	<b>Standard Cyberbezpieczeństwa OT</b> <hr/> Aktualna Konfiguracja Cyberbezpieczeństwa OT	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	1 / 10




## **Załącznik nr 1.1.2**

### **Standard Cyberbezpieczeństwa OT**


### **Aktualna Konfiguracja Cyberbezpieczeństwa OT**

---

	<b>Standard Cyberbezpieczeństwa OT</b> <hr/> Aktualna Konfiguracja Cyberbezpieczeństwa OT	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	2 / 10

## Spis treści

<b>1.</b>	Zbieranie informacji potrzebnych do wykonania Testów Odbiorowych Cyberbezpieczeństwa.....	3
1.	Przygotowanie katalogu .....	4
2.	Gromadzenie danych.....	4
3.	Test połączeń sieciowych .....	10

	<b>Standard Cyberbezpieczeństwa OT</b> Aktualna Konfiguracja Cyberbezpieczeństwa OT	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	3 / 10

## 1. Zbieranie informacji potrzebnych do wykonania Testów Odbiorowych Cyberbezpieczeństwa

**Aspekty konfiguracyjne systemu należy zebrać ze wszystkich stacjach komputerowych / serwerów / urządzeń sieciowych itp.**

### I. Stacje komputerowe / serwery


W przypadku stacji komputerowych można się posłużyć poniższymi komendami, jednakże ich zastosowanie zależy od rodzaju i konfiguracji urządzenia, jak również systemu operacyjnego i powinien być zweryfikowany przez administratora weryfikowanego systemu (poniższe polecenia dedykowane są do wybranych rodzajów systemów operacyjnego Windows przy zastosowanej odpowiedniej konfiguracji).

**Każde z poleceń należy zweryfikować czy jest obsługiwane w danym systemie operacyjnym przy stosowanej konfiguracji i nie powoduje działań niepożądanych.**

Polecenia zostały przetestowane na Win7, Win10, Windows Server 2008R2, Windows Server 2016 w wersji angielskiej) w konfiguracji stosowane na rozwiązanych testowych.

W przykładowych komendach zastosowano wyrażenia, które należy zastąpić odpowiednimi danymi np.:

- **%Nazwa\_Komputera%** - wpisać nazwę komputera, dla którego zbierane są dane
- **%Nazwa\_Instalacji%** - wpisać nazwę Instalacji, dla której zbierane są dane
- **%Nazwa\_Użytkownika%** - wpisać nazwę użytkownika, dla którego zbierane są dane
- **%Nazwa\_Grupy%** - wpisać nazwę grupy użytkowników

	<b>Standard Cyberbezpieczeństwa OT</b> Aktualna Konfiguracja Cyberbezpieczeństwa OT	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	4 / 10

## 1. Przygotowanie katalogu

1.1. Uruchom wiersz poleceń np. poprzez wykorzystanie polecenia

**„START-> Uruchom -> CMD” ( uruchom w trybie administratora !)**

1.2. Przejdź do miejsca na dysku w którym będziesz zbierał pliki z wynikami poszczególnych poleceń np. poprzez wykorzystanie polecenia

**„ cd C:\ ”**

1.3. Utwórz katalog, w którym będziesz gromadził pliki z wynikami poszczególnych poleceń np. poprzez wykorzystanie polecenia

**„ mkdir %Nazwa\_Instalacji% ”**

1.4. Przejdź do stworzonego katalogu np. poprzez wykorzystanie polecenia

**„ cd %Nazwa\_Instalacji% ”**

1.5. Utwórz katalog, w którym będziesz gromadził pliki z wynikami poszczególnych poleceń np. katalog o nazwie OS1, AS1, ES

1.6. Wejdź do stworzonego katalogu np. **OS1** dla którego będą zbierane dane np. poprzez zaproponowane polecenia.

## 2. Gromadzenie danych

Zgromadź informacje o konfiguracji komponentu (nazwa komputera, wersja OS, Nr.seryjny, Domena, data instalacji, zainstalowane oprogramowanie i poprawki, ustawienia kart sieciowych i firewall, lista użytkowników i grup użytkowników, lista serwisów, obciążenia zasobów itd).

Proszę o weryfikację pozyskanych informacji z danymi zamieszczonymi w pliku **OT\_Dane.xlsx** w zakładce z nazwą **Instalacji**. W przypadku wykrycia rozbieżności proszę o aktualizację w pliku **OT\_Dane.xlsx**

2.1. Informacja o BIOS i nr seryjnym np. poprzez wykorzystanie polecenia


**„wmic bios get manufacturer,version,name,serialnumber,description,smbiosbiosversion /FORMAT:CSV > %Nazwa\_Komputera%\_BIOS.txt”**

Pozyskaj dane min: wersja BIOS, nr seryjny

2.2. Informacje o systemie np. poprzez wykorzystanie polecenia

**„systeminfo > %Nazwa\_Komputera%\_systeminfo.txt”**

Pozyskaj dane min: Host Name, OS Name,OS Version, Registered Owner, Original Install Date,

	<b>Standard Cyberbezpieczeństwa OT</b> Aktualna Konfiguracja Cyberbezpieczeństwa OT	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	5 / 10

Domain, System Manufacturer, Time Zone

2.3. Informacje o konfiguracji kont dostępowych np. poprzez wykorzystanie polecenia

**„net accounts > %Nazwa\_Komputera%\_accounts.txt”**

Pozyskaj dane min: Wymuszanie wylogowywania, Max okres ważność haseł, Próg blokowania po ilu błędnych wprowadzeniach, czas trwania blokady

2.4. Informacje o kontach użytkowników np. poprzez wykorzystanie polecenia

**„wmic useraccount get accounttype,description,domain,disabled, localaccount,lockout,passwordchangeable, passwordexpires, passwordrequired,sid,name /FORMAT:CSV > %Nazwa\_Komputera%\_accounts\_WMIC.txt”**

W przypadku braku poprawnego wykonania polecenia powyżej można wykorzystać polecenie zapisane poniżej.

**„net users > %Nazwa\_Komputera%\_netusers.txt”**

2.5. Informacje o kontach poszczególnych użytkowników (w szczególności administracyjnych) np. poprzez wykorzystanie polecenia

**„net users %Nazwa\_Użytkownika% > %Nazwa\_Komputera%\_%Nazwa\_Użytkownika%.txt”**

**Wykonaj oddzielnie dla każdej grupy i i zapisz dane w oddzielnych plikach dla każdego użytkownika – (Należy wykonać ręcznie)**

np. net user administrator > OS1\_administrator.txt,

net user syseng > OS1\_syseng.txt

2.6. Informacje o grupach kont użytkowników np. poprzez wykorzystanie polecenia

2.6.1.Dla komputerów innych niż kontroler domeny

**„net localgroup > %Nazwa\_Komputera%\_netlocalgroup.txt”**


2.6.2.Dla kontrolera domeny

**„net group > %Nazwa\_Komputera%\_netgroup.txt”**

2.7. Informacje o poszczególnych grupach użytkowników np. poprzez wykorzystanie polecenia

2.7.1.Dla komputerów innych niż kontroler domeny

**„net localgroup %Nazwa\_Grupy% > %Nazwa\_Komputera%\_%Nazwa\_Grupy%.txt”**

	<b>Standard Cyberbezpieczeństwa OT</b> Aktualna Konfiguracja Cyberbezpieczeństwa OT	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	6 / 10

np. net localgroup Administrators > OS1\_Administrators.txt

net localgroup PowerUsers > OS1\_PowerUsers.txt

#### 2.7.2. Dla kontrolera domeny

**„net group %Nazwa\_Grupy% > %Nazwa\_Komputera%\_netgroup.txt”**

np. net group „Domain Admins” > OS1\_DomainAdmins.txt

net group „Domain Users” > OS1\_DomainUsers.txt

**Wykonaj oddzielnie dla każdej grupy i zapisz dane w oddzielnych plikach dla każdej grupy – (Należy wykonać ręcznie)**

2.8. Informacje o zainstalowanym oprogramowaniu np. poprzez wykorzystanie polecenia

**„wmic product get, Name, Description, Version, Vendor, InstallDate, InstallLocation, IdentifyingNumber > %Nazwa\_Komputera%\_oprogramowanie.txt”**

2.9. Informacje o procesach systemowych np. poprzez wykorzystanie polecenia

**„wmic process get caption,processid,parentprocessid, commandLine /FORMAT:CSV > %Nazwa\_Komputera%\_procesy.txt”**

W przypadku braku poprawnego wykonania polecenia powyżej można wykorzystać polecenie zapisane poniżej.

**„tasklist > %Nazwa\_Komputera%\_procesySVC.txt”**

2.10. Informacje o podmontowanych udziałach sieciowych np. poprzez wykorzystanie polecenia

**„net use > %Nazwa\_Komputera%\_netuse.txt”**

2.11. Informacji o udostępnianych zasobach np. poprzez wykorzystanie polecenia


**„net share > %Nazwa\_Komputera%\_netshare.txt”**

2.12. Informacji o dyskach np. poprzez wykorzystanie polecenia

**„wmic logicaldisk get name,filesystem,size,freespace,volumename,description /FORMAT:CSV > %Nazwa\_Komputera%\_logicaldisk.txt”**

2.13. Zgromadź informacje o zainstalowanych poprawkach w systemie operacyjnym np. poprzez wykorzystanie polecenia

**„wmic qfe > > %Nazwa\_Komputera%\_OSpoprawki.txt”**

	<b>Standard Cyberbezpieczeństwa OT</b> Aktualna Konfiguracja Cyberbezpieczeństwa OT	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	7 / 10

Pozyskaj dane min: data ostatnio zainstalowanej poprawki

2.14. Informacje o konfiguracji kart sieciowych np. poprzez wykorzystanie polecenia  
**„ipconfig /all > %Nazwa\_Komputera%\_ipconfigall.txt”**

2.15. Informacje o statusie połączeń sieciowych np. poprzez wykorzystanie polecenia  
**„netstat -anob > %Nazwa\_Komputera%\_netstatanob.txt”**

2.16. Informacje o konfiguracji firewall systemowego np. poprzez wykorzystanie polecenia  
**„netsh advfirewall firewall show rule name=all >> %Nazwa\_Komputera%\_advfirewallAllRules.txt ”**  
**„netsh advfirewall monitor show firewall > %Nazwa\_Komputera%\_advfirewall.txt ”**  
**„netsh firewall show config > %Nazwa\_Komputera%\_firewallConfig.txt”**


2.17. Informacje na temat połączeń np. poprzez wykorzystanie polecenia  
**„ipconfig /displaydns > %Nazwa\_Komputera%\_DisplayDNS.txt”**

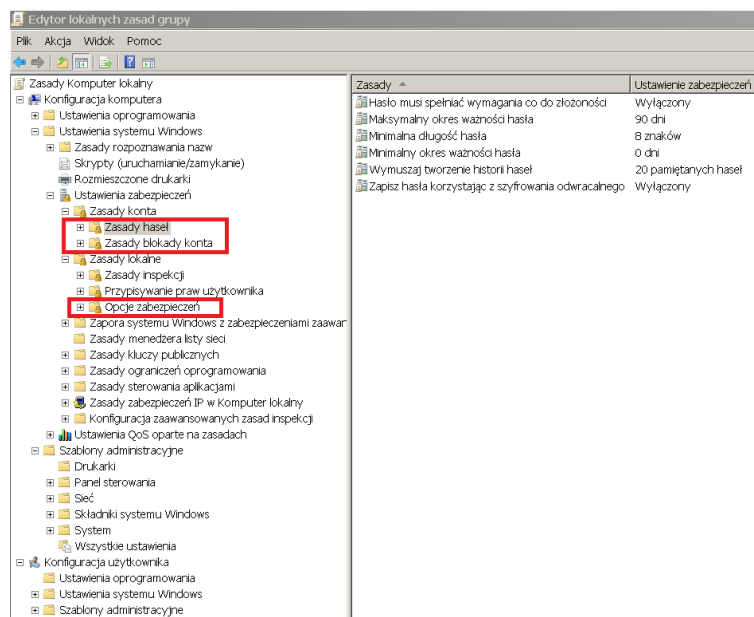
2.18. Informacje o usługach systemowych  
**„wmic service get Name, Caption, State, ServiceType, StartMode, pathname /FORMAT:CSV > %Nazwa\_Komputera%\_service.txt”**

2.19. Informacje o konfiguracji Security Policy – Zasady zabezpieczeń lokalnych np. poprzez wykorzystanie polecenia  
**„secedit.exe /export /cfg \%Nazwa\_Komputera%\_secpol.inf”**

2.20. Informacje o konfiguracji Local Group Policy / Global Group Policy np. poprzez wykorzystanie polecenia  
**„gpedit.msc”**

Wykonaj zrzuty ekranu min. z tych obiektów

	<b>Standard Cyberbezpieczeństwa OT</b> Aktualna Konfiguracja Cyberbezpieczeństwa OT	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	8 / 10

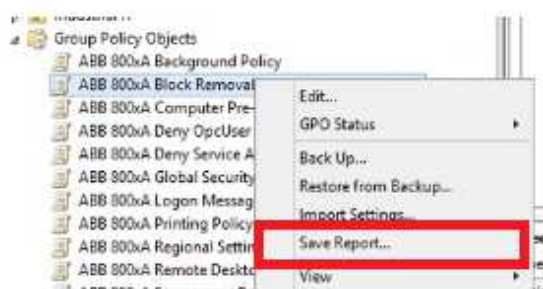


Lub wykonaj polecenie

**Gpresult /h %Nazwa\_Komputera%\_GPReport.html**

## 2.21. Informacje o konfiguracji polityk GPO (tylko dla kontrolera domeny)

Uruchom aplikację Group Policy Management. Wykonaj eksport polityk do formatu HTML GPO folderu o nazwie **%Nazwa\_Komputera%\_GPO**




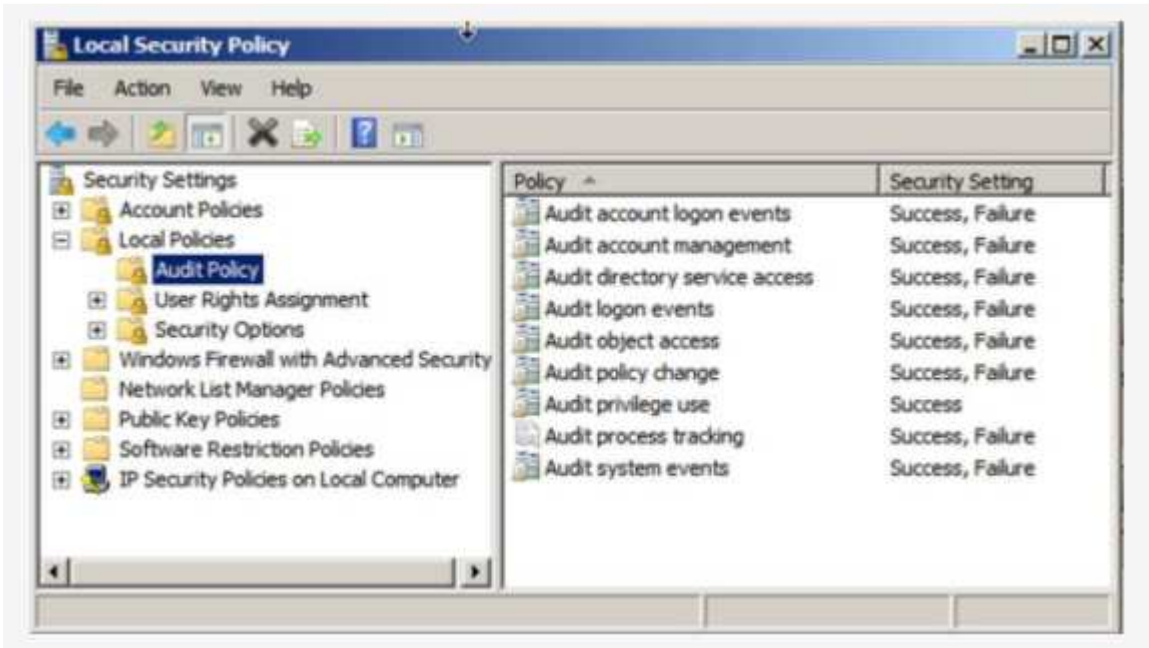
## 2.22. Informacje o konfiguracji lokalnych polityk audytowych


**„auditpol /get /category:\*> %Nazwa\_Komputera%\_auditpol.txt”**

Ewentualnie wykonaj zrzut ekranu konfiguracji polityk audytowych z „Local Security policy”



	<p><b>Standard Cyberbezpieczeństwa OT</b></p> <hr/> <p>Aktualna Konfiguracja Cyberbezpieczeństwa OT</p>	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	9 / 10



	<b>Standard Cyberbezpieczeństwa OT</b> <hr/> Aktualna Konfiguracja Cyberbezpieczeństwa OT	Wersja:	2.0
		Data wydania:	2025-01-27
		Strona:	10 / 10

### 3. Test połączeń sieciowych

Wykonaj próbę przejścia z sieci OT do IT np. poprzez wykorzystanie polecenia

**ping 8.8.8.8>% Computer\_Name% \_Ping\_IP1.txt**

**tracert 8.8.8.8>% Computer\_Name% \_Tracert\_IP1.txt**

**ping 10.1.108.192 >% Computer\_Name% \_Ping\_IP2.txt**

**tracert 10.1.108.192 >% Computer\_Name% \_Tracert\_IP2.txt**