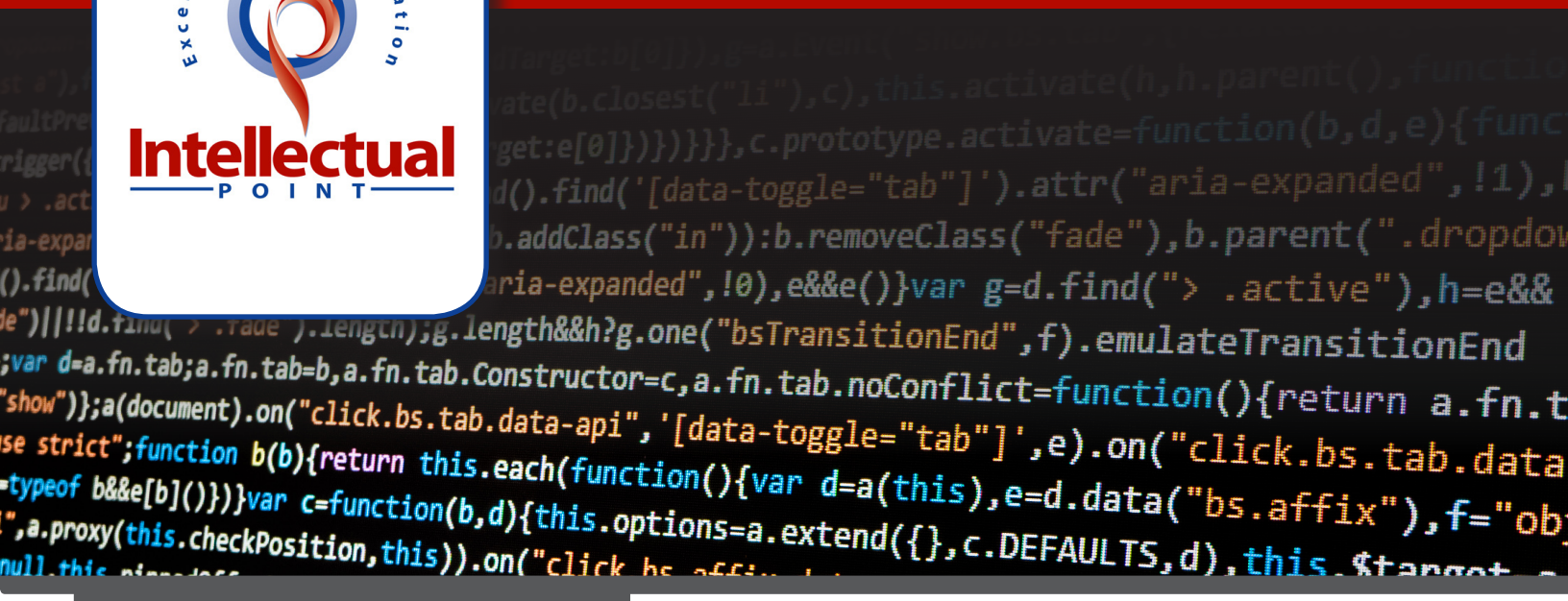
Real Training. Real Practice. Real Results.



Cyber Security Analyst

Prerequisites

Students are required to have at least five years of experience in cybersecurity management/analysis. A four-year degree from an accredited university is recommended although not required.

Program Goals

The Cyber Security Analyst Program is a highly technical 264 clock-hour 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 post-baccalaureate certificate will be empowered to identify and help remediate these vulnerabilities.

Intellectual POINT

Real Training. Real Practice. Real Results.

Professional 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 Cybersecurity. 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.
- Determine a risk level as an indicator of the penetration resistance of the system.
- Provide actionable results with information about possible remediation measures for the successful attacks performed. Please note the Course Curriculum details that follow (bottom left).

Curriculum:

- **ISA 1002:** Introduction to Cyber Security | 48 hours
- **NET 1003:** Introduction to Routing & Switching | 40 hours
- **BUS 1001:** Introduction to ITIL® | 24 hours
- **NET 1006:** Introduction to Linux | 40 hours
- **CLO 1001:** Introduction to Cloud Computing | 40 hours
- **ISA 1003:** Cyber Security Analyst | 40 hours
- **ISA 1005:** Introduction to Ethical Hacking | 40 hours
- **ISA 1006:** Advanced Information Systems Security | 40 hours
- **Total Program Clock Hours | 312**

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 the data using PKI and hash passwords using SHA and MD5
- Utilize SIEM tools for threat management and cyber incident response
- Perform operations of the TCP/IP protocol suite, IPv4/IPv6 addressing, IP subnetting and NAT
- Configure a router interface parameters for Ethernet, leased WAN, frame relay, ISDN and ATM
- Implement policies for security and network management to identify and mitigate risks
- Use Cisco tools like trace and debug to manage the network infrastructure

11321 Sunset Hills Road, Reston, VA 20190 • 571-577-7890
info@intellectualpoint.com • www.IntellectualPoint.com