Deep Security Training for Certified Professionals

Course outline

Module 1: Introduction to Deep Security

Module 1: Introduction to Deep Security provides an overview of the Deep Security platform and its features. It covers topics such as the architecture of the platform, the different components of the platform, and the various security capabilities that Deep Security provides. It also provides an introduction to the Deep Security Manager, the web-based management console for Deep Security.

Lessons

- Overview of Deep Security
- Understanding the Components of Deep Security
- Exploring the Deep Security User Interface
- Configuring Security Policies in Deep Security
- Deploying Agents in Deep Security
- Managing Updates and Patches in Deep Security
- Monitoring and Reporting in Deep Security
- Troubleshooting and Optimizing Deep Security
- Best Practices for Securing Your Environment with Deep Security

After completing this module, students will be able to:

- Understand the fundamentals of Deep Security and its components
- Identify the different types of threats and how Deep Security can protect against them
- Configure and manage Deep Security policies and settings
- Monitor and troubleshoot Deep Security deployments

Module 2: Deep Security Architecture

Module 2 of the Deep Security Training for Certified Professionals course provides an in-depth look at the architecture of Deep Security. It covers topics such as the components of the Deep Security architecture, the different deployment models, and the security features of the platform. It also provides an overview of the various components of the Deep Security platform, including the Deep Security Manager, the Deep Security Agents, and the Deep Security Virtual Appliance.

Lessons

- Introduction to Deep Security Architecture
- Understanding the Components of Deep Security Architecture
- Designing and Implementing a Secure Deep Security Architecture
- Best Practices for Securing a Deep Security Architecture
- Troubleshooting and Maintaining a Deep Security Architecture
- Advanced Topics in Deep Security Architecture
- Case Studies in Deep Security Architecture
- Security Compliance and Deep Security Architecture
- Cloud Security and Deep Security Architecture
- Automation and Orchestration of Deep Security Architecture

After completing this module, students will be able to:

- Understand the components of a deep security architecture and how they interact with each other.
- Design and implement a secure deep security architecture.
- Identify and mitigate security risks associated with deep security architectures.
- Troubleshoot and maintain deep security architectures.

Module 3: Deep Security Components

Module 3: Deep Security Components is a module in the Deep Security Training for Certified Professionals course that covers the components of Deep Security, including the Deep Security Manager, Agents, and Relays. It provides an overview of the architecture and components of Deep Security, and how they interact with each other. It also covers the installation and configuration of the components, as well as the management of the components.

Lessons

- Overview of Deep Security Components
- Understanding the Deep Security Agent
- Exploring the Deep Security Manager
- Configuring the Deep Security Relay
- Working with the Deep Security Notifier
- Utilizing the Deep Security API
- Deploying the Deep Security Virtual Appliance
- Managing Deep Security Updates
- Troubleshooting Deep Security Issues
- Best Practices for Deep Security Deployment

After completing this module, students will be able to:

- Understand the architecture and components of Deep Security
- Configure and manage Deep Security components such as the Deep Security Manager, Agents, and Relays
- Utilize the Deep Security API to automate and integrate with other security solutions
- Monitor and troubleshoot Deep Security components and deployments

Module 4: Deep Security Deployment

Module 4 of the Deep Security Training for Certified Professionals course covers the deployment of Deep Security. It provides an overview of the installation process, as well as best practices for configuring and managing the system. It also covers topics such as system requirements, deployment scenarios, and troubleshooting.

Lessons

- Understanding the Deep Security Architecture
- Installing and Configuring Deep Security
- Deploying Agents and Relays
- Managing Policies and Rules
- Integrating with Third-Party Solutions
- Troubleshooting and Monitoring Deep Security
- Best Practices for Deep Security Deployment
- Automating Deep Security Deployment
- Securing Cloud Environments with Deep Security
- Securing Containers with Deep Security

After completing this module, students will be able to:

- Understand the architecture of Deep Security and its components
- Configure and deploy Deep Security in a distributed environment
- Implement and manage Deep Security policies and rules
- Monitor and troubleshoot Deep Security deployments

Module 5: Deep Security Administration

Module 5 of the Deep Security Training for Certified Professionals course covers the fundamentals of Deep Security administration. It provides an overview of the Deep Security Manager, the Deep Security Agent, and the Deep Security API. It also covers the installation and configuration of the Deep Security components, as well as the management of policies, rules, and reports.

Lessons

- Understanding Deep Security Architecture
- Configuring and Managing Security Policies
- Implementing Intrusion Detection and Prevention
- Managing Anti-Malware Protection
- Implementing Web Reputation Services
- Managing Firewall Rules
- Configuring Logging and Reporting
- Troubleshooting and Maintaining Deep Security
- Integrating Deep Security with Other Security Solutions
- Best Practices for Deep Security Administration

After completing this module, students will be able to:

- Understand the architecture and components of Deep Security
- Configure and manage Deep Security policies
- Monitor and troubleshoot Deep Security
- Deploy and manage Deep Security agents on various platforms

Module 6: Deep Security Policies

Module 6 of the Deep Security Training for Certified Professionals course covers the fundamentals of creating and managing deep security policies. It covers topics such as policy templates, policy inheritance, policy optimization, and policy enforcement. It also provides hands-on exercises to help students gain a better understanding of how to create and manage deep security policies.

Lessons

- Understanding the Basics of Deep Security Policies
- Creating and Managing Deep Security Policies
- Best Practices for Implementing Deep Security Policies
- Troubleshooting Deep Security Policies
- Auditing and Monitoring Deep Security Policies
- Automating Deep Security Policies
- Integrating Deep Security Policies with Other Security Solutions
- Advanced Deep Security Policies for Compliance and Regulatory Requirements
- Deep Security Policies for Cloud and Virtual Environments
- Deep Security Policies for Mobile Devices

After completing this module, students will be able to:

- Understand the different types of Deep Security policies and how to configure them.
- Create and manage policies to protect virtual machines and applications.
- Utilize the policy templates to quickly deploy security policies.
- Monitor and troubleshoot policy-related issues.

Module 7: Deep Security Reporting

Module 7: Deep Security Reporting is a module in the Deep Security Training for Certified Professionals course that covers the fundamentals of creating and managing reports in Deep Security. It covers topics such as creating custom reports, scheduling reports, and managing report templates. It also covers the various reporting options available in Deep Security, such as the Dashboard, the Event Log, and the Security Report.

Lessons

- Overview of Deep Security Reporting
- Generating Reports in Deep Security
- Customizing Reports in Deep Security

- Scheduling Reports in Deep Security
- Analyzing Reports in Deep Security
- Exporting Reports in Deep Security
- Best Practices for Deep Security Reporting
- Troubleshooting Deep Security Reporting Issues
- Automating Reports in Deep Security
- Integrating Reports with Third-Party Applications

After completing this module, students will be able to:

- Understand the different types of reports available in Deep Security
- Create custom reports to meet specific security and compliance requirements
- Utilize the reporting API to automate report generation
- Analyze reports to identify security trends and anomalies

Module 8: Deep Security Troubleshooting

Module 8 of the Deep Security Training for Certified Professionals course covers the fundamentals of troubleshooting Deep Security. It provides an overview of the troubleshooting process, including how to identify and resolve common issues, as well as how to use the Deep Security Manager and the Deep Security Agent to diagnose and resolve problems. The module also covers best practices for troubleshooting and provides an introduction to the Deep Security Support Portal.

Lessons

- Identifying and Resolving Common Deep Security Issues
- Troubleshooting Deep Security Agent Connectivity
- Investigating and Resolving Deep Security Agent Performance Issues
- Analyzing and Resolving Deep Security Policy Conflicts
- Investigating and Resolving Deep Security Firewall Rule Issues
- Troubleshooting Deep Security Manager Connectivity
- Investigating and Resolving Deep Security Manager Performance Issues
- Analyzing and Resolving Deep Security Manager Database Issues
- Investigating and Resolving Deep Security Manager Logging Issues
- Troubleshooting Deep Security Manager User Access Issues

After completing this module, students will be able to:

- Identify and troubleshoot common issues related to Deep Security
- Utilize the Deep Security Manager to diagnose and resolve problems
- Understand the various log files and how to interpret them
- Implement best practices for monitoring and maintaining Deep Security deployments

Module 9: Deep Security Best Practices

Module 9 of the Deep Security Training for Certified Professionals course provides an in-depth look at

best practices for using Deep Security. It covers topics such as security policies, system hardening, patch management, and logging and auditing. It also provides guidance on how to use Deep Security to protect against threats and vulnerabilities.

Lessons

- Understanding the Basics of Deep Security
- Implementing Security Policies in Deep Security
- Securing Network Connections with Deep Security
- Automating Security Tasks with Deep Security
- Best Practices for Deploying Deep Security
- Troubleshooting Deep Security Issues
- Optimizing Performance with Deep Security
- Integrating Deep Security with Other Security Solutions
- Managing Deep Security in the Cloud
- Auditing and Reporting with Deep Security

After completing this module, students will be able to:

- Understand the best practices for deploying and managing Deep Security
- Implement the most effective security policies for Deep Security
- Utilize the most efficient methods for monitoring and responding to security threats
- Develop strategies for optimizing the performance of Deep Security

Module 10: Deep Security Automation

Module 10 of the Deep Security Training for Certified Professionals course covers the fundamentals of Deep Security Automation. This module provides an overview of the automation capabilities of Deep Security, including how to use the Deep Security API, how to create automation scripts, and how to use the Deep Security Automation Center. It also covers best practices for automating security operations and how to use automation to improve security posture.

Lessons

- Introduction to Deep Security Automation
- Automating Security Policies with Deep Security
- Automating Security Audits with Deep Security
- Automating Security Incident Response with Deep Security
- Automating Security Compliance with Deep Security
- Automating Security Monitoring with Deep Security
- Automating Security Reporting with Deep Security
- Automating Security Remediation with Deep Security
- Automating Security Orchestration with Deep Security
- Automating Security Threat Detection with Deep Security

After completing this module, students will be able to:

- Understand the fundamentals of Deep Security Automation and its components.
- Develop and deploy automation scripts to automate security tasks.
- Utilize the Deep Security API to integrate with other security solutions.
- Monitor and troubleshoot automation scripts and tasks.

Module 11: Deep Security Integration with Other Security Solutions

Module 11 of the Deep Security Training for Certified Professionals course covers the integration of Deep Security with other security solutions. It provides an overview of the various integration options available, including integration with SIEMs, vulnerability scanners, and other security solutions. It also covers the steps required to configure and manage the integration.

Lessons

- Overview of Deep Security Integration with Other Security Solutions
- Benefits of Integrating Deep Security with Other Security Solutions
- Best Practices for Integrating Deep Security with Other Security Solutions
- Troubleshooting Common Issues with Deep Security Integration
- Automating Deep Security Integration with Other Security Solutions
- Security Considerations for Deep Security Integration
- Case Studies of Deep Security Integration with Other Security Solutions
- Advanced Techniques for Deep Security Integration
- Security Auditing for Deep Security Integration
- Security Compliance for Deep Security Integration

After completing this module, students will be able to:

- Understand the integration of Deep Security with other security solutions such as firewalls, intrusion prevention systems, and antivirus solutions.
- Develop the ability to configure and deploy Deep Security to integrate with other security solutions.
- Learn how to monitor and troubleshoot Deep Security integration with other security solutions.
- Gain the skills to optimize the performance of Deep Security when integrated with other security solutions.

Module 12: Deep Security Compliance and Auditing

Module 12 of the Deep Security Training for Certified Professionals course covers the fundamentals of deep security compliance and auditing. It provides an overview of the different types of compliance and auditing standards, as well as the tools and techniques used to ensure compliance. It also covers the importance of security policies and procedures, and how to develop and implement them. Finally, it covers the basics of auditing and reporting, and how to use the results to improve security posture.

Lessons

- Understanding Security Compliance Frameworks
- Implementing Security Auditing and Monitoring
- Automating Security Auditing and Compliance

- Analyzing Security Audit Results
- Developing Security Compliance Policies
- Managing Security Compliance and Auditing
- Troubleshooting Security Compliance Issues
- Best Practices for Security Compliance and Auditing
- Security Compliance and Auditing in the Cloud
- Security Compliance and Auditing for Mobile Devices

After completing this module, students will be able to:

- Understand the principles of security compliance and auditing in the context of Deep Security.
- Identify and implement best practices for security compliance and auditing in Deep Security.
- Develop and execute security compliance and auditing plans for Deep Security.
- Analyze and interpret security compliance and auditing results for Deep Security.

Module 13: Deep Security Advanced Topics

Module 13: Deep Security Advanced Topics covers the more complex aspects of Deep Security, such as advanced configuration, troubleshooting, and automation. It provides an in-depth look at the features and capabilities of Deep Security, and how to use them to protect your environment. This module is designed for experienced Deep Security professionals who want to take their knowledge to the next level.

Lessons

- Advanced Configuration of Deep Security
- Automation and Orchestration of Deep Security
- Advanced Security Analytics with Deep Security
- Advanced Threat Detection with Deep Security
- Advanced Incident Response with Deep Security
- Advanced Security Policies with Deep Security
- Advanced Security Compliance with Deep Security
- Advanced Security Auditing with Deep Security
- Advanced Security Monitoring with Deep Security
- Advanced Security Reporting with Deep Security

After completing this module, students will be able to:

- Understand the architecture and components of Deep Security
- Configure and manage Deep Security policies
- Troubleshoot and optimize Deep Security deployments
- Implement advanced features such as virtual patching, application control, and intrusion prevention