CAREER PATHWAYS

DevOps Pathway

Core Courses
CompTIA Security+ |
72 hours

Certified Ethical Hacker (CEH) |
72 hours

Splunk Core Certified User |
72 hours

**Total DevOps Pathway
Clock Hours | 216**

_____

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

_____

Intellectual
P O I N T

EXCELLENCE
THROUGH
EDUCATION

Program Prerequisites

Basic Knowledge of Information Technology.

Program Goal

The DevOps Pathway is designed to impart students how to select, design, implement, operate, and maintain cyber security controls and make sure there are enough defenses in place to keep their organization safe. This pathway imparts the students with both conceptual and hands-on skills to understand the cyber security challenges in the areas of Development and Operations (DevOps) and how to implement the appropriate end-to-end security controls throughout the entire infrastructure. It also teaches the students how they can try to predict any possible attack and put up enough barriers to prevent them as well as the best practices to monitor any suspicious activity and detect if any cyber intruders could pass through the network defenses they created. This pathway ensures that the holder has a practical understanding of the phases of ethical hacking, the various attack vectors, and the preventative countermeasures used by ethical hackers. It certifies that the holder knows how to think and act like a malicious hacker to better position your organization's information security measures and defend against real-world attacks. It is premised on the idea that if you understand vulnerabilities and system weaknesses your organization faces, you can better strengthen system security controls in the face of malicious activity and attacks. This pathway is designed to teach you the fundamental skills and knowledge needed to use Splunk software to search, analyze, and visualize data stored in your organization's systems. This pathway will teach concepts such as indexing, searching, and reporting. We will cover creating and modifying simple reports and dashboards, Splunk's data input and management options, and use Splunk's visualization options. This pathway imparts hands-on skills in the areas of the latest operating systems, tools, tactics, exploits, and technologies, and is reflective of the most current threats and preventative countermeasures.

Educational Objectives

This program is designed to provide the necessary education and hands-on expertise needed to build the DevOps vocabulary and to understand its principles and practices. During the course of the program, students will be able to:

- Gain an in-depth understanding of Cyber Security Controls and Objectives.
- Apply appropriate cyber security policies and controls to protect against cyber attacks.
- Carry out vulnerability assessments, penetration testing and risk assessment.
- Improve the cyber security posture of the organization by implementing controls.
- Apply the Splunk SIEM tool skills for incident response and threat hunting.
- Anaylze the log data and be able to visualize, stop and respond to cyber breaches and emerging threats targeting the organization.

Learning Outcomes

Upon completion of the DevOps Program, graduates will be able to:

- Learn the fundamentals of cyber security including Confidentiality & Integrity.
- Learn the fundamentals of Ethical Hacking, Scanning and Penetration Testing.
- Learn how to secure the Development and Operations (DevOps) functions with cyber security controls.
- Learn how to carry out vulnerability assessments for various systems and devices.
- Learn how to monitor notable events and respond to incidents and carry out forensic analysis in systems that have been breached.
- Learn how to create visualizations, dashboards and alerts using Splunk SIEM tool.
- Learn how to strengthen the systems, devices and IT infrastructure and protect them against cyber attacks.

Professional Objectives & Job Titles

- Cyber Security Analyst
- Security Architect
- SOC Analyst
- Splunk Administrator
- Incident Responder

- DevSecOps Systems Administrator
- Help Desk / Tier 1 Tech Support
- Jr. Penetration Tester
- Red Team / Blue Team Analyst

Be Social With Us!

Core Courses

- CompTIA Security+ | 72 hours
- Certified Ethical Hacker (CEH) | 72 hours
- Splunk Core Certified User | 72 hours
- **Total DevOps Career Pathway Clock Hours | 216**

State Council of Higher Education for Virginia

EXCELLENCE THROUGH EDUCATION

Intellectual
P O I N T

intellectualpoint.com/