CSA - Certified SOC Analyst

Kestus: 24 academic hours

Veebikoolitus

Vaata kõiki toimumiskuupäevi

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

Target audience:

- SOC Analysts (Tier I and Tier II)
- Network and Security Administrators, Network and Security Engineers, Network Defense Analyst, Network Defense Technicians, Network Security Specialist, Network Security Operator, and any security professional handling network security operations
- Cybersecurity Analyst
- Entry-level cybersecurity professionals
- Anyone who wants to become a SOC Analyst.

In result of the training participants:

Learning Objectives of CSA

- Gain Knowledge of SOC processes, procedures, technologies, and workflows.
- Gain basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, etc.
- Able to recognize attacker tools, tactics, and procedures to identify indicators of compromise (IOCs) that can be utilized during active and future investigations.
- Able to monitor and analyze logs and alerts from a variety of different technologies across multiple platforms (IDS/IPS, end-point protection, servers and workstations).
- Gain knowledge of Centralized Log Management (CLM) process.
- Able to perform Security events and log collection, monitoring, and analysis.
- Gain experience and extensive knowledge of Security Information and Event Management.
- Gain knowledge on administering SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Understand the architecture, implementation and fine tuning of SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Gain hands-on experience on SIEM use case development process.
- Able to develop threat cases (correlation rules), create reports, etc.
- Learn use cases that are widely used across the SIEM deployment.
- Plan, organize, and perform threat monitoring and analysis in the enterprise.
- Able to monitor emerging threat patterns and perform security threat analysis.
- Gain hands-on experience in alert triaging process.
- Able to escalate incidents to appropriate teams for additional assistance.
- Able to use a Service Desk ticketing system.
- Able to prepare briefings and reports of analysis methodology and results.
- Gain knowledge of integrating threat intelligence into SIEM for enhanced incident detection and response.
- Able to make use of varied, disparate, constantly changing threat information.
- Gain knowledge of Incident Response Process.
- Gain understating of SOC and IRT collaboration for better incident response.

Additional information:

As the security landscape is expanding, a SOC team offers high quality IT-security services to actively detect potential cyber threats/attacks and quickly respond to security incidents. Organizations need skilled SOC Analysts who can serve as the front-line defenders, warning other professionals of emerging and present cyber threats.

The lab-intensive CSA program emphasizes the holistic approach to deliver elementary as well as advanced knowledge of how to identify and validate intrusion attempts. Through this, the candidate will learn to use SIEM solutions and predictive capabilities using threat intelligence. The program also introduces the practical aspect of SIEM using advanced and the most frequently used tools. The candidate will learn to perform enhanced threat detection using the predictive capabilities of Threat Intelligence.

Recent years have witnessed the evolution of cyber risks, creating an unsafe environment for the players of various sectors.

To handle these sophisticated threats, enterprises need advanced cybersecurity solutions along with traditional methods of defense. Practicing good cybersecurity hygiene and implementing an appropriate line of defense, and incorporating a security operations center (SOC) have become reasonable solutions. The team pursues twenty-four-hour and "follow-the-sun" coverage for performing security monitoring, security incident management, vulnerability management, security device management, and network flow monitoring.

A SOC Analyst continuously monitors and detects potential threats, triages the alerts, and appropriatley escalates them. Without a SOC analyst, processes such as monitoring, detection, analysis, and triaging will lose their effectiveness, ultimately negatively affecting the organization.

Length: *24 academic hours*

The prerequisite for issuing the certificate is full participation in training.

The training topics and description:

Course Outline

Module 0- SOC Essential Concepts
Module 1 – Security Operations and Management
Module 2 – Understanding Cyber Threats, IoCs, and Attack Methodology
Module 3 – Incidents, Events, and Logging
Module 4 – Incident Detection with Security Information and Event Management (SIEM)
Module 5 – Enhanced Incident Detection with Threat Intelligence
Module 6 – Incident Response

The training price also includes:
teaching materials;
a trainer's consultation on the topics learned by e-mail after the training;
certificate;
exam.

LISAINFO

Osalemise tingimused
Registreerudes e-poe, e-kirja või telefoni teel, saadame Teile arve ja täpsema info osalemise kohta.
Nädal enne koolitust saadame Teile e-kirjaga meenutuse osalemise infoga.

Koolitusel osalemine on nimeline, kuid saate osalejat tasuta muuta kuni koolituse alguseni.

Koolituse eest tasumine toimub arvel viidatud arveldusarvele. Arve saadetakse maksja aadressile e-postiga. Arve tuleb tasuda enne koolituse algust arvel märgitud maksetähtajaks.

Kui Te ei saa mingil põhjusel osaleda, palun andke sellest kindlasti teada e-posti aadressil info@koolitus.ee või telefonil 618 1727 . Kui teatate koolitusel mitteosalemisest kuni 10 tööpäeva enne algust, pakume mõnd muud samaväärset koolitust või tagastame 100% tasutud koolituse maksumusest. Mitteosalemisest vähemalt 5 tööpäeva varem teatades, tagastame 50%. Muul juhul kuulub arve tasumisele. Raha tagastame ette antud summas juhul, kui pole tehtud koolituse korraldamisega seotud kulutusi (ostetud õppematerjale jms). Koolitusele mitteilmumisel, sellest mitteteatamisel või koolituse poolelijätmisel õppetasu ei tagastata.

IT Koolitusel on õigus koolitusgrupi mitte täitumisel koolituse toimumine edasi lükata või koolitus ära jätta. Koolitusele registreerunuid teavitatakse kursuse edasi lükkumisest või ära jätmisest telefoni või e-posti teel. Koolituse ära jäämisel korraldajatest tulenevatel põhjustel makstakse õppetasu tagasi. .

IT Koolitus on Eesti Töötukassa koolituskaardi koostööpartner. Tutvuge koolituskaardi infoga SIIN.
Täpsema info saamiseks võtke meiega ühendust telefonil 618 1727 või info@koolitus.ee.