



C0170

## APTLC Playbook

Document... Document... Change Management...



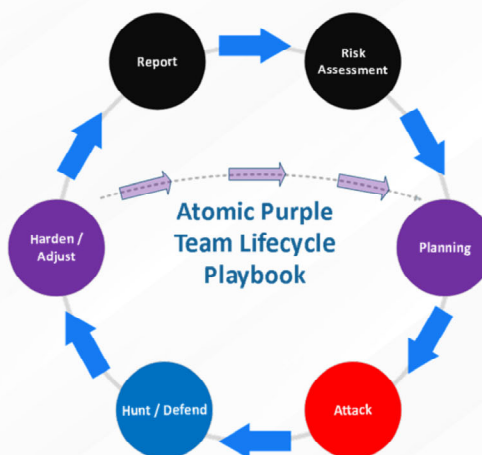
[defensiveorigins.com](http://defensiveorigins.com)

© Defensive Origins LLC C0170.1 – APT Lifecycle Playbook

### **Applied Purple Teaming – C0170 Atomic Purple Team Playbooks** Documentation of Work and Change Management

## Every phase of APTLC Needs Documentation

- Threat/Risk Assessment
- Planning
- Attack
- Defense
- Adjust/Harden
- Report & Deploy



## The goals of APTLC Documentation

Each section of the APTLC has information that needs documented.

Documentation Goals:

- Build confidence in validity of APT and APTLC
- Document evidence of risk/threat validation.
- Simplify Red/Blue/Purple team collaboration
- Generate repeatable and testable methodology
- Provide effective feedback to management
- Provide empirical evidence for Change Management when deploying to production.



defensiveorigins.com

© Defensive Origins LLC C0170.3 – APT Lifecycle Playbook



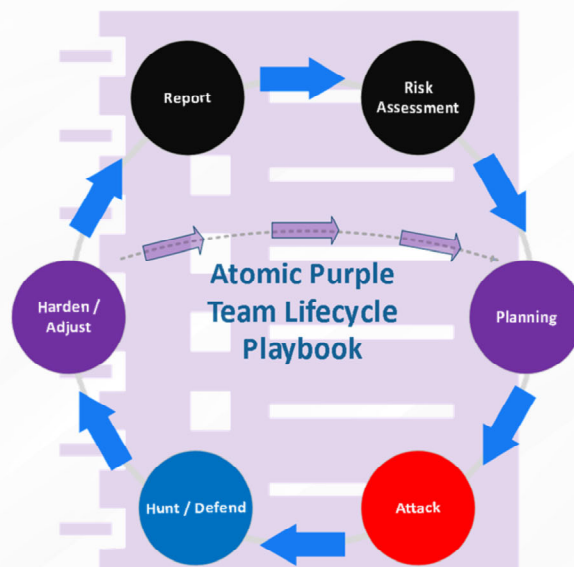
### Links:

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

# APTLC Playbook

## Designed to :

- Simplify alignment to APTLC
- Allow for effective collaboration
- Prove effectiveness
- Document work effort
- Simplify change management
- Requests for production deployment of security and configuration



defensiveorigins.com  
© Defensive Origins LLC C0170.4 – APT Lifecycle Playbook

## Links:

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

## APTLC Playbook Components

- Risk/Threat Assessment / Analysis
  - How was a Risk/Threat/Fidelity Checklist selected for APTLC
  - Define Objectives: [Stop Threat] [Identify Threat] [Alert Threat] [Fidelity Alignment/Audit]
- Planning
  - Document the research done. What tools are needed? Document lab environment. Document the objectives.
  - Do the tools require installation? Relaxation of AV / EDR for execution?



defensiveorigins.com

© Defensive Origins LLC C0170 5 – APT Lifecycle Playbook

### Links:

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

## APTLC Playbook Components

- Attack
  - Build a methodology for how the attack took place and its success
  - Document installation processes, requirements, and command usage
- Defend/Hunt
  - Build a methodology for how the attack was defended or identified.
  - If the attack was successful in not being stopped or defended, document and move to Adjust/Harden



defensiveorigins.com  
© Defensive Origins LLC C0170 6 – APT Lifecycle Playbook

### Links:

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

# APTLC Playbook Components

## Adjust / Harden

- Document the testing of changes that are necessary to meet the objectives of the Lifecycle [Stop Threat] – [Identify Threat] – [Alert Threat] – [Fidelity Alignment]
- If changes are necessary, document that the Lifecycle returned to Planning to test the new adjustments/configuration.

## Report and Prepare for Deployment

- Document lessons learned during the Lifecycle.
- Prepare for Change Management to move adjustments/configuration to Production Environment.



defensiveorigins.com  
© Defensive Origins LLC C0170.7 – APT Lifecycle Playbook

## Links:

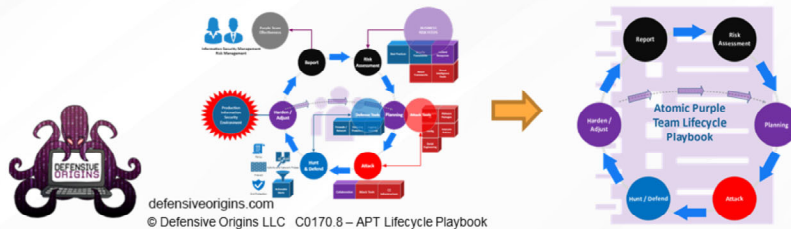
<https://github.com/DefensiveOrigins/AtomicPurpleTeam>

## The APTLC Playbook Template

Built to:

- Simplify documentation of APTLC
- Provide long-term storage of past APTLC work
- Allow for learning lessons and

# Make it easier!?

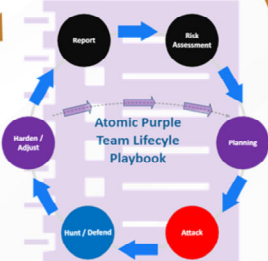
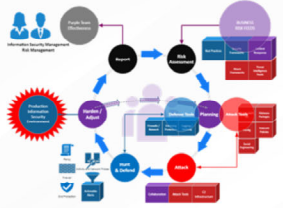


### Links:

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



# MAKE APTLC EASIER...



defensiveorigins.com  
© Defensive Origins LLC C0170.9 – APT Lifecycle Playbook

## Purple Team Lifecycle

Overall Status: [Status]

[Lifecycle Name]	
<b>Lifecycle Project Manager</b> [NAME] Office: [PHONE] Mobile: [Cell Phone] Email: [EMAIL]	<div style="border: 1px solid red; padding: 2px;"> <b>Lifecycle Type</b>  <input type="checkbox"/> Best Practice Deployment  <input type="checkbox"/> Attack Simulation  <input type="checkbox"/> Fidelity Check         </div> <div style="border: 1px solid red; padding: 2px;"> <b>Lifecycle Objective</b>  <input type="checkbox"/> Identify Attack (Optical)  <input type="checkbox"/> Stop Attack (Security Control)  <input type="checkbox"/> Identify and Stop Attack  <input type="checkbox"/> Research Only         </div> <div style="border: 1px solid red; padding: 2px;"> <b>Ingest Source:</b>  <input type="checkbox"/> Best Practices (Name)  <input type="checkbox"/> MITRE Framework (TF)  <input type="checkbox"/> Native (Plugin, etc.)  <input type="checkbox"/> Vulnerability (CVEs, etc.)  <input type="checkbox"/> IR Report  <input type="checkbox"/> Security Framework  <input type="checkbox"/> Attack Framework         </div>
Status Code Legend <input type="checkbox"/> Attack Simulation <input type="checkbox"/> Defense Simulation	<div style="border: 1px solid red; padding: 2px;"> <b>Lifecycle Context</b>          Provide the context of the best practice, simulation, or fidelity check. Briefly explain its importance to the organization. Provide additional information/resources regarding potential attack vectors, optics, and security controls.       </div> <div style="border: 1px solid red; padding: 2px;"> <b>Attack Methodology</b>          Provide a description of the attack methodology. Include sufficient detail to reproduce the same result/retesting. Include as much information as necessary.       </div> <div style="border: 1px solid red; padding: 2px;"> <b>Defense Methodology</b>          Provide a description of the defense methodology. Include sufficient detail to reproduce the same result/retesting. Include as much information as necessary. The goal of the Defense Methodology is to define the security controls or practice necessary to meet the Lifecycle Objective.       </div> <div style="border: 1px solid red; padding: 2px;"> <b>Adjustments</b>          Identify any adjustments to the security controls or optics configuration that were required changes to meet the lifecycle goal.       </div> <div style="border: 1px solid red; padding: 2px;"> <b>Change Management</b>          Before closure of the Lifecycle, research and discuss how the Adjustments identified can be presented to the Change Management board for rapid deployment.       </div> <div style="border: 1px solid red; padding: 2px;"> <b>Lessons Learned</b>          Distill lessons, tips, or tricks that were learned during the lifecycle process that may make future lifecycles more efficient. Include potential "patches" that were hard-lessons or other relevant information that was gained during the lifecycle engagement.       </div>
APTLifecycle Ingest and Research	<div style="border: 1px solid red; padding: 2px;"> <b>Attack Methodology Test</b> </div> <div style="border: 1px solid red; padding: 2px;"> <b>Defense Methodology</b> </div>
Attack methodology	
Defense methodology	
Lifecycle Adjustments	
Change Management	
Lessons Learned	



### Links:

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

**Related Atomic Purple Team Playbook Template: PB0170**

# Lifecycle Playbook Report – Lifecycle Metadata

## Purple Team Lifecycle

Overall Status: **[Status]**

[TEMPLATE]

### Lifecycle Project Manager

[NAME]

Office: [PHONE]

Mobile: [Cell Phone]

Email: [EMAIL]

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



defensiveorigins.com

© Defensive Origins LLC C0170.10 – APT Lifecycle Playbook

### Links:

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

**Related Atomic Purple Team Playbook Template: PB0170**

# Lifecycle Playbook Report – Define Lifecycle

## Lifecycle Type

- Best Practice Deployment
- Attack Simulation
- Fidelity Check

## Lifecycle Objective

- Identify Attack (Optics)
- Stop Attack (Security Control)
- Identify and Stop Attack
- Research Only

## Lifecycle Context

Provide the context of the best practice, simulation, or fidelity check. Briefly explain its importance to the organization. Provide additional information/resources regarding potential attack vectors, optics, and security controls.

## Ingest Source:

Best Practices (Name)  
MITRE Framework (T#)  
Nessus (Plugin, etc.)  
Vulnerability (CVE#, etc.)  
IR Report  
Security Framework  
Attack Framework

### Status Code Legend

- Attack Simulation
- Defense Simulation

- System Configuration Change
- Information

APT Lifecycle  
Ingest and Research

● Lifecycle Type: [TYPE]

● Lifecycle Objective [OBJECTIVE]

● Ingest Source: [SOURCE]

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



## Links:

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

**Related Atomic Purple Team Playbook Template: PB0170**

# Lifecycle Playbook Report – Methodologies

Attack methodology	<b><u>Attack Methodology</u></b> Provide a description of the attack methodology. Include sufficient detail to reproduce the same result if retesting. Include as much information as necessary.
Defense methodology	<b><u>Defense Methodology</u></b> Provide a description of the defense methodology. Include enough detail to reproduce the same result if retesting. Include as much information as necessary. The goal of the Defense Methodology is to define the security controls or practice necessary to meet the Lifecycle Objective
Lifecycle Adjustments	<b><u>Adjustments</u></b> Identify any adjustments to the security controls or optics configuration that were required changes to meet the lifecycle goal.



defensiveorigins.com  
© Defensive Origins LLC C0170.12 – APT Lifecycle Playbook

## Links:

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

**Related Atomic Purple Team Playbook Template: PB0170**

# Lifecycle Playbook Report – Change Management

Change Management	<ul style="list-style-type: none"><li>● Systems Requiring Configuration Change:</li><li>● Justification for change:</li><li>● Affected Users:</li><li>● Identified Key Parties:</li><li>● Potential issues:</li><li>● Deployment Procedure:</li><li>● Rollback Procedure:</li></ul>	<b>Change Management</b> Before closure of the Lifecycle, research and discuss how the Adjustments identified can be presented to the Change Management board for rapid deployment.
Lessons Learned	<ul style="list-style-type: none"><li>● List/summarize topics here.</li></ul>	




## Links:

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

**Related Atomic Purple Team Playbook Template: PB0170**

# Lifecycle Playbook Report



defensiveorigins.com  
© Defensive Origins LLC C0170.14 – APT Lifecycle Playbook

## Purple Team Lifecycle Overall Status: **[Status]**

[TEMPLATE]

---

**Lifecycle Project Manager**

[NAME]

Offices: [PHONE]

Mobile: [Cell Phone]

Email: [EMAIL]

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

State Code Legend

- Attack Simulation
- Defense Simulation
- System Configuration Change Information

<p>APT Lifecycle</p> <p>Ingest and Research</p>	<ul style="list-style-type: none"> <li>● Lifecycle Type: [TYPE]</li> <li>● Lifecycle Objective [OBJECTIVE]</li> </ul>	<ul style="list-style-type: none"> <li>● Ingest Source: [SOURCE]</li> </ul>
<p>● Identify the ingest/intended attack and/or defense techniques. Define source of technique and type of ingest.</p>		
<p>Attack methodology</p>	<ul style="list-style-type: none"> <li>● Attack Methodology Information</li> </ul>	
<p>Defense methodology</p>	<ul style="list-style-type: none"> <li>● Defense Methodology Information</li> </ul>	
<p>Lifecycle Adjustments</p>	<ul style="list-style-type: none"> <li>● Adjustments to system configuration to meet lifecycle objective</li> </ul>	
<p>Change Management</p>	<ul style="list-style-type: none"> <li>● Systems Requiring Configuration Change:</li> <li>● Justification for change:</li> <li>● Affected Users:</li> <li>● Identified Key Parties:</li> <li>● Potential Issues:</li> <li>● Deployment Procedures:</li> <li>● Rollback Procedures:</li> </ul>	
<p>Lessons Learned</p>	<ul style="list-style-type: none"> <li>● List/summarize topics here.</li> </ul>	

**Links:**

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

**Related Atomic Purple Team Playbook Template: PB0170**