TRAINING

SPECTEROPS

ADVERSARY TACTICS
DETECTION

Enterprise networks are under constant attack from adversaries of all skill levels and intentions. For many it feels that blue teamers are only facing a losing battle. The attacker "only needs to be successful once" to cause havoc; the blue team must prevent them every time, under every condition, at every step of the way.

The goal of this course is to turn that statement on its head and provide you confidence through a new defensive mindset. Preventative solutions are designed to stop attacks before they start, but against an adversary with enough time and resources; all eventually will fail. Rather than making the primary effort of security operations attempting to prevent any attack from being successful, assume breaches could (and likely would) occur and focus on developing robust detections around activity in all stages of the attack cycle. A strategy that focuses on deep understanding of post-exploitation activity (privilege escalation, lateral spread, pivot, persistence) produces high-quality alerts, creating a minefield where the attacker "only needs to be detected once" for blue teamers to respond.

This course builds on standard network defense and incident response (which often focuses on alerting for known malware signatures) by focusing on abnormal behaviors and the use of adversary Tactics, Techniques, and Procedures (TTPs). We will teach you how to engineer detections based on attacker TTPs to perform threat hunting operations and detect attacker activity. In addition, you will learn use utilize free and/or open source data collection and analysis tools (such as Sysmon, Windows Event Logs, and ELK) to analyze large amounts of host information and build detections for malicious activity. You will use the techniques and toolsets you learn to create threat hunting hypotheses and build robust detections in a simulated enterprise network undergoing active compromise from various types of threat actors.

DAY 1
- Threat Hunting Introduction
- MITRE ATT&CK and Adversary TTPs
- Interpreting Threat Intelligence
- Data Source Identification
- Configure Test Environment
- Implement Attacker Technique

DAY 2
- Data Modeling
- Data Quality Assessment
- Detection Engineering Methodology
- Threat Hunting Campaign Types

DAY 3
- Develop Detections
- Alerting & Detection Strategies
- Hypothesis Generation (based on Threat Intel Report)

DAY 4
- Threat Hunting Engagement
- Detection Development
- Detection Presentation and Peer Review

TRAINING

What will you teach that students can't get elsewhere?

We are teaching a methodology that can be applied to all detections - not just a few. Detection engineers are typically on the back foot from the beginning, tasked with creating detections for attacks they didn't design against technology they may not understand. Our class provides a repeatable and tested method to dissect techniques and determine where the best places are to create detections. Other courses would leave it there, but we take it a step further and map those layers to the telemetry necessary to detect them. We do this because detection engineers are often fighting on another front – convincing those in their own organization why they need a particular data source, especially if it looks similar to one already being collected. Understanding both the underlying technology for a technique, and the data sources required is essential if defenders are to win the battle against talented and resourceful attackers.

Why isn't this material taught in other places?

Other classes are usually taught by people without the breadth of knowledge and practice in all areas of detection. It's rare that you find a set of instructors and a class that tackles detection, research, and data quality in one place. Our methodology is proven across countless clients where we have seen these steps and frameworks turn detection programs around, this isn't just a theory that hasn't been proven. Our instructors, and the class itself, is born out of a team that has a very close relationship to extremely talented offensive researchers and practitioners – giving our class a massive advantage in how to detect what real threat actors actually do.

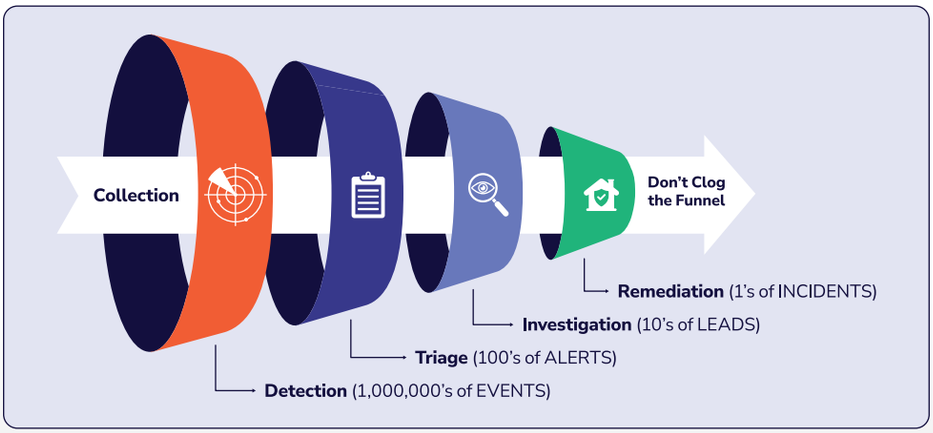
Who should take your courses?

This class is a great choice for new detection engineers or SOC analysts looking to learn how to create repeatable detections and truly understand the technology they are asked to protect. There is also a place for offensive-focused practitioners who want to know how they can be detected, or veteran detection engineers who want to take their detections and documentation to the next level.

Why SpecterOps?

SpecterOps is the premiere provider of offensive services in the industry – our defensive staff is experienced in detecting that same caliber of tradecraft. We don't employ professional instructors or public speakers. Our instructors are our practitioners.

Funnel of Fidelity



You bought all the latest detection tools, but somehow still can't seem to detect mimikatz. IT is screaming about the resource consumption from the multitude of security tools on the endpoints, analysts are barely staying afloat in the oceans of data your toolsets have created, and the latest red team report detailed how response actions were ineffective again. If this sounds familiar for your organization, this is the course for you. We'll walk you through starting with a detection engineering strategy first and then focusing on methodologies to build robust alerting, with the end result of improving detection and response capabilities throughout security operations. This course will provide you the understanding and ability to build robust detections, starting with the why and going all the way to the technical implementation of detecting threat actor activity. You will learn how to apply the methodologies and technical approaches practiced, regardless of the security toolsets deployed in your organization.

REAL RESULTS

A repeatable methodology for research and development of detections and data models.

A documentation framework for a completed alert, and its accompanying detection, data model, and research.

The ability to install and configure a detection data pipeline that livestreams data throughout the class for detection development and testing.

A chance to create and test a capstone detection in a production-like environment with attack data from a real attacker.

SPECTEROPS

Learn more at **specterops.io**

Email **info@specterops.io**