



WORKSHOP: AUTOMATING ATTACKS

September 8, 2023 • Alex Martirosyan, CRT0, OSCP, GPEN

HACK RED CON



WHOAMI

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



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/>

AGENDA

- Motivations and goals for the workshop
- Evolution of offensive security testing
- Definitions, frameworks, and matrices
- 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, Elastic Cloud, TailScale, Terraform, etc.

▀ Andy Robbins for template slides

- <https://bit.ly/3BE4zbj>

MOTIVATIONS

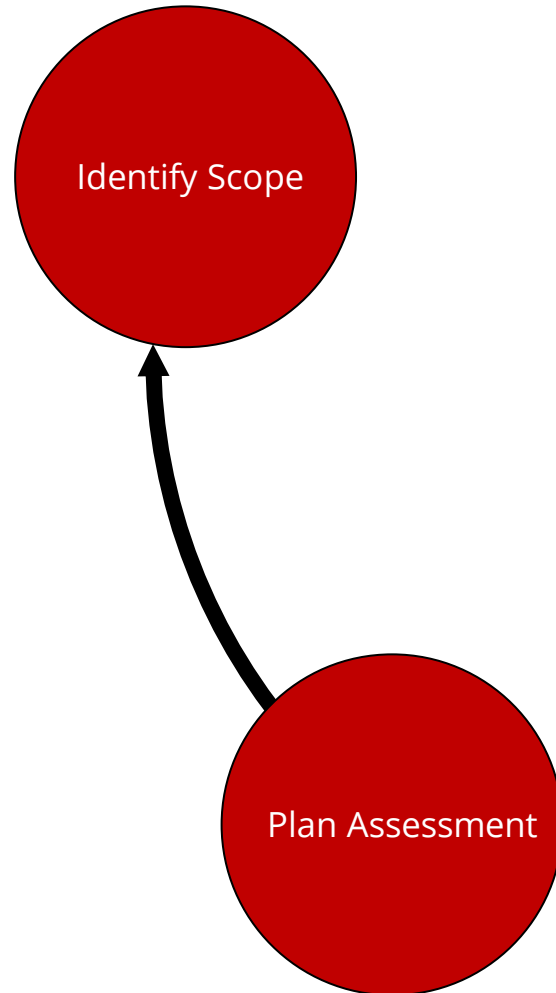
- ▀ Relatively new approach to security testing
 - Continuous vs Industry Standard
- ▀ Confusion behind varying testing methodologies
- ▀ Do our current approaches help solve cybersecurity challenges?
- ▀ Security controls are often times a black box

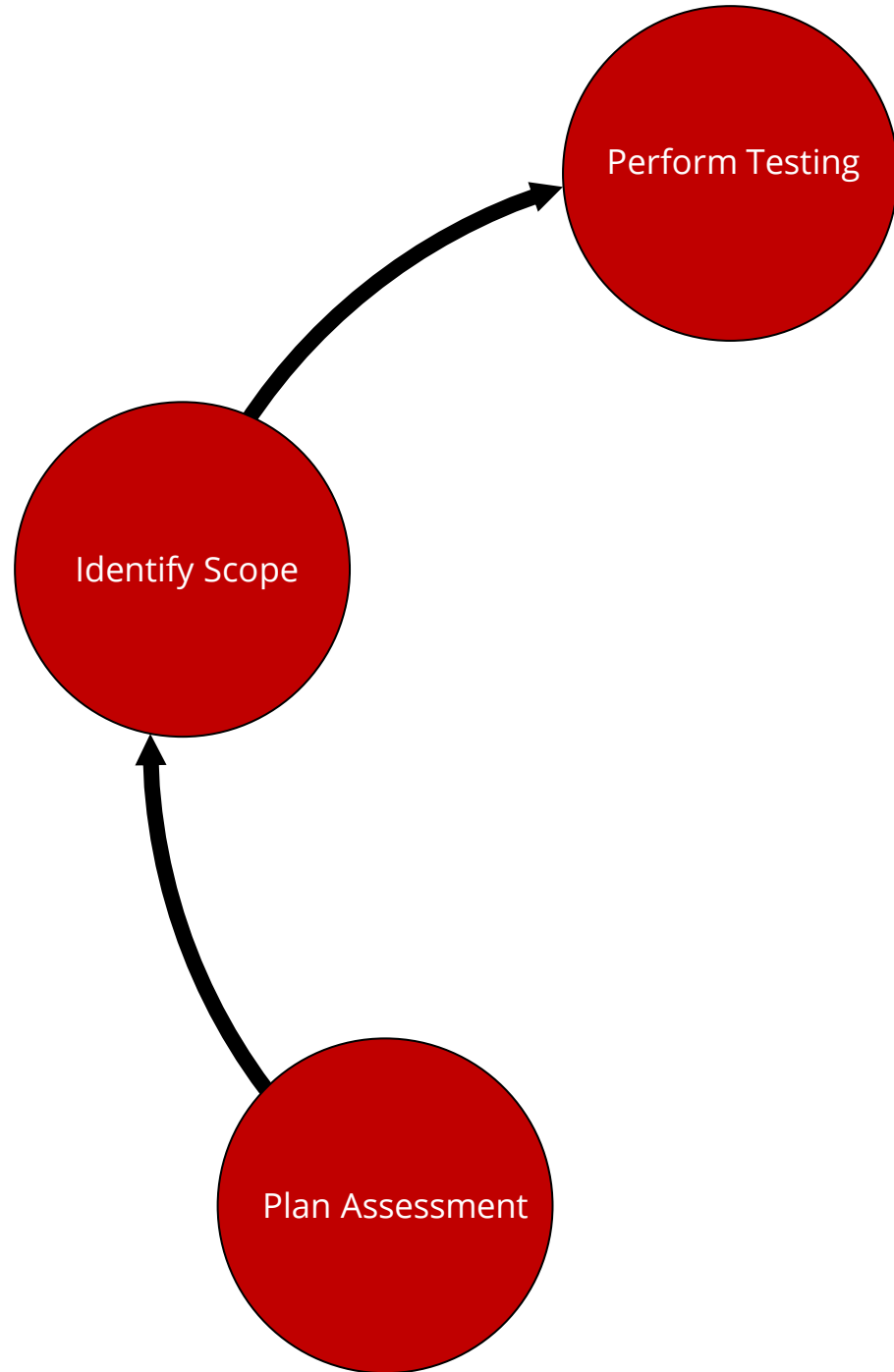
WORKSHOP GOALS AND LIMITATIONS

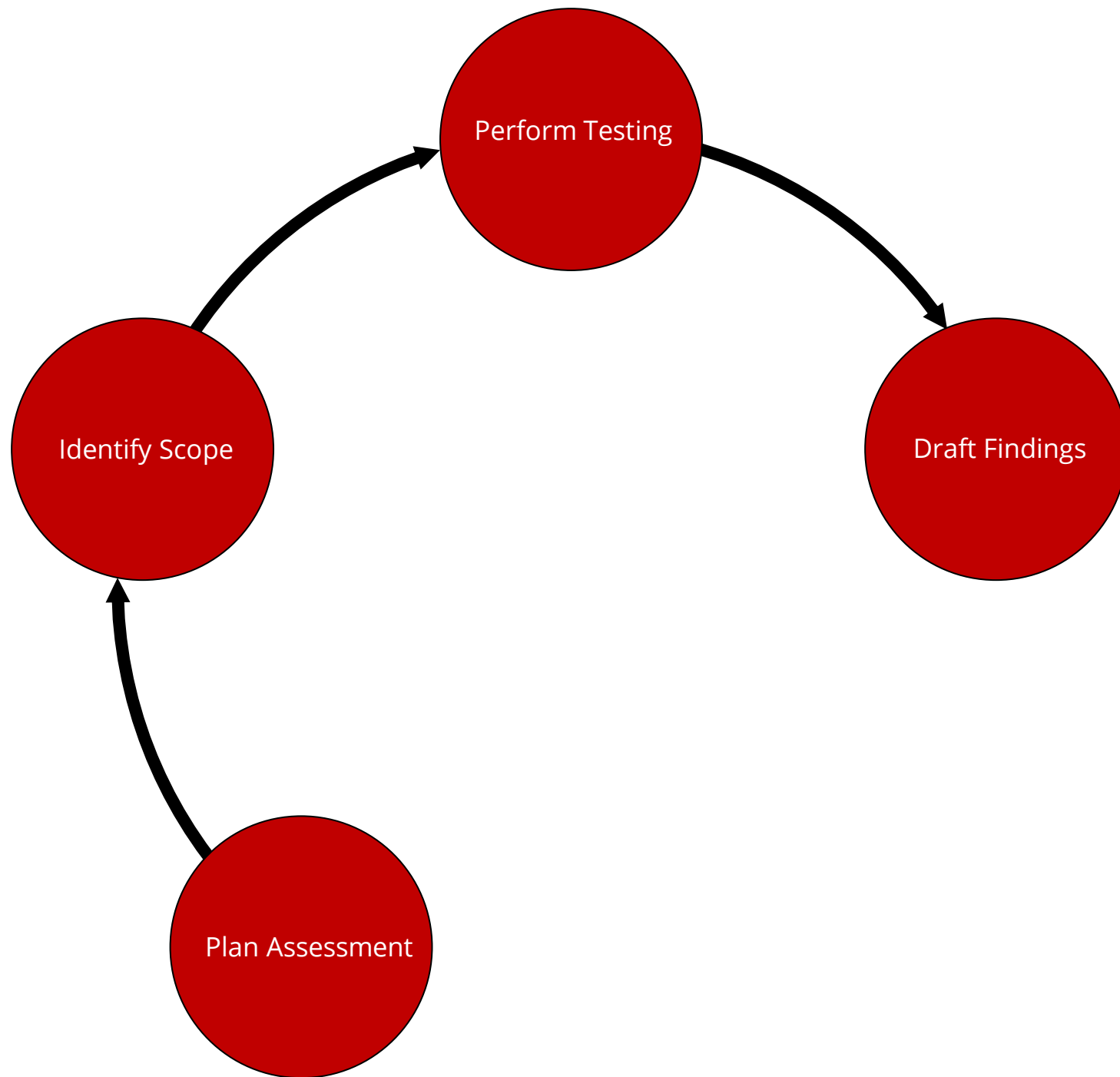
- ▀ **IDEA**: Relying on as many open-source tools as possible to building the environment
- ▀ **FOCUS**: Endpoint Detection & Response Solutions
- ▀ Lab != Production
- ▀ Understand the scale between accuracy and realism
- ▀ Windows endpoint focus (enterprise) with defaults

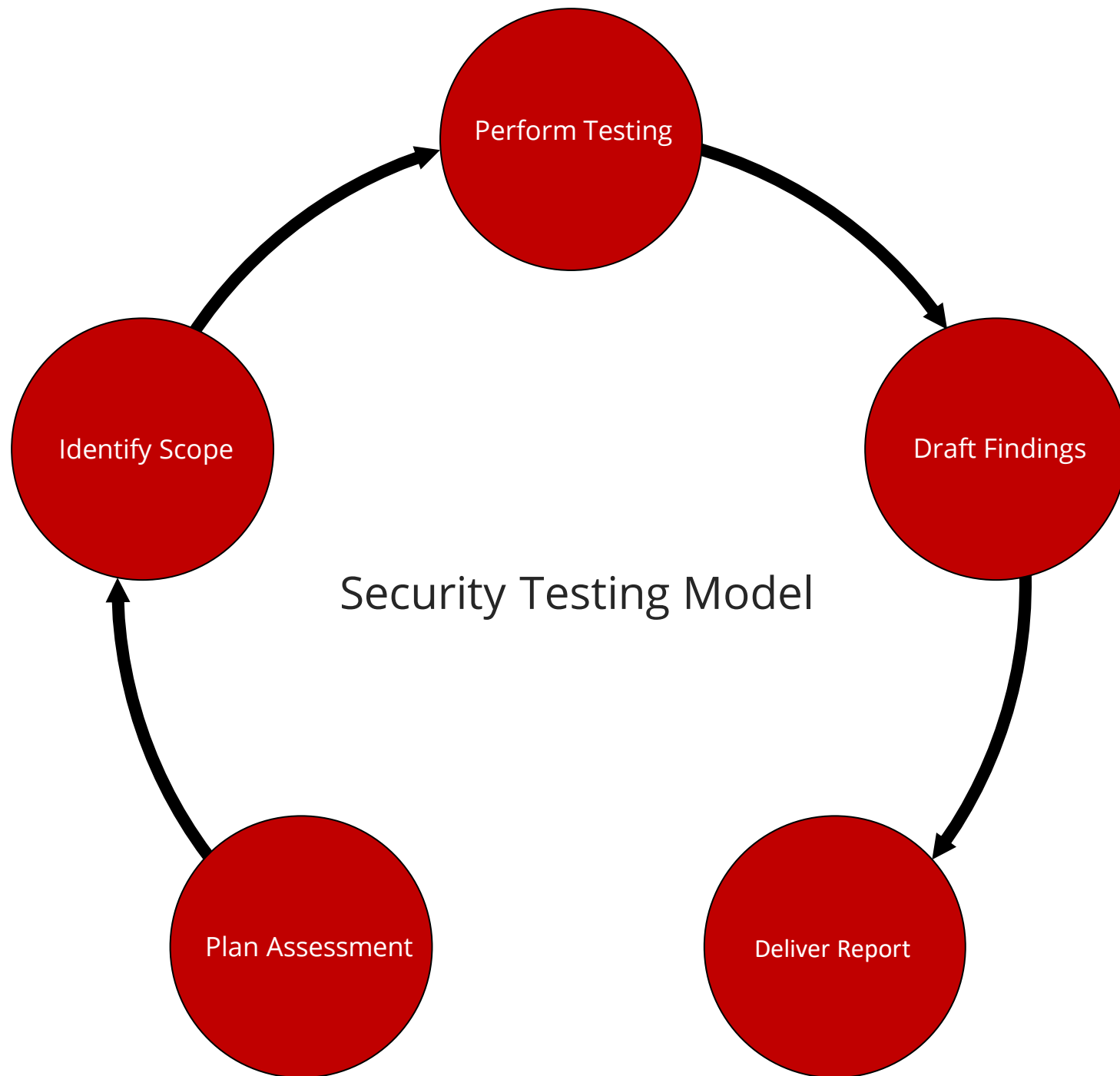
COMMON SECURITY TESTING MODEL







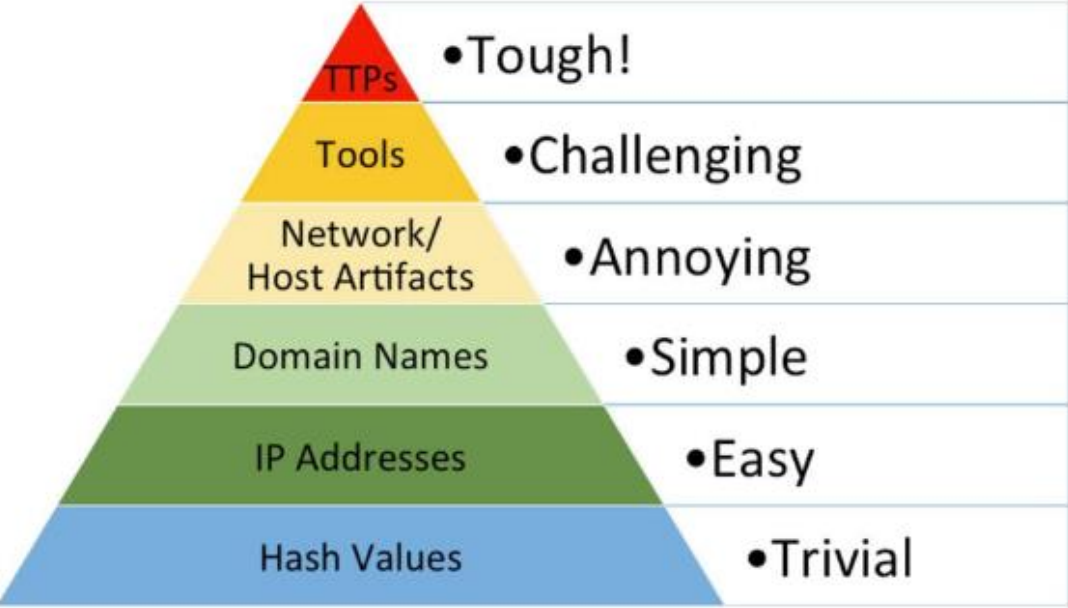




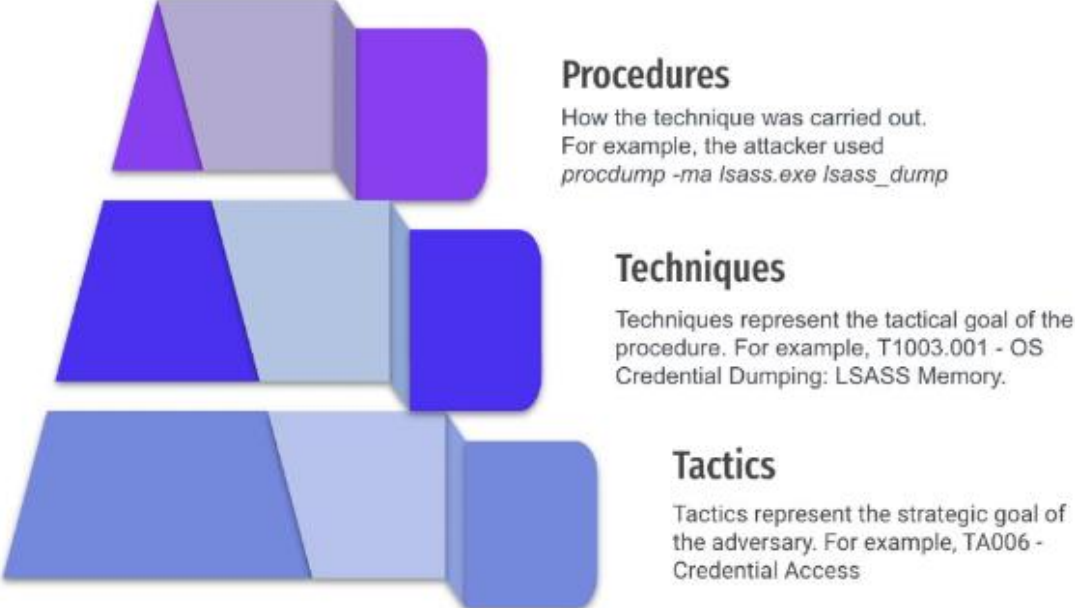
OFFENSIVE SECURITY THEORY

- ▀ 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>



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

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

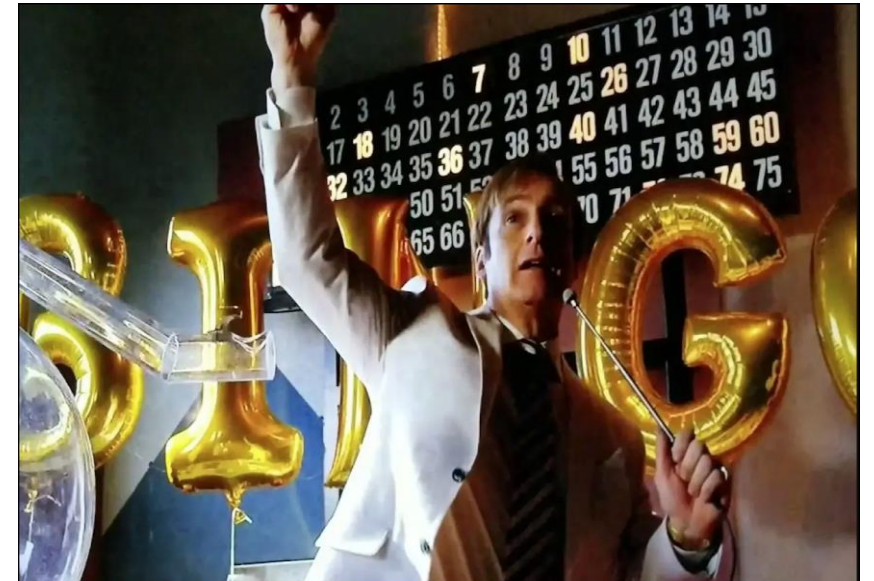
While all operating system vendors work to continuously improve the security of their products, two stand out as being “secure by design,” specifically, Chromebooks and iOS devices like iPads.

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

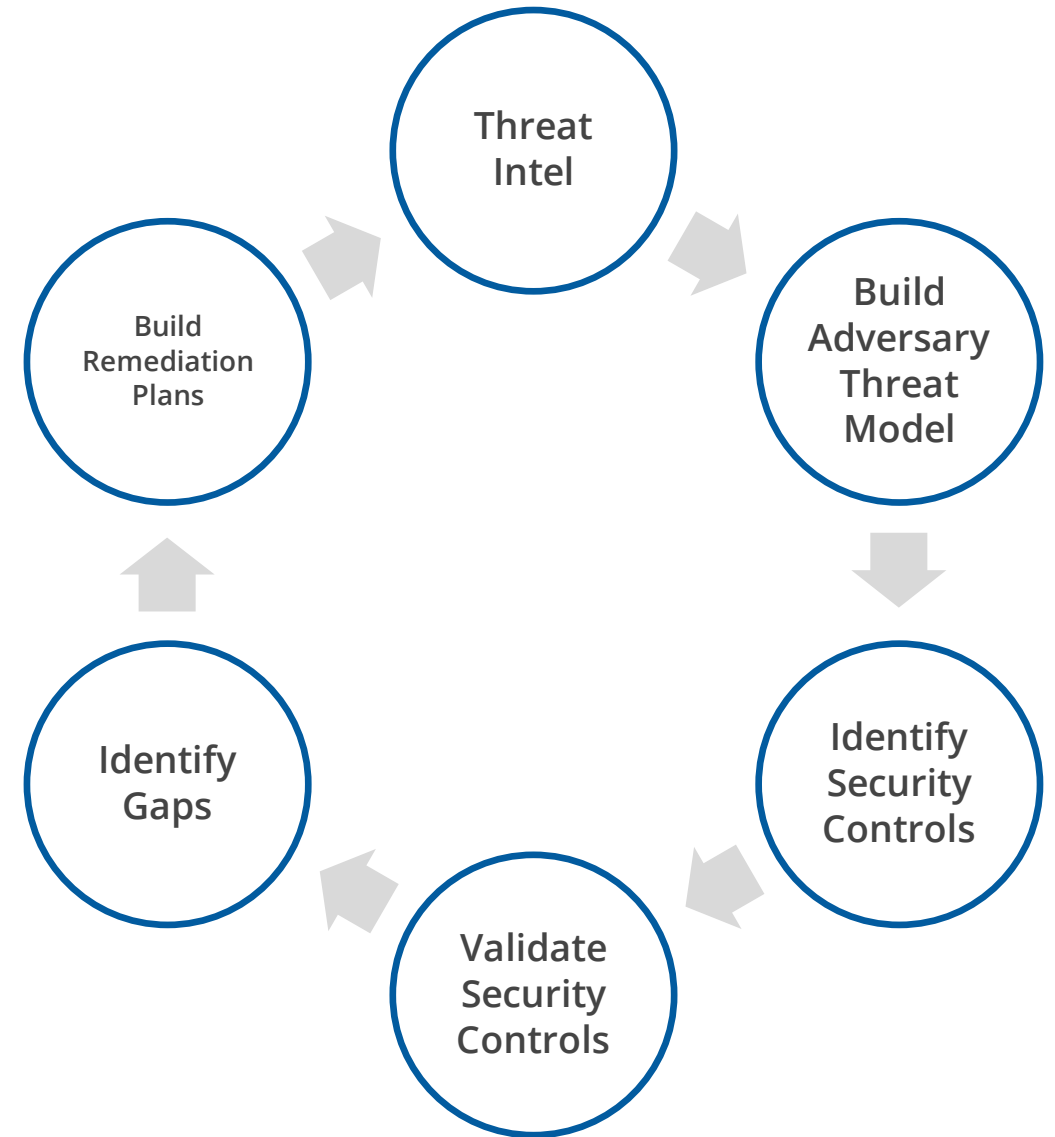
Step	High Level Overview of Emulation and Techniques Evaluated	Cited Intelligence	Open Invitation Contributor(s)	Emulation Content
1	<p>The scenario begins with an initial breach, where a legitimate user clicks (T1204) an executable payload (screensaver executable) masquerading as a benign word document (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.</p>	<p>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]</p> <p>SeaDuke and CozyDuke have used the RC4 cipher to encrypt data.[4] [7] [13] [16]</p> <p>CozyDuke can be used to spawn a command line shell. [16]</p>	Kaspersky	<p>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.</p>

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

<https://attacker.vals.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



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

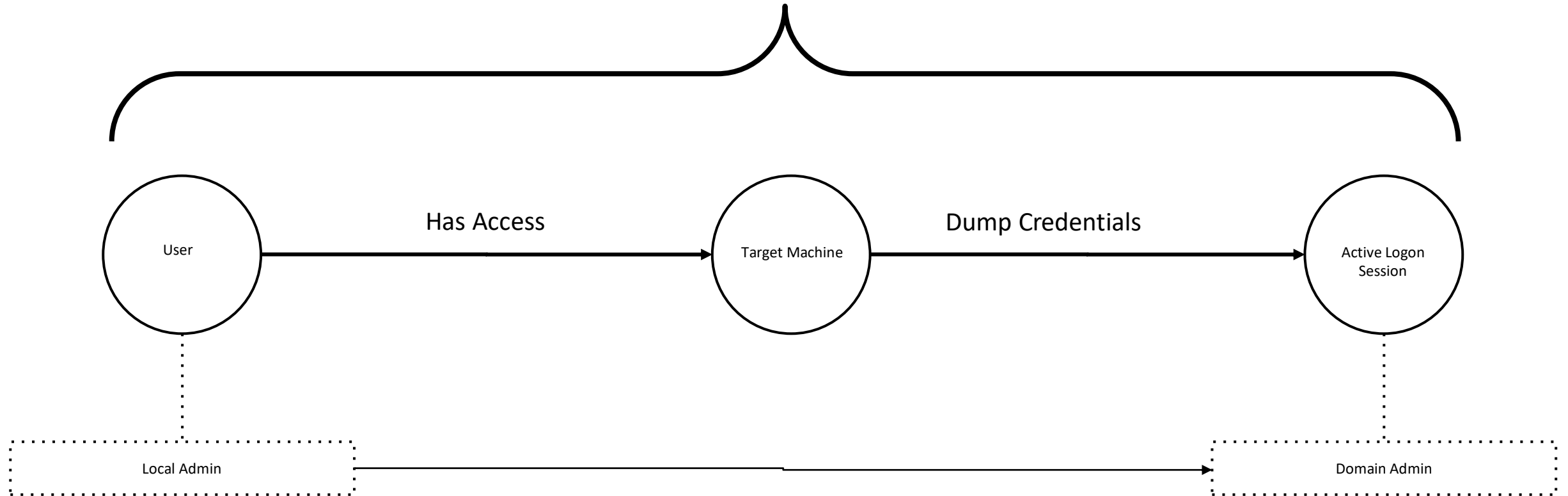
- ▀ Threats have intent
- ▀ Threats have a capability
- ▀ Threats have an opportunity (attacks are like water)

THREAT EMULATION



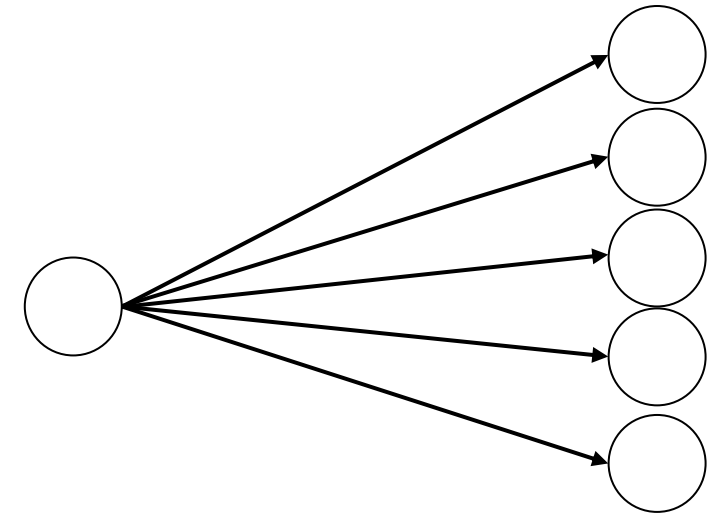
- ▀ Gather Cyber Threat Intelligence
 - DFIR Report, CISA, private alerts, etc.
- ▀ Identify Procedures to Emulate
- ▀ Identify Metrics
 - Data Sources, Detections, Response times
- ▀ Execution
 - May start with Tabletop Exercise (TTX)
- ▀ Lessons Learned
 - Critical to feed into the next cycle of testing

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

WALKTHROUGH EVALUATIONS

WORKSHOP STRUCTURE

- Access to the environment via GitHub/TailScale
 - <https://github.com/DenSecure-Lab>
- PurpleCloud used to automate deployment
 - <https://www.purplecloud.network/> (Jason Ostrom)
 - Integrated with Elastic Cloud EDR
 - AD domain environment
 - Access to personal workstation via RDP

WORKSHOP STRUCTURE

- ▀ Lab environment will be online until 9/9 @ 12:00pm
- ▀ 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

SYSMON INTEGRATION - HELK

Sysmon_ExecutedCommands						
Time ▼	host_name	event_id	user_account	process_guid	process_parent_command_line	process_command_line
> Sep 6, 2023 @ 18:00:09.324	win10-8.hackredcon.com	1	hackredcon\student	cec6feff-f669-64f8-d004-000000000500	"c:\windows\system32\windowspowershell\v1.0\powershell.exe"	"c:\windows\system32\whoami.exe"
> Sep 6, 2023 @ 17:59:49.255	win10-8.hackredcon.com	1	hackredcon\student	cec6feff-f655-64f8-cc04-000000000500	"c:\windows\system32\windowspowershell\v1.0\powershell.exe"	"c:\windows\system32\ipconfig.exe"
> Sep 6, 2023 @ 17:59:47.336	win10-8.hackredcon.com	1	hackredcon\student	cec6feff-f653-64f8-cb04-000000000500	"c:\windows\system32\windowspowershell\v1.0\powershell.exe"	"c:\windows\system32\hostname.exe"
> Sep 6, 2023 @ 17:59:43.952	win10-8.hackredcon.com	1	hackredcon\student	cec6feff-f64f-64f8-ca04-000000000500	"c:\windows\system32\windowspowershell\v1.0\powershell.exe"	"c:\windows\system32\hostname.exe"
> Sep 6, 2023 @ 17:59:43.176	win10-8.hackredcon.com	1	hackredcon\student	cec6feff-f64f-64f8-c904-000000000500	"c:\windows\system32\windowspowershell\v1.0\powershell.exe"	"c:\windows\system32\hostname.exe"
> Sep 6, 2023 @ 17:59:41.591	win10-8.hackredcon.com	1	hackredcon\student	cec6feff-f64d-64f8-c804-000000000500	"c:\windows\system32\windowspowershell\v1.0\powershell.exe"	"c:\windows\system32\hostname.exe"
> Sep 6, 2023 @ 17:59:37.181	win10-8.hackredcon.com	1	hackredcon\student	cec6feff-f649-64f8-c704-000000000500	"c:\windows\system32\windowspowershell\v1.0\powershell.exe"	"c:\windows\system32\whoami.exe"

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

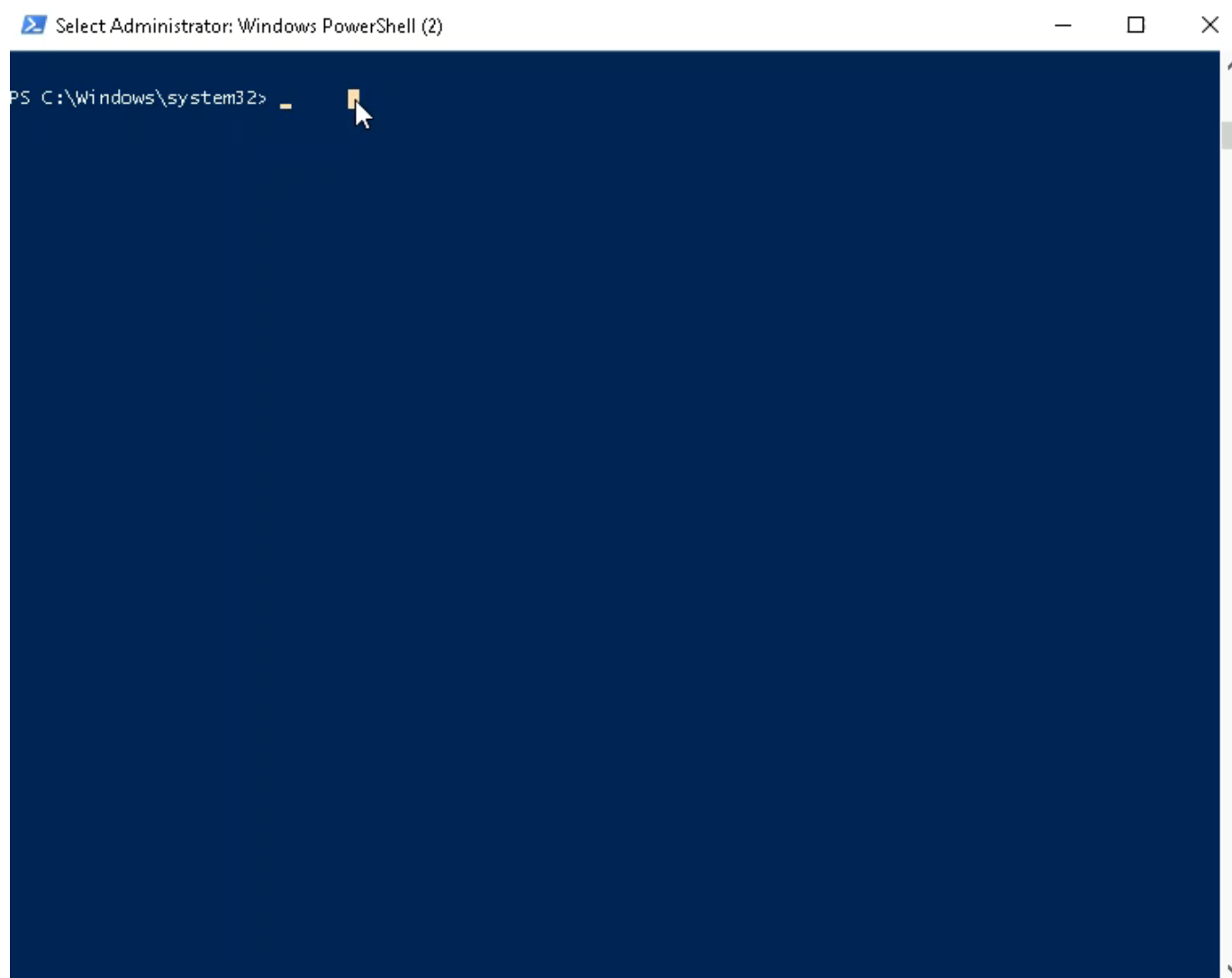
DEMONSTRATION

```
    | |  
_____) ) _-|_|_||_\\___) ___) ___)  
|__/_ \\ \\\\ ||| |D) __)|_|_|_|/  
|_| |_|_/|_/|_/|_/|(
```

v2.0.0

```
[*] Action: Kerberoasting  
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.  
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.  
[*] Target Domain       : hackredcon.com  
[*] Searching path 'LDAP://dc1.hackredcon.com/DC=hackredcon,DC=com' for '(&(samAccountType=805306368)(servicePrincipalName=*)'  
[*] Total kerberoastable users : 1  
[*] SamAccountName      : slugger  
[*] DistinguishedName   : CN=slugger,CN=Users,DC=hackredcon,DC=com  
[*] ServicePrincipalName : slugger/dc1.hackredcon.com:80  
[*] PwdLastSet          : 9/7/2023 11:00:50 PM  
[*] Supported ETypes     : RC4_HMAC_DEFAULT  
[*] Hash                : $krbtgs$23*$slugger$hackredcon.com$slugger/dc1.hackredcon.com:80@hackredcon.com*$226A837B726E06CEB1A8AFB181F381C6A3AFB4FF2EABE1D0CA169E5499C470BB83D641408462ACD63EFC110C6315F7EB4812E85D9F08FEC910368DD265606E76DEE29BE38F9528CC3B20A78BC5B3F217E75D39CE3FE224737BDB28B6AFCB01A4DCDE76DAAC8AA2178F1D743B8A17BB29B2F213841E368931511AA1625C8F76F5FF6BE2A249C0265AEDE5158FBD5BABCFD2B7402368B13A4920BD11F27C0AF0B2CBC68146CBF08ACE90D5E20DD04B85647D26B559BD58F801BBEB990F81F82E98E6A1A21A2C48CAC066GDEC1E16ACB63261B016CEE10D4360424PBD8050775041650DF1402D852670024872C1A5E326527C2560DD604266DDA215E1A8564237400008
```

DEMONSTRATION

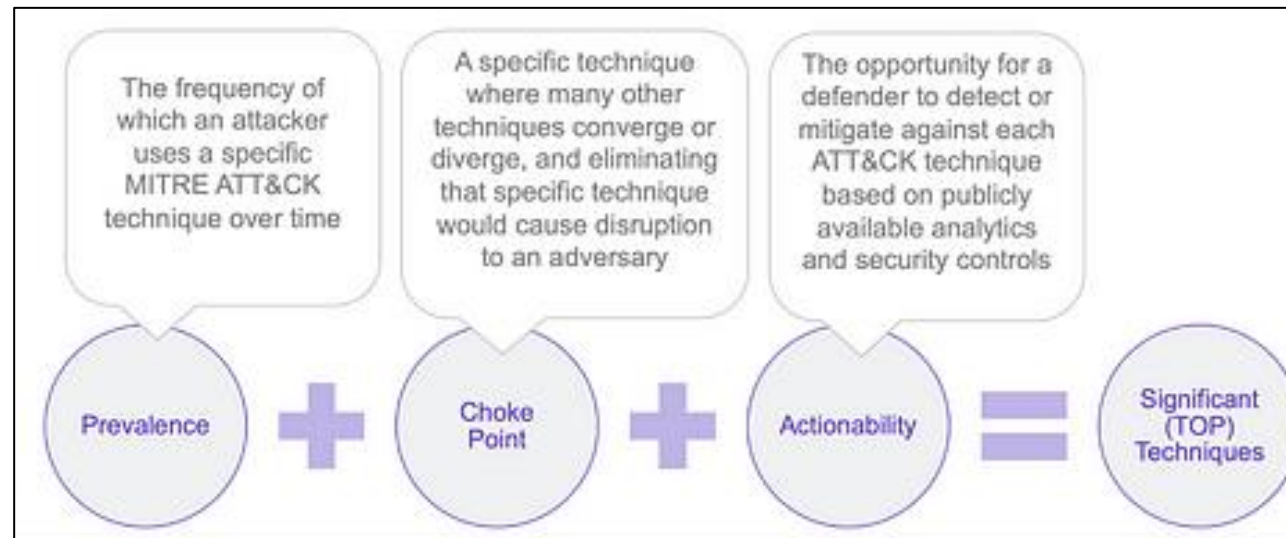


ATR OVERVIEW

- ▀ 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



ATOMIC RED TEAM

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
new group "Domain Admins" /domain
```

<https://thefirreport.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
- ▀ Fair to EDR?
- ▀ It is more efficient to work backwards from procedures
 - Naïve approach is to color code the matrix and run all atomics

MICRO EMULATIONS

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
<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

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

PASSWORD SPRAY

Brute Force: Password Spraying

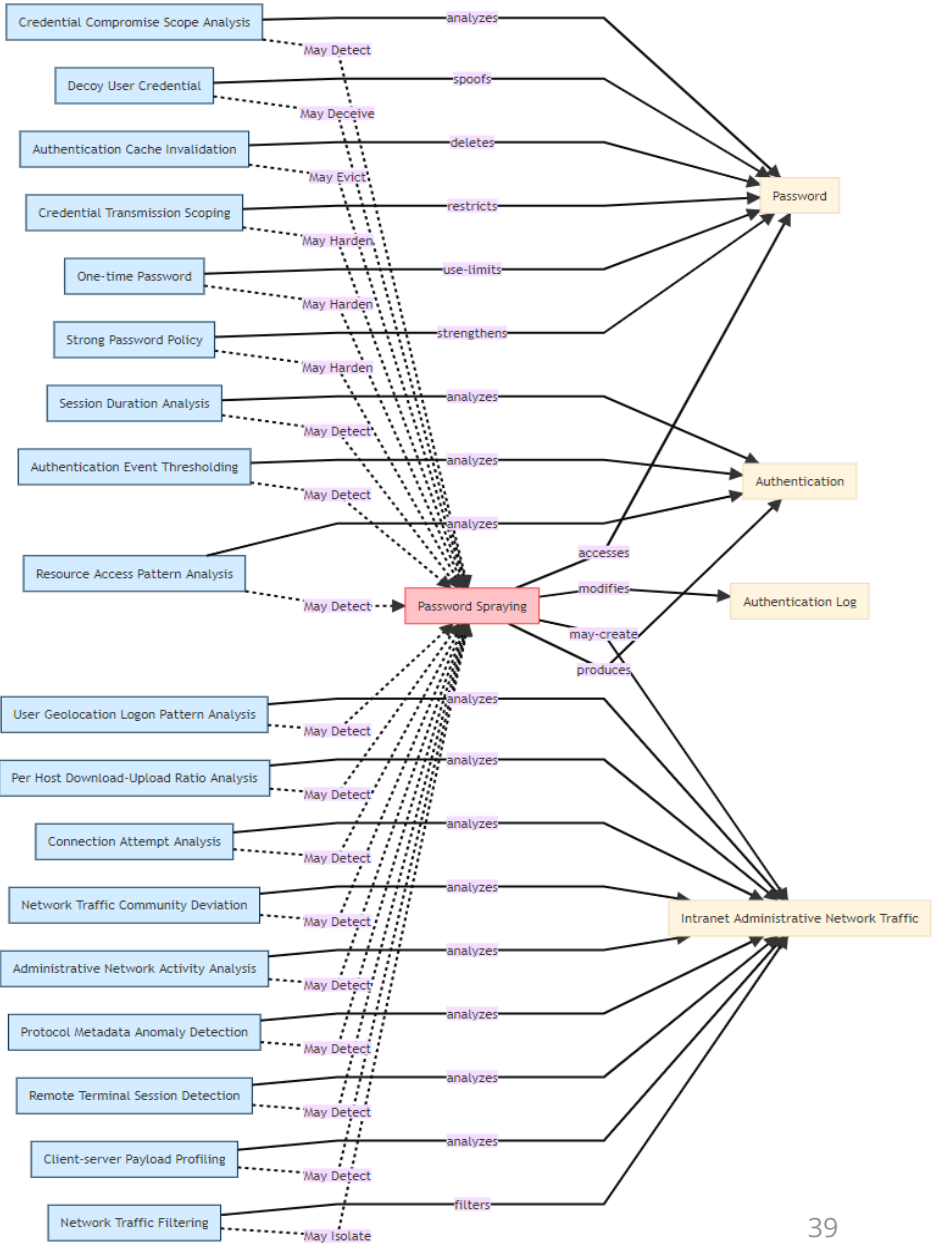
Other sub-techniques of Brute Force (4)		^
ID	Name	
T1110.001	Password Guessing	
T1110.002	Password Cracking	
T1110.003	Password Spraying	
T1110.004	Credential Stuffing	

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.



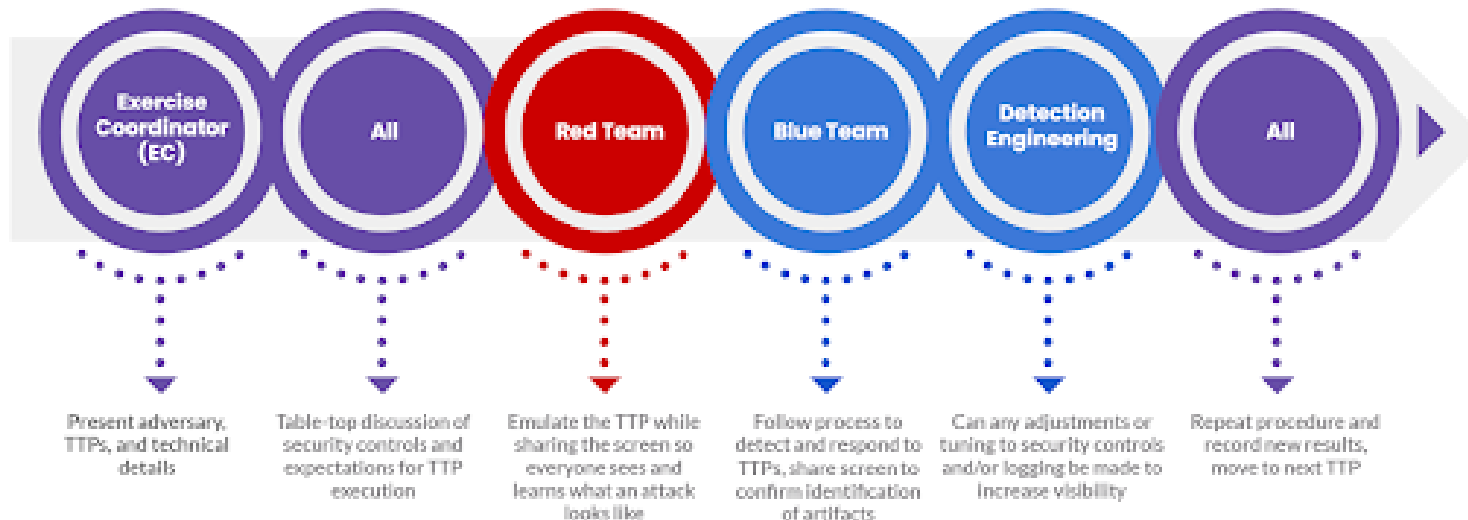
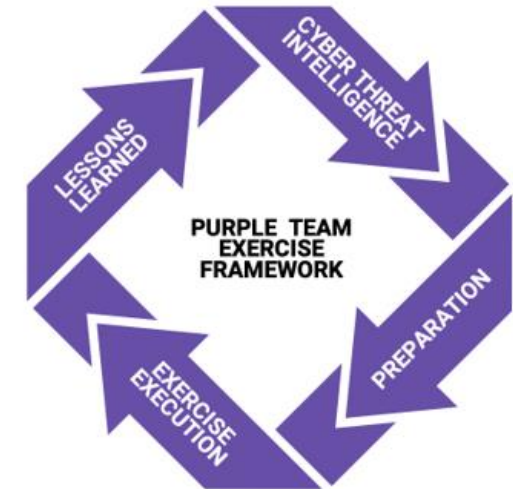
PURPLE TEAM

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)

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



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

AUDIT LOGGING



Cheat Sheets to help you in configuring your systems:

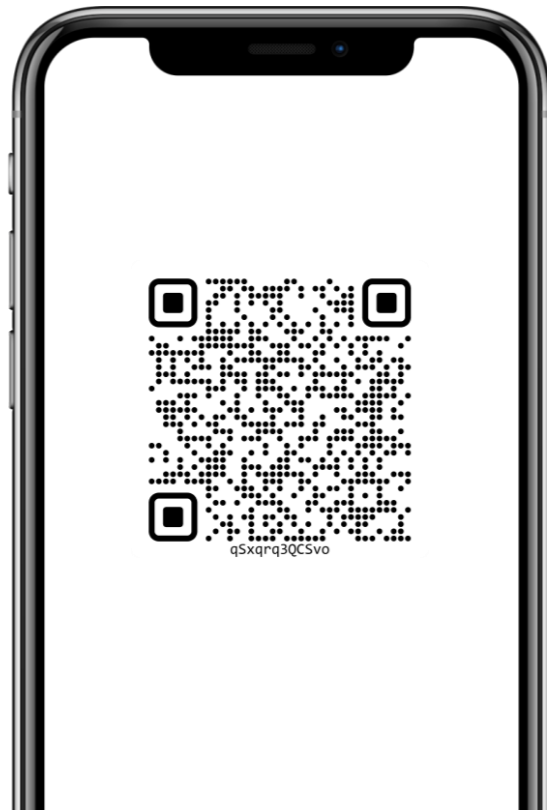
- The Windows Logging Cheat Sheet
- The Windows Advanced Logging Cheat Sheet
- The Windows HUMIO Logging Cheat Sheet
- The Windows Splunk Logging Cheat Sheet
- The Windows File Auditing Logging Cheat Sheet
- The Windows Registry Auditing Logging Cheat Sheet
- The Windows PowerShell Logging Cheat Sheet
- 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,
CRT0 , 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
- Threat Emulation
- Application Penetration Testing
- Continuous Penetration Testing
- Network Penetration Testing
- Social Engineering

WOLF
& COMPANY, P.C.

den
secure
by wolf & company, p.c.



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 hackredcon.com --admin Red --password HackRedCon2023 --ad_users 500 --endpoints 10 --domain_join -helk
```

```
terraform init
```

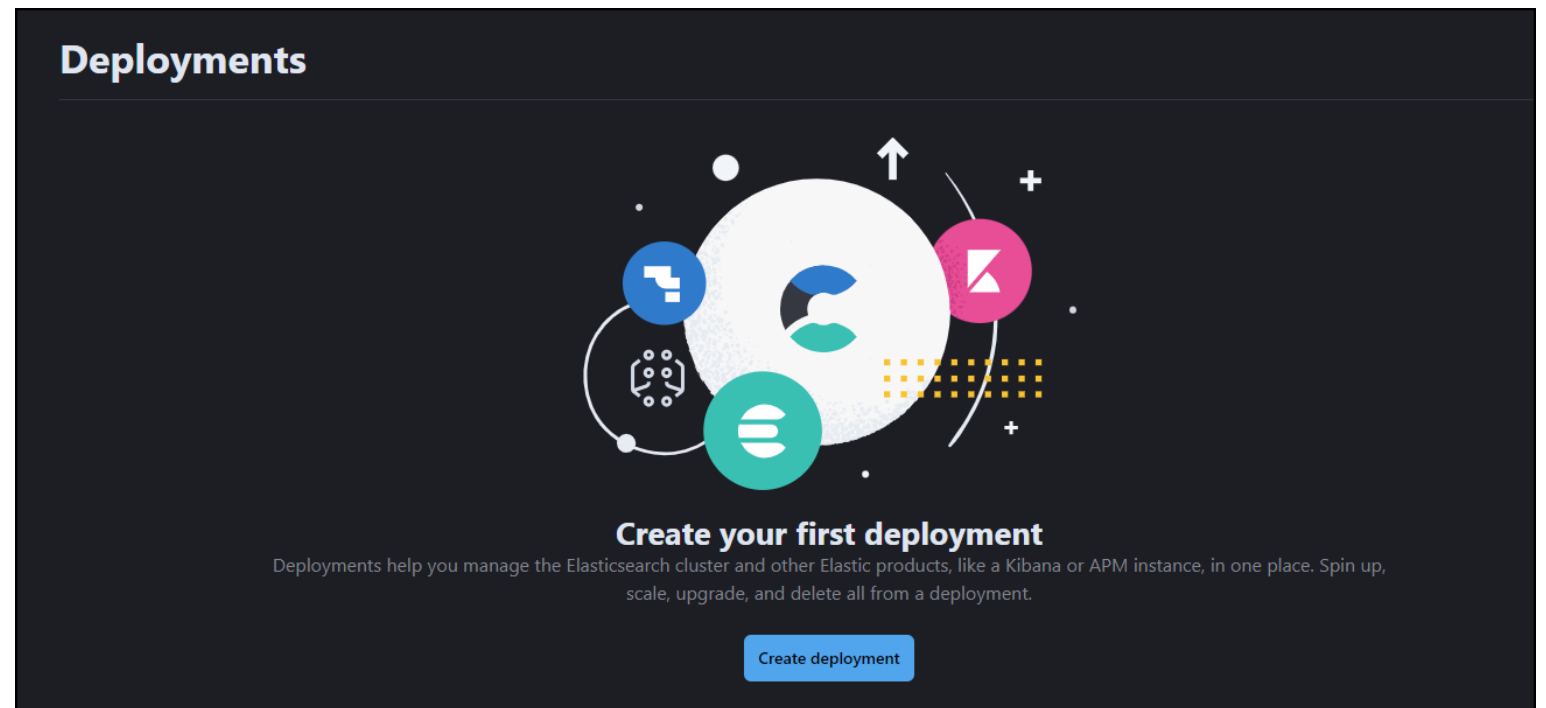
```
terraform plan -out=run.plan
```

```
terraform apply run.plan
```

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

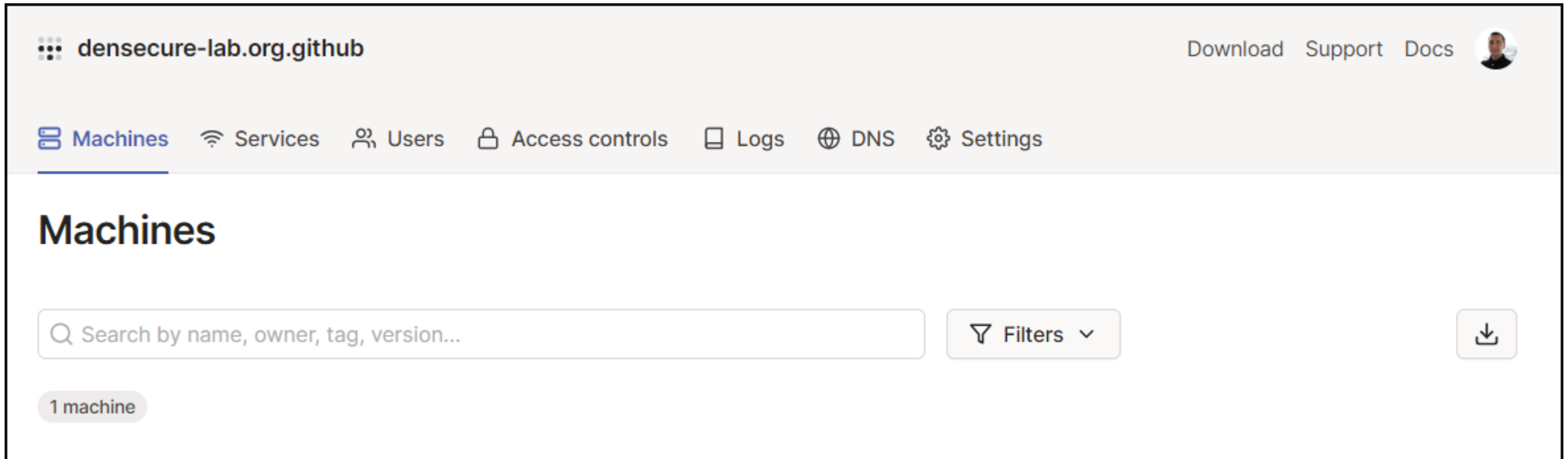
APPENDIX BUILD WORKSHOP

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



APPENDIX BUILD WORKSHOP

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



[Back to Home](#) →