

Table of Contents

PREFACE	i
Chapter Layout and Conventions	i
Chapter Layout	i
Conventions	i
Author's Notes and Findings	i
INTRODUCTION	1
The Security and Compliance Centers and PowerShell	1
Why PowerShell and Not the Security and Compliance Centers	1
Security and Compliance Center PowerShell Module	1
Command Structure	2
Cmdlet Examples	2
Piping	3
Protecting Yourself and What If	4
Command Discovery Techniques	4
PowerShell Modules	5
Getting Help!?!	6
Cloud-Only vs Synced Environments	7
Non-Synced Accounts (Cloud-Only)	8
Synced Accounts	8
What's Next?	8
-What's New -	9
Security and Compliance Center Changes	9
Book Formatting	10
Conclusion	10
1. PowerShell Basics	12
Security and Compliance Center PowerShell Module: Where to Begin	12
Variables	12
Arrays	13
Hash Tables	13
CSV Files	14
Operators	14
Loops	16
Foreach-Object	16
Do { } While ()1	16

Export-CSV	18
Functions.....	18
Visual Studio Code.....	19
VSC Plug-ins and More	22
Good Features	24
2. Beyond the Basics	27
Formatting.....	27
Capitalization.....	27
Commenting.....	28
Mind Your Brackets!.....	30
Command Output	31
Cmdlet Output Formatting	31
Filtering	33
Splitting.....	35
Scripting in Color	37
Miscellaneous.....	39
Quotes.....	39
Code Signing	41
Signing Your Code	43
3. Connecting with PowerShell	46
Introduction.....	46
Connecting to the Security and Compliance Centers.....	47
Security and Compliance Center PowerShell Cmdlets.....	48
Closing and Removing Connections.....	49
Removing PowerShell Sessions.....	50
Expired Session.....	51
4. Connecting to ExO (v3).....	52
Introduction.....	52
Prerequisites	53
Vetting Prerequisites	53
Connecting to Exchange Online with v3 Cmdlets.....	57
Office 365 Cmdlets.....	58
The New Exchange Online Cmdlets	59
Reducing Data.....	59
Property Sets	60
Properties.....	60
Real World Experience.....	61
Connect to Azure Active Directory	61

Managing Office 365 Mailboxes from On-Premises PowerShell	61
Exchange Online v3 Next Steps	68
Final Thoughts on the new ExO v3 cmdlets:	83
Azure CloudShell and Exchange Online	83
Azure Portal Access.....	83
Shell.Azure.Com.....	85
5. Identity Management	87
Introduction	87
Directory Synchronization (DirSync)	87
Preparing Your AD - IdFix	88
Install of Azure AD Connect	92
PowerShell and Directory Synchronization	98
What Needs to be Performed Where?	99
Active Directory	99
Azure Active Directory Connect	102
Licensing	108
Azure AD Recycle Bin	116
6. Security	118
Layered Security	118
Role Groups	118
Management Roles per Role Groups.....	121
Assigning Role Group Membership	122
Mail Flow Administrator Role.....	123
Reviewer Role	125
Records Management.....	126
Security Administrator	128
Organization Management.....	129
Supervisory Review	129
Security Reader	130
Compliance Administrator	131
eDiscovery Manager/Administrator	131
Security Operator.....	133
Compliance Data Administrator.....	133
Data Investigator.....	134
Global Reader.....	134
Insider Risk Roles	135
Quarantine Administrator.....	137
IRM Contributors	138

Content Explorer List Viewer and Content Explorer Content Viewer	138
Removing User(s) From Role Groups	139
Management Roles.....	144
Audit in Security and Compliance Center PowerShell	146
Searching the Admin Audit Log.....	148
7. Alerting	152
Introduction.....	152
Activity Alerts	152
Protection Alerts	157
Beyond the New	161
8. Defender for Office.....	163
Introduction.....	163
General MDO Cmdlets	163
Exchange Online Protection (EOP) Protection Policy Rule.....	168
Email & Collaboration Policies.....	171
Introduction	171
Anti-Phishing.....	171
Safe Attachments.....	183
Tenant Allow / Block List Items.....	190
Advanced Delivery	196
Phishing Simulation Overrides	197
SecOps Mailbox Overrides.....	201
Enhanced Filtering.....	203
Office 365 Advanced Threat Protection Recommended Configuration Analyzer (ORCA).....	206
Preview vs Stable Versions.....	206
How to Use ORCA	208
Configuration Analyzer	213
Microsoft Defender for Office 365 Evaluation Mode.....	215
9. Submissions	219
Introduction.....	219
User Submissions.....	219
End User Experience	219
Send the Reported Messages To.....	220
Turn Off Report Message for Outlook	220
Customize the end user confirmation message.....	221
Customizing the end user reporting options	221
Administrator Submissions	223
PowerShell.....	224

Submission Policy	224
Admin Notifications - Customized	226
Remove a Report Submission Policy.....	228
Conclusion.....	228
10. Threats and Mail Flow	229
Introduction.....	229
Threat Management.....	229
Investigations	229
Dashboard	230
Explorer	230
Campaigns.....	231
Threat Tracker	232
Attack Simulator.....	232
Security Admin Center.....	233
Mail Flow.....	237
Review.....	238
Quarantine	239
New Exchange Online Quarantine Cmdlets	243
Restricted Users.....	250
Conclusion.....	251
11. Compliance.....	253
Introduction.....	253
Compliance Cases	253
Compliance Searches	256
What is a Compliance Search?	256
Retention Compliance	268
Adaptive Scopes.....	273
Microsoft Compliance Configuration Analyzer (MCCA)	277
User Data Search	281
12. Communication Compliance.....	285
Introduction.....	285
Communication Compliance	285
Why Use Communication Compliance?	285
Compliance Center.....	286
New Policy	287
Policy States.....	288
Customizing Existing Policies.....	292
Notice Template.....	298

Privacy Settings.....	300
Recommendations	301
13. Data Loss Prevention	302
Introduction.....	302
Sensitive Information Types.....	302
Custom Sensitive Information Types.....	305
Fingerprints.....	311
Keyword Dictionaries	315
Exact Data Match (EDM).....	317
DLP Compliance.....	323
Fingerprints	324
Keyword Dictionary.....	324
Exact Data Match (EDM)	324
Other DLP Cmdlets	326
14. Device Management	329
Introduction.....	329
Connecting to Exchange Online	330
Tenant Policy and Rule	333
Device Conditional Access	335
Device Configuration.....	338
15. Information Barriers	342
Introduction.....	342
Information Barriers.....	342
What are Information Barriers?	342
Getting Started with Information Barriers.....	342
Permissions required.....	343
Filterable Attributes	343
Information Barrier Segments	344
Information Barrier Policies	345
PowerShell	347
Prerequisites	348
Administrative Consent.....	348
PowerShell.....	350
Real World Experience.....	354
Caveats to Blocking.....	355
Documenting Settings (Script)	355
PowerShell	355
Conclusion.....	362

16. Insider Risk Management.....	363
Introduction.....	363
Prerequisites.....	363
Policy Creation.....	364
Policy Indicators.....	366
Insider Risk Policy Creation.....	372
Creating a Policy Via PowerShell Only.....	377
Set-InsiderRiskPolicy.....	382
Removing Policies.....	384
Policy Templates.....	385
Further Use Case Scenarios for Insider Risk.....	385
New PowerShell Cmdlets.....	385
17. Labels.....	386
Introduction.....	386
Labels.....	386
Label Priorities.....	386
Labels in the Purview Compliance console.....	387
PowerShell.....	387
Creating Labels.....	388
New Labels and Policies.....	388
New-Label.....	391
Set-Label.....	392
Get-Label.....	393
Remove-Label.....	394
Label Policies.....	394
New-LabelPolicy.....	395
Set-LabelPolicy.....	395
Removing a Label Policy.....	398
Best Practices for Sensitivity Labels.....	398
AutoSensitivityLabel.....	398
Requirements.....	399
Create New Auto Sensitivity Label Policy.....	400
Removing a Policy.....	402
Modifying a Policy.....	403
Auto Sensitivity Label Rules.....	404
AIP Scanner.....	406
Installation.....	406
Concepts.....	409

AIP Repositories	411
Microsoft Information Protection (MIP) Discovery Cmdlets.....	412
Uninstalling the MIP Network Discovery Service	414
File Plans	416
How To Use File Plan Properties?	421
18. Privacy Management	423
Introduction	423
Purview Compliance Console	424
Policies Tabs.....	426
PowerShell.....	426
Conclusion.....	433
19. Building Scripts	435
How to Begin.....	435
Documenting the Defender and Purview Compliance Centers	435
Coding the Script	435
Where to Start.....	436
PowerShell and Change	441
Coding the Script	442
Script Summary	447
Script Building Summary	447
20. Reporting.....	448
Introduction	448
Screenshots.....	448
TXT Files.....	448
Explanation of the Script.....	450
CSV Files	451
HTML Files	453
Quick HTML Reports.....	454
Adding Polish – Refining HTML Reports	455
Detailed, Complex HTML Reporting.....	457
SMTP Delivery	460
File Copy.....	462
Conclusion.....	464
21. Troubleshooting	465
Introduction	465
Breaking up the Script	465
Pause and Sleep	465
Write-Host.....	467

Comments	468
Visual Studio Code.....	470
Debugging	471
Try and Catch	472
ErrorAction.....	473
Transcript	474
Deciphering Error Messages	475
Access Denied	476
Variables.....	477
Arrays	480
Conclusion.....	480
A. Best Practices.....	482
What is a Best Practice?	482
Summary of Best Practices.....	482
PowerShell Best Practices.....	482
Commenting	482
Useful Comments	483
Variable Naming	483
Variable Block.....	483
Matching Variables to Parameters.....	484
Preference Variables	484
Naming Conventions, this time for Functions and Scripts.....	485
Singular Task Functions.....	485
Signing Your Code	486
Filter vs. Where	486
Error Handling.....	486
Write-Output / Write-Verbose	486
'#Requires'	488
Capitalization.....	491
Using full command names	491
Cmdlet Binding	492
Script Structure	493
Quotes.....	494
Running Applications.....	494
Conclusion and Further Help.....	494
B. Miscellaneous	495
Introduction	495
Menus	495

Aliases	499
Foreach-Object (%).....	503
Code Summary	506
PowerShell Interface Customization	507
C. Microsoft Secure Score.....	512
Introduction.....	512
Metrics & Trends.....	518
PowerShell and Microsoft Secure Score.....	519
Detailed Analysis.....	519
Conclusion.....	519