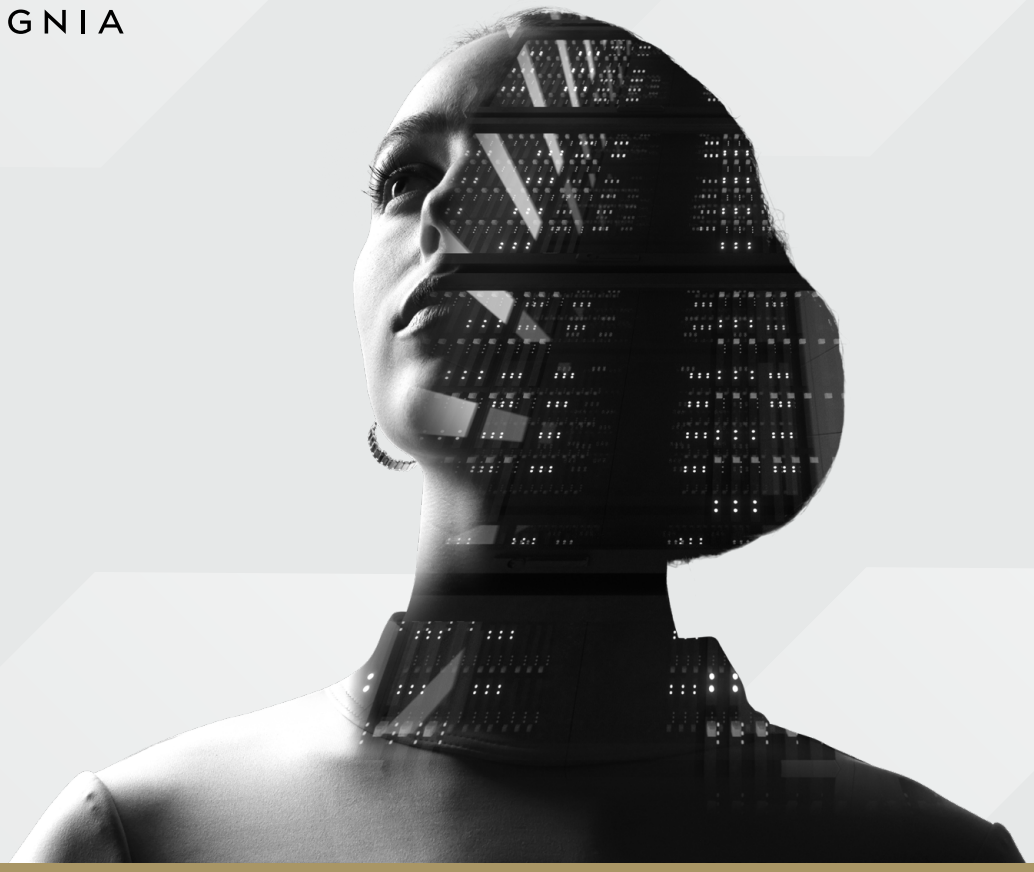
SYGNIA

INCIDENT RESPONSE AND SOC TRAINING SERVICES

COURSE CATALOGUE

SYGNIA



COURSE DESCRIPTIONS TABLE OF CONTENTS

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

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

SYGNIA

THREAT HUNTING SKILLS TO PROACTIVELY DETECT COMPROMISE

COURSE DESCRIPTION

Delivery Method:

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

Session Format:

- Focused exercises
- Guided threat hunts

Learning Level:

- Intermediate
- Advanced

Course Summary:

This course is designed to empower security teams with practical threat hunting skills and forensic log analysis techniques tailored to their specific environment.

Through a mix of lectures, real-world attack scenarios, and hands-on investigation exercises, students will gain the ability to proactively uncover malicious activity, triage threats, and conduct end-to-end investigations.

Threat hunting methodologies and technical query creation are also provided when needed.

How We Do It:

The tailored scenario is carefully designed by Sygnia, in collaboration with the client, to enhance security team capabilities in identifying, hunting, and analyzing threats within your operational environment. Performing as active defenders, students will fulfill structured threat hunting activities across multiple simulated attack scenarios, using real-world tools and logs.

Guided by Sygnia's seasoned instructors, your team will apply proven methodologies to identify indicators of compromise (IoCs), build investigative queries, and extract meaningful forensic insights to stop the attack before it occurs.

Course Outcomes:

After completing this course, students will be able to:

- Understand and implement structured threat hunting methodologies that suit your environment
- Develop log analysis capabilities aligned with internal toolsets
- Build and optimize queries for effective detection and triage
- Recognize and respond to malicious activities in enterprise environments
- Strengthen internal processes for effective detection, investigation, and response actions

For Who:

- Security Operations Center (SOC) analysts
- 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

SYGNIA

ADVANCING INCIDENT RESPONSE CAPABILITIES IN YOUR NETWORK

COURSE DESCRIPTION

Delivery Method:

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

Session Format:

- Hands-on purple teaming

Learning Level:

- Advanced

Course Summary:

The purpose of this course is to improve overall incident response readiness by enhancing your team's detection, investigation, and response capabilities in your environment—with your existing tools, where the real battle will take place.

Instructors teach students the processes that enable them to investigate as a team, write a forensic timeline, and execute the proper response, while pinpointing new opportunities to improve network visibility and posture.

How We Do It:

Using our collaborative purple team methodology, Sygnia red teamers simulate tailored, real-world attack scenarios within your active network while your security team performs as blue teamers to investigate the simulated breach alongside our hands-on instructors.

This simulation is followed by an in-depth debrief to review the actual attack lifecycle and document specific learnings that can be repeated to advance your in-house visibility strategies and tactical roadmap.

Course Outcomes:

After completing this course, students will be able to:

- Investigate and respond to modern attack scenarios using best practice approaches and frameworks relevant to your own environment
- Analyze real-world attacker techniques that are often difficult to identify as they will appear within your own environment
- Improve overall security monitoring and response strategies to reduce network visibility blockage
- Develop detailed, evidence-based incident timelines to prepare steps for remediation activities

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 principles; incident response is a plus but not required

Duration:

5 minimum – 8 maximum days depending on client objectives

Ideal Timeline:

This course is most beneficial when conducted:

- During rollout or tuning of EDR/SIEM/XDR or major log pipeline changes
- In accordance with cloud migrations, new business-critical application go-lives, or zero trust rollouts
- Prior to mergers, acquisitions, or major identity/privilege model changes
- Post-incident, once contained

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

SYGNIA

FOUNDATIONAL OT SECURITY BEST PRACTICES

COURSE DESCRIPTION

Delivery Method:

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

Session Format:

- Knowledge sharing
- Focused exercises

Learning Level:

- Basic
- Intermediate

Course Summary:

This foundational workshop is designed to raise awareness and promote secure practices for security and cross-functional industrial teams.

Students will explore OT-specific threat scenarios, common vulnerabilities, and essential security practices needed to improve their cyber resilience across legacy and modern industrial control systems.

Participants will gain understanding of the operational consequences attached to OT cyber risk and foster an improved collaboration across critical engineering and cyber defense teams.

How We Do It:

Sygnia instructors share field-proven security best practices developed from real-world use cases seen on the frontlines, including ransomware attacks and well-known OT breaches like Colonial Pipeline, TRISIS, and BlackEnergy.

Students are guided through the OT cyber kill chain and common attacker pathways that illustrate the security challenges of these tailored scenarios.

Practical recommendations are provided for remote access, backup strategies, network segmentation, patch management, and third-party vendor handling.

Course Outcomes:

After completing this workshop, participants will be able to:

- Identify cyber risks relevant to their OT environment
- Apply essential security practices that address your specific threat landscape
- Strengthen secure remote access, change control, and recovery measures
- Collaborate more effectively across OT & IT functions

For Who:

- Security teams
- CISOs
- OT cybersecurity owners
- OT engineers
- Control system integrators
- Site managers
- Asset operators

Prerequisites:

None required; content is designed for cross-functional participation

Duration:

2 hours minimum - 1 day maximum depending on client needs

Ideal Timeline:

This course is most beneficial when conducted:

- During onboarding of new OT engineers or security team members
- Prior to deploying or upgrading ICS/OT architecture or security controls
- Prior to a regulatory audit or compliance-driven assessment
- In accordance with digital transformation projects, particularly those involving new connectivity, remote access, or third-party integrations

SYGNIA

HOW TO BUILD AN EFFECTIVE OT DETECTION STRATEGY

COURSE DESCRIPTION

Delivery Method:

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

Session Format:

- Focused exercise
- Strategic planning exercises

Learning Level:

- Intermediate
- Advanced

Course Summary:

This workshop provides students with a structured and field-proven approach to building a detection strategy tailored for their OT environments.

Participants will define visibility objectives, map detection use cases using ICS threat models, and build a phased roadmap aligned with their environment's operational constraints, safety priorities, and available technologies.

How We Do It:

Sygnia instructors provide guidance and best practice recommendations for students to effectively map their OT architecture and identify visibility gaps that currently inhibit their cyber defense capabilities.

An understanding of the dedicated ICS MITRE ATT&CK framework is established and then detections are prioritized based on the asset criticality of your environment's crown jewels and most common threat vectors.

Students will leverage existing tools to design use cases and layer detection capabilities that will improve their ability to help proactively prevent compromise.

The course will conclude with the creation of a scalable detection roadmap that provides clear and actionable milestones.

Course Outcomes:

After completing this workshop, participants will be able to:

- Map system architecture, boundaries, and critical assets across your OT environment
- Identify detection gaps and visibility blind spots based on above mapping
- Design prioritized use cases for detection in your OT environment
- Integrate detection efforts with SOC/IT monitoring tools
- Build a scalable, phased detection strategy with technical justification
- Communicate detection priorities effectively to management and executive teams

For Who:

- Security Operations (SOC) teams
- OT detection engineers
- IR teams
- CISOs
- OT cybersecurity architects

Prerequisites:

Familiarity with industrial environments and basic detection concepts

Duration:

2 hours minimum - 1 day maximum, depending on client objecives and environment maturity

Ideal Timeline:

This course is most beneficial when conducted:

- During onboarding of OT detection engineers, SOC analysts, or IR team members
- Prior to planning or upgrading an ICS/OT detection strategy
- Post-incident or following a detection failure

SYGNIA

Sygnia is the foremost global cyber readiness and response team, applying creative approaches and battle-tested solutions to help organizations beat attackers and stay secure. Sygnia is a trusted advisor and service provider of technology and security teams, executives and boards of leading organizations worldwide.
Learn more at Sygnia.co.

A TEMASEK COMPANY AND MEMBER OF THE ISTARI COLLECTIVE

TEMASEK ISTARI

24/7
INCIDENT RESPONSE COVERAGE
Suspicious of an incident? Call +1-877-686-8680 now. Learn more at www.sygnia.co