CAREER PATHWAYS

Cyber Security Analyst Pathway

Program Prerequisites

High School Diploma and basic computer knowledge

Program Goal

The Cyber Security Analyst program is a highly technical program with a cohesive and progressive set of learning outcomes. Geared towards IT individuals desiring to gain security analyst skills, the program emphasizes a hands-on guide to identify, eliminate and protect against threats. The training focuses on the student's capability to discover, analyze and understand the implications of information security vulnerabilities in systems/networks/applications in order to identify solutions before others exploit these flaws. Taught by top experts in the field, students gain advanced skills and knowledge, along with experience regarding the available methodologies, tools and techniques, which are required to perform comprehensive information security penetration tests. Armed with a deep understanding of the offensive techniques used by malicious agents seeking to breach information security defenses, the professional who earns the Cyber Security Analyst Diploma will be empowered to identify and help remediate these vulnerabilities.

Educational Objectives

The Cyber Security Analyst program provides a path for professionals to specialize in a sub-area of the information security field, and this progression of courses would prepare them for a career in cyber security. Over the course of this program, students will be able to:

- Conduct vulnerability scanning and exploitation of various systems using a careful and documented methodology.
- Provide explicit proof of the extent and nature of IT infrastructure risks.
- Conduct threat hunting according to well-defined rules of engagement and a clear scope.
- Document activities performed during testing, including all exploited vulnerabilities and how those vulnerabilities were combined into attacks to demonstrate business risk.
- Produce an estimated risk level for a given discovered flaw by using the amount of effort the team needs to expend in penetrating the information system.
- Provide actionable results with information about possible remediation measures for the successful attacks performed.

Core Courses

CompTIA Security+ |
72 hours

Certified Ethical Hacker (CEH) |
72 hours

Total Cyber Security Analyst Pathway Clock Hours | 144

Contact Us

(571) 577-7890
(703) 554-3827
www.intellectualpoint.com
info@intellectualpoint.com

EXCELLENCE
THROUGH
EDUCATION

Intellectual
POINT

intellectualpoint.com/

Learning Outcomes

Over the course of this program, graduates will be able to:

- Set up access control lists, assessments and audits for network security and systems security
- Follow the best practices to encrypt data using PKI and hash passwords using SHA and MD5
- Utilize SIEM tools for threat management and cyber incident response
- Detect Malware Threats, Sniffing, Social Engineering, Denial-of-Service
- Implement policies for security and network management to identify and mitigate risks
- Analyzing, Calculating, Formatting Results
- Develop Charts and Dashboards in Tableau
- Introduction to Splunk Enterprise Security App

Professional Objectives

- SOC (Security Operations Center) Analyst
- Cyber Security Analyst
- Incident Responder
- Pen Tester
- Computer Security Specialist
- Application Support Analyst

Core Courses

- ISA 1002 CompTIA Security+| 72 hours
- ISA 1005 Certified Ethical Hacker (CEH) | 72 hours
- **Total Cyber Security Analyst Pathway Clock Hours | 144**

intellectualpoint.com/

Contact Us

(571) 577-7890
(703) 554-3827
www.intellectualpoint.com
info@intellectualpoint.com

46175 West Lake Drive
Suite 250/240
Sterling, VA 20165

Be Social With Us!

State Council of Higher Education for Virginia

EXCELLENCE THROUGH EDUCATION
Intellectual Point