Training: SECO-Institute
SOC Threat Analyst

TRAINING GOALS:

The Threat Analyst course was designed for SOC Analysts that are aiming to progress into a more senior role. More than just that, it is structured in a realistic way that will prepare students for a new SOC paradigm by developing dynamic learning, deploying top-notch automation and implementing ITIL-based SOC services. This course offers them the hands-on practice to work with the modern MDR technology stack and evolved processes, and structure their mind the right way to conduct deep investigations on escalated events and incidents and conduct Advanced Persistent Threats Analysis. It also aims to shift students towards a more pro-active defense role in the SOC: They will exercise Network and Asset Modeling as a basis for both risk-based log ingestion strategies and investigation prioritization. They'll improve threat detection and security monitoring capabilities using MAGMA and SIGMA Rules, conduct blind spot detection assessments, structure full Threat Hunting campaigns to detect threats that will inevitably slip through defenses and respond rapidly and accordingly. The course will close the loop by using the knowledge of attacker techniques and discovered IOCs from students' investigations to create alerts and rules to proactively detect both in the future, and work with a real Threat Intelligence platform and use it for situational awareness.

Heavily hands- on driven:

This course is very hands- on driven and exercises are conducted in a Capture the Flag format. The Virtual MDR – SOC offers a fully integrated toolset set up to work with each other to re-create your workplace environment as closely as possible:

- ITSM and CMDB
- Network and Asset Modelling
- A SOC Ticketing System
- SIEM (Splunk and Elastic)
- A Threat Intelligence platform
- Packet capture and analysis
- Automation tools
- An Incident Response tool
- XDR

Who should attend?

This training is designed for SOC Analysts that are aiming to progress into a more senior role and SOC Teams that want to set a baseline requirement for their Threat Analysts. The course offers a unique combination of the mindset, knowledge and skills required from a Threat Analyst, immediately applied

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

in a realistic work environment. To join this class, we recommend you have a minimum of 1- 1,5 years of experience as SOC Analyst. If you don't have this experience, we recommend you taking the SOC Associate Analyst training

CONSPECT:

- Setting the Stage: The SOC and the Threat Analyst

  This module offers students a strategic vision of a current SOC (Known as Next Generation SOC and lately, MDR), the different ways it can be structured and the actions to run and continuously improve a scalable and effective SOC. Students will get the mindset to work on a MDR SOC considering technology, processes, roles, tasks, services and will work on a business case, where they're assigned to process tasks within a virtual SOC via ITSM in a "Capture the Flag" format. They'll be asked to identify the SOC's business drivers and customers, roles and responsibilities, utilize MDR components and technologies in order to accomplish the SOC's mission and create relevant SOC metrics.

  - 1.1. SOC Services evolution to MDR and the impact on the Threat Analyst role:
    - Cloud SOC
    - On-prem SOC
    - Strategic SOC
  - 1.2. MDR Service Operations:
    - ITIL Service Management
    - Threat Modelling
    - Threat Analysis
    - Threat Hunting
    - Threat Intelligence
    - Create and improve security monitoring and threat detection use cases
    - Conduct blind spot detection assessments
    - Automate SOC processes
    - Respond rapidly to Incidents
  - 1.3. Business
    - New Drivers
    - Customers
    - New governance
    - New privacy regulation
    - SOC Metrics
  - 1.4. People
    - New roles and hierarchy
    - Training

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

        - Knowledge Management
        - SOC Career progression
        - Assessing the SOC team
    - Frameworks, best practices for this module (Hands-on):
        - SOC Maturity Model, SOC Implementation Model, The Library of Cyber Resilience Metrics, NIST NIC

- Key toolset of the Threat Analyst: Introduction to SECO-s Virtual SOC

  This module introduces students hands on to the Virtual SOC that they will be working in throughout the course, and how the various tools and technologies deployed are working together. Throughout the module, students will work on a business case, where they are assigned to process some tasks.

    - 2.1. ITSM and CMDB (Hands on)
    - 2.2. SOC Ticketing System (Hands on)
    - 2.3. SIEM (Hands on)
    - 2.4. Threat Intelligence platform (Hands on)
    - 2.5. Packet capture and analysis
    - 2.6. Automation tools
    - 2.7. Incident Response tool
    - 2.8. Security Automation tool and scripts

- Network and Asset Modelling, Risk Analysis, Log Ingestion Strategies

  This module starts with an exercise in Network and Asset Modelling and Risk Analysis. Students will model the network that they’re assigned to monitor and protect on our Virtual SOC; label, classify and document the assets using the CMDB module on their ITSM, and conduct risk analysis on those assets. They’ll create log ingestion strategies to set up the best visibility to detect cyberattacks, and conduct detection assessments to help find detection blind spots. Students will ingest several types of logs into the SIEM instances to enable quick searches and investigation of events and configure ITSM modules to define SOC services.

    - 3.1. Network Modelling, Asset Modelling, Risk Analysis (Hands- on)
    - 3.2. Logging, Log sources, Log ingestion (Hands- on)
    - 3.3. Blind Spot Detection Assessment (Hands- on)
    - 3.4. ITSM and defining SOC Services conform ITIL (Hands-on)

- Attacker Tactics and Techniques in- depth

  While junior and medior SOC Analysts are expected to have a thorough understanding of Attacker Techniques, the Threat Analyst must master them! This module dives deep into MITRE ATTACK&CK Framework by understanding the different environments, its navigators, their associated tactics and techniques and how to work with them at the same time as the Cyber Kill Chain. Students will integrate and apply this knowledge during the course of the training.

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

- 4.1. MITRE ATTACK&CK Framework (Hands-on)
- 4.2. MITRE ATTACK&CK Navigator (Hands-on)
- 4.3. Cyber Kill Chain (Hands-on)

- Threat Analysis

  Modules 3 and 4 have set the stage for deep investigations on escalated threats and incidents. This is where we start confusing students a bit, pushing their boundaries to activate their analytical brain, trigger their curiosity and use their creativity during investigations. The module is delivered in a Capture the Flag format replicating the real workplace as much as possible: Students will work on both Splunk and Elastic SIEM environments for investigation, correlation, alerting, escalation and reporting purposes; get assignments on a virtual ITSM system as in a real SOC, and interact with their SOC mates on the investigation, escalation and hand-over activities. The hands on sections prepare for a complex homework assignment that they'll receive on day 3.

  - 5.1. Splunk and Elastic SIEM (Hands – on)
  - 5.2. Threat Analysis , correlation and Attack Techniques (Hands – on)
  - 5.3. Alerting, Reporting, Dashboarding and Escalating (Hands – on)

- Monitoring Use Cases and Threat Intelligence

  Students will create security monitoring and threat detection use cases in both Splunk and Elastic environments and will use MaGMA UCF to measure, maintain, improve, scale and manage the SOC use case library. They will analyse SIGMA Rules' structure and create, maintain, scale and improve their own rules. They will dive into the Threat Intelligence process and use it in a real case scenario for situational awareness and threat investigation and detection using a real Threat Intelligence Platform (MISP). These investigations are extended to the fascinating world of the Dark Web for Threat Intelligence purposes. During the hands-on practice, students will discover, share, store and correlate Indicators of Compromise of targeted attacks, financial fraud information, vulnerability information and threat actors. The hands-on section prepares students for a complex homework assignment they will complete after this module.

  - 6.1. MITRE ATTACK&CK applied to monitoring, detection and threat intelligence
  - 6.2. Security Monitoring and Threat Detection Use Cases (Hands-on):
    - Security Monitoring
    - Threat Detection
    - Use Case Development
    - MaGMA UCF
  - 6.3. SIGMA Rules (Hands-on)
  - 6.4. Threat Intelligence (Hands-on):
    - Types
    - Protocols
    - Standards

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

        - Feeds
        - Platforms
        - STIX/TAXII/OpenIoC
    - 6.5. Threat Intelligence on the Dark Web (Hands-on)
    - Frameworks, best practices for this module (Hands-on):
        - CSAN Threat Actors
        - Threat intelligence protocols and standards
        - Pyramid of Pain and TTP's
        - Cyber Kill Chain versus MITRE ATT&CK
        - OODA loop Diamond model of intrusion analysis
        - Chatham House Rule.
        - MaGMa and MaGMa UCF Tool
        - MISP
        - NIST NICE
- Threat Hunting and Defense

  Module starts with TTP's and MITRE ATT&CK Framework in in depth. Students will collect IoC's and structure a full Threat hunting campaign, where they will create their own hypothesis and will either confirm or discard after being able to cross correlate events and determine their context, and identify and quantify vulnerabilities based on Splunk, Elastic and MISP. Students will track and document the entire process through their ITSM tool, just as next generation SOCs do. Once the threats are hunted, students will create their own rules to be shared and report the findings of their assignments. Finally, after an in- depth analysis, they will translate their technical findings to a management summary and deliver a board level presentation.

    - 7.1. Pyramid of Pain (Hands-on)
    - 7.2. TTPs (Hands-on)
    - 7.3. Threat Hunting Methodologies (Hands-on):
        - Cyber Threat Hunting Framework
        - TaHiTI
        - The Hunting Loop
    - 7.4. The Hunt Matrix (Hands-on)
    - 7.5. The Defense Chain
    - 7.6. Detection Feedback
    - 7.7. Advanced Persistence Defense
    - 7.8. Snort/Zeek Rules (Hands-on)
    - Frameworks, best practices, references for this module:
        - Threat intelligence protocols and standards
        - Pyramid of Pain and The Hunt Loop

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

- Cyber Kill Chain versus MITRE ATT&CK Framework
- The Defense Chain
- OODA loop, Diamond model of intrusion analysis
- MaGMa, MaGMa UCF Tool
- MISP
- NIST NICE

- Incident Response

Our last module is led by the Incident Response PICERL model and the NIST Computer Security Incident Handling Guide. It evaluates the policies that govern incident response, incident response plans, the required procedures in place and the tools and technologies they need to handle an incident. From thereon, the incident response process and activities are practiced hands on with 2 exercises where students will be assigned on the ITSM tool to manage an incident from preparation to post-incident evaluation. The hands-on section uses a platform that provides endpoint driven information security tools and infrastructure to help them investigate, process and lead incident response in our virtual SOC. The hands on exercises prepare students for a complex homework assignment that will be part of the exam.

- 8.1. Preparation Phase (Hands-on):
  - Policies
  - IR Plan
  - IR procedures
  - Playbooks
- 8.2. Identification/Detection(Hands-on):
  - Memory Analysis
  - Disk Analysis
  - Malware Analysis (YARA)
  - Network Analysis
- 8.3. Containment
  - Systems
  - Network
  - Users
  - Services
  - Cloud
- 8.4. Eradication
  - Systems
  - Network
  - Users
  - Services

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

- Cloud
- 8.5. Recovery
  - Systems
  - Data
- 8.6. Lessons Learned (Hands-on)
- 8.7. Dissemination and Security Awareness

- Exam

The hands-on section on the last day of training prepares students for a complex, hands on homework assignment in a Capture the Flag format that will be part of their exam and certification. Students must finalize their assignment before they can schedule their exam

- Exam:
  - Language: English
  - Delivered: Online via a certified proctor
  - 10 multiple choice questions
  - 5 open questions related to the CTF homework assignment
  - 1 case
  - Time: 120 minutes

REQUIREMENTS:

To join this class, we recommend you have a minimum of 1- 1,5 years of experience as SOC Analyst. If you don’t have this experience, we recommend you taking the SOC Associate Analyst training

Difficulty level

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.

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

ADDITIONAL INFORMATION:

Days of training:

Session: 1,8,15,22,29 April

Included in your training:

- 5 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