EDUCATION PATHWAY

Security Operations
**Training Institute**

The purpose of Education Pathways is to create a career map through Fortinet's 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.

**Workforce Framework for Cybersecurity (NICE Framework)**

The National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (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 common lexicon to describe cybersecurity work, and workers, regardless of where, or for whom, the work is performed.

**NICE 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 Training Institute courses and exams for the Security Operations education pathway align to the following NICE Framework Work Roles.

<table>
<thead>
<tr>
<th>Work Role</th>
<th>Introduction to the Threat Landscape</th>
<th>Technical Introduction to Cybersecurity</th>
<th>FortiGate Operator</th>
<th>FortiGate Security</th>
<th>FortiGate Infrastructure</th>
<th>FortiAnalyzer Analyst</th>
<th>FortiSEIM</th>
<th>FortISOAR</th>
<th>FortIEDR</th>
<th>Advanced Analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Defense Analyst</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PR-CDA-001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Defense Incident Responder</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PR-CIR-001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Defense Infrastructure Support Specialist</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PR-INF-001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Operations Specialist</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>OM-NET-001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Architect</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SP-ARC-002</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Administrator</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>OM-ADM-001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical Support Specialist</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>OM-STS-001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat/ Warning Analyst</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>AN-TWA-001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NSE Certifications

Below is a list of all the NSE certifications along with requirements to achieve your certification. Click on the “Learn More” links to access the self-paced courses and see detailed information on requirements, prerequisites, recertification, duration of courses and labs, class schedules and more.

Fortinet Certified Fundamentals in Cybersecurity  Learn More

The Fortinet Certified Fundamentals (FCF) in Cybersecurity certification validates that you have mastered the technical skills and knowledge that are required for any entry-level job role in cybersecurity. This curriculum will offer courses that cover today's threat landscape and the fundamentals of cybersecurity.

Candidates must successfully complete the core course and one elective course. This certification is valid for two years from completion of the second course.
CORE COURSE

Introduction to the Threat Landscape  Learn More
In this course, candidates will learn about the cyberthreat landscape. This landscape includes the threats that endanger computer networks, the cast of bad actors who are behind these threats, and the cybersecurity first principles that, if followed, can keep you and your computer network safe.

ELECTIVE COURSES

Getting Started in Cybersecurity  Learn More
This course is ideal for individuals in non-technical job positions that require a high-level understanding of the most important technical fundamentals of cybersecurity. Examples of those job roles are security product salespeople and company CEOs.

Technical Introduction to Cybersecurity  Learn More
This course is ideal for individuals in technical roles that require a more in-depth understanding of the fundamentals of cybersecurity. This course is also ideal for people that want to pursue a technical job in cybersecurity.

Fortinet Certified Associate in Cybersecurity  Learn More
The Fortinet Certified Associate (FCA) in Cybersecurity certification validates your ability to execute high-level operations on a FortiGate device. This curriculum covers the fundamentals of operating the most common FortiGate features.

There is one certification within the FCA level. To achieve this certification, candidates must complete the FortiGate Operator course and pass the exam. The FCA certification is valid for two years from the date of passing the FortiGate Operator exam.

FortiGate Operator  Learn More
In this course, candidates will learn how to harden the security of your network by using the most common FortiGate features. Through demos and interactive simulations, you will learn how to perform basic operation tasks on FortiGate.

Fortinet Certified Professional in Security Operations  Learn More
The Fortinet Certified Professional (FCP) in Security Operations certification validates your ability to secure networks and applications by deploying, managing, and monitoring Fortinet security operations products. This curriculum will cover the day-to-day tasks related to Fortinet security operation devices.

You must pass two elective exams.

ELECTIVE EXAMS

FortiGate
FortiAnalyzer Analyst
FortiSIEM
FortiSOAR
FortiEDR

RECOMMENDED TRAINING

FortiGate Security  SKU: FT-FGT-SEC  Learn More
In this course, candidates will learn how to use the most common FortiGate security features, including security profiles.
Security Operations

FortiGate Infrastructure  SKU: FT-FGT-INF  Learn More
In this course, candidates will learn how to use the most common FortiGate networking and infrastructure features.

FortiGate Immersion  SKU: FT-NSE4-IMM  Learn More
In this lab-only course, available for purchase only, candidates are assigned a series of do-it-yourself (DIY) configuration tasks in a virtual lab environment.

FortiAnalyzer Analyst  SKU: FT-FAZ-ANS  Learn More
In this course, candidates will learn the fundamentals of using FortiAnalyzer for centralized logging. This includes learning how to identify current and potential threats through log analysis, and examine the management of events, incidents, reports, and task automation with playbooks.

FortiSIEM  SKU: FT-FSM  Learn More
In this course, candidates will learn how to use FortiSIEM, and how to integrate FortiSIEM into your network awareness infrastructure.

FortiSOAR  SKU: FT-FSR-ADM  Learn More
In this course, candidates will learn about FortiSOAR architecture, and how to deploy, configure, manage, operate, and monitor FortiSOAR in a SOC environment.

FortiEDR  SKU: FT-EDR  Learn More
In this course, candidates will learn how to use FortiEDR to protect their endpoints against advanced attacks, with real-time orchestrated incident response functionality.

Fortinet Certified Solution Specialist in Security Operations  Learn More

The Fortinet Certified Solution Specialist (FCSS) in Security Operations certification validates your ability to design, administer, monitor, and troubleshoot Fortinet security operations solutions. This curriculum covers security operations infrastructures using advanced Fortinet solutions.

You must pass the core exam.

CORE EXAM

Advanced Analytics

RECOMMENDED TRAINING

Advanced Analytics  SKU: FT-ADA  Learn More
In this course, candidates will learn how to use FortiSIEM in a multi-tenant environment as well as some advanced configurations, baseline calculations, and remediation methods.

Learn more about our NSE Certification Program