Training: SECO-Institute
SOC Associate Analyst

TRAINING GOALS:

The Associate SOC Analyst course offers a comprehensive 3- day training that immerses students into the processes, data flows and capabilities of a SOC along with hands on, real-world tasks of a Tier 1 Analyst: Throughout the course students will work with SIEM, ITSM and SOC Ticketing Systems, the key toolset of the Tier 1 analyst. They will monitor, analyse and prioritize SIEM alerts based on host-based and security appliance logs and perform triage and effective decision making to confirm and declare if a security incident is taking place. They'll conduct threat analysis on datasets, use the ticketing system to report their findings and present the results of their investigations, and work together on a business case where they manage an incident from preparation to post-incident analysis. To support their hands- on investigations students will practice attacker techniques and vulnerabilities evaluation and identify companies' critical assets & key IT systems that they are assigned to monitor and protect. The course delivers a simulated SOC environment including a virtualized ITSM, SOC Ticketing system and 2 different SIEMs, fully set up to work together which will create an immersive experience in a virtual SOC and re-create their workplace environment as closely as possible.

Balance between Toolset and Mindset:

One of the most important takeaways from this course is understanding and applying the 'Analyst Mindset'. This training will trigger students' curiosity, activate their analytical brain and have them work together with their SOC Mates, Clients and Incident Responders, crucial assets for the successful Analyst. We'll dive deep into the analytical process and offer student a set of hypotheses with 'if-then' scenario's, what to look for and where to find 'go- to' resources to support their investigations. They'll learn how to deal with the huge number of logs, alerts and events in a SOC, which can be overwhelming if not treated correctly.

What will you learn?

The Associate SOC Analyst offers a unique combination of the analytical mindset, knowledge, collaboration skills and hands- on practice required from a SOC Analyst. The course is delivered in a simulated SOC environment including a virtualized ITSM, SOC Ticketing system and SIEM, fully set up to work together and create an immersive, real life experience. It benefits those that are pursuing a career as a SOC Analyst, junior team members looking to accelerate their learning curve and SOC Teams that want to set a baseline requirement for their Tier1 Analysts.

Who should attend?

This training is designed for those that are pursuing a career as a SOC Analyst, junior team members looking to accelerate their learning curve, SOC Teams that want to set a baseline requirement for their Tier1 Analysts and Universities that that want to have their students 'job- ready', with industry

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

subjects which lead to industry certifications. The course offers a unique combination of the mindset, knowledge and skills required from a SOC Analyst, immediately applied in a realistic work environment. If you are looking to grow into a senior role and/ or a deep dive in threat hunting, threat intelligence, Incident Response, XDR and security automation, we would recommend taking the SOC Threat Analyst course.

CONSPECT:

- Setting the Stage: The SOC and the Tier 1 Analyst

  This module briefly introduces students into the processes, data flows and capabilities of a Security Operations Center, the services that a SOC delivers, what technologies are deployed and how they interconnect. It then describes the different roles, responsibilities and tasks within the SOC, from Tier 1 up to management. From thereon, the module dives deep into the Tier 1 Analyst role, the associated Tasks and KSA matrix (Knowledge, Skills, Abilities) that are required, key tools and resources, major challenges and pitfalls for a junior Analyst, and how all of the above are addressed in the training process.

  - 1.1. Intro SOC, SOC-Services and Technology based on SOC-Maturity Model
  - 1.2. Roles within the SOC and associated escalation process, career paths
  - 1.3. Tasks of the Tier 1 Analyst
  - 1.4. Core skills of the Tier 1 Analyst, it is all about:
    - Understanding attacker techniques and vulnerabilities
    - Being able to identify critical company assets and key systems
    - Know where and how to collect data and logs
    - The analyst mindset: Analytical process and decision making when to declare a security incident
    - How to report your findings and escalate
  - 1.5. Key toolset of the Tier 1 Analyst:
    - SIEM
    - ITSM
    - SOC-Ticketing System
  - 1.6. Key data-sources initiating investigations:
    - SIEM alerts
    - IDS alerts, firewalls, network traffic logs, endpoints
    - Reported from users
  - 1.7. Key data-sources supporting investigations:
    - Vulnerability Management
    - Threat Intelligence
    - Malware Analysis

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Key toolset of the Tier 1 Analyst: SIEM, ITSM, Ticketing Systems, Mindset

  This hands on module introduces students to SIEM, ITSM and SOC Ticketing Systems and how they work together. They will understand the different SIEM technologies and data processing models, focusing on Elastic and Splunk, the most popular SIEM products in the market nowadays. Students will experience the Analyst feeling when working with different team members and transitioning from the ITSM to the rest of the tools in order to deliver a high quality service. Throughout this module, students will work on a business case, where they are assigned to process some tasks within a virtual SOC via a ticketing system. They will be introduced to the mindset of the security analyst and the analytical, step- by step process of an investigation.

  - 2.1. ITSM
  - 2.2. SOC Ticketing System
  - 2.3. SIEM (Elastic and Splunk)
  - 2.4. The mindset of a Security Analyst – introduction
  - 2.5. Hands On – Exercise using all of the above
- Log Collection, Use Cases, Threat Detection and Monitoring

  This module delivers the theory behind log monitoring and security monitoring systems along with hands-on exercises in security logging and analysing log collections. The module offers an introduction to attacker techniques and vulnerability finding, critical assets and key systems identification. Students will learn where and how to collect data (SIEM alerts, IDS alerts, firewalls, network traffic logs, endpoints, WAF, etc), how to investigate and detect threats based on a large realistic dataset and how use cases are applied to monitor the use of attack techniques. A large portion of the module is again spent on guiding students step by step through the analytical process, what to look for when analysing log collections and key data sources that will support their investigations.

  - 3.1. The mindset of a Security Analyst – in depth
  - 3.2. Introduction to Attacker techniques and processes
  - 3.3. Data Collection:
    - SIEM alerts
    - IDS alerts
    - Firewalls
    - Network traffic logs
    - Others
  - 3.4. Logs and Log Collection
  - 3.5. Critical and Key IT Systems and their logs (exercise)
  - 3.6. ITSM and SIEM (Hands on)
  - 3.7. Event Analysis, correlation and Attack Techniques (hands on)
  - 3.8. Alerting, Reporting and Dashboarding (hands on)

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 3.9. Security Monitoring Use Cases, MaGMA, MaGMA UCF

- Threat Intelligence, Threat Analysis vs Threat Hunting and Incident Response

  Module 4 starts with a high- level introduction of the threat intelligence process and how it is applied to obtain situational awareness. It then dives deeper into the Pyramid of Pain and MITRE ATT&CK framework for Threat Hunting and Threat Analysis purposes. Next up we'll dive deep into threat analysis and investigations, moving from Event-Analysis to Threat Analysis and bringing the analyst mindset covered throughout the course into a hands-on practice. Students will finalise understanding the incident declaration and escalation procedure as well as the overall Incident Response model and process. During the hands-on practice, students get to analyse a dataset to find indications of threats and work together on a business where they manage an incident from preparation to post-incident analysis. The hands-on section prepares students for a complex homework assignment they will complete after this module and that will be a part of their exam.

  - 4.1. Introduction to Threat Intelligence, situational awareness and attribution
  - 4.2. Pyramid of Pain and MITRE ATT&CK framework
  - 4.3. Threat Analysis versus Threat Hunting
  - 4.4. Threat Analysis in- depth
  - 4.5. Detection continuous improvement and Intelligence feedback
  - 4.6. Incident Response model and process
  - 4.7. Hands on threat analysis exercises and incident response business case
  - 4.8. Homework assignment and exam preparation

- Exam
  - Homework assignment in CTF format
    The hands-on section on the last day of training prepares you for a complex, hands on homework assignment in a Capture the Flag format that will be part of your exam and certification. You must finalize your assignment before you can schedule your exam.
  - Exam Language: English; Delivered: Online via a certified proctor; Questions: 40 multiple choice (5 questions related to your CTF homework assignment); Time: 60 minutes.

REQUIREMENTS:

Basic understanding of TCP/IP, operating system fundamentals and common security concepts. Students are expected to have a basic understanding of application layer protocols such as http, smtp, ssh and ftp. Understanding of Linux command-line is a big plus/ desirable.

Difficulty level

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

CERTIFICATE:

The participants will obtain certificates signed by SECO-Institute, SOC Associate Analyst Certificate if pass the exam.

Each participant in an authorized SOC Associate Analyst training will receive a one free attempt to SOC Associate Analyst exam.

TRAINER:

Certified SECO-Institute trainer.

ADDITIONAL INFORMATION:

Days of training:

First session: 10,17,24 March
Second session: 3,10,17 June

Included in your training:

- 3 days instructor led, virtual online training
- Access to SECO’s Virtual SOC
- Hands on labs
- All course materials
- Access to SECO’s student portal with practice exam & resources
- Exam voucher

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007