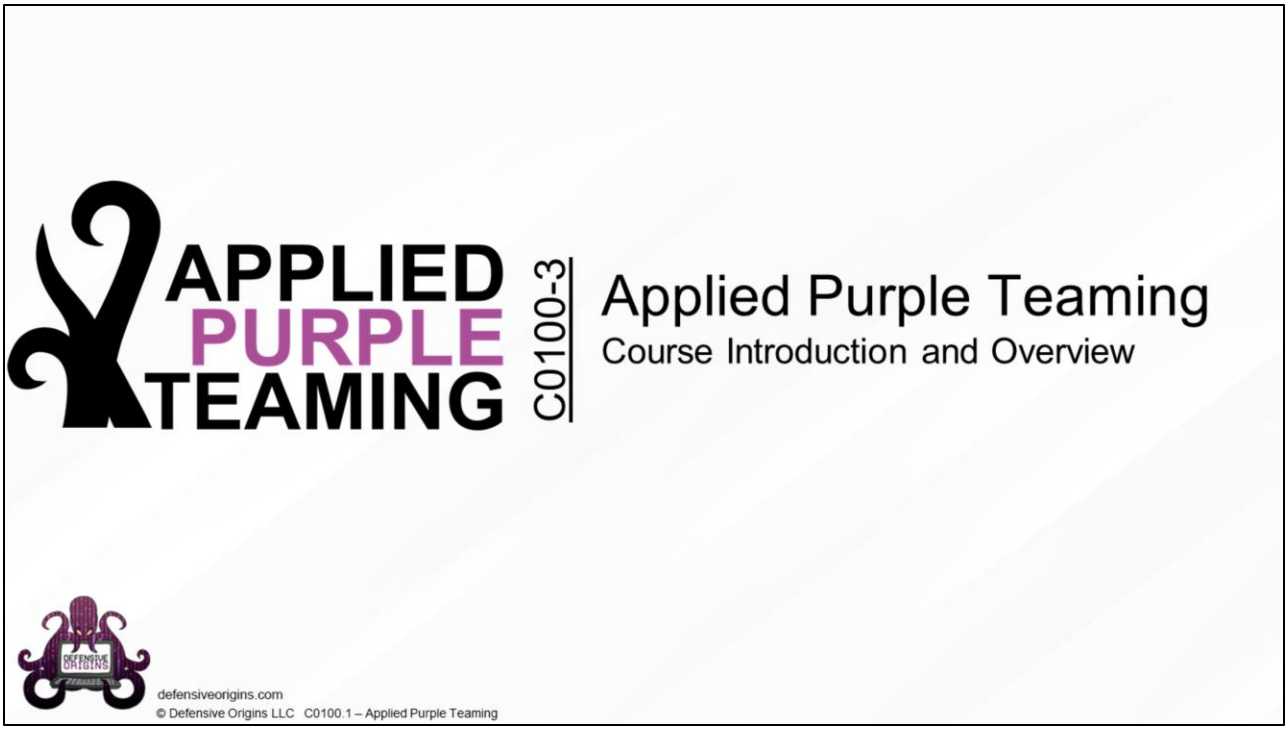


Applied Purple Teaming – C100-3
Course Introduction and Overview

Why?

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

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:

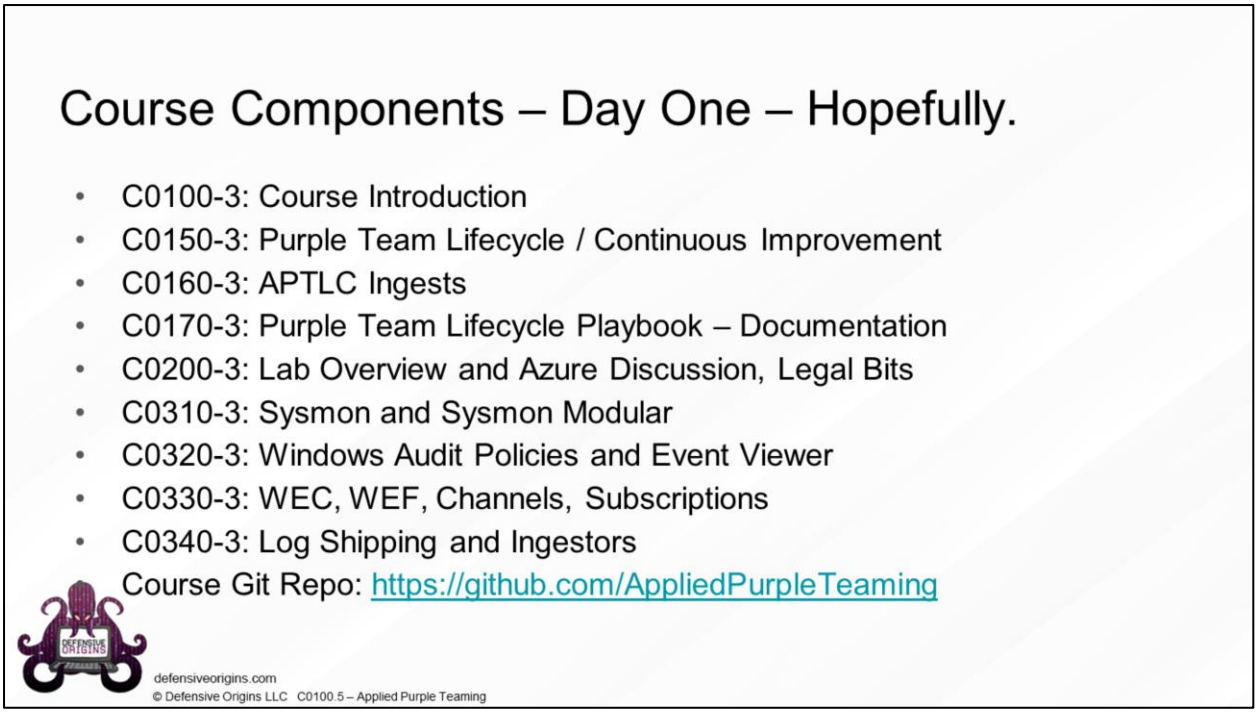
- Discord (**Preferred**) (Staff is monitoring for questions)
- GoToWebinar Chat (Staff is monitoring for questions)

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

Live Chat:
Discord (Preferred)
GoTo Webinar Chat

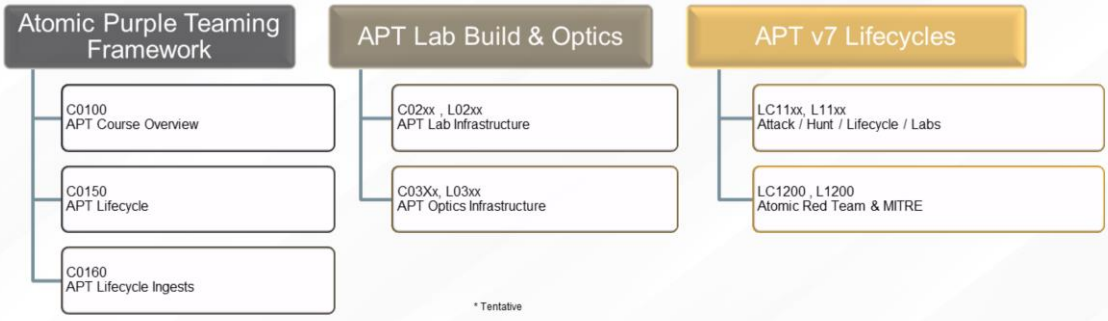
Course Objectives

- 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!



Links:
https://github.com/AppliedPurpleTeaming

Applied Purple Teaming Course Matrix



* Tentative

defensiveorigins.com

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

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

Links:
https://github.com/DefensiveOrigins/
https://github.com/AppliedPurpleTeaming