SYGNIA

AWS INCIDENT RESPONSE TECHNIQUES

COURSE DESCRIPTION

Delivery Method:

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

Session Format:

- Live simulation

Learning Level:

- Advanced

Course Summary:

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

Students will develop AWS incident response skills by working with real-world case studies, participating in a simulated exercise, writing a forensic timeline, and responding to a live threat actor—all within an AWS environment that students have full control over.

How We Do It:

The scenario is designed to enhance security team preparedness in investigating and responding to a sophisticated cyber-attack in a simulated AWS environment.

Your security team performs as blue teamers to investigate and respond to the attack alongside our hands-on instructors, who will share proven and proprietary Sygnia response methodologies.

Course Outcomes:

After completing this course, students will be able to:

- Develop foundational investigation skills for effectively managing security incidents in AWS
- Understand and apply core forensic analysis methodologies in AWS
- Build investigative timelines that are best suited for your team and AWS environment
- Gain key response skills for effectively remediating threat actors in complex AWS environments
- Strengthen teamwork and collaboration in your security operations approach to AWS environments

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, incident response, and AWS

Duration:

3 half days

Ideal Timeline:

This course is most beneficial when conducted:

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