Cyber Defense Certified Professional

Share

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

Issued on **Feb 9, 2022** at 11:00 PM

Offered by Level Effect

The CDCP is a practical application of the knowledge, tools, techniques, and procedures acquired through the Cyber Defense Analyst Bootcamp. This is accomplished through a battery of real-world security operations scenarios that students must overcome and articulate in a detailed report that... [more]

Badge Details

EARNING CRITERIA

Recipients must complete the earning criteria to earn this badge

Completion Criteria:

- Successfully complete the Cyber Defense Analyst Bootcamp.
- Successfully complete a 1-week long practical hands-on capstone exam and deliver a report outlining technical analysis, findings, remediation, and impact to organizational risk including supporting evidence.

Capstone Exam Criteria:

- Conduct Windows forensic triage and assess for indicators of compromise.
- Analyze suspicious binaries with both static and dynamic analysis techniques.
- Evaluate and analyze malicious network traffic.
- Respond to an insider threat, collect evidence, and provide containment and remediation steps.
- Curate detailed executive and technical threat intelligence reporting in conjunction with historical and ongoing incident response activities.
- Conduct Open Source Intelligence (OSINT) and reconnaissance against adversary infrastructure.
- Investigate MALSPAM to uncover the evasion and exploitation techniques in use.

TAGS

cybersecurity | cyber defense | threat hunting | threat intelligence | malware analysis | siem | security operations | vulnerability management | network defense | traffic analysis