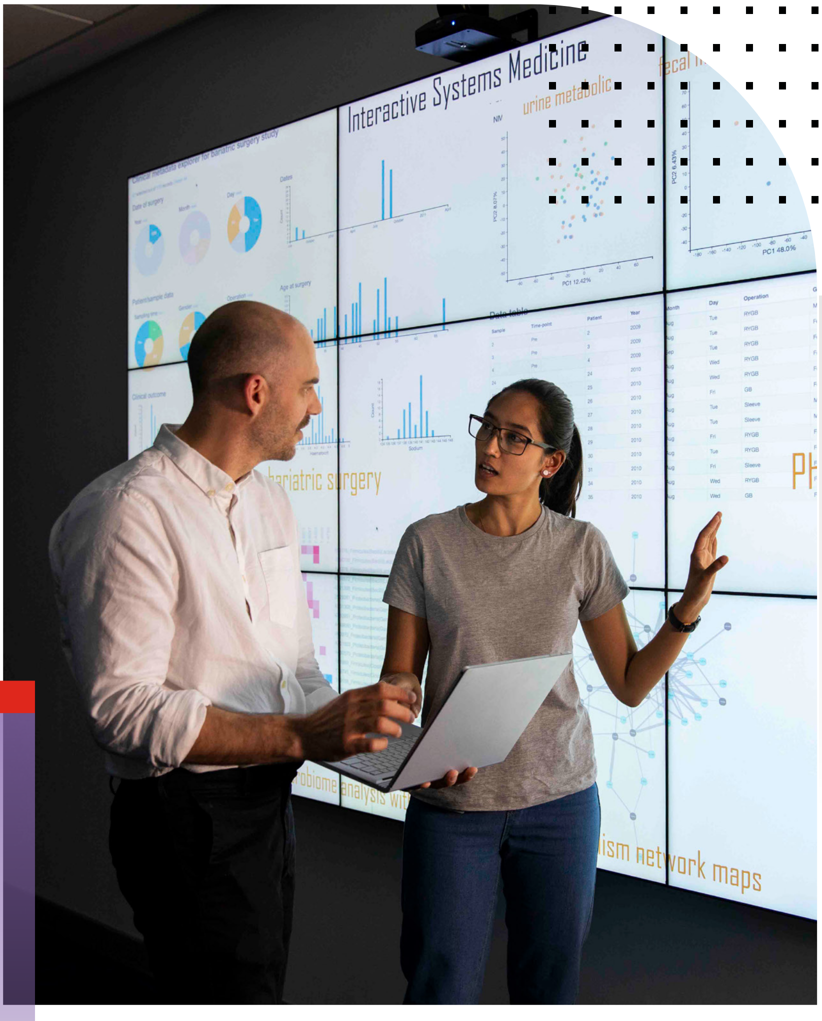
FORTINET
NSE Training Institute

EDUCATION PATHWAY

Security Operations



NSE Training Institute

The purpose of NSE Training Institute education pathways is to create a career map through Fortinet's NSE Training Institute learning. Allowing individuals to navigate their educational journey from curriculum to careers.

This education pathway focuses on Security Operations and the potential job opportunities that exist around the technology.

Security Operations

Fortinet utilizes artificial intelligence (AI) of varying types, in various locations for complementary purposes. From the global threat intelligence in our FortiGuard Labs, to inline security controls deployed throughout the organization, and centralized advanced threat detection and response in the SOC. Advanced analytics help your security solutions and teams keep pace with an accelerating threat landscape.

NIST/NICE Cybersecurity Workforce Framework

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), published by the National Institute of Standards and Technology (NIST) in NIST Special Publication 800-181, is a nationally focused resource that establishes a taxonomy and common lexicon to describe cybersecurity work, and workers, regardless of where, or for whom, the work is performed.

NICE Cybersecurity Workforce Framework—Work Roles

Work Roles act as the most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks. Work Roles are not specific job titles.

Fortinet's NSE Training Institute's Security Operations education pathway aligns to the below NICE Cybersecurity Workforce work roles.

Certifications

	NSE4	NSE5	NSE7
All-Source Analyst (AN-ASA-001)		X	
Information Systems Security Developer (SP-SYS-001)	X		
Product Support Manager (OV-PMA-003)	X		
Information Systems Security Manager (OV-MGT-001)	X		
Database Administrator (OM-DTA-001)		X	
Cyber Operator (CO-OPS-001)		X	
Cyber Crime Investigator (IN-INV-001)		X	
Cyber Defense Forensics Analyst (IN-FOR-002)		X	
Systems Developer (SP-SYS-002)	X		
Vulnerability Assessment Analyst (PR-VAM-001)	X		
Technical Support Specialist (OM-STS-001)	X		
Cyber Defense Analyst (PR-CDA-001)		X	
Cyber Defense Incident Responder (PR-CIR-001)		X	
Threat/Warning Analyst (AN-TWA-001)			X
Cyber Defense Infrastructure Support Specialist (PR-INF-001)	X		
Systems Requirements Planner (SP-SRP-001)	X		

The Network Security Expert (NSE) Certification Program is an eight-level program that is designed to provide individuals with cybersecurity career skills and experiences.

The NSE program includes a wide range of courses that allow individuals to demonstrate mastery of complex cybersecurity concepts.

Security Operations Courses

Security Operations courses are organized to give individuals the ability to develop the skills necessary to have a career in Security Operations. Mapped to the NICE Framework job roles, each course below provides an individual with another skill/ability to progress in their career.

NSE 4: The Network Security Professional

- FortiGate Security
- FortiGate Infrastructure

NSE 5: The Fortinet Network Security Analyst

- FortiAnalyzer
- FortiSIEM

NSE 7: The Network Security Architect

- Advanced Threat Protection
- FortiSOAR Design and Development

NSE 4 FortiGate Security *24 content hours* *NSE 4*	**In this course, participants will learn how to use basic FortiGate features, including security profiles.** Participants will explore firewall policies, security fabric, user authentication, secure sockets layer virtual private network (SSL VPN), antivirus, web filtering, application control, and more. These administration fundamentals will provide participants with a solid understanding of how to implement basic network security.
FortiGate Infrastructure *16 hours* *NSE 4*	**In this course, participants will learn how to use advanced FortiGate networking and security.** Topics include features commonly applied in complex or larger enterprise or managed security service providers (MSSP) networks, such as advanced routing, transparent mode, redundant infrastructure, site-to-site IPsec VPN, single sign-on (SSO), web proxy, and diagnostics.

NSE 5 FortiAnalyzer *16 hours* *NSE 5*	**In this class, participants will learn the fundamentals of using FortiAnalyzer for centralized logging and reporting. Students will learn how to configure and deploy FortiAnalyzer, and identify threats and attack patterns through logging, analysis, and reporting. Finally, students will examine some helpful troubleshooting techniques.** Participants will explore administration and management; register devices for log collection with FortiAnalyzer; use FortiAnalyzer to centrally collect logs; perform a forensic analysis of logs based on simulated network attacks; create reports; and explore solutions to common misconfiguration issues.
FortiSIEM *24 hours* *NSE 5*	**In this course, participants will learn how to use FortiSIEM, and how to integrate FortiSIEM into your network awareness infrastructure.** Participants will learn about initial configurations, architecture, and the discovery of devices on the network. Participants will also learn how to collect performance information and aggregate it with syslog data to enrich the overall view of the health of the environment. Additionally, participants will learn how you can use the configuration database to greatly facilitate compliance audits.
NSE 7 Advanced Analytics *24 hours* *NSE 7*	**In this three-day course, participants will learn how to use FortiSIEM in a multi-tenant environment.** Participants will learn to add various organizations to FortiSIEM and discover devices from each organization. They will learn to differentiate logs and events from each organization and apply appropriate rules. They will dive deep into rules and their architecture and will also learn about incidents and how they are generated when a rule is triggered. Participants will also dive deep into baseline calculations performed on FortiSIEM and learn to create their own baseline profile and run queries based on the profile.
FortiSOAR Design and Development *24 content hours* *NSE 7*	**In this interactive course, participants will learn how to use FortiSOAR to design simple to complex playbooks.** Participants will learn to create dashboards using various built-in widgets, and install widgets from the widget library. They will review the dashboards that are built-in to FortiSOAR and learn to edit them according to their requirements. They will explore the role of FortiSOAR in mitigating malicious indicators and creating interactive dashboards to display relevant information about alerts and incidents.

Security Operations Workshops

AI-based Threat Prevention and Detection With FortiDeceptor

To protect an enterprise against sophisticated threats, it is important to establish a comprehensive and cohesive security infrastructure that is broad enough to cover all attack vectors, powerful enough to run the latest security technologies, and automated to keep pace with it.

Detecting Zero Day Threats With FortiSandbox

In this workshop, participants learn how to protect an enterprise against sophisticated threats by establishing a comprehensive and cohesive security infrastructure that is broad enough to cover all attack vectors, powerful enough to run the latest security technologies, and automated to keep pace with fast-moving environments.

Empowering Security Operations Leveraging FortiSOAR

FortiSOAR is a holistic and enterprise-built security orchestration and security automation workbench that empowers security operation teams. FortiSOAR increases a team's effectiveness by increasing efficiency, allowing for response in near real time.

In this workshop, participants learn how:

- **Powerful Security Information and Event Management With FortiSIEM**

  FortiSOAR is a holistic and enterprise-built security orchestration and security automation workbench that empowers security operation teams. FortiSOAR increases a team's effectiveness by increasing efficiency, allowing for response in near real time.

- **Simplify SOC Operations for the Security Fabric With FortiAnalyzer**

  Security teams around the world are struggling with the complexity of operations. Common issues include: too many consoles, too many alerts, manual and slow response, and shortage of cybersecurity personnel.

Fortinet Company Overview

Fortinet (NASDAQ: FTNT) secures top Fortune 100 enterprises, leading service providers, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface, enabling them to meet the ever-increasing performance requirements of the borderless network both today and into the future.

Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments.

Fortinet ranks #1 in the most security appliances shipped worldwide, and provides the broadest protection on the market from IoT to the cloud. As the leading security innovator, Fortinet holds more patents than any other vendor. More than 385,000 customers trust Fortinet to protect their businesses with the Fortinet Security Fabric.

Learn more at Fortinet.com, FortiGuard Labs, NSE Certification Program, NSE Training Institute, or the Veterans Program.

FORTINET.
NSE Training Institute

www.fortinet.com

July 16, 2021 9:25 PM
773602-B-0-EN