



# Applied Purple Teaming

## Course Introduction and Overview



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

© Defensive Origins LLC C0100.1 – Applied Purple Teaming

## Applied Purple Teaming – C100-3

### Course Introduction and Overview

## Why?

- Why are we here?
- Who's all here?
- Where will you go from here?
- Where will we go from here?



defensiveorigins.com

© Defensive Origins LLC C0100.2 – Applied Purple Teaming

## **Applied Purple Teaming – C100-3** Course Introduction and Overview

# Support Staff Shout-out

This wouldn't be possible without them!!

People are here to help you if you get stuck! If you need help, reach out!

## Ask for help in:

- Discord (**Preferred**) (Staff is monitoring for questions)
- GoToWebinar Chat (Staff is monitoring for questions)

If someone asks a question in Discord and you know the answer, answer 😊



defensiveorigins.com

© Defensive Origins LLC C0100.3 – Applied Purple Teaming

## **Live Chat:**

Discord (Preferred)

GoTo Webinar Chat

# Course Objectives

- Deploy Baseline Security Logging for Active Directory Systems
- Implement Event Channels, Subscriptions, Event Collection and Forwarding
- Review Sysmon, Modular Configurations, and Noise Reduction Strategies
- Understand Enterprise OSINT and Reconnaissance
- Dive into MITRE ATT&CK and Atomic Red Team frameworks
- Discuss and Review Secure Network Designs
- Demonstrate Attack Tactics, Defense, and Hunt Methodologies
- Review Event IDs, Kibana Queries, and Associated SIGMA Rules
- ElastAlert, SIEMs, MSSPs, and a multitude of other topics!



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

© Defensive Origins LLC C0100.4 – Applied Purple Teaming

## Course Components – Day One – Hopefully.

- C0100-3: Course Introduction
- C0150-3: Purple Team Lifecycle / Continuous Improvement
- C0160-3: APTLC Ingests
- C0170-3: Purple Team Lifecycle Playbook – Documentation
- C0200-3: Lab Overview and Azure Discussion, Legal Bits
- C0310-3: Sysmon and Sysmon Modular
- C0320-3: Windows Audit Policies and Event Viewer
- C0330-3: WEC, WEF, Channels, Subscriptions
- C0340-3: Log Shipping and Ingestors

Course Git Repo: <https://github.com/AppliedPurpleTeaming>



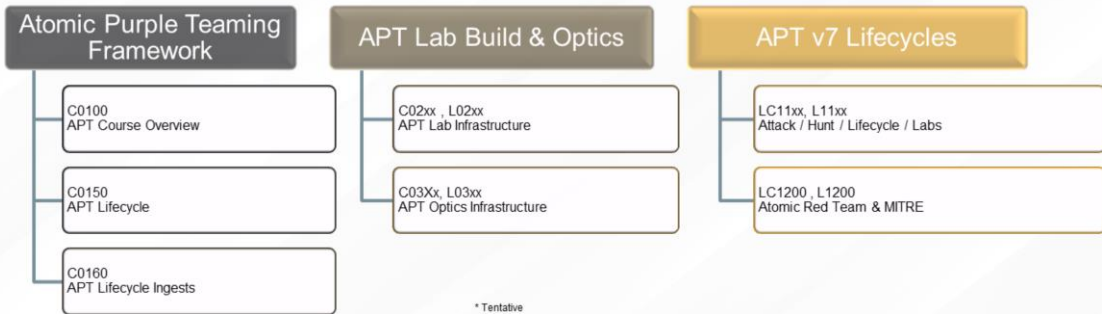
defensiveorigins.com

© Defensive Origins LLC C0100.5 – Applied Purple Teaming

### Links:

<https://github.com/AppliedPurpleTeaming>

# Applied Purple Teaming Course Matrix



defensiveorigins.com

© Defensive Origins LLC C0100.6 – Applied Purple Teaming

## Have everything?

- Laptop
- Wired Connection / Wireless
- Sanity?
  
- Applied Purple Team Courseware (GitHub Repo)
- Applied Purple Team GitHub Team Membership
  
- Discord Membership
- WWHF Discord Server
  
- <https://github.com/DefensiveOrigins/>
- <https://github.com/AppliedPurpleTeaming>



defensiveorigins.com

© Defensive Origins LLC C0100.7 – Applied Purple Teaming



### Links:

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

<https://github.com/AppliedPurpleTeaming>

# Course Information

- Four (4hr) Days ( 10am – 2PM Mountain Time)
- Breaks around the 50-minute mark of each hour (10 min)
- Lunch around Lunch time
- Live Chat: Discord (WWHF Server)
- Live Video: GoToWebinar
- Live Video Alternative: YouTube Stream
- Recorded Sessions (Info will be sent to you)

## Ask for help:

1. Discord
2. GotoWebinar
3. Email

- <https://github.com/DefensiveOrigins/>
- <https://github.com/AppliedPurpleTeaming>



defensiveorigins.com

© Defensive Origins LLC C0100 8 – Applied Purple Teaming



## Links:

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

<https://github.com/AppliedPurpleTeaming>