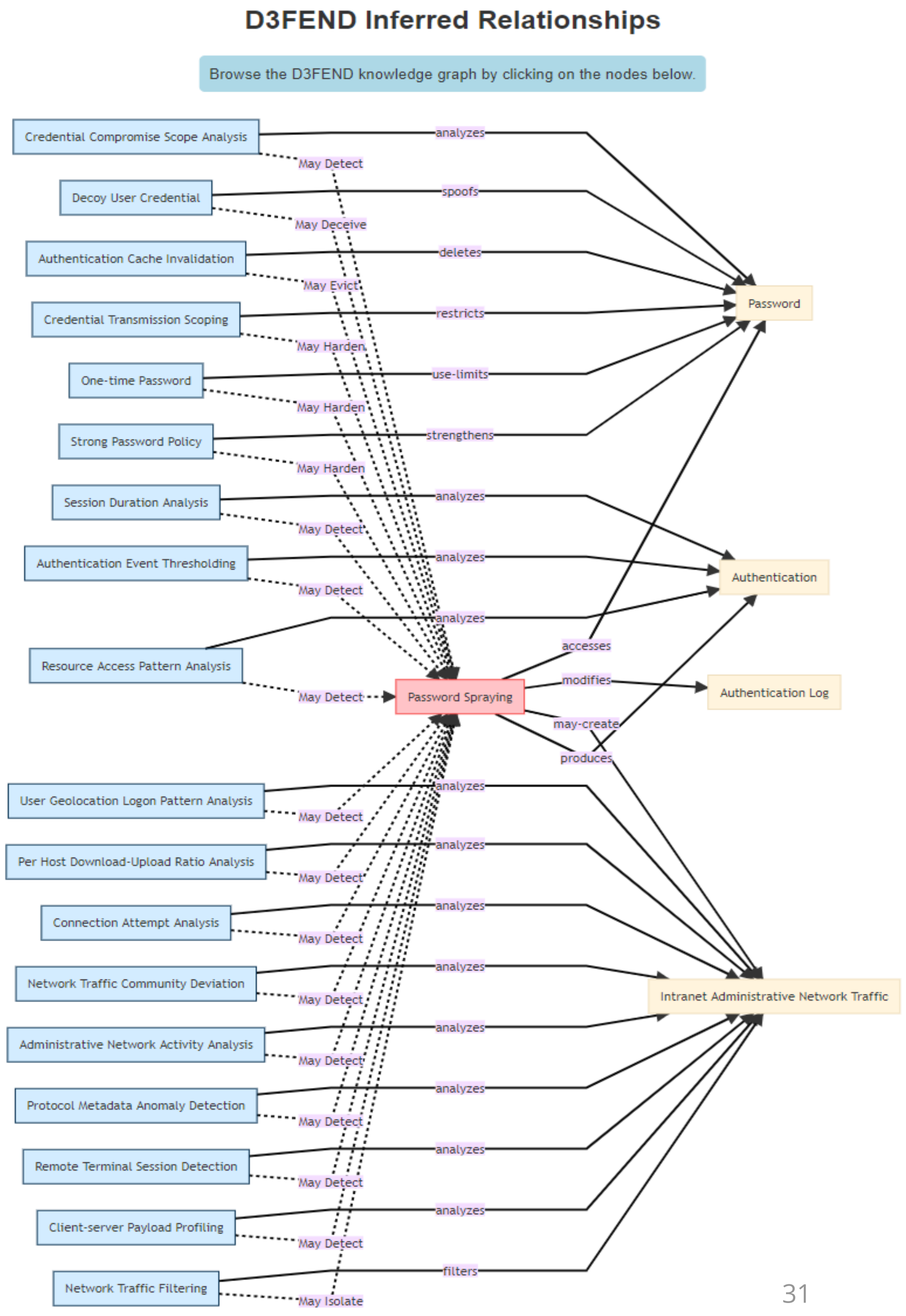


Brute Force: Password Spraying

Other sub-techniques of Brute Force (4)

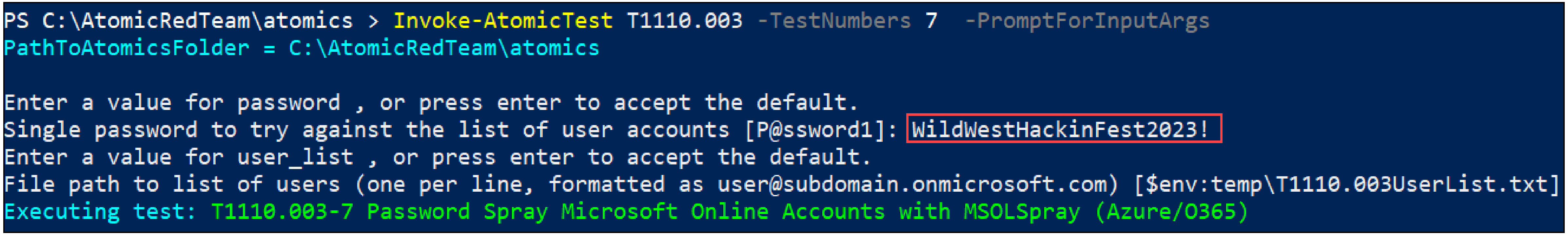
ID	Name
T1110.001	Password Guessing
T1110.002	Password Cracking
T1110.003	Password Spraying
T1110.004	Credential Stuffing

Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. [1]



D3FEND Inferred Relationships
Browse the D3FEND knowledge graph by clicking on the nodes below.
Credential Compromise Scope Analysis
analyzes
May Detect
Decoy User Credential
spoofs
May Deceive
Authentication Cache Invalidation
deletes
May Evict
Credential Transmission Scoping
restricts
May Harden
One-time Password
use-limits
May Harden
Strong Password Policy
strengthens
May Harden
Session Duration Analysis
analyzes
May Detect
Authentication Event Thresholding
analyzes
May Detect
analyzes
Resource Access Pattern Analysis
May Detect
Password Spraying
accesses
modifies
may-create
produces
Password
Authentication
Authentication Log
Intranet Administrative Network Traffic
User Geolocation Logon Pattern Analysis
analyzes
May Detect
Per Host Download-Upload Ratio Analysis
analyzes
May Detect
Connection Attempt Analysis
analyzes
May Detect
Network Traffic Community Deviation
analyzes
May Detect
Administrative Network Activity Analysis
analyzes
May Detect
Protocol Metadata Anomaly Detection
analyzes
May Detect
Remote Terminal Session Detection
analyzes
May Detect
Client-server Payload Profiling
analyzes
May Detect
Network Traffic Filtering
filters
May Isolate

DEMONSTRATION



```
PS C:\AtomicRedTeam\atomics > Invoke-AtomicTest T1110.003 -TestNumbers 7  -PromptForInputArgs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Enter a value for password , or press enter to accept the default.
Single password to try against the list of user accounts [P@ssword1]: WildWestHackinFest2023!
Enter a value for user_list , or press enter to accept the default.
File path to list of users (one per line, formatted as user@subdomain.onmicrosoft.com) [$env:temp\T1110.003UserList.txt]
Executing test: T1110.003-7 Password Spray Microsoft Online Accounts with MSOLSpray (Azure/O365)
```

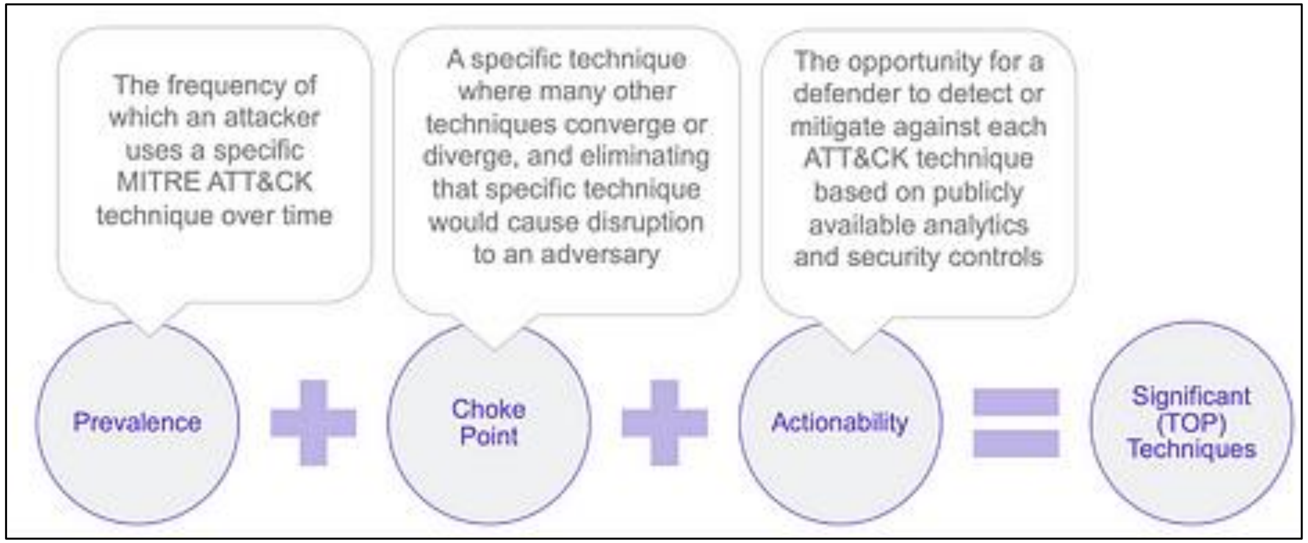
ATR OVERVIEW

- Atomic testing should be the first place we start
- Low cost / barrier of entry
- Easy to run and automate
- Main goal here should be to focus on telemetry

ATR OVERVIEW

- Easy to get overwhelmed or know where to begin

- Important to prioritize / understand why we want to execute something



The frequency of which an attacker uses a specific MITRE ATT&CK technique over time

A specific technique where many other techniques converge or diverge, and eliminating that specific technique would cause disruption to an adversary

The opportunity for a defender to detect or mitigate against each ATT&CK technique based on publicly available analytics and security controls

ATOMIC TESTING

Conti Discovery

```
ipconfig /all
systeminfo
whoami /groups
net config workstation
nltest /domain_trusts
nltest /domain_trusts  /all_trusts
net view /all /domain
net view /all
net group "Domain Admins" /domain
```

https://thedfirreport.com/2021/05/12/conti-ransomware/

- T1016
- T1082
- T1033
- T1482
- What else is missing?

DISCOVERY - ATR

- Basic example from Conti Ransomware playbook 2021
  - Still common commands executed in many environments
  - Will our default controls catch this “standard behavior”?
  - Notice that more than one technique can be attributed to a procedure

- Fair to EDR?

- It is more efficient to work backwards from procedures
  - Naïve approach is to color code the matrix and run all atomics

ATR CONTINUED

- T1219 - Remote Access Software
  - Common for EDR defaults to ignore

- What are some lower “risk” procedures we expect our controls to not alert?
  - Detection engineering can help fill in the gaps

- It is more efficient to work backwards from procedures
  - Naïve approach is to color code the matrix and run all atomics

MICRO EMULATIONS

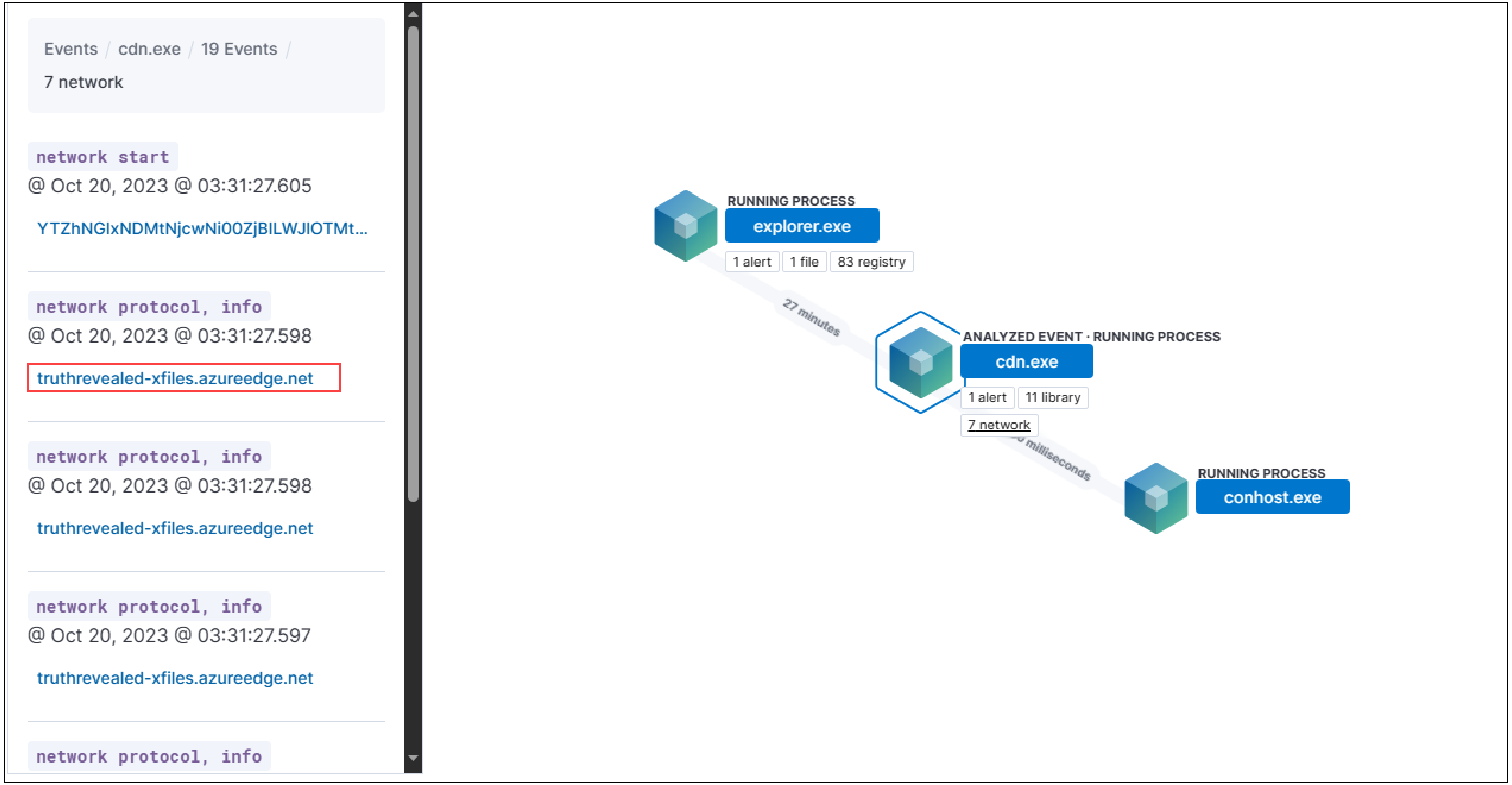
PURPLE TEAM

C2 – INCREASING ACCURACY

- A new trend may be seen from our understanding:
  - We are limited to singular processes / atomic actions
  - Element of realism may be missed due to our approach
  - We can scale / implement more resources to create an accurate plan

- Threat actors use a C2 and we can too (CALDERA)

Find the C2



Events / cdn.exe / 19 Events /

7 network

network start

@ Oct 20, 2023 @ 03:31:27.605

YTZhNGIxNDMtNjcwNi00ZjBlLWJlOTMt...

network protocol, info

@ Oct 20, 2023 @ 03:31:27.598

truthrevealed-xfiles.azureedge.net

network protocol, info

@ Oct 20, 2023 @ 03:31:27.598

truthrevealed-xfiles.azureedge.net

network protocol, info

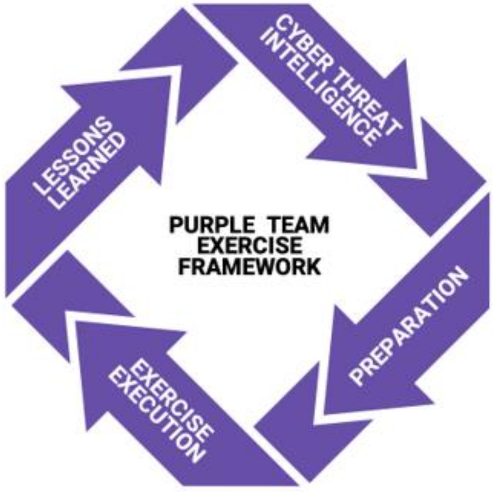
@ Oct 20, 2023 @ 03:31:27.597

truthrevealed-xfiles.azureedge.net

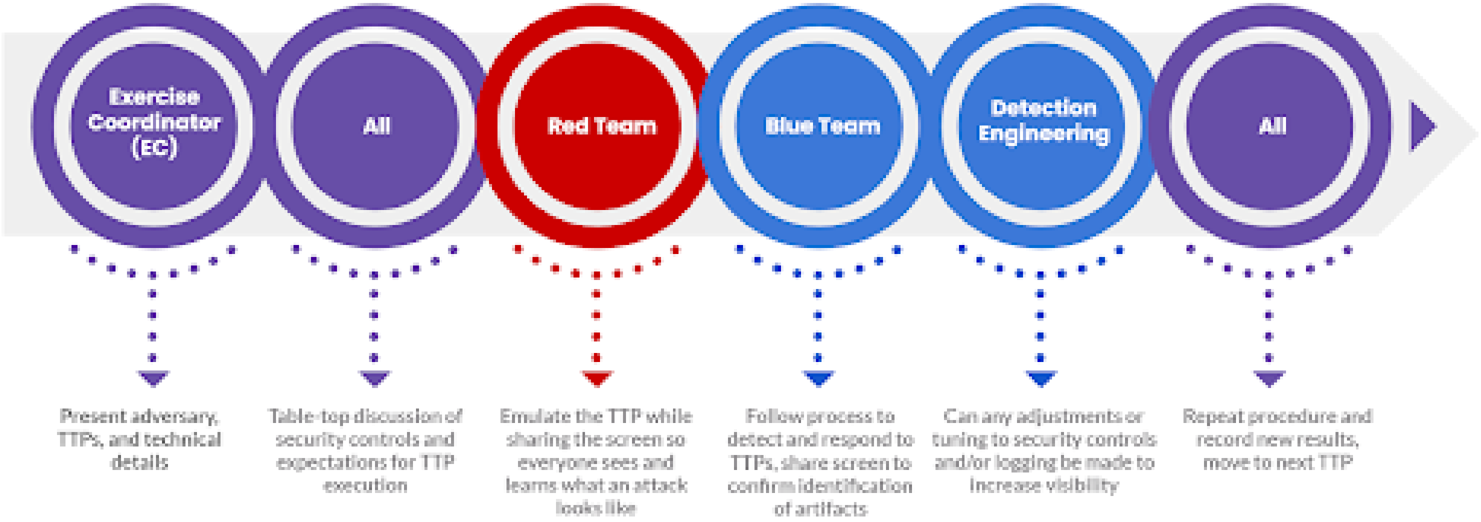
network protocol, info

THREAT EMULATION MAKE A PLAN

- Plan for the long-term success
- Iteration is key – get processes in place before looking to smash a home run
- PTES outlines procedural support for this program
  - Start with a TTX to introduce terms and approach



PURPLE TEAM EXERCISE FRAMEWORK



Exercise Coordinator (EC): Present adversary, TTPs, and technical details

All: Table-top discussion of security controls and expectations for TTP execution

Red Team: Emulate the TTP while sharing the screen so everyone sees and learns what an attack looks like

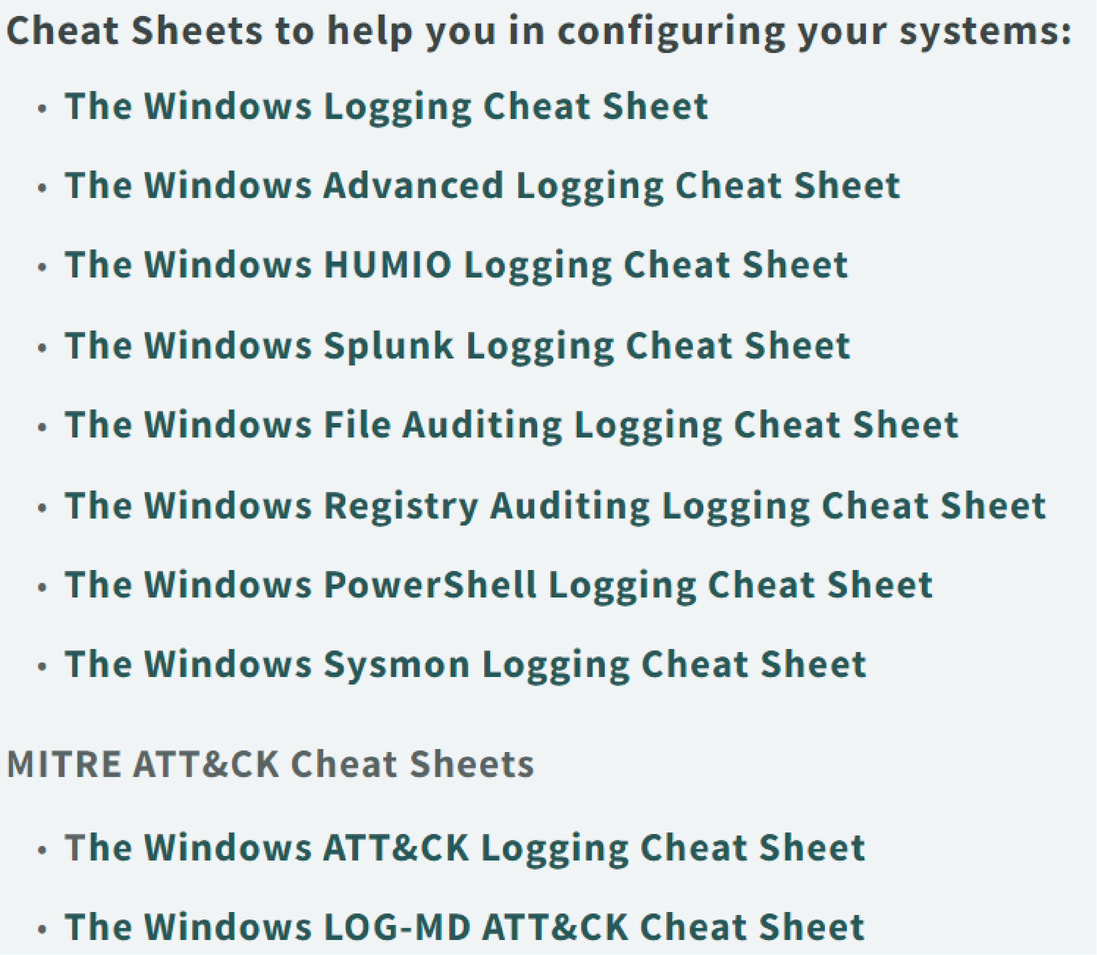
Blue Team: Follow process to detect and respond to TTPs, share screen to confirm identification of artifacts

Detection Engineering: Can any adjustments or tuning to security controls and/or logging be made to increase visibility

All: Repeat procedure and record new results, move to next TTP

https://github.com/scythe-io/purple-team-exercise-framework

AUDIT LOGGING



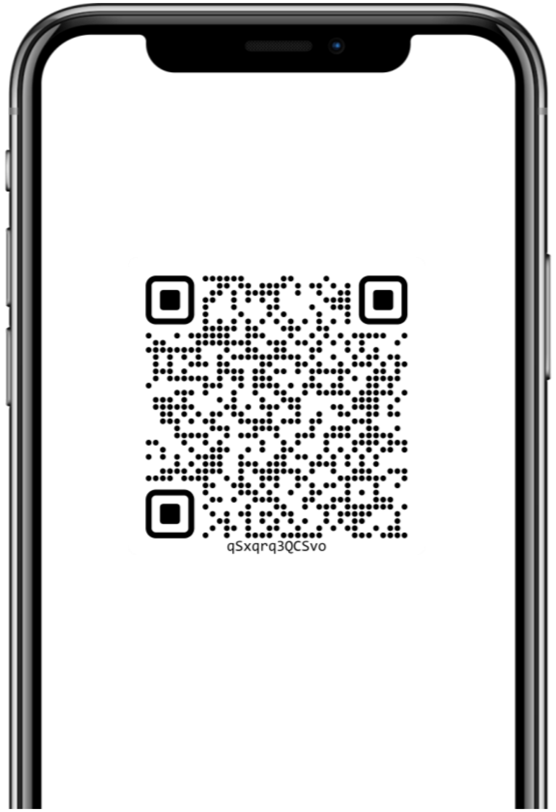
Cheat Sheets to help you in configuring your systems:

- The Windows Logging Cheat Sheet
- The Windows Advanced Logging Cheat Sheet
- The Windows HUMIO Logging Cheat Sheet
- The Windows Splunk Logging Cheat Sheet
- The Windows File Auditing Logging Cheat Sheet
- The Windows Registry Auditing Logging Cheat Sheet
- The Windows PowerShell Logging Cheat Sheet
- The Windows Sysmon Logging Cheat Sheet

MITRE ATT&CK Cheat Sheets

- The Windows ATT&CK Logging Cheat Sheet
- The Windows LOG-MD ATT&CK Cheat Sheet

QUESTIONS



Alex Martirosyan,
CRTO , OSCP, GPEN
Senior Penetration Tester, DenSecure
AMartirosyan@wolfandco.com
617.261.8138
https://www.linkedin.com/in/alex-martirosyan/
https://twitter.com/almartiros
https://www.wolfandco.com/services/densecure/

ABOUT DENSECURE

Wolf & Company's IT Assurance & Advisory team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.

DenSecure's core services include:

- Red Team Assessment
- Application Penetration Testing
- Network Penetration Testing
- Social Engineering
- Threat Emulation
- Continuous Penetration Testing

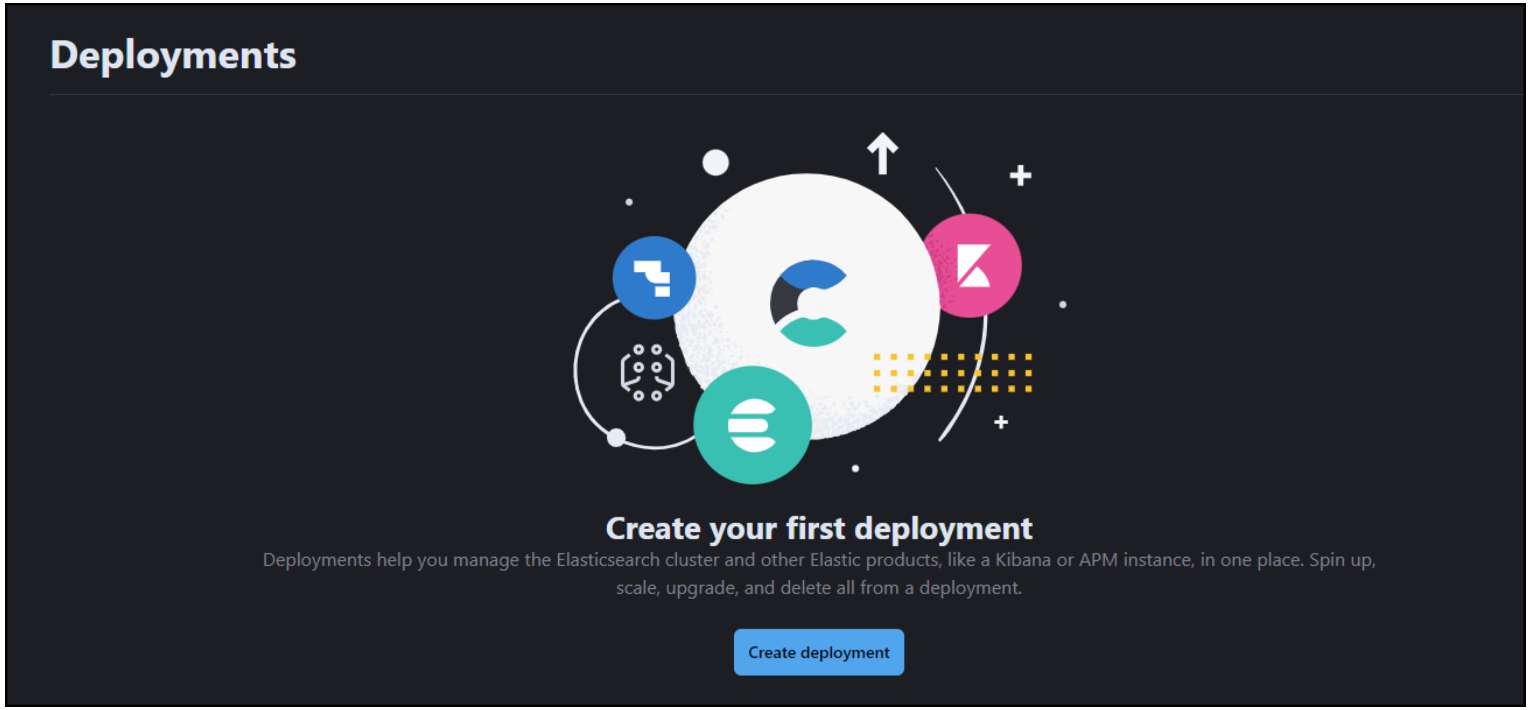
APPENDIX BUILD WORKSHOP

```
# Below are commands ran to build the workshop (used wsl Ubuntu)

apt-get install git-lfs

git clone https://github.com/iknowjason/PurpleCloud.git

pip3 install faker

az login # Install az cli and login as a global administrator

python3 ad.py --domain_controller --ad_domain xfiles.com --admin Red --password <password>--ad_users 500 --endpoints 10 --domain_join –helk

terraform init

terraform plan -out=run.plan

terraform apply run.plan
```

https://www.purplecloud.network/install/

APPENDIX BUILD WORKSHOP

- Elastic Cloud deployed in the background
  - Used to test "detection/protection" only policies within Elastic Defend
  - PurpleCloud can be deployed with HELK/Sentinel/Sysmon



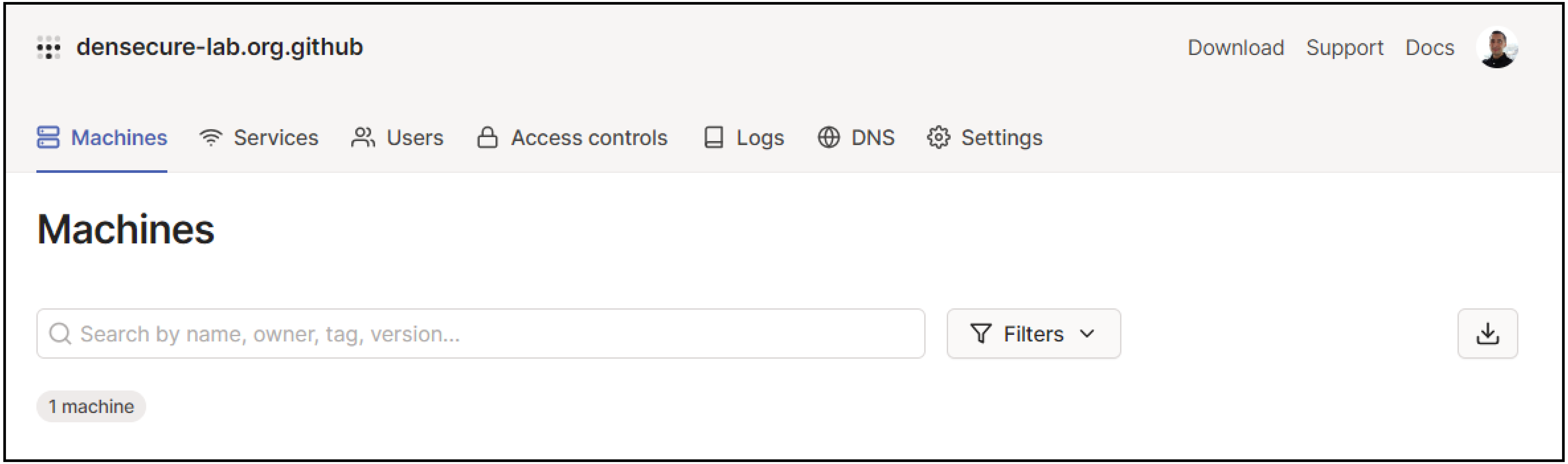
Deployments

Create your first deployment

Deployments help you manage the Elasticsearch cluster and other Elastic products, like a Kibana or APM instance, in one place. Spin up, scale, upgrade, and delete all from a deployment.

APPENDIX BUILD WORKSHOP

- TailScale used for student experience and to quickly access machines
  - **<u>FUTURE</u>**: TailScale can be integrated with Terraform deployment process
  - PurpleCloud by default will only allow list your public IP



densecure-lab.org.github

Machines

1 machine

Back to Home ⟶