PowerShell Scripting for Security Administrators Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the face of relentless cyber threats and the complexity of modern IT environments, manual security administration is no longer tenable. PowerShell Scripting for Security Administrators Training Course is designed to transform IT and security professionals into automation experts proficient in hardening, monitoring, and responding to threats across Windows and hybrid cloud platforms. Participants will master offensive and defensive PowerShell techniques, moving beyond basic cmdlets to write robust, secure scripts for tasks like rapid incident response, system configuration auditing, and advanced forensics. The focus is on leveraging PowerShell's deep system access a double-edged sword often used by adversaries to implement Just Enough Administration (JEA) and robust logging and auditing to significantly reduce the organizational attack surface.

This course is a critical deep dive into security automation and DevSecOps principles applied to Microsoft ecosystems. You'll gain practical, hands-on experience in building defensive scripts that integrate with core security infrastructure like Active Directory, Windows Defender, and cloud security APIs. By adopting a "Blue Team" mindset informed by "Red Team" tactics, you will learn to detect and mitigate fileless attacks, strengthen security baselines using Desired State Configuration (DSC), and generate clear, actionable compliance reports. This essential skillset positions you at the forefront of modern security operations, empowering you to scale your security efforts and enforce a state of continuous compliance and proactive defense.

Programme Curriculum

PowerShell Scripting for Security Administrators Training Course

Introduction

In the face of relentless cyber threats and the complexity of modern IT environments, manual security administration is no longer tenable. PowerShell Scripting for Security Administrators Training Course is designed to transform IT and security professionals into automation experts proficient in hardening, monitoring, and responding to threats across Windows and hybrid cloud platforms. Participants will master offensive and defensive PowerShell techniques, moving beyond basic cmdlets to write robust, secure scripts for tasks like rapid incident response, system configuration auditing, and advanced forensics. The focus is on leveraging PowerShell's deep system access a double-edged sword often used by adversaries to implement Just Enough Administration (JEA) and robust logging and auditing to significantly reduce the organizational attack surface.

This course is a critical deep dive into security automation and DevSecOps principles applied to Microsoft ecosystems. You'll gain practical, hands-on experience in building defensive scripts that integrate with core security infrastructure like Active Directory, Windows Defender, and cloud security APIs. By adopting a "Blue Team" mindset informed by "Red Team" tactics, you will learn to detect and mitigate fileless attacks, strengthen security baselines using Desired State Configuration (DSC), and generate clear, actionable compliance reports. This essential skillset positions you at the forefront of modern security operations, empowering you to scale your security efforts and enforce a state of continuous compliance and proactive defense.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Automate Incident Response workflows using PowerShell, significantly reducing mean time to detection (MTTD) and mean time to resolution (MTTR).
2. Implement and enforce the Principle of Least Privilege across Windows infrastructure using Just Enough Administration (JEA).
3. Design and deploy secure, robust scripts utilizing Advanced PowerShell Functions for enterprise-level automation.
4. Master PowerShell Logging and Auditing configurations for superior threat hunting and forensics.
5. Develop scripts for Configuration Auditing of critical system settings, identifying deviations from security baselines.
6. Understand and mitigate Fileless Malware and Living-Off-The-Land (LOTL) attack techniques that leverage native PowerShell.
7. Apply Desired State Configuration (DSC) to automate security baseline hardening and achieve continuous compliance.
8. Securely handle and manage sensitive data like Credentials and Secrets within scripts using secure strings and vaults.
9. Leverage PowerShell to manage security components in a Hybrid Cloud environment
10. Integrate PowerShell scripts with Security Information and Event Management (SIEM) and ticketing systems for alert automation.
11. Perform basic Digital Forensics and Endpoint Analysis by scripting log collection and process inspection.
12. Utilize Antimalware Scan Interface (AMSI) logging and bypass techniques to improve detection capabilities.
13. Write Idempotent and fault-tolerant scripts with robust Error Handling for reliable security automation.

Target Audience

1. Security Administrators / Engineers.

2. System Administrators
3. Security Analysts.
4. Incident Response (IR) Team Members.
5. Compliance and Audit Officers.
6. DevSecOps Engineers.
7. Penetration Testers
8. IT Managers.

Course Modules

Module 1: PowerShell Security Fundamentals and Core Scripting

- Understanding PowerShell's core security features.
- Mastering the pipeline and working with objects for security data manipulation.
- Writing secure, modular scripts using Advanced Functions and parameter validation.
- Securely handling sensitive inputs using Read-Host -AsSecureString and storing credentials.
- Case Study: The Credential Harvesting Bypass.

Module 2: Auditing and Hardening Windows Security Baselines

- Scripting system configuration auditing for critical settings
- Utilizing built-in cmdlets to check and enforce Group Policy Object settings remotely.
- Automating patch and vulnerability status checks across multiple servers.
- Developing scripts to audit and remediate local user accounts and administrator group memberships.
- Case Study: Compliance-as-Code Implementation.

Module 3: Advanced Logging, Auditing, and Threat Hunting

- Deep dive into Script Block Logging, Module Logging, and Transcription Logging for forensic readiness.
- Configuring Windows Event Forwarding and Sysmon via PowerShell for centralized security visibility.
- Writing scripts to filter, parse, and analyze massive volumes of security log data for IOCs.
- Integrating PowerShell to push security event data to a SIEM or log aggregation platform.
- Case Study: Detecting Fileless Attacks.

Module 4: Just Enough Administration (JEA)

- Defining its purpose and the security principle of least privilege.
- Configuring Role Capability Files and Session Configuration Files to restrict user access.
- Creating a JEA endpoint to delegate specific, non-administrative tasks
- Testing and troubleshooting JEA configurations to ensure the security boundary holds.
- Case Study: JEA for Help Desk Operations.

Module 5: Security Automation with Desired State Configuration (DSC)

- Components, configuration documents, and the Local Configuration Manager
- Writing DSC configurations to enforce security baselines
- Implementing the Pull Server or using Azure Automation for large-scale, continuous state management.
- Auditing current system state against the DSC baseline to flag non-compliance.
- Case Study: Automated Infrastructure Hardening.

Module 6: Incident Response and Digital Forensics Scripting

- Rapidly gathering volatile and non-volatile forensic data
- Scripting the automatic quarantine of compromised endpoints and disabling of user accounts.
- Using PowerShell to interact with Windows Defender or third-party AV/EDR APIs.
- Developing scripts for quick file integrity checks and finding known bad hashes.
- Case Study: WannaCry/NotPetya Response Script.

Module 7: Red Team Tactics and Defensive Scripting

- Understanding how attackers utilize PowerShell for reconnaissance, privilege escalation, and lateral movement.
- Implementing Constrained Language Mode to block advanced attack techniques.
- Scripting checks for common adversary techniques
- Leveraging PowerShell to query and manage the Antimalware Scan Interface for script defense.
- Case Study: Blue Team and Red Team Simulation

Module 8: Hybrid Cloud Security Automation

- Utilizing Azure PowerShell for cloud resource security management
- Scripting security and compliance reports for Microsoft 365
- Automating user access review and license management for cloud identities.
- Securing access to cloud resources from PowerShell using managed identities and service principals.
- Case Study: Cloud Misconfiguration Remediation.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com