SNIPESEC

TRAINING ACADEMY

SNIPESEC

Snipesec Training Academy provides a wide range of trainings in the direction of Information Technology. We teach the most in-demand skills which will help to enhance your career.

You can get trained in Database, Cybersecurity, Web, Virtualization, Mobile Apps, Malware trainings, etc. Courses include online Lab Environment where you get all the necessary tools to work simultaneously with the instructor.

At the end of the training, an internationally valid certificate is aquired which will benefit your career in IT.

BASIC TRAININGS

DATABASE

SECURITY

VIRTUALIZATION

WEB

MOBILE

MALWARE

ADVANCED LEVEL TRAININGS

AUTOMATION

SNIPESEC

BASIC TRAININGS

SNP100 - IT Law and Legal Regulations in Cybersecurity

What you will learn in this course

In this course you will encounter a range of topics which include cloud computing, information rights, e-commerce, media law, etc. By the end of your training session you should emerge with an understanding of information technology law not just in its legal but also its social, ethical, cultural and commercial contexts; state and identify concepts relating to organizational cybersecurity policy, governance mechanisms, applicable legislation and compliance requirements for information security; describe the role of corporate governance with regards to cybersecurity, and the business reasons for implementing a cybersecurity function; recognize and explain major applicable legislation and regulatory framework (local, European, international), and define, explain and exemplify compliance requirements in relation to cybersecurity, information security, data protection (privacy, anonymity) and critical information infrastructure protection.

Career opportunities

- Law Firms
- Information Communication Technology Companies
- Public Agencies
- International Organizations
- Consulting Firms and Scientific Institutions

Outline

- Concepts of Cybersecurity and Related Law
- Information Security Components and Concepts
- Role of Policy in an Organization
- Role of Cybersecurity and Information Security in the Organization
- Relevant laws and legal/regulatory frameworks
- Copyright in Cyberspace
- Content liability
- Trademarks, the internet and domain names
- Cybercrime
- Online Privacy
- Cloud computing

Duration

1 day / 6 hours

Study Type

Online / Onsite

Prerequisites

None

SNP110 - Information Security Management System

What you will learn in this course

In the given course you will gain Awareness of the importance of information security, Knowledge of responsibilities and duties as part of the information security management system, Acquire basic information on information security, Gain knowledge about the general concepts of information security and the general structure of the information security management system, Acquire basic technical information about system security, Gain the ability to establish ISMS, and knowledge about the concepts related to auditing.

Who should enroll

- Information Security Managers
- Information Security Consultants and Auditors
- Information Security Officers
- Information Security Risk Specialists
- Managers and Business Owners
- People Involved in the Implementation and Administration of Information Security Management Systems According to ISO/IEC 27001

Outline

- ISO 27001 Standard and Processes
- Information Security Management System Method and Process Approach
- Benefits of Establishing an ISO 27001 Information Security Management System
- Planning the Establishment of ISO 27001 Information Security Management System
- Information Security Management System Scope
- Internal Audits of ISMS
- ISMS Monitoring and Review
- Improving ISMS
- Misconceptions and Truths about ISMS
- ISO 27001 Certification Process

Duration

4 days / 24 hours

Study Type

Online / Onsite

Prerequisites

None

BASIC TRAININGS

SNP120 - Cyber Security Risk Assessment Training

What you will learn in this course

This risk assessment training course will teach you how to conduct a security risk assessment to protect your organization. You will learn about the laws and regulations that impose strict cybersecurity requirements on all organizations. You will also gain the skills to develop a compliance assessment plan and employ a standards-based risk management process while maintaining a satisfactory security posture.

Who should enroll

- Security engineers
- Compliance directors
- Managers
- Auditors
- System administrators

Outline

- Introduction to Risk Assesment and Management
- Characterizing System Security Requirements
- Selecting Appropriate Security Controls
- Reducing Risk Through Effective Control Implementation
- Assessing Compliance Scope and Depth
- Authorizing System Operation
- Maintaining Continued Compliance

Duration

2 days / 12 hours

Study Type

Online / Onsite

Prerequisites

None

BASIC TRAININGS

SNP130 - Cyber Security Training for Administrators

What you will learn in this course

This course covers fundamental cybersecurity concepts and skills relevant to the day-to-day management and responsibilities of Administrators and other information technology roles. For example, how to detect & prevent social engineering attacks, how to create strong passwords & why some passwords aren't effective, why using a Virtual Private Network (or VPN) has advantages, the importance of cloud security, etc.

Who should enroll

- Database Administrators
- Network Administrators
- Server/Web Administrators
- Security System Administrators

Outline

- Introduction to Cybersecurity
- Social Engineering Manipulation
- Phishing and Other Data-Retrieval Attempts
- Malware and Other Hardware Attacks
- How to Keep Your Accounts Safe
- How to Make Your Internet Usage More Secure
- Cloud Security

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

BASIC TRAININGS

SNP140 - Cyber Incident Management and Response

What you will learn in this course

Basic Level Cyber Incident Management and Response course is designed those who might be required to manage the response to a cyber-attack or breach. The course introduces the concepts of incident response preparation together with the fundamentals of incident management, and assumes an awareness of information security and the need to respond to cyber-attacks or breaches.

Who should enroll

- Incident managers
- Security officers and data protection representatives
- IT managers

Outline

- The Basics of the Incident Response Process
- Cyber Security Frameworks
- Technical Capabilities That Should Be Available When Dealing With an Incident
- Case Studies Enforcing Why Incident Response Preparation and Management is Key to Mitigating Business Disruption

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

None

BASIC TRAININGS

SNP150 - Basic Principles of Network Protection

What you will learn in this course

In this course you will explore the fundamentals of computer networking security and monitoring. At the end of this course you will be able to identify information security threats, identify the OSI Model layer, identify Network Attack, identify Network Protection Method, etc.

Who should enroll

- Anyone who wants to Start the Career in Network Security
- Science Background Students
- Engineering Background Students

Outline

- Concept of Network Security and types of the Network
- Types of layer in OSI Model
- Types of network attack, which harm the computer and network system
- Network Protection
- Firewalls
- VPN Encryption

Duration

5 days /

Study Type

Online / Onsite

Prerequisites

SNP151 - Linux System Administration Training

What you will learn in this course

Linux is the #1 operating system for web servers, cloud computing, smart phones and consumer electronics. You'll learn how to administer, configure and upgrade Linux systems running one of the three major Linux distribution families (Red Hat, SUSE, Debian/Ubuntu). You'll also learn all the tools and concepts you need to efficiently build and manage a production Linux infrastructure.

Who should enroll

- People who are new to IT, or those who have worked with operating systems other than Linux and want to move into a career administering Linux systems
- Cloud Engineers
- Science Background Students
- IT personnel
- CSIRT personnel

Outline

- Course Introduction
- Linux Filesystem Tree Layout
- Processes
- Signals
- Package Management Systems
- Linux Filesystems
- Managing Swap Files and Partitions
- Configuring Outgoing Mail Server
- Managing Packages on Debian and Ubuntu System
- Adding an IP Address and Static Route
- Archiving Files and Directories with Compression
- Managing User and Group Accounts
- Using File Attributes and Permissions
- Creating and Mounting an Encrypted Filesystem

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

None

SNP152 - Linux Operating Systems Auditing and Hardening Training

What you will learn in this course

The intention of this course is to cover the concepts, techniques and skills used to harden Linux systems. This course serves as general guidance for Debian based systems and how to install, configure and provide and overall secure environment for both desktop and server based systems. You will learn about BIOS Security, GRUB Hardening, SSH and remote access, Determining firewall configuration, etc.

Who should enroll

- People who are new to IT, or those who have worked with operating systems other than Linux and want to move into a career administering Linux systems
- Cloud Engineers
- Science Background Students
- IT personnel
- CSIRT personnel
- System Administrator

Outline

- Memory Attacks and Overflows
- OS Minimazation
- OS Patching
- Boot Configuration
- Malware
- Host-Based Firewalls
- Physical Attacks
- Kernel Tuning
- File Integrity
- SSH Hardening
- Apache Hardening
- Syslog

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

None

SNP160 - Windows Server Fundamentals Tutorial

What you will learn in this course

In this course, you will begin exploring the basics of Windows Server administration on Windows Server. This will include hardware components, installation, and basic management of a Windows Server. You'll get a base foundation of knowledge in Windows Server. This course is designed for entry-level IT Pros and Developers. Some experience with Windows operating systems and networking will be helpful, but is not a requirement to be successful.

Who should enroll

- Science Background Students
- IT personnel
- CSIRT personnel
- System Administrator

Outline

- Introduction
- Server Hardware and Resources
- Installing Windows Server
- Server Configuration and Management
- Storage in Windows Server
- Performance Monitoring in Windows Server
- Device Drivers and Services in Windows Server
- Understand and Create a DHCP Server
- Understand DNS and Create a DNS Server
- Create Group Policies Objects GPOs

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

None

SNP161 - Windows Server Administration Training

What you will learn in this course

In this course, you will unnderstand how Winndows Server works and you will be comfortable with basic Windows Server Administration. You will build and manage Microsoft Windows Servers, Active Directory, system recovery tools, and account management.

Career Opportuninties

- System Administrator
- Windows System Engineer
- Infrastructure Engineer - Windows
- System Analyst

Outline

- Basic Windows Server Concepts
- Configure Device Drivers
- Configure Operating System Services
- Server Roles Basics
- FIle and Print Servers
- Application Servers
- Web Servers
- Remote Access Servers
- Virtualization Servers
- Understanding Active Directory Infrastructure
- Understanding Windows Server Storage Distribution
- Wroking with Event Logs and Alerts

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

None

SNP162 - Windows Server Auditing and Hardening Training

What you will learn in this course

Windows servers are the heart of many corporate networks and may contain sensitive company data that, if leaked or stolen by an attacker, would be catastrophic. Protecting the Windows Server assets and preventing a security compromise is an important skill for IT security professionals to master. In this course, you'll learn how to help prevent security incidents by hardening the Windows Server and reducing the attack surface. You'll learn how to follow common security best practices to lock down a Windows system by hardening user accounts, passwords, services, the file system, and common network services, such as DNS and IIS.

Who should enroll

- Science Background Students
- IT personnel
- CSIRT personnel
- System Administrator
- Blue Team Member

Outline

- Windows Server Hardening Best Practices
- Removing Unnecessary Windows Server Software
- Hardening Network Services on a Windows Server
- Windows Server User Account Hardening
- Securing Windows Accounts with a Password Policy
- Windows Server File System Hardening Techniques
- Hardening Windows Servers with Additional Software
- Hardening Windows DNS Servers
- Hardening Windows IIS Web Servers
- Auditing and Windows Server Hardening
- Using Auditing to Monitor Windows Server Activity

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

None

SNP170 - Introduction to Digital Forensics

What you will learn in this course

In this course, you will understand the basics of Digital Forensics. Also will learn about Inident Response. How to find out information about someone from their devices, how to exploit data found, what happens when the file is deleted, how files are stored in the device all this will be covered in this course. You will learn Digital Forensics methodologies and so you can become a Digital Forensincs Analyst and deepen your knowledge in the future.

Who should enroll

- Digital Forensics Analyst
- Information Security Professionals
- Legal Professionals
- HR Professionals
- Managers and Executives

SNP170

Introduction to Digital Forensics

Outline

- Introduction to Digital Investigation
- Digital Forensics
- The Legal Framework
- Incident Response
- Digital Evidence Acquisition Essentials
- Digital Forensic Analysis
- Digital Forensics Management
- Information Representation and File Systems
- File Signatures and File Carving
- Reporting
- Forensic Tools

Duration

3 days/ 18 hours

Study Type

Online / Onsite

Prerequisites

None

SNP180 - Fundamentals of Cryptography

What you will learn in this course

This course is an introduction to the foundations of modern cryptography. It will cover different existing security definitions, proofs by reductions, private/public key cryptosystems and their underlying computational hardness assumptions. By the end of this course you will be able to use cryptographic primitives and their basic propertie, use public-key primitives and their applications, apply appropriate known cryptographic techniques for a given scenario, describe real-world applications of cryptographic primitives and protocols, etc.

Who should enroll

- IT personnel
- CSIRT personnel
- Blue Team Member
- Security Analyst
- Science Background Students

Outline

- Introduction to Cryptography
- Stream Ciphers
- Data Encryption Standard and Alternatives
- Advanced Encryption Standard
- More About Block Ciphers and Modes of Operation
- Introduction to Public-Key Cryptography
- The RSA Cryptosystem
- Cryptosystems Based on the Discrete Logarithm Problem
- Elliptic Curve Cryptosystems
- Digital Signatures
- Hash Functions
- Message Authentication Codes (MACs)
- Key Establishment

Duration

3 days/ 9 hours

Study Type

Online / Onsite

Prerequisites

None

SNP200 - NoSQL Database Training

What you will learn in this course

After successfully completing this course, you will be able to distinguish the different types of NoSQL databases, demonstrate an understanding of the detailed architecture, define objects, load data, query data and performance tune Column-oriented NoSQL databases, explain the detailed architecture, define objects, load data, query data and performance tune Document-oriented NoSQL databases, evaluate NoSQL database development tools and programming language, and more.

Career Opportunities

- Data Scientist/Data Analyst
- Database Architect
- Database Administrator
- Business Analyst
- SQL Developer
- Full-Stack Developer
- Software Engineer

Outline

- The Definition of the Four Types of NoSQL Databases
- Column-oriented NoSQL databases using Apache HBASE
- Column-oriented NoSQL databases using Apache Cassandra
- NoSQL Key/Value databases using MongoDB
- NoSQL Key/Value databases using Riak
- Graph NoSQL databases using Neo4J
- NoSQL database development tools and programming languages

Duration

2 days/12 hours

Study Type

Online / Onsite

Prerequisites

None

DATABASE

SNP201 - Oracle-SQL Training

What you will learn in this course

Since SQL is an industry standard language, many of the topics presented and many of the skills you will acquire will be applicable to other database platforms, such as Microsoft SQL Server, IBM DB2, the open-source databases MySQL and PostgreSQL, and others. By the end of this course the student will be able to create reports using SQL*Plus and formulate advanced SQL queries including correlated subqueries and outer joins. The student will also learn basic Oracle PL/SQL and learn the basic language constructs.

Who should enroll

- Business and Non-IT Professionals
- Application Designers and Database Developers
- Business Intelligence (BI) analysts and consumers
- Database Administrators
- Web Server Administrators
- Full-Stack Developer
- Software Engineer

Outline

- Relational Databases & Data Models
- Selection & Setup of the Database Interface
- Using the Database Interface
- Introduction to the SQL Language
- The Select Statement
- Restricting Results with the WHERE Clause
- Sorting Data with the ORDER BY Clause
- Pseudo Columns, Functions & Top-N Queries
- Joining Tables
- Using the SET Operators
- Summary Functions
- Aggregating Data Within Groups
- Use DDL to Create & Manage Tables

Duration

2 days/12 hours

Study Type

Online / Onsite

Prerequisites

None

SNP210 - Cyber Attack Detection, Analysis and Log Management Training

What you will learn in this course

In the given course you will learn to Use log data to establish security control effectiveness, Combine data into active dashboards that make analyst review more tactical, Simplify the handling and filtering of the large amount of data generated by both servers and workstations, Apply large data analysis techniques to sift through massive ammounts of endpoint data, Quickly detect and respond to the adversary, etc.

Who should enroll

- IT Personnel
- CSIRT Personnel
- Red Team Member
- Blue Team Member
- Pentest Specialist
- Software Engineer
- Security Analyst

Outline

- Introduction to Log Analysis
- Introduction to web servers
- Apache web server on Ubuntu server
- Nginx web server on Ubuntu server
- SSH & FTP services logging
- Metasploitable Vulnerable machine setup
- Importing Kali Linux VM in Virtualbox
- Generating test traffic for SSH server
- Generating test traffic for FTP server
- Generating file upload vulnerabilities traffic
- Bruteforce SSH & FTP services
- Theoretical concepts of log analysis
- Setting up Log analysis tool on local system
- Threat agents to logging
- Benefits of security logging

Duration

5 days/30 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals
SNP200 - NoSQL Database Training
or equivalence

SNP211 - Pentest Training

What you will learn in this course

IThe Penetration Testing Course is designed to provide practitioners with working knowledge of the cyber security challenges facing their environments. This knowledge is vital when managing the day to day running of all aspects of security risk for those environments. This course is aimed at teaching students the basics of penetration testing to prepare them for the boot camp certification level course.

Who should enroll

- IT Personnel
- CSIRT Personnel
- Red Team Member
- Blue Team Member
- Pentest Specialist
- Software Engineer
- Security Analyst

Outline

- Performing basic OSINT and reconnaissance of a target network
- Footprinnting and Gathering Intelligence
- Evaluating Human and Physical Vulnerabilities
- Preparing the Vulnerability Scan
- Scanning Logical Vulnerabilities
- Analyzingn Scanning Results
- Avoiding Detection and Covering Tracks
- Exploiting the LAN and Cloud
- Testing Wireless Networks
- Targeting Mobile Devices
- Attacking Specialized Systems
- Web Application-Based Attacks
- Performing System Hacking
- Scripting and Software Development
- Leveraging the Attack: Pivot and Penetrate
- Summarizing Report Components

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP212 - PfSense Firewall Training

What you will learn in this course

PfSense is a free and open source operating system for routers and firewalls. In this course you will Understand pfSense, its features and benefits, Configure pfSense as a firewall, Get familiar with other advanced features of pfSense like failover, load balancing, VPN connectivity.

Who should enroll

- IT Administrators
- Security Administrators
- Anyone Running a Home or Small Office Network
- Technical Architects
- Founders and CXOs

Outline

- Introduction to pfSense
- pfSense hardware requirements
- Deploy virtual machine for pfSense
- Install pfSense
- pfSense features
- pfSense as a firewall
- pfSense load balancing and failover
- Get familiar with OpenVPN
- pfSense and OpenVPN

Duration

2 days / 12 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP213 - Snort IPS (Intrusion Prevention System) Training

What you will learn in this course

In this course you will learn how to build and manage a Snort sensor using open source tools, plug-ins, and the Snort rule language to help manage, tune, and deliver feedback onsuspicious network activity. Hands-on labs help you construct solid, secure Snort installations and write Snort rules using proper syntax and structure. You will also test their rule writing skills in two challenges: a theoretical challenge that tests their knowledge of rule syntax and usage and a practical challenge in which an exploit is presented for you to analyze and research so they can defend their installations against the attack.

Who should enroll

- Network Administrators
- Security Administrators
- Security Consultants

Outline

- Detecting Intrusions with Snort 3.0
- Sniffing the Network
- Architecting Nextgen Detection
- Choosing a Snort Platform
- Operating Snort 3.0
- Examining Snort 3.0 Configuration
- Managing Snort
- Analyzing Rule Syntax and Usage
- Use Distributed Snort 3.0

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SECURITY

SNP214 - Fortinet Firewall Training

What you will learn in this course

In this course you will gain a solid understanding of how to integrate the FortiGate unit into their existing environment, and the operational maintenance involved to ensure optimal performance and full protection of their corporate assets. The Fortinet Network security training program introduces you to the basic concepts of network security and gives them an all round view of how networks can achieve more security, while optimizing network performance. This is a fully hands on training and each attendee is given the opportunity to configure a network security device in a live-like and hands-on environment

Who should enroll

- Network Administrators
- Security administrators
- Security consultants

Outline

- Introduction
- Logging and Monitoring
- Firewall Policies
- Firewall Authentication
- Secure Sockets Layer VPN
- Antivirus
- Explicit Proxy
- Web Filtering
- Application Control
- Routing
- Virtual Domains
- Transparent Mode
- High Availability
- Intrusion Prevention Systems IPS
- Fortinet Single Sign On
- Advanced IPSec VPN
- Data Leak Prevention

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP215 - Wireless Network (WLAN) Security Training

What you will learn in this course

Wireless security, with the use of wireless networks, prevents unwanted access or damage to computers. This course will discuss a variety of topics including the differences between wireless network and wired network, wireless technical standards and current and future applications of wireless technology. The course will also examine challenges and types of wireless security, its vulnerabilities and security issues. Lastly the course will discuss securing wireless technology and its future.

Who should enroll

- Network Administrators
- Security Administrators
- Security Consultants

Outline

- Introduction to Wireless Network
- Risk Assessment
- Threat Analysis and Hacking Methodology
- Rudimentary Security Measures
- Intermediate Security Measures
- Advanced Security Measures
- Wireless LAN Auditing Tools
- Hardware and Software Solutions
- Prevention and Countermeasures
- Implementation and Management
- Hands On Lab Exercises

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP216 - DNS Security Training

What you will learn in this course

In this course you will will review the theory behind the DNS hierarchy, the DNS protocol, forward and reverse mapping zone files. DNS (DNSSEC) security is based on modern cryptographic techniques and processes. You will learn the underlying principles without requiring mathematical knowledge. Specific implementation of shared-secret (symmetric) and public-key (asymmetric) implementations will be detailed covering Zone Transfer, Dynamic DNS (DDNS) and Zone Integrity. Secure DDNS integration with DHCP is covered and procedures and requirements for key management and key-rollover are illustrated. The course includes a number of hands on configuration exercises.

Who should enroll

- DNS Administrators
- Network and System Administrators
- Security Specialists

Outline

- TCP/IP Fundamentals Review
- Introduction to DNS
- Domain and Zone Concepts
- Server Architecture
- BIND Setup
- General Information Security Approach
- DNS Security
- DNS Attacks
- Advanced DNS Issues

Duration

3 days/12 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP217 - Database Logging, Audit and Security Training

What you will learn in this course

Auditing database activity is a core component to any company data governance. A company policy often set up auditing for security, privacy, or protection purposes, for example, to ensure that those without the permission to access information do not access it. It involves observing a database so as to be aware of the actions of database users.

In this course you will learn how to manage databases, how to audit them and most importantly, how to secure the database so all the information is safe.

Who should enroll

- Database Administrators
- Network and System Administrators
- Security Specialists

SNP217

Database Logging, Audit and Security Training

Outline

Duration

2 days / 12 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP200 - NoSQL Database Training
or equivalence

- Understanding Logging
- Transaction Log Architecture
- Log Records
- Checkpoints
- Transaction Log Operations
- Database Audit Approaches
- Audit Execution

SNP218 - Python for Cybersecurity Training

What you will learn in this course

Python is one of the most popular and widely-used programming languages in the world due to its high usability and large collection of libraries. This learning path provides an application-driven introduction to using Python for cybersecurity. Python can help to automate tasks across the cyberattack life cycle for both cyber attackers and defenders. This learning path demonstrates some of these applications and how Python can be used to make cybersecurity professionals more efficient and effective.

Who should enroll

- DNS Administrators
- Network and System Administrators
- Security Specialists
- Cybersecurity Analyst

Outline

- Setting Up the Development Environment
- Introduction to Python
- Pinging Targets
- Cryptography
- Hacking of Passwords
- Introduction to APIs
- Cybersecurity APIs

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
or equivalence

SNP219 - Disaster Recovery and Business Continuety Training

What you will learn in this course

In this disaster recovery and business continuity course, you will gain the skills to identify mission-critical continuity needs, define sources of risk, create an incident response team charter, implement a Business Continuity Management System (BCMS), and improve organizational resilience. Learn how to build a disaster recovery plan and implement a BCMS to ensure your organization is protected from the constant risk of business disruptions caused by internal and external threats.

Who should enroll

- IT Support Technicians
- IT Managers

Outline

- Defining Business Continuity Management
- Running BCMS development as a project
- Setting goals for the BCMS
- Determining the needs of interested parties
- Identifying mission-critical continuity needs
- Performing Business Impact Analysis (BIA)
- Characterizing risks
- Developing appropriate responses
- Creating the incident response plan
- Directing the incident response team
- Establishing a standby site
- Selecting backup and restore strategies
- Restoring communications and recovering users
- Maintaining and improving the BCMS

Duration

2 days / 12 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

VIRTUALIZATION

SNP220 - Virtualization Training

What you will learn in this course

Virtualization is the creation of a virtual version of something, such as an operating system (OS), a server, a storage device or network resources. By the end of this course you will understand what virtualization is, how to create a virtual machine, understand what is Hypervisor and its interaction with the Virtual Machine, and you will understand what is cloud copmuting. You will be able to configure Virtual Machine, install Operating System on it, and many more...

Career Opportunities

- Virtualization Administrator
- Virtualization Engineer
- Systems Engineer
- Virtualization Architect
- Data Virtualization Specialist

Outline

- Introduction to Virtualization
- Understanding Virtual Machines
- Creating a Virtual Machine
- Installing Linux in a Virtual Machine
- Managing vCPUs
- Managing VM Memory
- Virtual Networking
- Managing Virtual Devices
- Understanding Availability
- Understanding Hypervisors
- Introduction to ESXi

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals
or equivalence

SNP221 - Kubernetes and Containers Management Training

What you will learn in this course

This course offers an introduction to Kubernetes and includes technical instructions on how to deploy a stand-alone and multi-tier application. You'll learn about ConfigMaps and Secrets, and how to use Ingress.
Upon completion, you will have a solid understanding of the origin, architecture and building blocks for Kubernetes, and will be able to begin testing the new cloud native pattern to begin the cloud native journey. You will learn the origin, architecture, primary components, and building blocks of Kubernetes, how to set up and access a Kubernetes cluster using Minikube, ways to run applications on the deployed Kubernetes environment and access the deployed applications, etc.

Career Opportunities

- DevOps Engineer
- Kubernetes Engineer
- Backend Engineer
- Software Engineer
- Principal DevOps Engineer
- Systems Engineer

Outline

- Introduction
- From Monolith to Microservices
- Container Orchestration
- Kubernetes
- Kubernetes Architecture - Overview
- Installing Kubernetes
- Setting Up a Single Node Kubernetes Cluster Using Minikube
- Accessing Minikube
- Kubernetes Building Blocks
- Services
- Deploying a Stand-Alone Application
- Kubernetes Volume Management
- ConfigMaps and Secrets
- Ingress
- Advanced Topics - Overview
- Kubernetes Community

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP222 - Backup and Backup Systems Training

What you will learn in this course

In this course you will learn how to make backups using Veeam Backup and Replication for Backup and Replication. You will learn the architecture of Veeam's backups, getting to know the three unique methods that Veeam can use to store data. Armed with this information, you'll configure and execute a series of backup jobs, exploring the variety of ways that backup jobs can be configured. Next, you'll extend your reach by configuring replication jobs to a secondary disaster recovery site. Then, you'll restore that data, whether it be entire VMs all the way down to individual files. Finally, having done all these activities atop the VMware vSphere hypervisor, you'll see their similarities and differences atop Microsoft's Hyper-V. By the end of this course, you'll be armed with the experience you need to backup, replicate, and recover any virtual or physical workload using your Veeam Backup and Replication infrastructure.

Who should enroll

- IT personnel
- CSIRT personnel
- Blue Team Member
- Security Analyst
- Science Background Students

Outline

- Introduction
- Veeam Components
- Veeam Backup Concepts
- Prerequisites and Diagram
- Installation Files
- Building Veeam Backup LAB
- Perform Backup And Restore
- Backup and Restore Physical Server
- VM copy and File copy
- Perform Quick Backup
- Offsite data protection Using Job Copy
- Backing UP Hyper-v
- Tape Drive

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals
or equivalence

SNP301 - Frontend Web Applications Development Training

What you will learn in this course

In this course you will learn how to design a Frontend of the website. Following topics will be covered: Web development basics with HTML, Cascading Style Sheets (CSS), JavaScript programming, jQuery JavaScript library, Bootstrap framework. At the end of this course you will be able to design your own interactive website.

Career Opportunities

- Front End Developer
- .NET Developer
- Web UI Developer
- HTML Developer
- Web (JavaScript) Developer Apprentice

Outline

- Web Development Basics - HTML
- Advanced HTML Concepts
- Introduction to Cascading Styling Sheets (CSS)
- Advanced CSS
- JavaScript for Beginners
- More JavaScript Concepts
- Getting Started with JQuery
- Advanced JQuery
- BootStrap Basics
- Project

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

None

WEB

SNP302 - Backend Web Applications Development Training

What you will learn in this course

In this course you will learn about back-end development and programming servers, about APIs (Application Programming Interfaces). Working with APIs will enable you to work with data stored on remote servers how to create back-end servers and APIs in JavaScript using the popular Express.js framework, how to integrate a PostgreSQL database into your applications, how to build an API with Node, Express, PostgreSQL and deploy it to Heroku, and many more.

Career Opportunities

- Back-End Developer
- .NET Developer
- Database administrator

Outline

- Introduction to PHP
- PHP Language Basics
- Forms, Cookies, and Session
- MySQL Basics
- PHPMyAdmin
- MySQL Statements
- PHP Object Oriented Programming
- Introduction to XML
- Introduction to JSON
- Introduction REST and API

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

None

SNP303 - Web Service (API) Development Training

What you will learn in this course

In the given course you will learn how to create a traditional SOAP web service using Visual Studio 2019, create a REST API web service using Visual Studio 2019, describe the relationship between URLs and URIs and when to use each, perform Web API routing using Visual Studio with convention-based routing, implement Web API attribute routing in Visual Studio, create a REST API using the OpenAPI language with the Swagger Editor to generate source code.

Career Opportunities

- Web Developer
- Full Stack Web Developer
- .NET Application Developer
- Software Developer

Outline

- Creating a SOAP API Web Service
- Consuming a SOAP API Web Service
- Creating a REST API Web Service
- Consuming a REST API Web Service
- URLs vs. URIs
- Performing Web API Routing
- Implementing Web API Attribute Routing
- Schema-first Design
- Using OpenAPI

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP304 - Project Management Training

What you will learn in this course

By the end of this course you will be able to get Project Manager Professional certification. You will understand vrious methods of Project Management as Agile, Waterfall, etc. You will be able to measure performance with Performance Domains. Moreover, you will easily learn PMP Math. With the PMP certificate you will be able to go further in your career and enhnce your skills.

Career Opportunities

- Project Manager
- Project Management Office Manager
- Technical Project Manager

Outline

- Traditional/Predicitve Project Management
- Waterfall Project Management
- Agile Project Management
- Agile Events
- Agile Roles
- Agile Artifacts
- Performance Domains

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

None

SNP305 - Security Training in Web Applications

What you will learn in this course

In Security Training course you will learn intermediate concepts in web security including prevention techniques for common threats, how to protect your resources with authorization and authentication techniques, secure your data using Transport Layer Security, Role-Based Access Control, and more, explore common threats that web applications face and how to mitigate them

Who should enroll

- Software Developer
- Web App Developer
- Security Administrator

SNP305

Security Training in Web Applications

Outline

- Web Security Fundamentals
- User Authentication and Authorization
- Cryptography
- Data Security
- Common Attacks on Web Applications
- Mitigating Attacks

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP211 - Pentest Training
or equivalence

WEB

SNP306 - Web Security and Penetration Techniques

What you will learn in this course

In this course you will come to understand common web application flaws, as well as how to identify and exploit them with the intent of demonstrating the potential business impact. Along the way, you follow a field-tested and repeatable process to consistently find flaws. Information security professionals often struggle with helping your organizations understand risk in terms relatable to business. The goal is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws not only through exploitation but also through proper documenting and reporting.

Who should enroll

- Software Developer
- Web App Developer
- Security Administrator

Outline

- Web application assessment methodologies
- The penetration tester's toolkit
- DNS reconnaissance
- Open-source intelligence (OSINT)
- Secure Sockets Layer (SSL) configurations and weaknesses
- Logging and monitoring
- Learning tools to spider a website
- Analyzing website content
- Username harvesting and password guessing
- Burp sequencer
- Session management and attacks
- Command injection
- SQL injection
- Cross-Site Scripting (XSS)

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP211 - Pentest Training
or equivalence

SNP307 - Web Application Firewall Management

What you will learn in this course

Web Application Firewall course provides you with an in-depth understanding of what is a Web Application Firewall (WAF), types of WAFs, and the approach to installing WAFs for protecting their web applications against external threats and preventing data leakage. Using the examples of industry-leading WAFs with sufficient hands-on exercises, the training course dives into the details of configuration, administration, fine-tuning, alerting, and reporting aspects of WAFs.

Who should enroll

- Network and Desktop Engineers
- Incident Management Team
- System Administrators
- Security Administrators
- Technical Support Staff
- IT Managers

Outline

- State of Web Application Security
- Traditional Network Defenses
- Why Web Application Firewalls
- WAF Market Overview
- Deployment Options
- Working of a WAF
- WAF Challenges
- WAF Demo & Lab

Duration

4 days / 24 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP308 - Web Programming with Node.js

What you will learn in this course

The given course teaches the Back-End programming with Node.js programming language. After taking this course, you will understand nodeJS, express and mongodb, You will be able to apply for Jr. backend development directly, You will be able to create most type of backend, totally independent of front end tech, and many more.

Career Opportunities

- Node.js Developer
- Back-End Developer
- Full-Stack Developer
- Software Engineer

Outline

- Introduction to Node.js
- Installing and Exploring Node.js
- Node.js Module System
- File System and Command Line Args
- Debugging Node.js
- Asynchronous Node.js
- Web Servers
- Accessing API from Browser
- Application Deployment
- MongoDB and Promises
- REST APIs and Mongoose
- API Authentication and Security
- Sorting, Pagination, and Filtering
- Testing Node.js

Duration

4 days / 24 hours

Study Type

Online / Onsite

Prerequisites

None

MOBILE

SNP306 - Mobile Application Security Training

What you will learn in this course

In this course you will learn and understand typical mobile application security issues in detail. You will learn security arhitectures of Android and iOS, their vulnerabilities, how to conduct a penetration test on mobile applications, exploiting vulnerabilities, etc.

Who should enroll

- Security Enthusiasts
- IT professionals
- Mobile Application Developers
- Security Analyst

Outline

- Mobile Application Security
- Android Security Architecture
- Setting up Android Pentesting Environment
- Android Applications Components
- Logging Based Vulnerabilities
- Bypassing SSL Pinning
- Insecure Data Storage
- Android Application Interaction
- Internet Manipulation with Drozer
- Exploiting Android Devices with MetaSploit
- MVC and Event Driven Architecture
- ARM Processor
- iOS Security Mechanisms
- Jailbreaking
- Creating a Pentest Platform
- Runtime Analysis
- Exploiting iOS Apps

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP200 - NoSQL Database Training
SNP211 - Pentest Training
SNP303 - Web Service (API) Development Training
or equivalence

SNP307 - iOS Mobile Application Development Training

What you will learn in this course

Given course guides you through development of an iOS Mobile Application. By end of the course you will gain experience with swift application and software, iOS software and development environment, Mobile OS, XCode, Objective-C, User Interface frameworks, Testflight, UI storyboard, Model–view–controller, Application Programming Interfaces. You will be able to set up and explore the XCode environment, write Swift code and create UI with the use of Swift playgrounds, avigate the Swift UI, and more.

Who should enroll

- Science Background Students
- IT enthusiasts

Outline

- Introduction to Mobile Application Development
- Simulation and Development
- The Swift Programming Language
- Establishing an Apple Developer Account
- UI with Two View Controllers That Display Table Cells
- Lists: The Data Model & Linking the UI to Code
- Met Gallery: Assets, Launch Screen, & Home View Controller
- Met Gallery: View Controller with a Collection View
- Met Gallery: The Painting Detail View Controller
- Met Gallery: Full Screen View Controller with a Scroll View
- Met Gallery: Adding a Spinner, Data Model, & Gallery VC
- Met Gallery: Painting Detail & Adding Gesture Recognizers

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

SNP200 - NoSQL Database Training
SNP303 - Web Service (API) Development Training
or equivalence

SNP308 - Android Application Development Training

What you will learn in this course

This Android training course is designed to quickly get you up to speed how to make Android apps for Android devices. This Android development training course will teach you the basis of the Android platform and the application lifecycle. You will be able to write simple GUI applications, use built-in widgets and components, work with the database to store data locally, and much more by the end of this Android training course course.

Who should enroll

- Science Background Students
- IT enthusiasts

Outline

- Introduction to Android Programming
- Android Stack
- Software Development Kit Overview
- Creating your first project
- Running your app on Emulator
- Activities
- Services
- Content Providers
- Broadcast Receivers
- Basic Android User Interface
- Android System Overview
- Advanced Android User Interface
- Multimedia in Android
- SQL Database
- Data Storage, Retrieval and Sharing
- Mapping and Location Based Services
- Working in the Background

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

SNP200 - NoSQL Database Training
SNP303 - Web Service (API) Development Training
or equivalence

SNP400 - Introduction to Reverse Engineering

What you will learn in this course

This training will introduce you to the intricacies of reverse-engineering, machine code, assembly language, system-level and code-level reversing and the legality of reverse-engineering. Take a closer look at everything from the different levels of computer instructions to the challenges of optimizing compilers and even individual tools like RegMon and FileMon.

Who should enroll

- Red Team Member
- Blue Team Member
- Security Analyst
- Security Administrator
- Threat Hunter

Outline

- Assembly Language Basics
- Decompiling and extraction using exe2aut
- Disassembling and Decompiling with Ghidra
- Debugging with xdbg
- VirtualAlloc, VirtualAllocEx and NtAllocateVirtualMemory - v2
- Dumping Memory Using Process Hacker
- File and Packer Identification
- Debugging and Unpacking with xdbg and Process Hacker
- Identifying Abnormal Epilogues

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP401 - Reverse Engineering in x86 Environment

What you will learn in this course

In this training you will learn the underlying environment binaries operate on (x86, Boot process (UEFI|BIOS), PE32/32+ formats, Page Table concepts & Kernel/Hypervisor) alongside actual exercises in writing your own Kernel drivers and working with Rust and make the most of static reverse engineering tools to understand different Windows & x86/x64 targets (malware, vulnerability research targets, obfuscated code, arbitrary software)

Who should enroll

- Red Team Member
- Blue Team Member
- Security Analyst
- Security Administrator
- Threat Hunter

Outline

- Common Mnemonics
- Malware Reversing 1
- x86 & Windows Basics
- Scripting to Automate Code Deobfuscation
- Batch Analysis & Large Scale Reversing
- Windows Kernel Drivers Overview
- Kernel Rootkit Analysis Walkthrough
- Kernel Driver Analysis for Vulnerability Hunting

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP402 - Malware Analysis Training

What you will learn in this course

Malware analysis is a critical skill in the information security community. This course is logically designed to help you leap through the complicated steps of static and dynamic malware analysis in an easy and proactive way. After this course, you will be able to understand the core skills required in malware incident response investigations and analysis of Advance persistent threats. The course will guide you trough the basic requirements and necessary skillsets required in order to take your knowledge to the next level

Who should enroll

- Red Team Member
- Blue Team Member
- Security Analyst
- Security Administrator
- Threat Hunter

Outline

- Course Introduction and Overview of Cyber Kill Chain
- Understanding Recon and Weaponization stages
- Spearphishing Emails as Delivery Mechanisms
- Analyzing Malicious Office File Using Oledump
- Analyzing malicious OLE Files using Oletools
- Understanding PDF file structure
- Analyzing Malicious PDF files
- Analyzing Malicious PDF file using PDF Stream Dumper
- Packet capture and analysis
- Wireshark Packet capture and filter Demo
- Analyzing Exploit kits Through Wireshark
- Analyzing Ransomware through static analysis tools

Duration

4 days / 24 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
or equivalence

SNP500 - Cyber Threat Intelligence and Threat Hunting Training

What you will learn in this course

By the end of this course you will Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios, Identify and create intelligence requirements through practices such as threat modeling, Generate threat intelligence to detect, respond to, and defeat focused and targeted threats, Create Indicators of Compromise (IOCs) in formats such as YARA and STIX/TAXII, Understand and exploit adversary tactics, techniques, and procedures, and leverage frameworks such as the Kill Chain, Diamond Model, and MITRE ATT&CK, Understand attacker tradecraft to perform compromise assessments, Track adversaries and develop threat intelligence to scope a network, Hunt down additional breaches using knowledge of the adversary.

Career Opportunities

- Cyber threat intelligence analyst
- Cyber Threat Hunter
- Financial Data Analyst
- Computer Defense and Network Vulnerability Specialist

Outline

- Cyber Threat Intelligence and Requirements
- The Fundamental Skillset: Intrusion Analysis
- Collection Sources
- Analysis and Production of Intelligence
- Dissemination and Attribution
- Capstone
- Advanced Threat Hunting
- Threat Hunting Across Enterprise

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP211 - Pentest Training
or equivalence

SNP501 - Advanced Digital Forensics Training

What you will learn in this course

In Advanced Forensic course you will learn RAM forensics analysis and acquisition, Pros and cons of live forensics acquisitions, Examination of non-traditional devices such as smart devices, Gaming systems and drones, Forensics elements in the Windows registry and how to examine those elements, Basics of testifying in a court of law, and more.

Career Opportunities

- Computer Forensics Investigator
- Computer Forensics Technician
- Information Security Analyst
- Information Systems Security Analyst
- Forensic Computer Analyst
- Security Consultant

Outline

- Introduction
- RAM Acquisition and Analysis
- Windows Registry Forensics
- USB and Network Connections
- Live Forensics
- Search Signatures
- Not Traditional Data Sources Evidence and Strategies for Acquisition and Reports
- Testifying on a Court Law

Duration

4 days / 24 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals
or equivalence

ADVANCED LEVEL TRAININGS

SNP502 - Red and Blue Team Trainings

What you will learn in this course

By the end of this course you will be able to Consume threat intelligence and plan a Red Team engagement, Set up the required infrastructure to have a successful operation taking into account operational security, Create weaponization that will allow you to infiltrate an organization, Enumerate and extract valuable data required to achieve your objectives using automated tooling, but also manually, if required, Elevate privileges using a variety of attack vectors and misconfigurations that you will now be able to identify. For the Blue Team practice you will get acquainted with tools and techniques required to stop advanced cyberattacks, you will learn how to defend your organization.

Career Opportunities

- Red Team Member
- Blue Team Member

Outline

- Red Team Fundamentals
- Information Gathering & Enumeration
- Initial Access
- Post Compromise
- Host Evasions
- The Metasploit Framework
- Privilege Escalation
- Lateral Movement & Pivoting Techniques
- Advanced Web Attacks
- Mitre ATT&CK Red Teaming
- Network Security Evasion
- Compromising Active Directory
- Getting In and Staying In
- Blue Team Tools and Operation
- Understanding Your Network
- Triage and Analysis
- Deliverables – Report Writing

Duration

5 days / 30 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals
SNP211 - Pentest Training
or equivalence

SNP503 - Social Engineering and Phishing Training

What you will learn in this course

In this course, we'll look at various different social engineering techniques that can be used to compromise systems. We'll also look at both computer-based and behavior-based tools to help defend against this risk.

Who should enroll

- Red Team Member
- Blue Team Member
- Security Analyst
- Security Administrator
- Threat Hunter

Outline

- Humans: The Soft Center within the Hard Shell
- A Walkthrough of a Social Engineering Attack
- Reconnaissance and OSINT
- Phishing Attacks
- Identity Theft and Impersonation
- Social Engineering Countermeasures

Duration

3 days / 18 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals
or equivalence

ADVANCED LEVEL TRAININGS

SNP504 - Memory Overflow Vulnerabilities and Exploit Development Training

What you will learn in this course

This comprehensive course is designed to turn you into high-level security experts. You will learn how to find critical vulnerabilities everywhere in the platforms and exploit them. This training is a must-have knowledge for anyone who aims to work as a professional hands-on performer in the security field. You will be given practical skills in core subjects of information security, terminology, entering systems, and will put great emphasis on hands-on practice.

Who should enroll

- Red Team Member
- Blue Team Member
- Security Analyst
- Security Administrator
- Threat Hunter

SNP504

Memory Overflow Vulnerabilities and Exploit Development Training

Outline

- Anatomy of a Program in Memory
- Stack Overflow
- Format String Vulnerability
- Heap Overflow and Heap Memory
- Advance Overflow Techniques
- Buffer Overflow Exploit Development
- Making Exploits Harder to Detect

Duration

4 days / 24 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals
SNP211 - Pentest Training
SNP401 - Reverse Engineering Education in x86 Environment
SNP402 - Malware Analysis Training
or equivalence

AUTOMATION

SNP510 - PowerShell Automation Training

What you will learn in this course

In this course you will learn how to automate processes with PowerShell. You will learn necessary commandlines, how to handle files, and many more.

Who should enroll

- Linux Administrator
- Network Engineer
- System Administrator
- IT Administrator

Outline

- Introduction to Powershell
- An Infrsatructure Setup
- Powershell Essentials for Automation
- File Handling in Powershell
- Output Display Options with Powershell
- Scripting Using Powershell
- Automation with Powershell
- Ad hoc Scripts

Duration

2 days / 12 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals

AUTOMATION

SNP520 - Python Automation Training

What you will learn in this course

In this course you will learn how to design and implement scalable automation solutions using Python. You will be able to create your own modules in Python which will help you automate everyday tasks.

Who should enroll

- Linux Administrator
- Network Engineer
- System Administrator
- IT Administrator

SNP520

Python Automation Training

Outline

- Python Language Basics
- Advanced File Handling
- Manipulating Images
- Interacting with Web Services
- Automatic Output Generation
- GUI Automation
- Email Automation

Duration

2 days / 12 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals

AUTOMATION

SNP530 - Ansible Automation Training

What you will learn in this course

In this course you will learn how to automate redundant and monotonous daily tasks with Ansible. Ansible is not the only automating tool but it is the easiest one. You will learn how to quickly and reliably configure almost anything with Ansible. By the end of this course you will move beyond manually configuring applications, networks, servers, etc.

Who should enroll

- Linux Administrator
- Network Engineer
- System Administrator
- IT Administrator

Outline

- Ad Hoc Configuration with Idempotent Modules
- Declaring Desired State with Playbooks
- Configuring Multiple Hosts
- Learning and Using Ansible
- Exploiting Roles and Collections with Ansible-Galaxy

Duration

1 day / 6 hours

Study Type

Online / Onsite

Prerequisites

SNP150 - Basic Principles of Network Protection
SNP151 - Linux System Administration
SNP160 - Windows Server Fundamentals

SNIPESEC