

Get rid of recurring management tasks with PowerShell in 5 steps

Automate. Delegate. Relax.

Heiko Brenn  @heikobrenn





ScriptRunner®

The #1 for PowerShell Management

Unlock the Power of PowerShell

+49

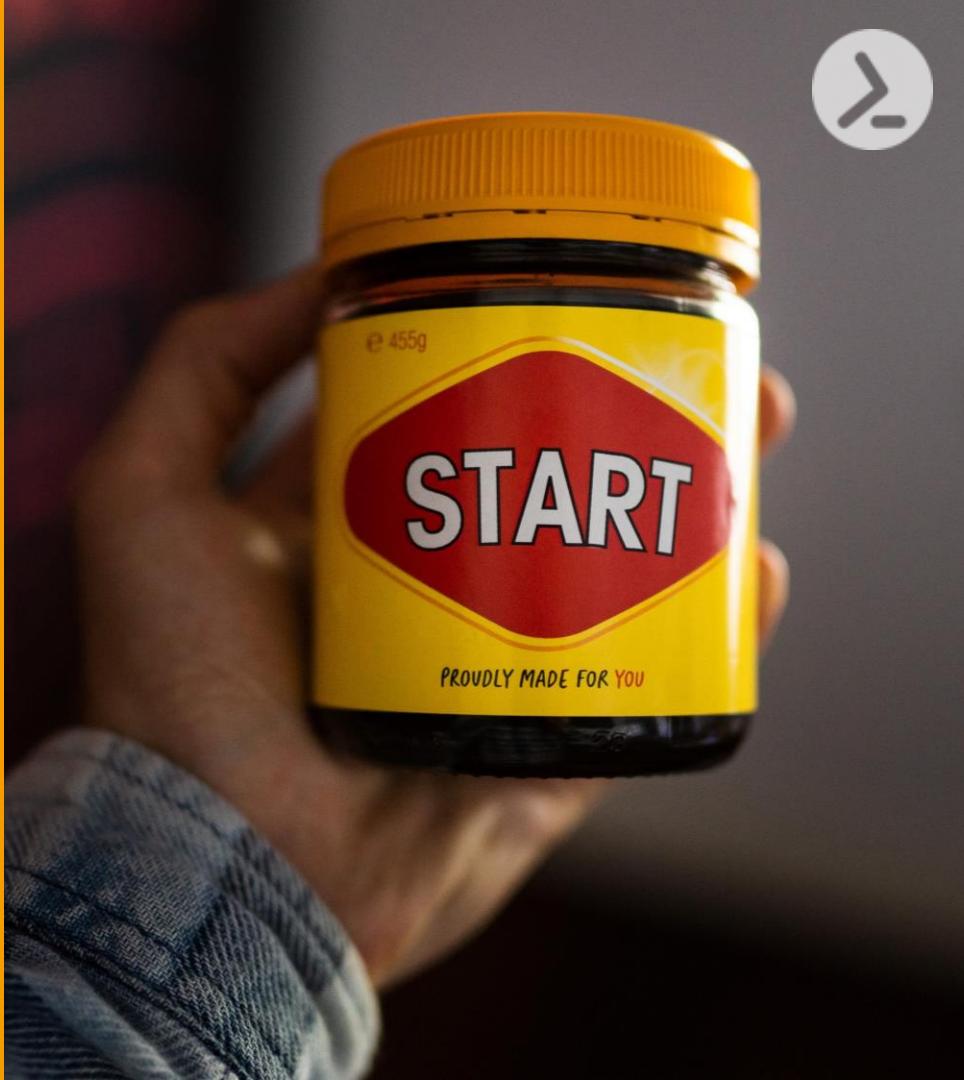
2014

24

1819

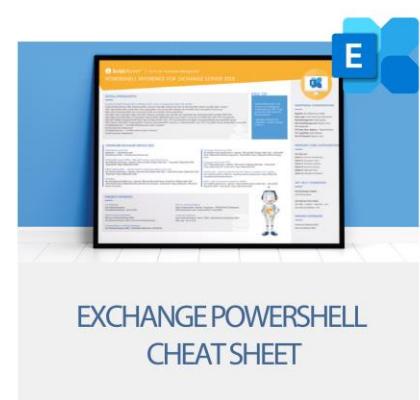
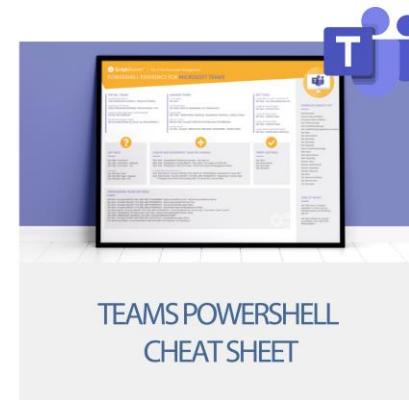
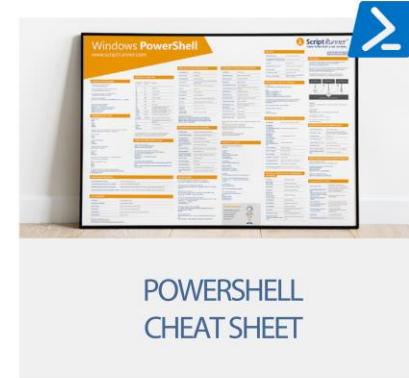
Hundreds of free
and ready-to-use
PowerShell scripts.

github.com/scriptrunner/ActionPacks



Get your free PowerShell goodies

lp.scriptrunner.com/en/powershell-goodies



STANDARDIZATION, AUTOMATION AND DELEGATION OF RECURRING TASKS



AUTO-CREATED
USER FRIENDLY
WEB FORMS

SECURE
CREDENTIAL
ADMINISTRATION

CENTRALIZED SCRIPTS AND
MODULES MANAGEMENT

INTERACTIVE, SCHEDULED
AND EVENT-DRIVEN
SCRIPT EXECUTION

COMPREHENSIVE
MONITORING AND
REPORTING





Automating with
PowerShell
-
Potential
and
Challenges

Let's unlock the
Power of PowerShell

Why PowerShell?

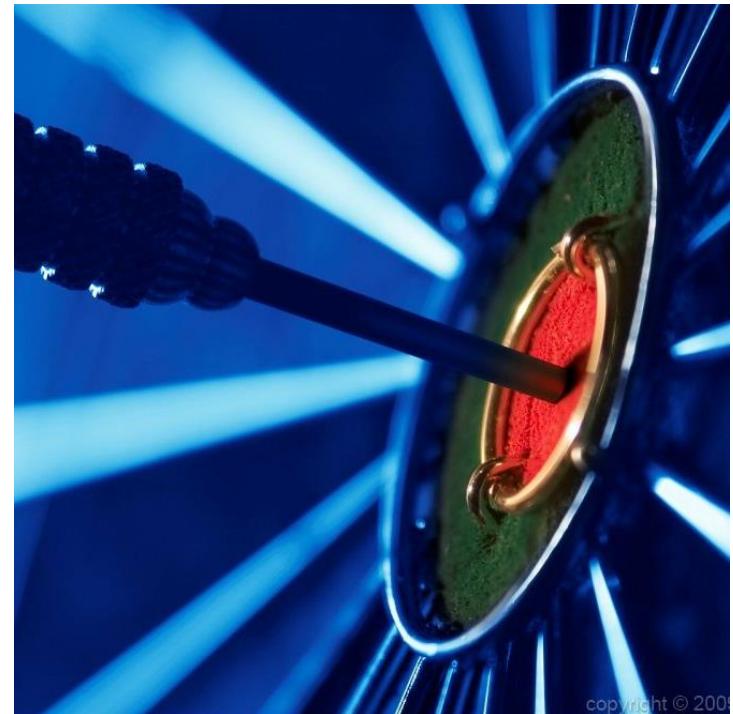
Very mature command-line shell
and scripting language for IT automation

Great framework to automate
recurring tasks consistently

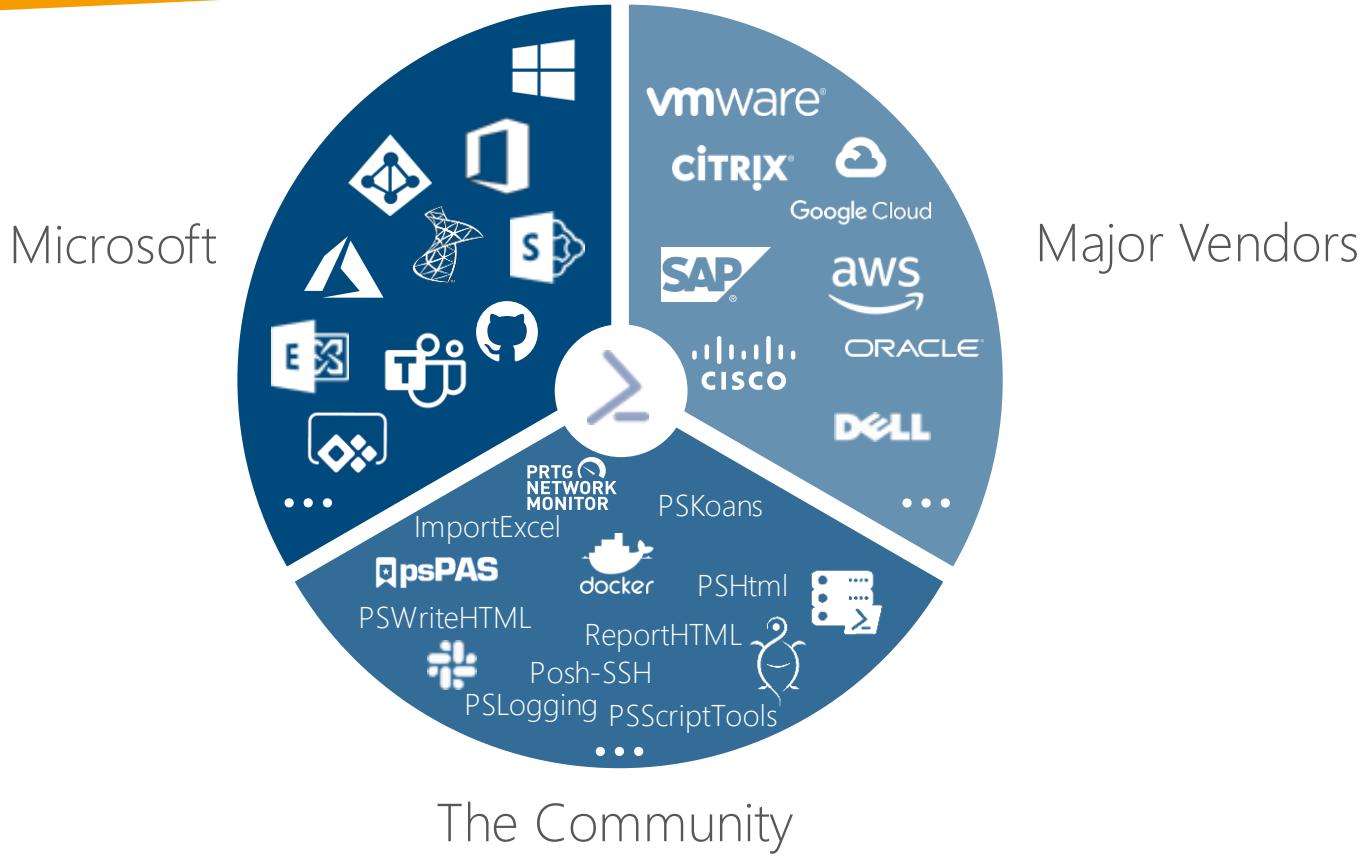
Simplifies administration of your
entire IT infrastructure

Strong commitment from Microsoft
and many other vendors

Very vital worldwide community

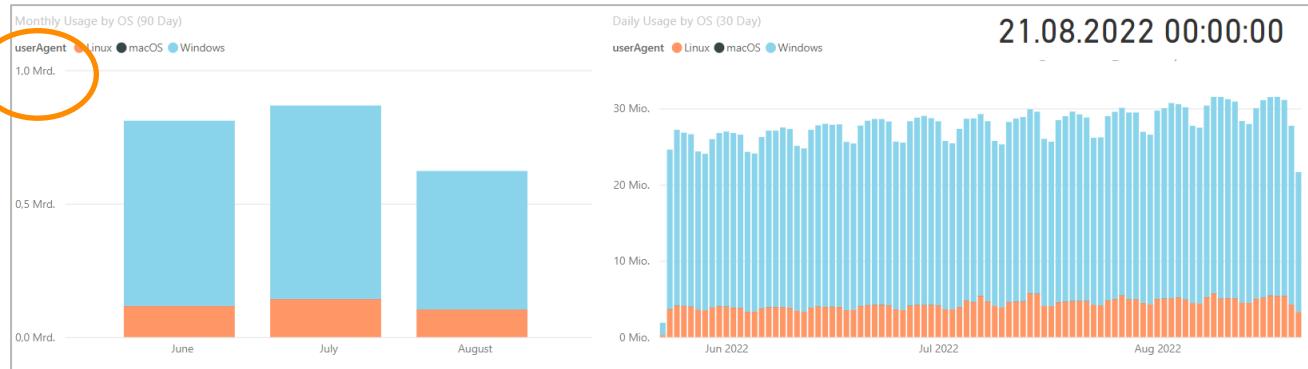
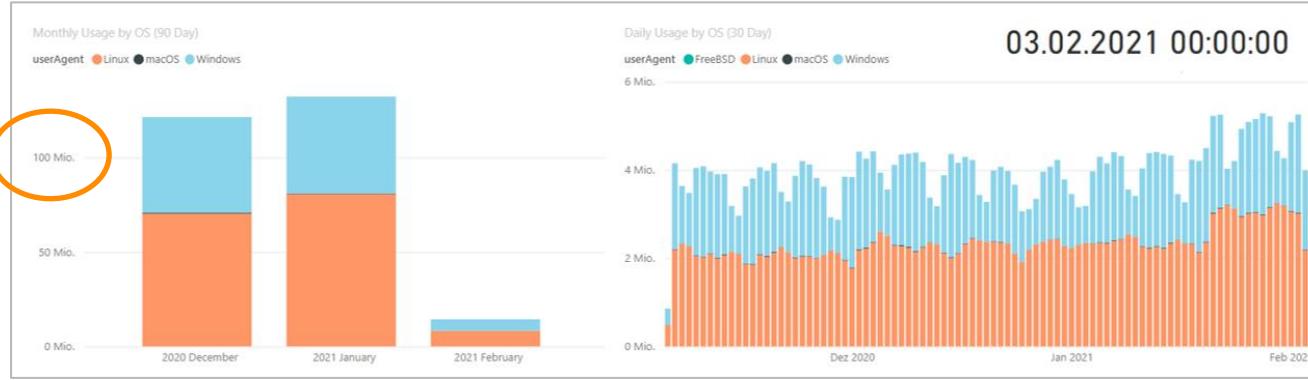


The PowerShell Ecosystem



The Community

PowerShell 7 usage is growing



Two ways of using PowerShell



PowerShell challenges



Let's face it.
Not everyone is a scripting expert

„De-centralized“ PowerShell landscape

How to enable support teams & LOB
users to use PowerShell?

Know-how bottlenecks
Security concerns (credentials)

PowerShell is only used by
a few IT experts



Unlock the power of PowerShell in 5 steps



Centralized script and module management

Secure credential and permission management

Great user experience
Easy-to-use interface

Flexible & secure delegation

Comprehensive monitoring and reporting



Centralized script and module management



Screenshot of the ScriptRunner web interface showing a centralized management of scripts and modules.

The left sidebar includes:

- Dashboard
- Run
- Authorize & Delegate
- Monitoring
- Configuration (selected)
- Actions
- Queries
- Targets
- Scripts (selected)
- Credentials
- Settings

The main area shows the "Scripts" list with 9 of 1282 scripts:

- Get-EOOutOfOffice.ps1
- Set-EOOutOfOffice - Copy (2).ps1
- Set-EOOutOfOffice - Copy.ps1
- Set-EOOutOfOffice.ps1** (Checked out by me)
- Set-EOOutOfOffice.ps1
- Set-EOOutOfOffice.ps1
- Set-EOOutOfOffice_orig.ps1
- TeamsWithOutOwner-Scheduled.ps1
- TeamsWithOutOwner.ps1
- Webinar_Set-ExOutOfOffice.ps1

The selected script, "Set-EOOutOfOffice.ps1", is shown in the details view:

- Configuration tab (General, Header information)
- Code editor** tab (selected)
- Information tab (Change history, Used by)

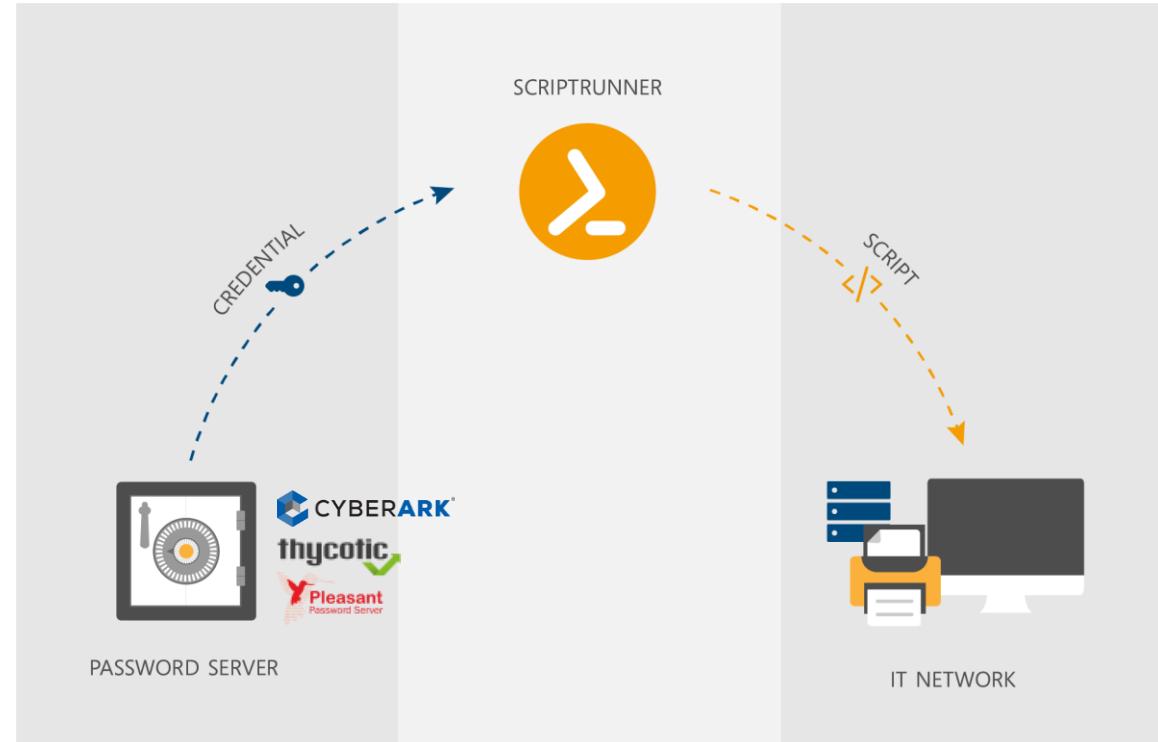
The code editor displays the PowerShell script content:

```
$PSCmdlet = Get-Module -Name PSOutlook -ListAvailable | Select-Object -First 1
$AutoReplyType = $PSCmdlet.ParameterSetName
$cmdargs = @()
if($AutoReplyType -eq "Disable Auto Reply"){
    $cmdargs.add("AutoReplyState", "Disabled")
    $msg += "disabled"
}
else{
    if($AutoReplyType -eq "Only contact list members"){
        $ReplyType = "Known"
    }
    if($AutoReplyType -eq "Internal only"){
        $ReplyType = "None"
    }
}
```

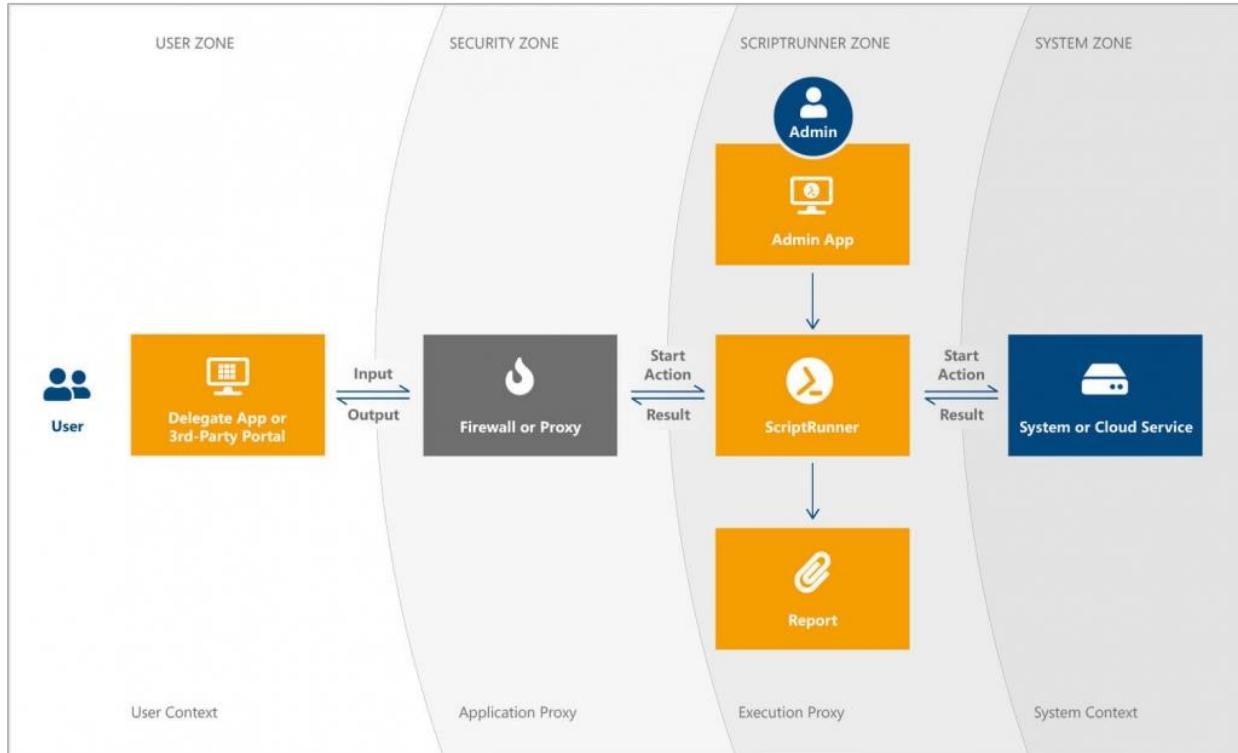
Password Server Support



- Centralized password safes
 - CyberArk Password Vault
 - Pleasant Password Server
 - Thycotic Secret Server
- No credentials are stored locally
- Automatic password rotation
- One single secure password repository for multiple ScriptRunner instances



Secure delegation without back-end access/permissions



The Register®

using the hijacked H1 account to post updates on bounty submissions to brag about the degree of their pwnage, claiming they have all kinds of superuser access within the ride-hailing app biz.

It also means the intruder has access to Uber's security vulnerability reports.

Infosec watcher Corben Leo, meanwhile, [said](#) he spoke to the miscreant responsible for this mess.

We're told that an employee was socially engineered by the attacker to gain access to Uber's VPN, through which the intruder scanned the network, found a PowerShell script containing the hardcoded credentials for an administrator user in Thycotic, which were then used to unlock access to all of Uber's internal cloud and software-as-a-service resources, among other things.

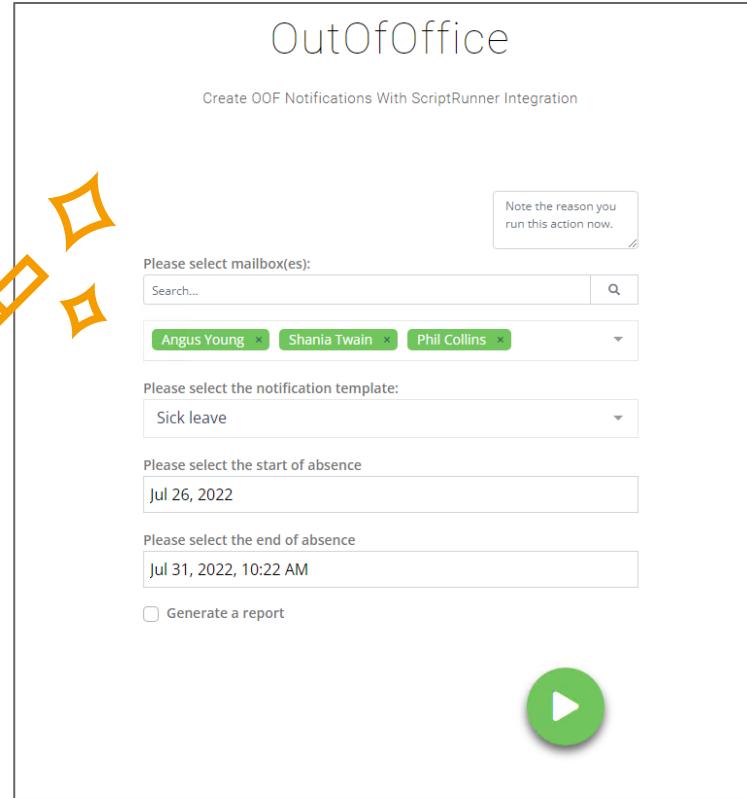
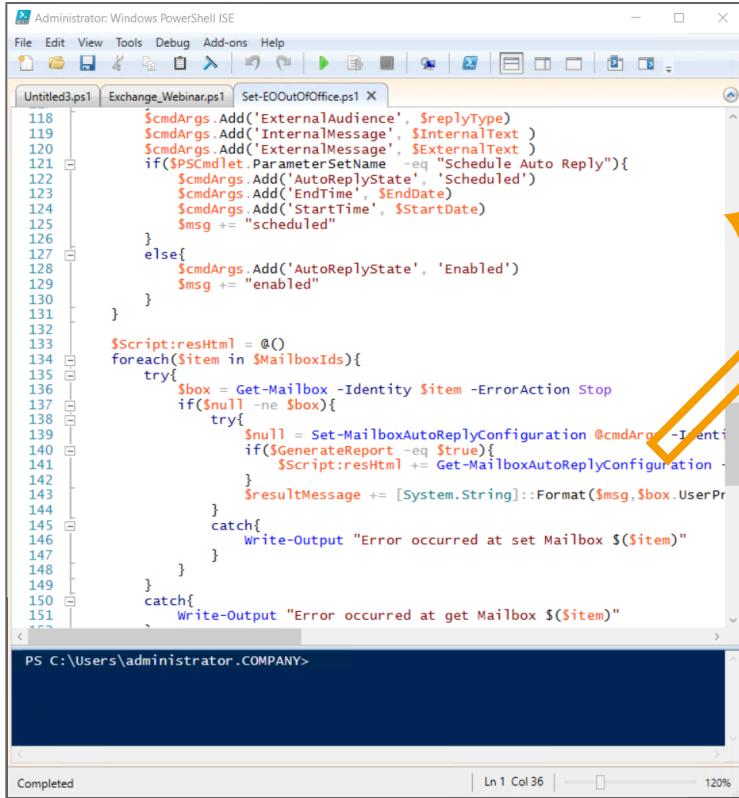
After that, everything was at the intruder's fingertips, allegedly.

Judging from screenshots leaked onto Twitter, though, an intruder has compromised Uber's AWS cloud account and its resources at the administrative level; gained [admin control over the corporate Slack workspace](#) as well as its [Google G Suite account that has over 1PB of storage in use](#); has control over Uber's [VMware vSphere deployment](#) and virtual machines; [access to internal finance data](#), such as corporate expenses; and more.

If this correct, Uber has been significantly compromised with data and infrastructure at multiple levels available to the intruder. This likely includes customers and drivers' personal data.

There have been further claims of [unauthorized access to a Confluence installation](#), private source code repositories, and a [SentinelOne security dashboard](#) used by the app developer's incident response team.

PowerShell for Everyone



The Script

Flexible & secure delegation



The screenshot shows the ScriptRunner web application interface for managing Active Directory delegations. The left sidebar has a dark blue header with the "ScriptRunner" logo and navigation links: Dashboard, Run, Authorize & Delegate (selected), Monitoring, Configuration, and Settings. The main content area has a light gray header with a back arrow, the text "End users", and a "Authorize & Delegate" link. Below this is a title "Active Directory Self-Services" and a sub-header "Delegations". On the left, a sidebar titled "CONFIGURATION" lists "Main administrator", "Administrators", "Help desk users", and "End users" (with a count of 3). The "Delegations" item under "End users" is highlighted with a blue bar. At the top of the main content area are "Save" and "Delete" buttons. The main content area contains a section titled "Delegations" with a sub-section "Assigned actions (More ...)" containing several items:

- AD: Show Active Directory User Properties (Get-ADUser) (highlighted with a yellow background)
- Advanced Active Directory Report
- Reset password for Active Directory user
- Change Active Directory User Properties

Below this is a section titled "Local: Add two values" with a list of actions:

- Simulate Set-ADUserPropertiesDemo
- Test-Cascaded ADQueries
- Get-ExMailboxProperties
- Remove-PrintJob
- Validation possibilities

A "Press enter to remove" button is located at the bottom right of the assigned actions list.

Comprehensive monitoring and reporting



Screenshot of the ScriptRunner interface showing the 'Live Monitor' dashboard.

The dashboard displays the following information:

- Running scripts:** 3 (indicated by a large number '3').
- Script status chart:** A horizontal bar chart showing 3 'Running' scripts and 0 'Queued' scripts.
- Metrics summary:** 2 Actions, 0 Queued, 1 Scheduled, 1 Queries.
- Advanced Active Directory Report:** A report window showing the progress of a report execution.
 - Logs:

```
99: WARNING: Cannot resolve the manager, on the group 'Bass-AU'.
100: Done!
101: Working on Organizational Units Report...
102: Done!
103: Working on Users Report...
104: Done!
105: Working on Group Policy Report...
106: Done!
107: Working on Computers Report...
108: Done!
109: Compiling Report...
110:
```
 - Progress bar: Shows the report is nearly complete.
- Action filters:** Buttons for Actions (checked), Scheduled (checked), Queued (unchecked), and Queries (unchecked).
- Filter by servers:** A dropdown menu.
- Table:** A table listing the report details.

Action or scripted query	Started	Target	Runtime	Started by	Server
Simple Active Directory Report	a few seconds ago	AD local	Running...	COMPANY\itina	ScriptRunner

Demo

Unlock the power of PowerShell



Automate & Delegate in 5 Steps



Centralize your PowerShell scripts and modules



Manage credentials & permissions securely



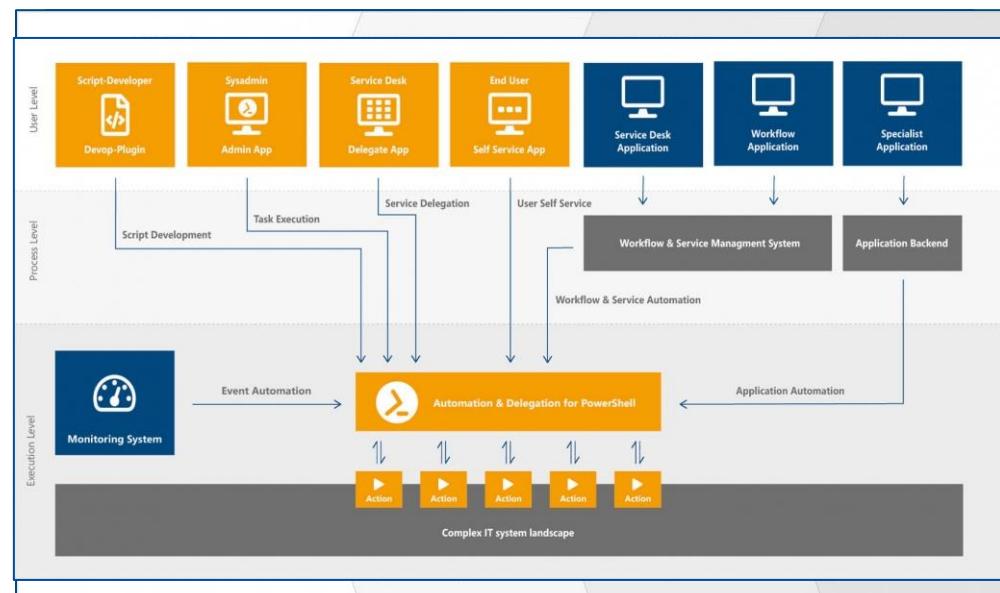
Automatically transform PowerShell scripts into Web GUIs



Delegate recurring tasks to help desk and end users



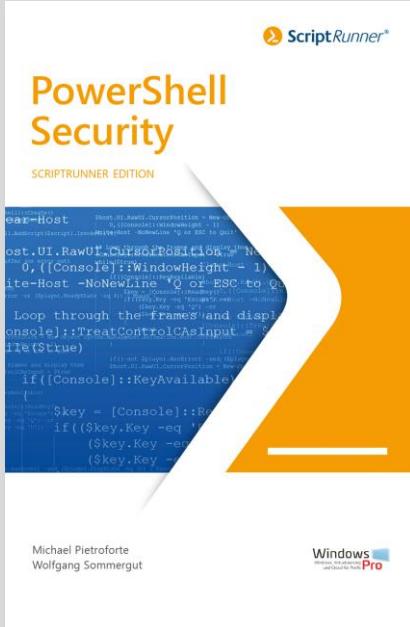
Integrate with ITSM, Monitoring & Workflow systems and more





Free ebook: PowerShell Security

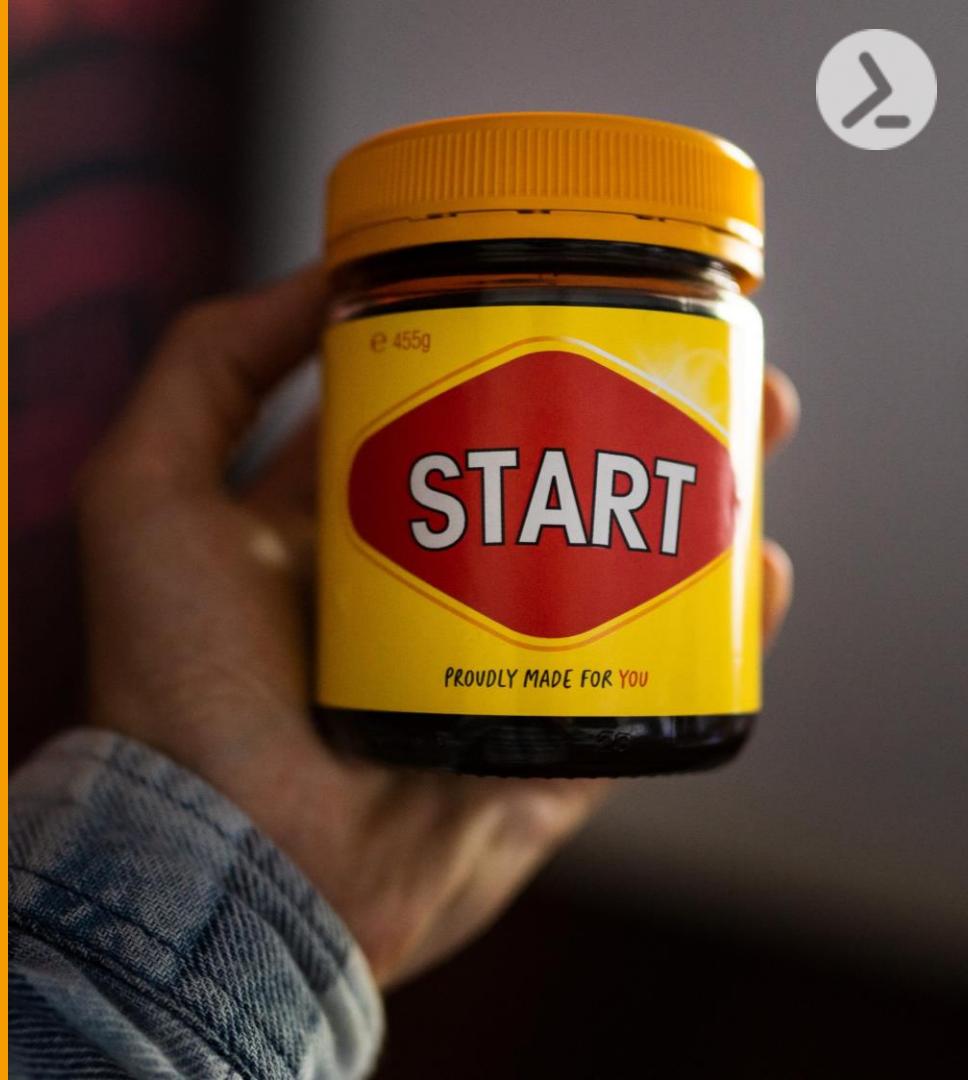
ip.scriptrunner.com/en/powershell-security-guide



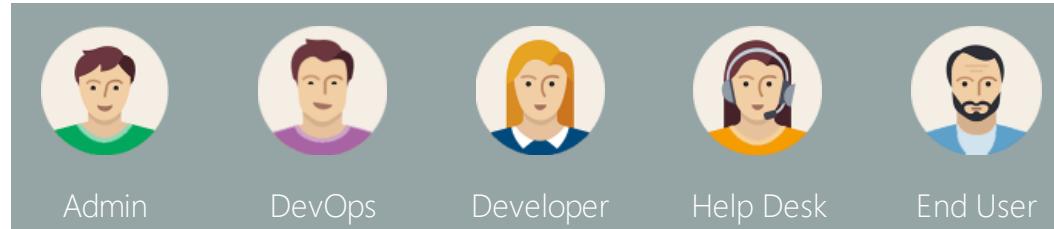
PowerShell Security	
Table of contents	
1.	PowerShell as a hacking tool: Prevent abuse of scripts 8
1.1.	Lax default configuration of PowerShell 9
1.2.	Hacking tools for PowerShell 10
1.3.	General blocking of PowerShell 12
1.4.	Circumvention through alternative shells 14
1.5.	Secure PowerShell with integrated mechanisms 15
2.	Restrict execution of scripts 20
2.1.	Setting an execution policy 20
2.2.	Siging PowerShell scripts 25
2.3.	Reduce PowerShell risks with Constrained Language Mode 36
3.	Secure communication 48
3.1.	Installing OpenSSH on Windows 10 and Server 2019 48
3.2.	PowerShell remoting with SSH public key authentication 57
3.3.	Creating a self-signed certificate 64
3.4.	Remoting over HTTPS with a self-signed certificate 71
4.	Just Enough Administration 81
4.1.	JEA Session Configuration 81
4.2.	Defining and assigning role functions 92
5.	Audit PowerShell activities 98
5.1.	Log commands in a transcription file 98
5.2.	Scriptblock logging: Record commands in the event log 106

Hundreds of free
and ready-to-use
PowerShell scripts.

github.com/scriptrunner/ActionPacks



Unlock the Potential of PowerShell across your organization



Unlock the Power of PowerShell across your organization



Manager

Our organization becomes more productive

Deliver great scripts in a secure environment



DevOps

Delegate recurring tasks and save time



Administrator

Deliver more & better services in less time



HelpDesk

Develop scripts for more use cases/users



Developer



EndUser

Faster task completion with self-services

STANDARDIZATION, AUTOMATION AND DELEGATION OF RECURRING TASKS



AUTO-CREATED
USER FRIENDLY
WEB FORMS

SECURE
CREDENTIAL
ADMINISTRATION

CENTRALIZED SCRIPTS AND
MODULES MANAGEMENT

INTERACTIVE, SCHEDULED
AND EVENT-DRIVEN
SCRIPT EXECUTION

COMPREHENSIVE
MONITORING AND
REPORTING





Put ScriptRunner
to the test.
30 days for free.

lp.scriptrunner.com/en/demo-download





Let's talk about your
automation use cases.
Book a 30 minutes
online session.

lp.scriptrunner.com/meetings/heiko-brenn/demo-en



ScriptRunner product review



4sysops

ScriptRunner Portal Edition R4: A portal for PowerShell scripts

Home / Blog / ScriptRunner Portal Edition R4: A portal for PowerShell scripts
4sysops - The online community for SysAdmins and DevOps

Brandon Lee · Wed, Aug 3 2022 · devops, powershell · 0 comments

ScriptRunner is a solution that centrally manages the running of PowerShell scripts across the environment. The new ScriptRunner Portal Edition R4 release provides many new features and capabilities.

Write for 4sysops, one of the leading sites for IT pros
We pay rates above average and offer a traffic-based bonus.

You have
Experience in Windows administration, cloud computing (AWS, Azure,) or DevOps
Ability to explain technical matters
Good English writing skills

[Apply now!](#)

Author Recent Posts

 **Brandon Lee** ·
Brandon Lee has been in the IT industry 15+ years and focuses on networking and virtualization. He contributes to the community through various blog posts and technical documentation primarily at [Virtualizationhowto.com](#).

Contents

1. What is ScriptRunner?
2. Installing and configuring ScriptRunner



Windows Server 2022
Free eBook
New Roadmap
Fewer Editions
More Security
[Download now!](#)



<https://4sysops.com/archives/scriptrunner-portal-edition-r4-a-portal-for-powershell-scripts/>



I'm speaking at Experts Live Netherlands 2022

Unlock the Power of PowerShell in 5 steps

Sep/30/2022 — 's-Hertogenbosch, Netherlands



Heiko Brenn

www.expertslive.nl



EUROPEAN CLOUD SUMMIT

Mainz, Germany
26-28 September 2022

www.cloudsummit.eu





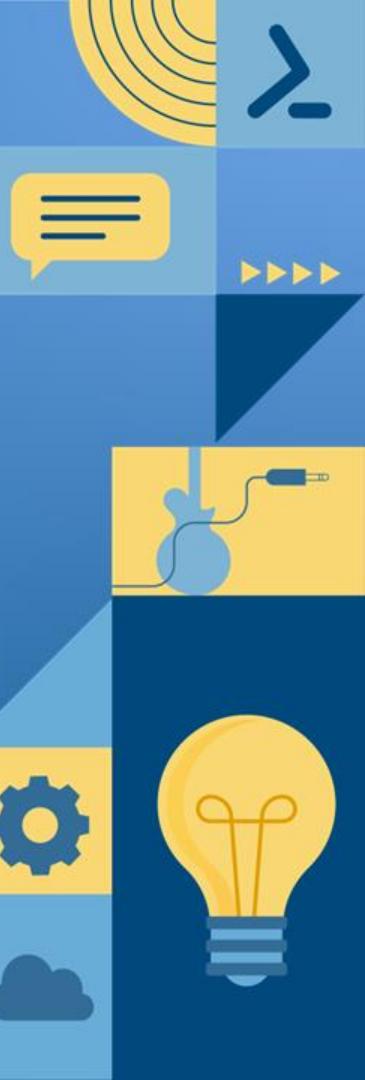
AMA

Ask Me Anything Session



With Heiko Brenn & Markus Hipp

Live: Friday, September 23rd | 11 am EDT | 4 pm BST | 17:00 CEST



Let's get in touch



@HeikoBrenn



@HeikoBrenn



heiko.brenn@scriptrunner.com



Github.com/HeikoBrenn



[Heiko's music channel](#)



Put
ScriptRunner
to the test.
30 days for
free.

lp.scriptrunner.com/en/demo-download

www.scriptrunner.com



Ludwig-Erhard-Straße 2 | 76275 Ettlingen | Germany

Tel: +49 7243 20715-0
Mail: info@scriptrunner.com