



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ DEPARTAMENTAS

**ESXI SERVERIO SAUGUMO BŪKLĖS AUTOMATIZUOTAS
VERTINIMAS NAUDOJANT POWERCLI IR VSAT ĮRANKIUS**

Virtualios infrastruktūros ir debesų kompiuterijos sauga

Parengė: Simonas Riška

Tikrino: lekt. [REDACTED]

VILNIUS 2025

Norint atlikti automatizuotą *ESXi* serverio saugumo konfigūracijos analizę, pirmiausia buvo būtina paruošti *PowerShell* aplinką naudojant *VMware PowerCLI* modulį. Tai leidžia naudotojui prisijungti prie *ESXi* serverio ir vykdyti įvairias valdymo bei tikrinimo komandas.

Pirmame žingsnyje modulis įdiegtas naudojant komandą *Install-Module -Name VMware.PowerCLI -Scope CurrentUser*. Kadangi sistemoje nebuvo įdiegtas NuGet tiekėjas, jis buvo įtrauktas automatiškai, taip pat buvo patvirtintas diegimas iš nepatikimo šaltinio, kas būdinga darbui mokymosi ar testavimo aplinkose.

1 pav. *PowerShell* komanda „Install-Module“ su *NuGet* tiekėjo įdiegimu ir sutikimu naudoti *PSGallery* saugyklą

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Install-Module -Name VMware.PowerCLI -Scope CurrentUser

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\simon\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\WINDOWS\system32>
```

Toliau, kad būtų galima įkelti ir vykdyti išorinį modulį, buvo pakeista *PowerShell* vykdymo politika, leidžiant vykdyti pasirašytus skriptus iš vietinio naudotojo aplinkos ir tuomet įkeltas pagrindinis *PowerCLI* modulis *VMware.VimAutomation.Core*.

2 pav. Įjungiamas *PowerShell* scenarijų vykdymas („Set-ExecutionPolicy“) ir įkeliamas *VMware PowerCLI* modulis

```
PS C:\WINDOWS\system32> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\WINDOWS\system32> Import-Module VMware.VimAutomation.Core
WARNING: Please consider joining the VMware Customer Experience Improvement Program, so you can help us make PowerCLI a
better product. You can join using the following command:

Set-PowerCLIConfiguration -Scope User -ParticipateInCEIP $true

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to
improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As
part of the CEIP, VMware collects technical information about your organization's use of VMware products and services
on a regular basis in association with your organization's VMware license key(s). This information does not
personally identify any individual.

For more details: type "help about_ceip" to see the related help article.

To disable this warning and set your preference use the following command and restart PowerShell:
Set-PowerCLIConfiguration -Scope User -ParticipateInCEIP $true or $false.
```

Kad išvengtume trikdžių dėl *self-signed* arba negaliojančių SSL sertifikatų, buvo nustatyta *PowerCLI* konfigūracija ignoruoti tokius įspėjimus konkrečioje sesijoje - tai svarbus žingsnis siekiant užtikrinti sklandų prisijungimą prie serverio testavimo aplinkoje.

3 pav. *VMware PowerCLI* konfigūracija nustatoma ignoruoti netinkamus SSL sertifikatus

```
PS C:\WINDOWS\system32> Set-PowerCLIConfiguration -Scope Session -InvalidCertificateAction Ignore

Perform operation?
Performing operation 'Update VMware.PowerCLI configuration.'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y

Scope      ProxyPolicy      DefaultVIServerMode InvalidCertificateAction DisplayDeprecationWarnings WebOperationTimeout
-----      -
Session    UseSystemProxy    Multiple           Ignore                  True                      300
User
AllUsers
```

Galiausiai, naudojant komandą *Connect-VIServer -Server 10.21.49.62* buvo sėkmingai prisijungta prie *ESXi* serverio, įvedus „root“ naudotojo autentifikacijos duomenis, o prisijungimo faktas patvirtinamas gautu atsaku, nurodančiu serverio IP, prievado numerį ir naudotojo vardą.

4 pav. Prisijungimo langas prie *ESXi* serverio – įvedami root naudotojo prisijungimo duomenys



5 pav. Sėkmingas prisijungimas prie *ESXi* serverio per *PowerCLI*

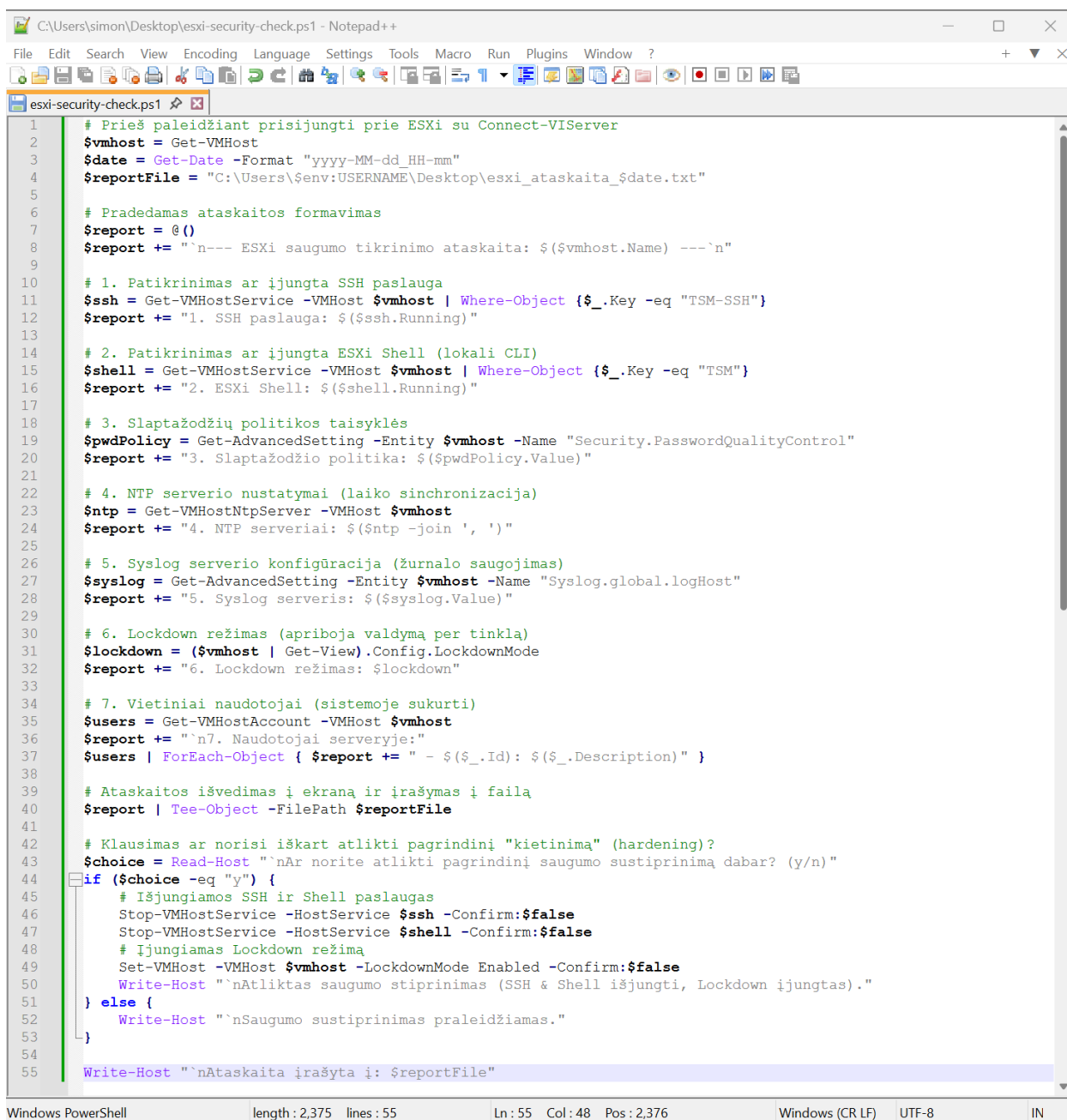
```
PS C:\WINDOWS\system32> Connect-VIServer -Server 10.21.49.62

Name          Port  User
----          -
10.21.49.62    443   root
```

Siekiant automatizuoti *ESXi* serverio pagrindinių saugumo parametrų patikrą, buvo sukurtas *PowerShell* skriptas, pasitelkiant *VMware PowerCLI* modulį. Šis skriptas jungiasi prie nurodyto *ESXi* serverio ir automatiškai surenka informaciją apie svarbiausius konfigūracijos aspektus: SSH ir *ESXi Shell* būseną, slaptažodžių politiką, NTP ir *Syslog* serverių nustatymus, *Lockdown* režimą bei įdiegtus naudotojus.

Skripte taip pat leidžia pasirinkti, ar norima iš karto atlikti pagrindinį saugumo „kietinimą“ (angl. *hardening*), išjungiant nepageidaujamas paslaugas bei įjungiant *Lockdown* režimą.

6 pav. PowerShell scriptas, kuris atlieka saugumo parametrų tikrinimą ir (pasirinktinai) jų koregavimą



```
1 # Prieš paleidžiant prisijungti prie ESXi su Connect-VIServer
2 $vmhost = Get-VMHost
3 $date = Get-Date -Format "yyyy-MM-dd_HH-mm"
4 $reportFile = "C:\Users\$env:USERNAME\Desktop\esxi_ataskaita_$date.txt"
5
6 # Pradedamas ataskaitos formavimas
7 $report = @()
8 $report += "`n--- ESXi saugumo tikrinimo ataskaita: $($vmhost.Name) ---`n"
9
10 # 1. Patikrinimas ar įjungta SSH paslauga
11 $ssh = Get-VMHostService -VMHost $vmhost | Where-Object {$_.Key -eq "TSM-SSH"}
12 $report += "1. SSH paslauga: $($ssh.Running)"
13
14 # 2. Patikrinimas ar įjungta ESXi Shell (lokalio CLI)
15 $shell = Get-VMHostService -VMHost $vmhost | Where-Object {$_.Key -eq "TSM"}
16 $report += "2. ESXi Shell: $($shell.Running)"
17
18 # 3. Slaptažodžių politikos taisyklės
19 $pwdPolicy = Get-AdvancedSetting -Entity $vmhost -Name "Security.PasswordQualityControl"
20 $report += "3. Slaptažodžio politika: $($pwdPolicy.Value)"
21
22 # 4. NTP serverio nustatymai (laiko sinchronizacija)
23 $ntp = Get-VMHostNtpServer -VMHost $vmhost
24 $report += "4. NTP serveriai: $($ntp -join ', ')"
25
26 # 5. Syslog serverio konfigūracija (žurnalo saugojimas)
27 $syslog = Get-AdvancedSetting -Entity $vmhost -Name "Syslog.global.logHost"
28 $report += "5. Syslog serveris: $($syslog.Value)"
29
30 # 6. Lockdown režimas (apriboja valdymą per tinklą)
31 $lockdown = ($vmhost | Get-View).Config.LockdownMode
32 $report += "6. Lockdown režimas: $lockdown"
33
34 # 7. Vietiniai naudotojai (sistemoje sukurti)
35 $users = Get-VMHostAccount -VMHost $vmhost
36 $report += "`n7. Naudotojai serveryje:"
37 $users | ForEach-Object { $report += " - ($_.Id): $($_.Description)" }
38
39 # Ataskaitos išvedimas į ekraną ir įrašymas į failą
40 $report | Tee-Object -FilePath $reportFile
41
42 # Klausimas ar norisi iškart atlikti pagrindinį "kietinimą" (hardening)?
43 $choice = Read-Host "`nAr norite atlikti pagrindinį saugumo sustiprinimą dabar? (y/n)"
44 if ($choice -eq "y") {
45     # Išjungiamos SSH ir Shell paslaugos
46     Stop-VMHostService -HostService $ssh -Confirm:$false
47     Stop-VMHostService -HostService $shell -Confirm:$false
48     # Įjungiamas Lockdown režimas
49     Set-VMHost -VMHost $vmhost -LockdownMode Enabled -Confirm:$false
50     Write-Host "`nAtliktas saugumo stiprinimas (SSH & Shell išjungti, Lockdown įjungtas)."
51 } else {
52     Write-Host "`nSaugumo sustiprinimas praleidžiamas."
53 }
54
55 Write-Host "`nAtaskaita įrašyta į: $reportFile"
```

Skriptui pradėjus veikti *PowerShell* lange pateikiama ataskaita su reikšmingiausiais *ESXi* serverio saugumo parametrais – sistemos naudotojas gauna aiškų atsakymą apie kiekvieno parametro būklę bei galimybę nuspręsti, ar nedelsiant atlikti saugumo sustiprinimą.

7 pav. Tikrinimo paleidimas ir sugeneruotos saugumo tikrinimo ataskaitos rezultatai

```
PS C:\WINDOWS\system32> & "C:\Users\simon\Desktop\esxi-security-check.ps1"

--- ESXi saugumo tikrinimo ataskaita: 10.21.49.62 ---

1. SSH paslauga: True
2. ESXi Shell: False
3. Slaptažodžio politika: retry=3 min=disabled,disabled,disabled,7,7
4. NTP serveriai: ntp1.litnet.lt
5. Syslog serveris:
6. Lockdown režimas: lockdownDisabled

7. Naudotojai serveryje:
  - root: Administrator
  - dcui: DCUI User
  - vpxuser: VMware VirtualCenter administration account
  - student: ESXi User

Ar norite atlikti pagrindinį saugumo sustiprinimą dabar? (y/n): n

Saugumo sustiprinimas praleidžiamas.

Ataskaita įrašyta į: C:\Users\simon\Desktop\esxi_ataskaita_2025-05-08_17-54.txt
PS C:\WINDOWS\system32>
```

Tokia ataskaita yra automatiškai išsaugoma tekstiniame faile, kurį galima naudoti kaip dokumentacijos įrodymą ar palyginimo šaltinį su kitų tikrinimo įrankių rezultatais – ataskaita įrašo pagrindinius patikrintus saugumo elementus bei naudotojų, turinčių prieigą prie sistemos, sąrašą.

Komentariai apie rezultatus:

1. SSH paslauga: Įjungta – rekomenduojama išjungti SSH, kai jis nenaudojamas, siekiant sumažinti paviršių atakoms.
2. *ESXi Shell*: Išjungtas – gera praktika, kadangi sumažina galimų lokalių ar nuotolinių atakų riziką.
3. Slaptažodžio politika: nustatyta slaptažodžio bandymų politika, bet reiktų patikrinti ar slaptažodžių kompleksškumas, senumo limitai ir istorijos ribojimai taip pat taikomi.
4. NTP serveriai: nurodytas validus NTP serveris ntp1.litnet.lt, tai užtikrina sinchronizuotą laiką – svarbu žurnalų ir autentifikacijos nuoseklumui.
5. *Syslog* serveris: neapibrėžtas – rekomenduojama konfigūruoti centralizuotą žurnalinimo sprendimą, kad įvykiai nebūtų prarasti perkrovimo metu.
6. *Lockdown* režimas: išjungtas (*lockdownDisabled*) – rekomenduojama įjungti „Normal Lockdown“ režimą, kad būtų apribota prieiga net ir žinant root slaptažodį.
7. Naudotojai serveryje:
 - a. *root*: būtina reguliariai keisti slaptažodį ir, jei įmanoma, nenaudoti šios paskyros tiesiogiai.
 - b. *dcui*: tipinis vartotojas su fizine prieiga – būtina stebėti naudojimą.
 - c. *vpxuser*: naudojamas *vCenter* – neturėtų būti naudojamas tiesioginiam prisijungimui.
 - d. *student*: reikėtų patikrinti ar paskyra turi ribotas privilegijas ir tik laikiną naudojimą.

8 pav. Sugeneruotas ataskaitos failas .txt formatu, kuriame pateikiami visi tikrinimo rezultatai suprantamu ir aišku būdu

```
esxi_ataskaita_2025-05-08_17-54.txt
File Edit View

--- ESXi saugumo tikrinimo ataskaita: 10.21.49.62 ---

1. SSH paslauga: True
2. ESXi Shell: False
3. Slaptažodžio politika: retry=3 min=disabled,disabled,disabled,7,7
4. NTP serveriai: ntp1.litnet.lt
5. Syslog serveris:
6. Lockdown rezimas: lockdownDisabled

7. Naudotojai serveryje:
  - root: Administrator
  - dcui: DCUI User
  - vpxuser: VMware VirtualCenter administration account
  - student: ESXi User
```

Norint įvertinti ESXi serverio saugumo būklę, atlikome rankinį patikrinimą naudojant automatizuotą VSAT (*VMware Security Assessment Tool*) skriptą. Šis įrankis įgalina įvertinti serverio atitikimą CIS (*Center for Internet Security*) rekomendacijoms. Pirmiausia, buvo paleistas pagrindinis VSAT skriptas, kuris leidžia įvesti tikslio serverio IP adresą ir inicijuoti skenavimą.

9 pav. VSAT paleidimas

```
PS C:\WINDOWS\system32\VSAT> .\vsat.ps1
Enter the vCenter/ESXi Server Hostname or IP Address: 10.21.49.62
```

Vienas iš pagrindinių patikrinimų – ar SSH paslauga yra išjungta. Kadangi SSH prieiga laikoma saugumo rizika, CIS kontrolė 5.3 (L1) rekomenduoja šią paslaugą išjungti. Analizės rezultatai rodo, kad SSH yra įjungtas, todėl ši kontrolė laikoma neįvykdyta.

10 pav. SSH neįvykdytas reikalavimas

```
* CIS control 5.3 (L1) Ensure SSH is disabled
- 10.21.49.62: Failed
  SSH is not disabled.

Passed: 0
Failed: 1
Unknown: 0
-1
```

Kita svarbi kontrolė – *ESXi Shell* paslaugos būklė. Pagal CIS kontrolę 5.2 (L1) ši paslauga taip pat turi būti išjungta, nebent reikalinga trumpalaikė prieiga administraciniais tikslais. Mano atveju ji yra išjungta, todėl ši kontrolė įvykdyta sėkmingai.

11 pav. ESXi Shell reikalavimas įvykdytas

```
* CIS control 5.2 (L1) Ensure the ESXi shell is disabled
- 10.21.49.62: Passed
  The ESXi shell is disabled.

Passed: 1
Failed: 0
Unknown: 0
1
```

Slaptažodžių kompleksumo politika yra labai svarbi užkertant kelią neteisėtai prieigai. CIS kontrolė 4.2 (L1) reikalauja, kad slaptažodžiai būtų sudėtingi. Tačiau mano tikrinimo metu įrankis negalėjo automatiškai patikrinti šio parametro ir nurodė, kad reikia atlikti papildomą rankinę verifikaciją pagal CIS dokumentaciją.

12 pav. Slaptažodžių kompleksškumo būklė nežinoma

```
* CIS control 4.2 (L1) Ensure passwords are required to be complex
- Check Unknown
  This control needs to be verified manually, refer to the CIS Benchmark for details

Passed: 0
Failed: 0
Unknown: 1
0
```

Sistemų laiko sinchronizacija su NTP serveriu yra esminė saugumui ir įvykių koreliacijai. VSAT sėkmingai patvirtino, kad serveris sinchronizuojasi su ntp1.litnet.lt, todėl CIS kontrolė 2.1 (L1) laikoma įvykdyta.

13 pav. NTP sinchronizacija sėkminga

```
* CIS control 2.1 Ensure NTP time synchronization is configured properly
- 10.21.49.62: Pass
  NtpServers: ntp1.litnet.lt

Passed: 1
Failed: 0
Unknown: 0
1
```

Svarbi CIS kontrolė 3.3 (L1) numato, kad *ESXi* serverio žurnalai būtų konfigūruoti siųsti į išorinį (*syslog*) serverį. Tai leidžia užtikrinti įvykių išsaugojimą net jei serveris būtų pažeistas. Mūsų atveju ši funkcija nėra sukonfigūruota, todėl ši kontrolė laikoma neįvykdyta.

14 pav. *Syslog* nenurodytas – kontrolė neįvykdyta

```
* CIS control 3.3 (L1) Ensure remote logging is configured for ESXi hosts
- Check Failed
  Remote logging is not configured for 10.21.49.62

Passed: 0
Failed: 1
Unknown: 0
-1
```

CIS kontrolė 5.5 (L1) rekomenduoja įjungti „Normal Lockdown“ režimą, kuris riboja prieigą prie *ESXi* valdymo sąsajos. Mūsų rezultatai rodo, kad Lockdown režimas nėra aktyvuotas, todėl tai identifikuojama kaip saugumo pažeidžiamumas.

15 pav. *Lockdown* režimas išjungtas

```
* CIS control 5.5 (L1) Ensure Normal Lockdown mode is enabled
- 10.21.49.62: Failed
  Normal Lockdown mode is not enabled.

Passed: 0
Failed: 1
Unknown: 0
-1
```

Galiausiai, kontrolė 4.1 (L1) numato, kad turėtų būti sukurtas ne-*root* vartotojas, turintis administravimo teises. Tokia praktika sumažina riziką susijusią su „root“ paskyros kompromitavimu. Kaip ir slaptažodžių politika, šis parametras nebuvo automatiškai nustatytas, todėl pažymėtas kaip nežinomas.

16 pav. Ne-root vartotojas – būklė nežinoma

```
* CIS control 4.1 (L1) Ensure a non-root user account exists for local admin access
- Check Unknown
  This control needs to be verified manually, refer to the CIS Benchmark for details

Passed: 0
Failed: 0
Unknown: 1
0
```

Nors mūsų sukurtas skriptas atlieka pagrindinius *ESXi* saugumo patikrinimus, tokius kaip SSH būklė, NTP sinchronizacija, slaptažodžių politika ar *Lockdown* režimas, jis ženkliai nusileidžia automatizuotam VSAT įrankiui tiek apimties, tiek analizės gilumo prasme. Pirmiausia, mūsų skripte trūksta automatinio komponentų versijų tikrinimo pagal CIS 1.1 kontrolę: VSAT aptinka daugiau nei 120 tvarkyklių ir branduolio modulių neatitikimus, nurodo laukiamas bei faktines versijas – tokia analizė padeda identifikuoti neatnaujintą ar pasenusią sisteminę programinę įrangą, kuri gali kelti saugumo riziką, o be to, VSAT atlieka išsamius patikrinimus dėl visų likusių CIS kategorijų – komunikacijos, žurnalų kaupimo, autentifikacijos, tinklo saugos, virtualių mašinų konfigūracijos ir kitų. Kiekvienai kontrolei pateikiamas „Pass“, „Fail“ arba „Unknown“ statusas, leidžiantis aiškiai identifikuoti problemines vietas ir planuoti tolesnius veiksmus – mano skriptas šiuo metu neturi nei tokios vertinimo logikos, nei kontrolės identifikacijos pagal CIS numeraciją. Galiausiai trūksta kitų CIS kontrolės taškų mano sprendime.

Apibendrinant galima teigti, kad norint priartėti prie profesionalaus VSAT įrankio lygio, mano skriptui reikia iš esmės plėsti funkcionalumą, įtraukiant komponentų versijų tikrinimą pagal CIS 1.1, detalią automatizuotą CIS kontrolės identifikavimą ir įvertinimą, „Pass/Fail/Unknown“ rezultatų logiką ir išvestį, tinklo, prisijungimų, žurnalų, VM ir branduolio būklės analizę.