**CISCO Cybersecurity Operations Associate (CyberOps)**

You’ll be trained by Cisco Certified Trainers who, through our unique **Lecture | Lab | Review**technique, will take you through key security principles and provide hands-on, practical examples. This technique will help you better retain knowledge and will ensure you are capable of applying your skills to real-life scenarios.

Upon completing this certification, you will have:

* The skills to prepare for more advanced job roles in cyber security operations
* A basic understanding of Security Operations Centre (SOC) teams including an understanding of the type of metrics used to detect and respond to security incidents
* An understanding of how to protect your organization’s information from common attack vectors and endpoint attacks
* Knowledge in security monitoring, including identifying sources and types of data and events.
* Knowledge of how organization’s are detecting and responding to cyber crime, cyber espionage, insider threats, advanced persistent threats and regulatory requirements
* An understanding of security challenges involved with network applications

You'll also be prepared to sit exams **210-250 SECFND: Understanding Cisco Cyber security Fundamentals**and **210-255 SECOPS: Implementing Cisco Cyber security Operations.** You'll sit these at the Firebrand Training Centre as part of the course, covered by your Certification Guarantee.

This course, which is 40% faster than traditional training, is aimed at Security Operations Center (SOC) Analysts at an associate or beginner level. The certification does require some knowledge of basic cyber security technologies and principles.

**Course – Curriculum**

Module 1 – The Danger

Module 2 – Fighters in the War Against Cybercrime

Module 3 – The Windows Operating System

Module 4 – Linux Overview

Module 5 – Network Protocols

Module 6 – Ethernet and Internet Protocol (IP)

Module 7 – Connectivity Verification

Module 8 – Address Resolution Protocol

Module 9 – The Transport Layer

Module 10 – Network Services

Module 11 – Network Communication Devices

Module 12 – Network Security Infrastructure

Module 13 – Attackers and Their Tools

Module 14 – Common Threats and Attacks

Module 15 – Network Monitoring and Tools

Module 16 – Attacking the Foundation

Module 17 – Attacking What We Do

Module 18 – Understanding Defense

Module 19 – Access Control

Module 20 – Threat Intelligence

Module 21 – Cryptography

Module 22 – Endpoint Protection

Module 23 – Endpoint Vulnerability Assessment

Module 24 – Technologies and Protocols

Module 25 – Network Security Data

Module 26 – Evaluating Alerts

Module 27 – Working with Network Security Data

Module 28 – Digital Forensics and Incident Analysis and Response