CYBERTECH DEFENDER

Let's Defend the World Together !

# The Ultimate Cybersecurity Training Institute

About Us

We At CyberTechDefender, we're dedicated to shaping the next generation of cybersecurity experts. Our mission is to equip you with the knowledge and skills to defend against digital threats and embark on a rewarding career in this ever-evolving field.


Contact us

Info@cybertechdefender.com
+919494969524

CYBERTECH DEFENDER
Let's Defend the World Together !

# SOC Analyst Syllabus

## Course description

- SOC (Security Operations Center) training is an essential program designed to provide aspiring individuals with a comprehensive foundation to enter the cyber security field. This course offers an immersive learning experience, starting from the very basics and progressing to advanced topics, ensuring that students acquire a well-rounded understanding of the subject matter.

- This comprehensive course is designed to equip aspiring Security Operations Center (SOC) analysts with a deep understanding of essential tools and technologies, enabling them to start from scratch and progress to an intermediate level of expertise. Through a hands-on and practical approach, students will gain proficiency in crucial areas such as Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR) solutions, Threat Intelligence platforms, and Vulnerability Management tools. The course content is meticulously curated to mirror real-time scenarios, ensuring that analysts are fully prepared to tackle the challenges they'll encounter in their professional roles after securing employment in an organization.

- By delving into SIEM, students will learn how to aggregate, correlate, and analyze vast quantities of security data, enabling them to detect and respond to threats efficiently. EDR training will empower them to proactively protect endpoints and investigate security incidents, while exploring Threat Intelligence will provide insights into understanding the evolving threat landscape. Vulnerability Management expertise will be honed to identify and mitigate weaknesses in an organization's infrastructure. Instructors with practical experience in the field will guide students through hands-on exercises, real-world case studies, and simulations, ensuring they are well-prepared to make a valuable contribution to a SOC team upon entering the workforce. Whether it's monitoring network traffic, investigating potential breaches, or staying ahead of emerging threats, this course equips SOC analysts with the skills and knowledge they need to excel in real-world

CYBERTECH DEFENDER

Let's Defend the World Together !

# Course Outline

**Module 01**

Basic concepts of Networking and Cyber security

**Module 02**

Understanding on different types of malwares and attacks

**Module 03**

Incident handling with  Security Information and Event Management (SIEM)

**Module 04**

Analysing and performing Root cause analysis on True postive incidents

**Module 05**

DLP, Threat Intelligence,IOC, IOA and frameworks

**Module 06**

Incident Response cycle and vulnerability assesment

# Hands-On Tools

**SIEM** IBM Qradar, Splunk

**EDR** Malwarebytes, Xcitium

**Antivirus** Mcafee

**Ticketing tools** Servicenow

CYBERTECH DEFENDER
Let's Defend the World Together !

# Candidates who can enroll for this course

**This course caters to a diverse range of individuals with varying backgrounds and career aspirations within the cybersecurity domain**

## 1.Fresher's:

**For those eager to launch a career in cyber security, this course provides the perfect foundation. It equips them with the knowledge, skills, and hands-on experience required to make a successful entry into the field, offering a solid starting point for a promising career in cyber security.**

## 2.Career Changers

**Individuals with experience in the broader IT field who aspire to pivot towards cyber security will find this course invaluable. It helps bridge the knowledge gap and provides them with the specialized skills needed to transition smoothly into the cyber security domain.**

## 3.Experienced Cyber security Professionals

**Even for those already working in the cyber security field, this course offers a unique opportunity to deepen their expertise. By focusing on practical knowledge and analysis of diverse data sources, logs, and leveraging a multitude of tools, it helps experienced professionals sharpen their skills, stay current with industry trends, and further enhance their capabilities to respond effectively to real-world cyber threats.**

## 4. Network and Security administrators

## 5. Network and Security Engineers

## 6. Anyone who wants to become a SOC Analyst

**This comprehensive course is designed fulfill the needs of Network and Security Administrators, Network and Security Engineers, and individuals aspiring to become proficient Cybersecurity Analysts. It offers a profound opportunity to bolster your expertise by deep diving into a diverse array of multiple tools and technologies, equipping you to navigate and excel in the dynamic and challenging landscapes of real-world scenarios.**

CYBERTECH DEFENDER
Let's Defend the World Together !

# Objectives of this course

- This comprehensive course designed to fulfill the entire expert level knowledge with all the basic concepts to till the Expert level concepts. Where one wanted to be survived with necessary skill sets with multiple real-time tools and technologies with technical skills covered with incident management, incident response, malware analysis, email security, information security, incident handling, Endpoint detection response, threat intelligence and vulnerability assessment with root cause analysis.

- This course will empower participants with multiple tools like SIEM (Security information event management), ANTIVIRUS, EDR (Endpoint detection response), EMAILGATEWAY, VULNERABILITY MANAGEMENT and technologies like INCIDENT MANAGEMENT, INCIDENT RESPONSE, INFORMATION SECURITY, VULNERABILITY ASSESSMENT, MALWARE ANALYSIS and EMAIL SECURITY.

- For those eager to launch a career in cyber security, this course provides the perfect foundation. It equips them with the knowledge, skills, and hands-on experience required making a successful entry into the field, offering a solid starting point for a promising career in cyber security.

- Individuals with experience in the broader IT field who aspire to pivot towards cyber security will find this course invaluable. It helps to bridge the knowledge gap and provides them with the specialized skills needed to transition smoothly into the cyber security domain

- This course is designed to mold individuals into advanced level SOC analysts assisting with all the capabilities to stand out in today's competitive cyber security landscape. By undergoing the comprehensive program, participants will gain the expertise required to excel in the market as highly skilled professionals. They will emerge from this course with the proficiency and knowledge necessary to meet the challenges of the modern SOC environment, effectively contributing to the security and well-being of organizations while demonstrating their value as top-tier cyber security specialists.

- This course covers all the topics and knowledge essential for success in interviews and real time job environments. It not only provides theoretical understanding but also provides practical exposure to real world tools and participants can gain the hands-on experience necessary to transition from the classroom to the workplace, fully prepared to excel in the demanding field of cyber security.

CYBERTECH DEFENDER
Let's Defend the World Together !

# Objectives of this course

- Upon successful completion of this course, individuals will experience a remarkable transformation, evolving from a foundational understanding of security to advanced level proficiency on multiple tools and technologies. This comprehensive program not only builds expertise from the ground up but also empowers participants to navigate the complexities of modern cyber security with confidence and mastery. It's a journey that takes learners from a beginner's level to an advanced one, providing them with the essential skills and knowledge to excel in the multifaceted world of security

- SOC analyst course is offered with an agenda that to cover all the topics that are related the SOC analyst to enhance with the complete real time scenarios which empowers with the real time use cases

- In addition to the comprehensive SOC content, this course extends its focus to the dynamic domain of threat intelligence, offering an enriched syllabus that remains constantly updated to reflect the latest threats and vulnerabilities. Participants will delve into the intricacies of threat intelligence, acquiring the ability to gather valuable Indicators of Compromise (IOCs) and Indicators of Attack (IOAs) in a proactive and responsive manner. This acquired intelligence becomes a potent weapon in the cyber security arsenal, allowing organizations to leverage the latest data from threat intelligence which can prevent the organization from the Advanced Persistent Threats (APTs).

- Participants will learn how to stay updated on the latest threats and vulnerabilities and acquire the skills to collect and utilize Indicators of Compromise (IOCs) and Indicators of Attack (IOAs). By leveraging threat intelligence feeds, they can proactively identify and mitigate potential security risks, helping organizations stay one step ahead of Advanced Persistent Threats (APTs) and other security challenges.

- In conclusion, a comprehensive SOC analyst training course with a strong focus on real-world scenarios, hands-on experience including threat intelligence, information security and vulnerability assessment can be an valuable resource for individuals. It equips them with the knowledge and tools needed to excel in the rapidly evolving field of security operations.

CYBERTECH DEFENDER
Let's Defend the World Together !

# Learning objectives of this course

## I.Introduction to Cyber security and SOC Operations

- Understanding the role of a SOC Analyst and responsibilities
- Cyber security fundamentals with respective to the tools
- Overview of SOC structure and operations
- Incident response process and Lifecycle

## II. Networking and Network Security

- TCP/IP fundamentals and Network protocols and services
- IP Internet Protocol and classification of IP Address
- Ranges of protocols
- Network segmentation and zoning
- Firewall and IDS/IPS technologies
- VPNs and secure communication

## III. Operating Systems and Endpoint Security

- ·Endpoint protection solutions
- ·Malware types and attacks analysis
- ·Patch management and vulnerability assessment
- Host-based security controls

## IV. Threat Intelligence and Research

- Cyber threat landscape
- Threat actors and their motives
- Open-source intelligence (OSINT)
- Threat feeds and indicators of compromise (IOC)
- Analysis of historical attacks

## V. Security Information and Event Management (SIEM)

- SIEM architecture and components
- Log collection and correlation
- Rule creation and customization
- Incident investigation using  different SIEM tools
- Reporting and alerting and root cause analysis

## VI. Incident Detection and Analysis

- Identifying anomalies and potential threats
- Signature-based and behavior-based detection
- Triage and prioritization of incidents
- Malware analysis and reverse engineering

CYBERTECH DEFENDER
Let's Defend the World Together !

# Learning objectives of this course

## VII. Incident Response and Mitigation

- Security Tools and Technologies
- Malware analysis and Ransomware analysis
- Incident handling lifecycle
- Containment and eradication of threats
- Communication and coordination during incidents with concern teams
- Documentation and lessons learned and post-incident reviews

## VIII. Security Tools and Technologies

- Antivirus and anti-malware tools
- Intrusion detection and prevention systems (IDS/IPS)
- Vulnerability assessment tools
- Data loss prevention (DLP)

## IX. Security Best Practices

- Security policies and procedures
- Encryption and data protection
- Security awareness and training
- Compliance and regulatory requirements with different frameworks

## X. Communication and Collaboration

- Effective communication skills
- Teamwork and collaboration within a SOC
- Interactions with other IT and security teams
- Reporting to management and stakeholders

## XI. Continuous Learning and Professional Development

- Staying updated with the latest threats and technologies
- Career advancement and specialization opportunities
- Networking and participating in cyber security communities

## XII. Practical Labs and Hands-on Experience

- Real-world scenarios and simulations
- Hands-on experience with security tools and technologies
- Creating and analyzing incident cases
- Building and configuring security systems

## XIII. Mock interviews

- Conducting mock interviews and enhancing interviewer performance is a valuable service, particularly for job seekers looking to improve their interview skills.

CYBERTECH DEFENDER
Let's Defend the World Together !

# FAQ

## 1. What is a SOC Analyst?

A SOC Analyst is a cybersecurity professional responsible for monitoring, detecting, analyzing, and responding to security incidents within an organization's network. They play a crucial role in maintaining the security posture of an organization by identifying and mitigating threats.

## 2. What will I learn in this SOC Analyst course?

Our SOC Analyst course covers a range of topics including:

- Understanding cybersecurity fundamentals
- Network security protocols and technologies
- Security information and event management (SIEM) tools
- Incident response and handling techniques
- Threat intelligence analysis
- Vulnerability assessment and management
- Forensic analysis and investigations

## 3. What prerequisites are required to enroll in the course?

While there are no strict prerequisites, a basic understanding of networking concepts and familiarity with operating systems would be beneficial. This course is designed for individuals looking to start or advance their career in cyber security.

## 5. Will I receive any certification upon completion?

Upon successfully completing the course, you will receive a certificate of completion. Additionally, some courses offer preparation materials for industry-standard certifications such as CompTIA Security+, Certified SOC Analyst (CSA+), or GIAC Certified Incident Handler (GCIH), which can be pursued separately.

## 6. How is the course delivered?

The course is delivered through a combination of lectures, practical hands-on labs, case studies, and simulations. You can access course materials online through our learning platform at your convenience.

## 7. What kind of job roles can I expect after completing this course?

After completing the SOC Analyst course, you can pursue roles such as SOC Analyst, Security Analyst, Incident Responder, Threat Analyst, or Security Operations Center (SOC) Engineer in various industries.

## 8. Will I have access to any career support or job placement assistance?

While direct job placement is not guaranteed, we provide career guidance, resume building tips, interview preparation, and access to job boards or networking opportunities within the cybersecurity field.

CYBERTECH DEFENDER
Let's Defend the World Together !

# FAQ

## 9. Can I study at my own pace?

Yes, the course is self-paced, allowing you to study according to your schedule. However, it is recommended to follow the suggested timeline to ensure timely completion.

## 10. How do I enroll in the course?

You can enroll by visiting our website, selecting the SOC Analyst course, and following the enrollment instructions provided. If you have further queries, feel free to contact our support team.

## 11. What sets this SOC Analyst course apart from others available in the market?

Our SOC Analyst course stands out due to its comprehensive curriculum developed by industry experts, hands-on practical labs, real-world simulations, and an emphasis on the latest cybersecurity trends and technologies. Additionally, we offer personalized mentorship and support throughout the learning journey.

## 12. Are there any prerequisites for the labs or simulations in the course?

No prerequisites are needed for the labs and simulations. The course provides step-by-step guidance to ensure learners can engage effectively with the practical components regardless of their prior experience.

## 13. Can I interact with instructors or seek clarification during the course?

Yes, our course includes avenues for interaction with instructors, either through live sessions, discussion forums, or dedicated Q&A sessions. Additionally, we provide email support to address any queries or clarifications you might have during the learning process.

## 14. How current is the course content in relation to evolving cybersecurity threats?

We continuously update our course content to reflect the latest cybersecurity threats, trends, and industry best practices. We strive to ensure that learners are equipped with the most relevant and up-to-date information to tackle contemporary security challenges.

## 15. Will I gain practical experience that is applicable to real-world scenarios?

Absolutely, our course emphasizes practical learning. You'll work on simulated environments mirroring real-world scenarios encountered by SOC Analysts. These exercises prepare you to handle actual incidents and threats effectively in a professional setting.

CYBERTECH DEFENDER
Let's Defend the World Together !

# FAQ

## 16. Can I access course materials after completing the program?

Yes, upon completing the course, you'll retain access to the course materials for a specified period, allowing you to review the content and stay updated with any new additions or changes.

## 17. Is there a community or networking platform associated with the course?

Yes, we offer access to a community platform where learners can engage with peers, share knowledge, discuss relevant topics, and potentially collaborate on projects. Networking opportunities within the cybersecurity field are also facilitated through this platform.

## 18. Are there any opportunities for practical internships or work placements?

While we do not directly provide internships or work placements, we offer guidance on seeking internships and provide resources to aid in securing practical experience within the cybersecurity domain.

## 20. Is financial aid or payment plans available for the course?

We offer various payment options, including installment plans and potential financial aid options. Please contact our support team for further information on available payment arrangements

CYBERTECH DEFENDER

Let's Defend the World Together !

Don't just dream about a career in cybersecurity – make it a reality. Join our training program in CyberTechDefender and set yourself up for success!

## Contact us

Info@cybertechdefender.com
+919494969524