SOC Analyst Mastery: Incident Response & Digital Forensics Training Course

Ref: #CYB1840

Course Introduction / Overview:

This comprehensive training course is designed to provide aspiring and current Security Operations Center (SOC) analysts with the real-world skills needed to detect, analyze, and respond to cyber threats. The SOC is the front line of an organization’s cybersecurity defense. This program goes beyond a theoretical overview to focus on the practical, hands-on tasks performed daily by an analyst. Participants will learn how to use a Security Information and Event Management (SIEM) system to monitor alerts, perform threat hunting, and conduct a basic digital forensic analysis. We will cover key topics like incident triage, malware analysis, and the documentation needed for a successful incident response. Drawing from the academic research of renowned authors like David J. Stang and his work in his book "Digital Forensics for the Cyber Analyst," this program provides a strategic and practical framework for ensuring a rapid and effective response to security incidents. His work highlights the importance of a structured approach to investigations, ensuring no critical evidence is missed. This course at BIG BEN Training Center will empower you to become a highly effective and a confident SOC analyst who can make a real difference in protecting your organization.

Target Audience / This training course is suitable for:

- Security Operations Center (SOC) analysts.
- Cybersecurity analysts.
- Incident response team members.
- Threat hunters.
- IT administrators.
- Digital forensics investigators.
- Security engineers.

Target Sectors and Industries:

- Managed Security Service Providers (MSSPs).
- Financial services.
- Technology and software.
- Government agencies and equivalents.
- Telecommunications.
- Healthcare.
- Global corporations.

Target Organizations Departments:

- Security Operations Center (SOC).
- Information Security.
- IT.
- Incident Response.
- Threat Intelligence.
- IT Audit.
- Digital Forensics.

Course Offerings:

By the end of this course, the participants will have able to:

- Triage and analyze security alerts.
- Perform threat hunting using a SIEM.
- Conduct a basic digital forensics investigation.
- Develop a comprehensive incident response plan.
- Analyze malware and other malicious artifacts.
- Communicate security incidents to stakeholders.
- Document all steps of an incident response.

Course Methodology:

This training course at BIG BEN Training Center uses a highly practical, lab-intensive methodology that simulates the day-to-day work of a SOC analyst. The program includes a series of virtual labs where participants will work with a simulated SIEM environment to analyze real-world attack scenarios. You will learn to use industry-standard tools for log analysis, network traffic analysis, and malware investigation. The course emphasizes a structured approach to incident response. It teaches you how to quickly triage a high-priority alert, contain a threat, and begin the recovery process. The instructor will provide expert guidance and feedback throughout the labs, ensuring that you develop the critical thinking and problem-solving skills required for high-stakes security operations roles. This approach ensures the knowledge and skills gained are directly applicable to the front lines of cybersecurity.

Course Agenda (Course Units):

Unit One: The Role of a SOC Analyst

- Introduction to the SOC.
- The incident responded to the lifecycle.
- The tools of a SOC analyst.
- Understanding alerts and logs.
- Triage and prioritization.
- Threat intelligence integration.
- Case study: a phishing attack.

Unit Two: Incident Triage and Analysis

- Analyzing network traffic.
- Investigating suspicious files.
- Understanding common attack techniques.
- The pyramid of pain.
- Log analysis and correlation.
- The role of threat hunting.
- Practical lab: a log analysis exercise.

Unit Three: Digital Forensics Fundamentals

- The digital forensics process.
- Collecting and preserving evidence.
- Analyzing a compromised host.
- Memory and disk analysis.
- Forensic readiness.
- Chain of custody.
- Practical lab: a disk image analysis.

Unit Four: Incident Response and Communication

- Developing an incident response plan.
- Containment and eradication.
- Recovery and post-incident activities.
- Communicating with stakeholders.
- Creating an incident report.
- Working with law enforcement.
- Tabletop exercise: a simulated incident.

Unit Five: The Future of the SOC

- Security automation and orchestration.
- Threat intelligence platforms.
- The role of AI in the SOC.
- Proactive threat hunting.
- Career paths for SOC analysts.
- Final project: a comprehensive incident report.
- Continuous learning.
- Frequently Asked Questions:

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

While a SOC analyst must focus on the immediate detection and response to a security incident, how can they also effectively contribute to long-term improvements in the organization's security posture?

What unique qualities does this course offer compared to other courses?

This course stands out by providing a unique and vital focus on the practical, day-to-day skills of a SOC analyst. Unlike many certification-focused programs that offer only a broad overview, this course is designed to make you a more effective and confident analyst on your very first day on the job. The curriculum is built around hands-on, real-world labs and simulated attack scenarios. It teaches you to use the same tools and methodologies as a professional SOC analyst to analyze alerts, hunt for threats, and respond to incidents. The emphasis on practical skills, incident response, and digital forensics distinguishes this course from others. It is for professionals who are ready to work on the front lines of cybersecurity defense.