SYGNIA

INCIDENT INVESTIGATION TECHNIQUES

COURSE DESCRIPTION

Delivery Method:

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

Session Format:

- Focused exercise

Learning Level:

- Basic
- Intermediate
- Advanced

Course Summary:

The purpose of this course is to introduce best practice investigation methodologies drawn from the frontlines through hands-on, scenario-based training.

Students will develop core cyber incident investigation skills by working with real-world case studies and structured exercises, writing a forensic timeline, and analyzing forensic artifacts.

How We Do It:

Students choose from several different attack scenarios: Windows-based breach (basic), Linux-based breach (intermediate), Active Directory-based breach (intermediate), Entra ID+O365-based breach (intermediate), Chinese intelligence state sponsored attacks (intermediate), and AWS-based breach (advanced).

Each scenario possesses a different difficulty level and is designed to test and enhance security team preparedness in identifying, analyzing, and investigating the chosen cyber threat. Your security team performs as blue teamers to investigate the scenario breach alongside our hands-on instructors who share proven and proprietary Sygnia investigation methodologies along the way.

Course Outcomes:

After completing this course, students will be able to:

- Develop foundational investigation skills for effectively managing security incidents
- Understand and apply core forensic analysis methodologies
- Build investigative timelines best suited to their team and environment
- Strengthen teamwork and collaboration in their security operations approach

For Who:

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

Prerequisites:

A basic understanding of cybersecurity and incident response

Duration:

1 minimum – 3 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 in your environment