Cyber Defense Analyst Bootcamp Graduate

Share ⋮

Offered by **Level Effect**

Awarded to **Tom Ferguson** (thoscofer@gmail.com)

Issued on **Jan 5, 2022** at 11:00 PM

Graduates of the Cyber Defense Analyst Bootcamp are beyond introductory in their mastery of foundational cyber techniques. Holders of this badge have demonstrated their ability to conduct sophisticated analysis across multiple telemetry sources and log formats, and are able to triage compromised hosts to extract and analyze malware through both static and dynamic methods. Holders of this badge can extend this technical analysis and research through thoughtful communication and reporting of their findings with relation to risk, threat, and response strategies that will minimize both current and future incidents of the reported type. Individuals who've attained this achievement have excelled in roles ranging from Penetration Tester, Security Operations Analyst 1/2, Cybersecurity Analysts, Governance Risk Compliance (GRC) Analysts, and Cyber Consultants both in the private and public sectors. [less]

Badge Details

EARNING CRITERIA

Recipients must complete the earning criteria to earn this badge

- Complete 12-hour Cybersecurity Foundations course (Course Prerequisite)
- 14 weeks, 93+ technical labs, 280+ hours of content including 120+ hours of live class challenges and scenarios
- Perform deep network traffic analysis of malicious traffic following trails of obfuscation, exfiltration, and encoded attacks
- Triage a series of Windows and Linux endpoints for all indicators of compromise including persistence mechanism(s), perform remediation, and prepare reports to present on findings
- Submit multiple compromised host and malicious traffic analysis reports through endpoint triage, log analysis with a SIEM
- Research and deliver cyber threat intelligence on advanced threat actors, preparing reports and technical analysis of findings, and ultimately presenting this information live in simulated attack and tabletop scenarios
- Perform and analyze advanced adversary techniques, tactics, and procedures including attacks such as pass-the-hash, lateral movement, privilege escalation, SQL injection, DC takeover, exfiltration, hive, and lsass secrets dumping and more - performed both manually and with a C2 framework for comparison and contrast
- Design and implement signature rules verifying user and threat actor activity through log analysis challenges including shipping event logs to a SIEM for further analysis
- Create and reverse engineer custom malware using industry tools
- Create custom security tools with scripting languages to solve real-world business needs
- Holders are eligible to attempt the Cyber Defense Certified Professional CDCP.

We Issue Open Badges

View JSON