

PREREQUISITES & QUALIFICATIONS

Qualification

- Undergraduate degree in Computer Science or relevant field (Preferred)
- High school Diploma

Technical Knowledge

- Fundamental IT knowledge (computer networks, operating systems, software applications, etc.)
- Introductory Programming Skills

Skills and Attributes

- Analytical & Problem-Solving Skills
- Report Writing Skills
- Communication Skills
- Eagerness to Learn

TRAINER'S EXPERIENCE & ACCOMPLISHMENTS




- MSc Information Security
- 15 years of consultant & training experience in government, Military & Private Organisations
- Certified CISSP, CYSA+, SANS SEC560, OSCP, OWSP, CEHV11, and ISO27001 Auditor
- Speaker at various international conferences & workshops with over 15 research articles in renowned journals and conferences

TRAINING DURATION:
12 WEEKS
SAT/SUN 4HRS/DAY

ORIENTATION: **JULY 20, 2024**
START DATE: **AUGUST 03, 2024**
END DATE: **OCTOBER 27, 2024**

ABOUT US

Next Generation Trainings (NGT) is affiliated with NGT Solutions

-  www.ngt.training
-  Info@ngt.training
-  1 (848) 242-4142

04



NEXT GEN IT
NEXT GENERATION TRAININGS

CYBER SECURITY ANALYST TRAINING PROGRAM

Master the Art of Cyber Defense: Become a Cyber Security Analyst!

For Enrollment

Email: Info@ngt.training
Phone: 1 (848) 242-4142

For Orientation

01

WHY CHOOSE THIS PROGRAM?



- 01 Hands-on training led by highly qualified trainers
- 02 Real-life security events and incidents triaging - learn what actually happens at work in the analyst's day-to-day life
- 03 Program enriched by guest lecturers from successful CISOs in the industry
- 04 Cybersecurity Analysts earn a lucrative six-figure income for their skills and expertise
- 05 The demand for Security Analysts is soaring due to the rise in cyberattacks and a shortage of skilled professionals
- 06 No prior experience is needed

ROLE DESCRIPTION

A Cyber Security Analyst is responsible for safeguarding an organization's information systems and networks against cyber-attacks. This role involves monitoring, detecting, analyzing, and responding to security incidents. The Cyber Security Analyst collaborates closely with IT teams and other departments to implement and maintain security measures, ensuring the protection of sensitive data and the confidentiality, integrity, and availability of information systems.

WHAT YOU WILL LEARN



Our curriculum, featuring practical, high-quality hands-on exercises, covers the most comprehensive array of topics and tools, led by highly experienced industry cyber professionals.

- 01 **CYBERSECURITY LANDSCAPE**
Understand core concepts foundational to security, networks, information systems, and compliance
- 02 **ANALYST TOOLS**
Learn about cybersecurity tools, including data protection, endpoint protection, SIEM, firewalls, and intrusion detection systems
- 03 **VULNERABILITY ASSESSMENTS**
Conduct and analyze vulnerability assessments, prioritize vulnerabilities, and recommend mitigation strategies
- 04 **INCIDENT RESPONSE & FORENSICS**
Develop skills in incident response and forensics through real-world cybersecurity case studies
- 05 **INCIDENT DOCUMENTATION**
Learn to document and escalate incidents that may have immediate or ongoing impacts
- 06 **HANDS-ON SECURITY TOOLS**
Gain experience with industry-specific and open-source security tools, enabling you to apply various cybersecurity techniques effectively

Upon successful completion of the course, candidates will be considered for job placement opportunities, including CYSA+ certification, job search, resume building, mock interviews, and networking strategies.