SYGNIA

# BLUE TEAM SKILLS FOR INCIDENT PREPAREDNESS

## COURSE DESCRIPTION

### Delivery Method:

- Instructor-led
- On-site guided workshops
- Remote web-based

### Session Format:

- Hands-on blue teaming
- Live simulations
- Knowledge sharing

### Learning Level:

- Basic
- Intermediate

### Course Summary:

The purpose of this course is to enhance your security team's capabilities in detecting, investigating, and responding to advanced cyber threats targeting real-world infrastructure by learning best practice blue team methodologies drawn from the frontlines.

Through hands-on, scenario-based simulations and proprietary lecture, students will improve their incident response skills by working with real-world case studies and structured exercises, practice threat hunting, and collect evidence-bearing forensic artifacts.

### How We Do It:

Based on a tailored mix of hands-on technical exercises and targeted lectures, your team will operate as blue teamers by responding to simulated attacks that align with your environment.

Guided by seasoned Sygnia instructors, students will collect and analyze forensic artifacts, perform threat hunting exercises, and execute full-scope investigations using proven and proprietary Sygnia methodologies.

### Course Outcomes:

After completing this workshop, participants will be able to:

- Establish repeatable log- and artifact-collection methodologies suited to their environment
- Detect, triage, and scope multi-stage intrusions
- Construct investigation timelines that accelerate root cause analysis and response
- Apply threat hunting techniques to proactively uncover malicious activity
- Contain and eradicate threat actors while preserving forensic evidence
- Strengthen collaboration and confidence across SOC and IR teams

### For Who:

- Security Operations (SOC) teams
- IR teams
- Threat hunters
- Forensic analysts
- Any team members responsible for cyber defense

### Prerequisites:

Basic understanding of cybersecurity principles, log data, security operations, and your organization's detection tools

### Duration:

3 minimum – 5 maximum half days depending on client objectives

### Ideal Timeline:

This course is most beneficial when conducted:

- Post-IR event to improve investigative techniques
- Upon hiring new security team members (SOC, IR analysts, forensic investigators, etc.)
- After introducing new security monitoring tools or methodologies into your environment