DETECTION ENGINEERING

LEARN THE THEORY BEHIND SECURTY OPERATIONS AND DETECTION ENGINEERING.

11 HOURS OF MATERIALS

THIS COURSE IS INCLUDED AS PART OF OUR ACADEMY – MEMBERSHIPS START AT $29.99

OTHER TOPICS INCLUDE

- CREATING AD-HOC OFFENSIVE TESTS TO GENERATE LOGS FOR DETECTION CREATION
- WORKING IN A TESTING FRAMEWORK TO GENERATE LOGS FOR DETECTION CREATION
- PROPERLY DOCUMENTING YOUR DETECTIONS
- USING PYTHON TO INTERACT WITH A SIEM'S API TO PUSH AND PULL DETECTION DATA
- USING GITHUB ACTIONS TO FACILITATE ALL CUSTOM CHECKS AND API INTERACTIONS

THIS IS ONE OF SEVERAL BLUE TEAM COURSES WE OFFER AT TCM SECURITY, WHICH INCLUDE:

- ✓ SECURITY OPERATIONS (SOC) 101
- ✓ PRACTICAL WINDOW FORENSICS
- ✓ THE DEFINITIVE GRC MASTERCLASS
- ✓ PRACTICAL PHISHING CAMPAIGNS
- ✓ PRACTICAL MALWARE AND TRIAGE

AND THE SOON TO BE RELEASED SOC 201 COURSE – COMING IN THE NEAR FUTURE!