Rekomendācijas auditēšanas iestatījumiem Windows domēna infrastruktūrā

(Materiāls paredzēts MS Windows domēnu administratoriem)

CERT.LV pastāvēšanas laikā esam novērojuši, ka situācijās, kad organizācijām/uzņēmumiem ir nācies saskarties ar reālu IT drošības incidentu, nereti pietrūkst informācijas to risināšanā.

Viens no pamatuzdevumiem, drošības incidentu risināšanā, ir žurnālierakstu analīze. Diemžēl jāatdzīst, ka bieži vien iestādei/uzņēmumam ieraksti ir, bet tie ir nepilnīgi t.i. svarīgākās komponentes, kas varētu palīdzēt saprast, kad un kas ir noticis, un kā tieši notikumi ir attīstījušies netiek žurnalētas (jāpiemin, ka pēc noklusējuma Microsoft Windows daļu no ļoti kritiskām auditācijas komponentēm ir izslēdzis). Tāpēc CERT.LV ir izstrādājis minimālās ieteicamās prasības auditācijas iestatījumiem – balstoties gan uz pašu pieredzi risinot incidentus, gan uz padomiem no citu valstu CERTu kopienām, gan paša Microsoft rekomendācijām.

==========

Sagatavošanās un izpēte:

Lokālo žurnālfailu izmēri (kā minimums):

Application, System logs – 256KB vai vairāk

PowerShell logs – 256KB vai vairāk

Security Log –1,024,000KB darbstacijās un 2,048,000KB serveros

Pārliecināmies, ka domēnā ir iespējota šāda politika:

Group Policy Management Editor ->

ComputerConfiguration\Policies\WindowsSettings\SecuritySettings\LocalPolicies\Security Options ->

***" Audit:Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings"* - ENABLED.**

Vairāk par šīs politikas nozīmi un kā to iespējot var lasīt šeit: **https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing#to-ensure-that-advanced-audit-policy-configuration-settings-are-not-overwritten**

Noderīgas utilītprogrammas (iebūvētas MS OS un kuras var palaist no komandrindas interpretatora jeb cmd.exe):

AUDITPOL.exe: Lietojam šo utilītprogrammu, lai pārskatītu pašreizējos žurnalēšanas uzstādījumus. Piemēram, lai apskatītu, kāds ir esošais stāvoklis visās audita kategorijās un to apakškategorijās:

```
AuditPol /get /category:*
```

REG.exe: Lietojam šo utilītprogrammu, lai veiktu dažādus vaicājumus reģistrā – šeit pieminētie reģistru ceļi ir labs sākums, lai saprastu, ko tieši monitorēt no reģistra (populāras vietas, kur „dzīvo" ļaunatūra).

Piemēram:

Izmaiņas AppInit_Dlls –

```
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v AppInit_Dlls
```

Izmaiņas Servisos –

```
reg query "HKLM\System\CurrentControlSet\Services"
```

Izmaiņas Machine Run atslēgā –

```
reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
```

Izmaiņas Machine RunOnce atslēgā –

```
reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce"
```

Izmaiņas User Run atslēgā -

```
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"
```

Izmaiņas User RunOnce atslēgā –

```
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce"
```

P.S. `Run` un `RunOnce` reģistra atslēgas – programma tiek palaista ikreiz, kad lietotājs piesakās sistēmā (log on)

SC.exe: Lietojam šo utilītprogrammu, lai pārskatītu servisus. Piemēram:

Atgriež visus servisus jebkurā stāvoklī –

```
sc.exe query state= all (Jāatceras par atstarpi aiz = zīmes)
```

Atgriež konkrētu servisu –

```
sc.exe query state= all | find /I "telnet"
```

Komandrindas notikumu auditēšana:

Group Policy Editor ---> Computer Configuration -> Administrative Templates -> System->Audit Process Creation -> **Include command line in process creation events -> Enabled**

PowerShell notikumu auditēšana:

Group Policy Editor ---> Computer Configuration -> Administrative Templates -> Windows Components- > Windows PowerShell -> **Turn on PowerShell Script Block Logging->Enabled**

- **Turn on Powershell Script Block Logging***
- **Turn on Module Logging***
- **Turn on Powershell Transcription – pēc noklusējuma dati glabāsies lietotāja "My Documents" mapē, bet ir iespējams norādīt pašu izvēlētu direktoriju. Šos datus ieteicams monitorēt centralizēti.**

Paplašinātā auditācijas konfigurācija Windows domēna kontrollerī

Group Policy Management Editor -> Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies

Audit Category	Audit Subcategory	Success	Failure
Account Logon	Credential Validation*	+	+
	Kerberos Authentication Service*	+	+
	Kerberos Service Ticket Operations*	+	+
	Other Account Logon Events	+	+
Account Management	Computer Account Management	+	
	Distribution Group Management	+	
	Other Account Management Events	+	
	Security Group Management	+	
	User Account Management	+	+
Detailed Tracking	DPAPI Activity	+	+
	PNP Activity	+	
	Process Creation (var aizvietot ar Sysmon**)	+	
DS Access	Directory Service Access*	+	+
	Directory Service Changes*	+	+
Logon/Logoff	Account Lockout	+	
	Group Membership	+	
	Logoff	+	
	Logon	+	+
	Other Logon/Logoff Events	+	+
	Special Logon	+	
Object Access	Audit Registry (var aizvietot ar Sysmon**) – vēlams monitored konkrētas reģistra atslēgas citādi būs grūti atrast vertigo info.	+	
	Audit Detailed File Share		+
	File Share*	+	+
	Audit Sam*	+	
	Audit Other Object Access Events	+	+
Policy Change	Audit Policy Change	+	
	Authentication Policy Change	+	
	Authorization Policy Change	+	
	MPSSVC Rule-Level Policy Change	+	
Privilege Use	Sensitive Privilege Use*	+	+
System	Other System Events	+	+
	Security State Change	+	
	Security System Extension	+	
	System Integrity	+	+

Paplašinātā auditācijas konfigurācija Windows serveriem

Group Policy Management Editor -> Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies

Audit Category	Audit Subcategory	Success	Failure
Account Logon	Credential Validation	+	+
	Other Account Logon Events	+	+
	Other Account Management Events	+	
	Security Group Management	+	
	User Account Management	+	+
Detailed Tracking	DPAPI Activity	+	+
	PNP Activity	+	
	Process Creation (var aizvietot ar Sysmon**)	+	
Logon/Logoff	Account Lockout	+	
	Group Membership	+	
	Logoff	+	
	Logon	+	+
	Other Logon/Logoff Events	+	+
	Special Logon	+	
Object Access	Audit Detailed File Share (failu serverī *)		+
	File Share (failu serverī*)	+	+
	Audit Other Object Access Events	+	+
	Audit Registry (var aizvietot ar Sysmon**) – vēlams monitored konkrētas reģistra atslēgas citādi būs grūti atrast vertigo info.	+	
	Audit Sam	+	
Policy Change	Authentication Policy Change	+	
	Audit Policy Change	+	
	MPSSVC Rule-Level Policy Change	+	
Privilege Use	Sensitive Privilege Use*	+	+
System	Security State Change	+	
	Other System Events	+	+
	Security System Extension	+	
	System Integrity	+	+

Paplašinātā auditācijas konfigurācija darbstacijām (Windows 7, Windows 8, Windows 10)

Group Policy Management Editor -> Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies

Audit Category	Audit Subcategory	Success	Failure
Account Logon	Credential Validation	+	+
	Other Account Logon Events	+	+
	Other Account Management Events	+	
	Security Group Management	+	
	User Account Management	+	+
Detailed Tracking	DPAPI Activity	+	+
	PNP Activity	+	
	Process Creation (var aizvietot ar Sysmon**)	+	
Logon/Logoff	Account Lockout	+	
	Group Membership	+	
	Logoff	+	
	Logon	+	+
	Other Logon/Logoff Events	+	+
	Special Logon	+	
Object Access	Audit Detailed File Share		+
	File Share	+	+
	Audit Other Object Access Events	+	+
	Audit Registry (var aizvietot ar Sysmon**) – vēlams monitored konkrētas reģistra atslēgas citādi būs grūti atrast vertīgo info.	+	
	Audit Sam	+	
Policy Change	Audit Policy Change	+	
	Authentication Policy Change	+	
	MPSSVC Rule-Level Policy Change	+	

Privilege Use	Sensitive Privilege Use*	+	+
System	Other System Events	+	+
	Security State Change	+	
	Security System Extension	+	
	System Integrity	+	+

* izveidos apjomīgu ierakstu skaitu

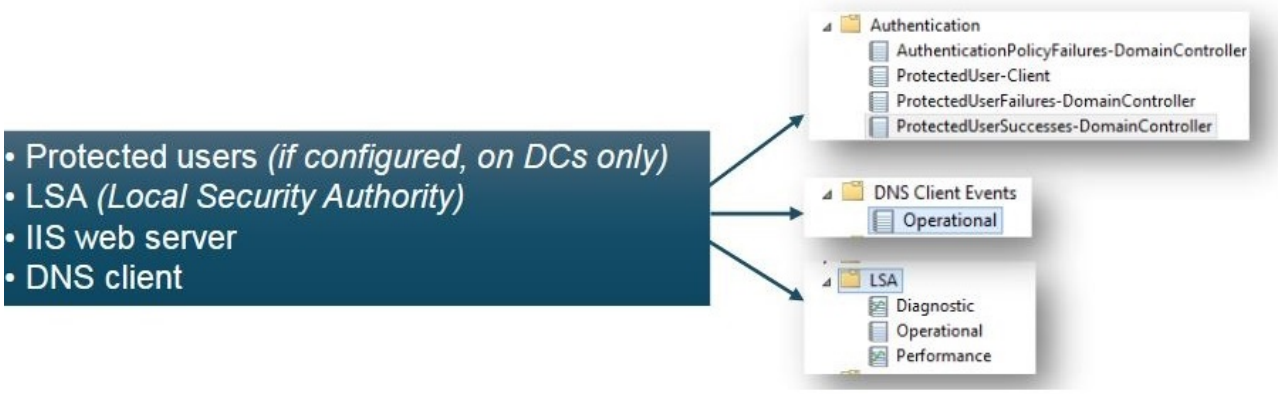
** https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon iesakām izmantot kopā ar šo konfigurācijas failu, kas būs kā labs sākums, bet laika gaitā to noteikti var papildināt pēc konkrētās organizācijas vajadzībām - https://github.com/SwiftOnSecurity/sysmon-config

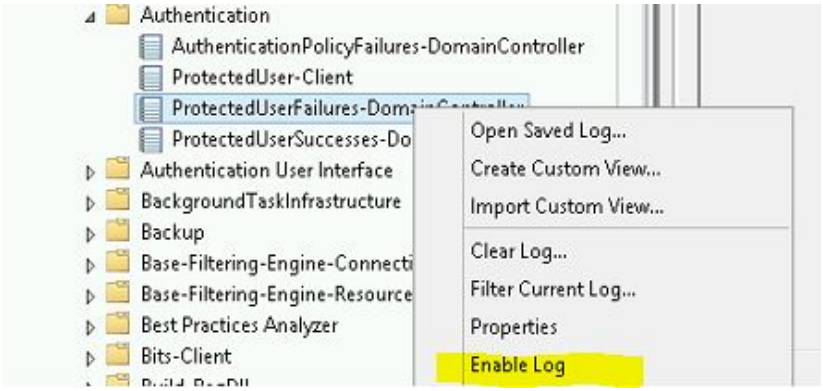
!!! JĀUZSVER, KA KATRA INFRASTRUKTŪRA IR INDIVIDUĀLA UN NOTEIKTI, JA NE PĒC KATRAS APAKŠKATEGORIJAS IESLĒGŠANAS, TAD VISMAZ TĀS KURAS IR ATZĪMĒTAS AR *, IR RŪPĪGI JĀIZVĒRTĒ ĢENERĒTAIS IERAKSTU APJOMS UN PIEEJAMIE RESURSI – ŠEIT VAR NĀKT TALKĀ SYSMON AR KONFIGURĀCIJAS FAILU, KURĀ VAR PIEVIENOT DAŽĀDUS IZŅĒMUMUS, LAI APJOMU SAMAZINĀTU.

Noderīgas piezīmes:

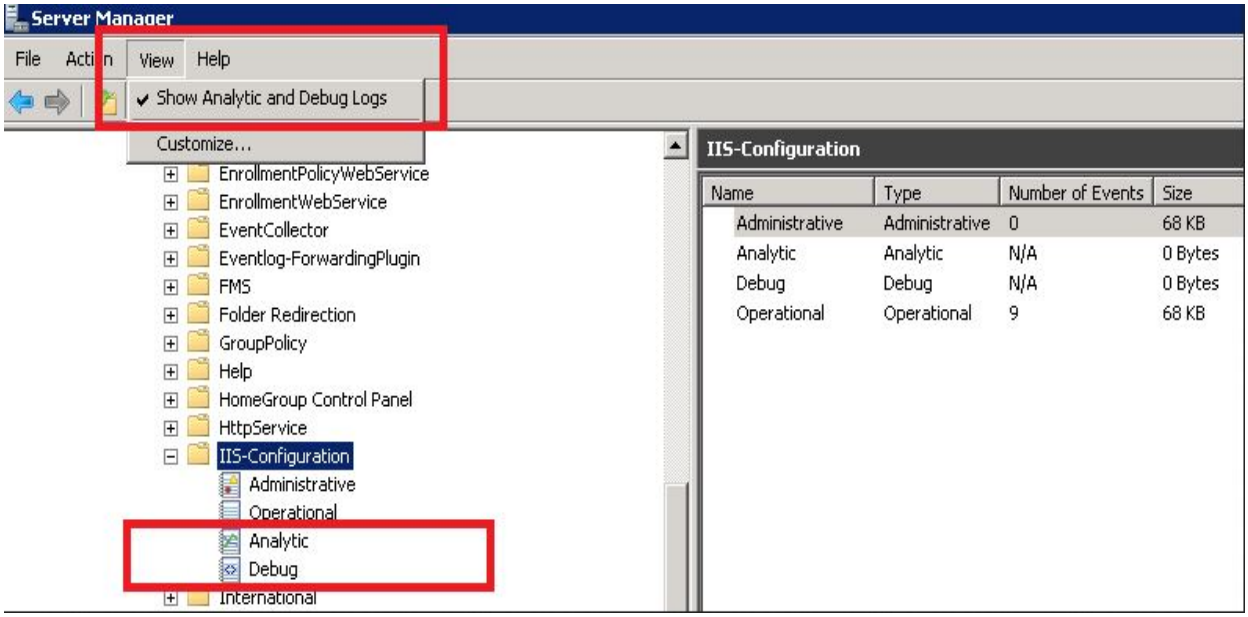
Pēc noklusējuma daži no žurnālfailiem neuzrāda nekādus notikumus, jo tie ir **izslēgti**. Svarīgākie no tiem ir uzskaitīti zemāk redzamajā attēlā.



Lai notikumu reģistrēšanu iespējotu, ir jāatver Event Viewer un ar labo peles klikšķi uz izvēlētās apakškategorijas ir jāuzspiež „Enable Log”.



Reizēm noderīga informācija ir pieejama Analytic, Debug vai Trace ierakstos, bet, lai tie būtu pieejami, tos ir speciāli jāatzīmē pie Event Viewer vai Server Manager ar View-> „**Show Analytic and Debug Logs**” opciju: Tāpat tagad redzamās sadaļām ir vēl papildus jāiespējo (iepriekš aprakstīts kā Enable Log). Pēc noklusējuma Analytic, Debug un Trace notikumi ir paslēpti un izslēgti



Neskaidrību gadījumā papildus informācija pieejama šeit:

1. **Detalizētāk par paplašinātās auditācijas iestatījumiem, to nozīmi** - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
2. **Jautājumi un atbildes par paplašināto auditācijas konfigurāciju**- https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq
3. **Utilītprogramma Auditpol.exe** - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731451(v=ws.11)
4. **Utilītprogramma Reg .exe** - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc732643(v=ws.11)
5. **Utilītprogramma Sc.exe** - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc754599(v=ws.11)
6. **Komandrindas notikumu auditēšana** - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
7. **PowerShell notikumu auditēšana** - https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html