CLOUD VISION TECHNOLOGIES

Cyber Security

The Best Training Institute in Hyderabad

+91 8520002606 www.cloudvisiontechnologies.com
#Samhitha Enclave, 3rd Floor, KPHB Phase 9, Kukatpally, Hyderabad, Telangana - 500072

Cyber Security

About Us

We At Cloud vision Technologies, 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.

Learning objectives of this course

1. 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

2. 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

3. Operating Systems and Endpoint Security

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

4. 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

5. 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

6. 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

7. 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

8. Security Tools and Technologies

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

9. Security Best Practices

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

10. Communication and Collaboration

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

11. 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

12. 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

13. Mock interviews

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

Modules

1. Basic concepts of Networking and Cyber security
2. Understanding on different types of malwares and attacks
3. Incident handling with Security Information and Event Management (SIEM)
4. Analysing and performing Root cause analysis on True postive incidents
5. DLP, Threat Intelligence,IOC, IOA and frameworks
6. Incident Response cycle and vulnerability assesment

Hands On Tools

- SIEM : IBM Qradar, Splunk, Azure sentinel
- EDR : Xcitium verdict EDR
- Antivirus : Mcafee
- Vulnerability Tool : Rapid 7 Insight VM
- Ticketing Tool : Servicenow

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.

4. 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 sepately.

5. 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.

6. 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

7. 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 cyber security field.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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

14. 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.

15. 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.

16. 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.

17. 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.

18. 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

CLOUD VISION TECHNOLOGIES

+91 8520002606 www.cloudvisiontechnologies.com

#Samhitha Enclave, 3rd Floor, KPHB Phase 9, Kukatpally, Hyderabad, Telangana - 500085