Data Sheet

Detection Engineering and Threat Hunting Training

Empower your security team to outsmart adversaries with hands-on training based on real-life scenarios. Dive into critical concepts, improve practical skills, and accelerate threat hunting and detection engineering maturity through enhanced expertise.

Overview

DETECTION ENGINEERING TRAINING

1 day

- What is Detection Engineering?
- Turning logging into detection logic
- Detection-as-code
- Understanding your environment
- "Jack of all trades" in Detection Engineering
- Pattern recognition
- Simple (baseline) vs complex
- Signature (IOC) vs behavioral
- Intro to resilient detections

2 day

- From Threat to Detection
- Writing an actual detection from source material
- Validation & testing
- Tuning

3 day

- Scenario
- Detecting LOL attacks
- Q&A

400,000+

Library of rules & queries maintained by SOC Prime Team.

30+

SIEM, EDR, and Data Lake platforms we are experts in

100+

Training courses delivered

Highlights

- Become more specific in your hunts and research
- Know how adversaries think and act
- Become resilient in situations that require ultra-responsiveness
- Create your custom detection rules
- Avoid financial & reputation damage by minimizing the risk of a security incident
- Stay ahead of cyber attacks challenging your business

THREAT HUNTING TRAINING

1 day

- What is Threat Hunting?
- Introduction to concepts (frameworks, outputs, CI/CD, threat hunting maturity)

2 day

- Practical training: Proactive vs. Reactive
- Approaches to Threat Hunting (hypothesis-based, targeted, freeform)

3 day

- Introduction to a Threat Hunting scenario
- Practical training
- Scenario review
- Q&A

SOC Prime Expert Team

30+

Seasoned experts

SOC Prime's engineering expertise includes a diverse skill set ranging from Threat Hunting, Detection Engineering, Incident Response, Forensics, and Risk assessment. Our team involves certified experts, including GREM, GCFE, CISSP, CEH, Security+ recognized professionals and MITRE ATT&CK Defenders.

About Us

SOC Prime operates the industry-first modular platform for collective cyber defense against attacks of any sophistication and fast attribution. The Platform is backed by the world's largest library of detection algorithms and tailored threat intelligence powered by our mature engineering team, global CERTs, third-party consultancy, and the global crowdsourcing program for cyber defenders. We have established a dedicated Professional Services team to help our enterprise clients maximize their security investments and turn their strategic vision into an actionable roadmap for long-term success.

Reach out to your local sales representative at sales@socprime.com to explore the full list of SOC Prime Professional Services.