



Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT

Standard Cyberbezpieczeństwa OT

Załącznik 1.1.1 Dokumentacja konfiguracyjna cyberbezpieczeństwa OT

Zatwierdził	Data	Podpis
Robert Oleński Dyrektor Biura Cyberbezpieczeństwa	15.06.2026	<i>Dokument podpisany elektronicznie dnia 2026.06.16. Oryginał dostępny w Dziale Cyberbezpieczeństwa OT.</i>
Zaakceptował	Data	Podpis
Artur Sidorko Kierownik Działu Cyberbezpieczeństwa OT	21.01.2025	<i>Dokument podpisany elektronicznie dnia 2026.06.16. Oryginał dostępny w Dziale Cyberbezpieczeństwa OT.</i>

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	2 / 13

Historia zmian dokumentu			
Wersja	Data	Osoba	Opis zmian
1.0	21.01.2019 r.	Dział Cyberbezpieczeństwa OT	Utworzenie dokumentu
2.0	15.03.2021 r.	Dział Cyberbezpieczeństwa OT	Aktualizacja dokumentu
3.0	06.02.2023 r.	Dział Cyberbezpieczeństwa OT	Aktualizacja dokumentu
4.0	20.01.2025 r.	Dział Cyberbezpieczeństwa OT	Aktualizacja dokumentu

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	3 / 13

Spis treści

1.	Dokumentacja konfiguracyjna cyberbezpieczeństwa	4
2.	General Information	4
3.	INDEX LIST	5
4.	Network diagrams	5
5.	Infrastructure	6
6.	Log_Sources.....	7
7.	Firewalls_Settings.....	7
8.	Applications_List	8
9.	Systems Services.....	8
10.	Local Accounts	8
11.	Domain Account.....	8
12.	AD_OU.....	9
13.	GPO	9
14.	Name_of_device_L2	10
15.	Name_of_device_L3	10
16.	TLS certificate.....	11
17.	vSphere Host configuration	11
18.	VM list and resources.....	12
19.	Labels	12
20.	Postanowienia końcowe	13
21.	Załączniki	13

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	4 / 13

1. Dokumentacja konfiguracyjna cyberbezpieczeństwa

W poniższych punktach zostaną opisane szczegółowo wymagania, jeśli chodzi o dane, jakie należy zebrać. Komplet informacji, należy wprowadzić do pliku excel, który jest załącznikiem do niniejszego dokumentu (*Zał. 1.1.5. Dokumentacja konfiguracyjna cyberbezpieczeństwa – Arkusz z danymi*). W przypadku, gdy we wdrażanym rozwiązaniu nie występują poszczególne elementy, należy zamieścić w odpowiednim arkuszu pliku excel adnotację: Nie ma zastosowania. Poniżej przykład – dla systemu, gdzie nie została zastosowana wirtualizacja, nie będzie miało zastosowania wypełnienie arkusza dotyczącego maszyn wirtualnych:

INDEX	Nie ma zastosowania			
VM resource requirement estimation				
	CPU Allocation (MHz)	CPU Quantity	Virtual Memory (GB)	Disk Average (IOPs)
Backup	x000	3	x	:
Service AV (Symantec)	x000	2	xx	:
WSUS	x000	2	xx	:

2. General Information

Pierwszy arkusz zawiera podstawowe informacje o wdrażanym/modernizowanym systemie.

Jakiegolwiek zmiany w niniejszym szablonie dokumentacji muszą być zaakceptowane przez Obszar Cyberbezpieczeństwa OT GK ORLEN.

Dane zawarte w niniejszej dokumentacji stanowią własność ORLEN, a ich nieuprawnione udostępnianie stroną trzecią stanowi naruszenie bezpieczeństwa teleinformatycznego.

Configuration documentation: *name of installation*

Type of automation system: *for example DCS*

Detail Information about documentation

Documentation Name:	
Documentation Number:	
Version:	
Status:	
Date:	2024-10-15

Detail information about contracts

Project Name:	
Agreement Number:	
Provider:	
End User:	ORLEN S.A.

Detail information about author

Company Name	
Author Name	
Approver Name	

REFERENCE DOCUMENTS

No.	Date	Name	Company	Author



	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	5 / 13

3. INDEX LIST

Arkusz ze spisem indeksów oraz odnośników do poszczególnych arkuszy. W przypadku potrzeby dodania dodatkowych arkuszy dla urządzeń sieciowych należy je dodać w grupie 3 (Network Devices):

INDEX

1. Infrastructure

Name
Network Diagrams
Infrastructure

3. Network Devices

Name of Network device	Type of Device
Name of device L2	Switch L2
Name of device L3	Switch L3

2. Computer infrastructure

Log Sources	Log Sources
Firewalls Settings	Firewall Settings
Applications List	Application List
Systems Services	Systems Services
Local Accounts	Local Accounts
Domain Accounts	Domain Accounts
AD Organizational Unit	OU
GPO settings	GPO

4. Vmware

Vmware	vSphere Host configuration
	VM list and resources
	EMC Settings

5. Physical connection

Cable labels	Labels
--------------	------------------------

6. TLS certificate

Certificate settings	Certificate
----------------------	-----------------------------

4. Network diagrams

W tym arkuszu należy przekazać diagram wdrażanej/modernizowanej infrastruktury. Na schemacie należy wyraźnie zaznaczyć zakres wdrożenia/modernizacji. Zamieszczony dokument musi być w formacie, który umożliwia skalowanie i zawiera czytelne wszystkie szczegóły.

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	6 / 13

5. Infrastructure

W tym arkuszu należy wprowadzić komplet urządzeń, wykorzystanych do wdrażanego/modernizowanego rozwiązania. Trzeba uwzględnić takie urządzenia, jak: hosty wirtualizatora, macierze dyskowe, wirtualne i fizyczne serwery, wirtualne i fizyczne stacje robocze/operatorskie/inżynierskie, cienkie klienty, urządzenia sieciowe takie jak switchy, routery itp.

INDEX										
Hostname	System Vendor	System Type	Description	Placement of installation	Address					
					IP address	Subnet mask	Default Gateway	DNS 1	DNS 2	MAC address
		np.. DCS	np. ESKI 1		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
					xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
					xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
					xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
		np.. DCS	np. Macierz		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
					xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
					xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
					xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. DCS	np.. DCS	np. Backup Server		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. DCS	np.. DCS	np. Log Collector		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. DCS	np.. DCS	np.. Domain Controller		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. SCADA	np.. SCADA	np. Historian Collector		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. SCADA	np.. SCADA	np.. Advance Process Control		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. ESD	np.. ESD	np. Symantec SEPM		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. ESD	np.. ESD	np. WSUS		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. ESD	np.. ESD	np. Switch L2		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. ESD	np.. ESD	np. FireWall		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00
	np.. DSC	np.. DSC	np.. Thin Client 1		xx.xx.xx.xx	255.255.255.0	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	00:00:00:00:00:00

INDEX		Hardware				
Hostname	Device vendor	Virtual Host Machine	Model	BIOS version	Processor	
	np. Dell Inc.	NA	np. PowerEdge R760	np. Dell Inc. x.x.x, 11/8/2022	np. Intel® Xeon™ Silver-4410Y (2.0 GHz - 3.9 GHz, 12 rdzeni/24 wątki, 30 MB cache, 150 W)	
	np. Dell Inc.	NA	np.. PowerVault ME5024	np. Dell Inc. x.x.x, 11/8/2022		
	np. VMware, Inc.	np. ESKi1	np. VMware Virtual Platform	np. Phoenix Technologies LTD 6.00, 9/21/2022	np. [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2997 Mhz	
	np. VMware, Inc.	np. ESKi1	np. VMware Virtual Platform	np. Phoenix Technologies LTD 6.00, 9/21/2022	np. [01]: Intel64 Family 6 Model79 Stepping 1 GenuineIntel ~2997 Mhz	
	np. Dell Inc.	NA	np. VMware Virtual Platform	np. Phoenix Technologies LTD 6.00, 9/21/2022	np. [01]: Intel64 Family 6 Model79 Stepping 1 GenuineIntel ~2997 Mhz	
	np.. HP	NA	np. VMware Virtual Platform	np. Phoenix Technologies LTD 6.00, 9/21/2022	np. [01]: Intel64 Family 6 Model79 Stepping 1 GenuineIntel ~2997 Mhz	
	np. VMware, Inc.	np. ESKi1	np. VMware Virtual Platform	np. Phoenix Technologies LTD 6.00, 9/21/2022	np. [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2997 Mhz	
	np. VMware, Inc.	np. ESKi2	np. VMware Virtual Platform	np. Phoenix Technologies LTD 6.00, 9/21/2022	np. [01]: Intel64 Family 6 Model79 Stepping 1 GenuineIntel ~2997 Mhz	
	np. VMware, Inc.	np. ESKi2	np. VMware Virtual Platform	np. Phoenix Technologies LTD 6.00, 9/21/2022	np. [01]: Intel64 Family 6 Model79 Stepping 1 GenuineIntel ~2997 Mhz	
	np. CISCO	NA	np. Catalyst 9300L-24T-4X-A	np. Phoenix Technologies LTD 6.00, 9/21/2022	np. [01]: Intel64 Family xx Model 79Stepping 1 GenuineIntel ~2997 Mhz	
	np. Palo Alto Networ	NA	np.. PA-460			
	np. Dell Inc.	NA	np.. Optiplex 3000 Thin Client	np.. Dell Inc.x.x.x, 08/09/2024	np.. Intel Pentium N6004 (2.0-3.3 GHz, 4 rdzenie/4 wątki, 4 MB cache, 10 W)	

INDEX		Operating System								BIOS hardening	
Hostname	Memory	Disk [GB]	Service Tag/ Serial Number	Final data support	OS name	OS Edition	OS version	Domain	numer licencji (dla OS)	Access Password Protection	Boot only from Hard Drive
	128 GB	2000	XXXXXXX	np. 08.2028	np.. VMware ESKi 8.0 Update3c		np.. 8.0.3.00300	np. WORKGROUP		Yes	Yes
	4*24 GB	20000	XXXXXXX	np. 08.2028	np.. VMware ESKi 8.0 Update3c		np.. 8.0.3.00300	np. WORKGROUP		Yes	Yes
	8,192 MB	C:100 D:5000	VMware-xx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	np. 08.2028	np. Microsoft Windows Server 2022	np. Standard	np. 21H2 Build 20348.2700	np. Domain_Name		NA	NA
	4,096 MB	C:50 D:0	VMware-xx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	np. 08.2028	np. Microsoft Windows Server 2022	np. Datacenter	np. 21H2 Build 20348.2701	np. Domain_Name		NA	NA
	4,096 MB	C:50 D:0	VMware-xx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	np. 08.2028	np. Microsoft Windows Server 2022	np. Datacenter	np. 21H2 Build 20348.2702	np. Domain_Name		NA	NA
	8,192 MB	C:200 D:0	VMware-xx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	np. 08.2028	np. Microsoft Windows Server 2022	np. Standard	np. 21H2 Build 20348.2703	np. Domain_Name		NA	NA
	16,384 MB	C:40 D:0	VMware-xx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	np. 08.2028	np. Microsoft Windows Server 2022	np. Standard	np. 21H2 Build 20348.2704	np. Domain_Name		NA	NA
	4,096 MB	C:50 D:0	VMware-xx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	np. 08.2028	np. Microsoft Windows Server 2022	np. Standard	np. 10.0.14393 N/A Build 14393	np. Domain_Name		NA	NA
	4,096 MB	C:50 D:0	VMware-xx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	np. 08.2028	np. Microsoft Windows Server 2022	np. Datacenter	np. 10.0.14393 N/A Build 14393	np. Domain_Name		NA	NA
	8,191 MB	16		np. 05.2026	np. IOS XE Software		np. Dublin-17.12.4	np. Domain_Name		Yes	NA
		240		np. 08.2026	np.. PAN-OS		np. 10.0.9	np. WORKGROUP		Yes	Yes
	8,191 MB	64	XXXXXXX	np.. 10.2029	np.. Dell Thin OS		np.. 9.07.02	np. WORKGROUP		Yes	Yes

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	7 / 13

6. Log_Sources

Arkusz jest formatką do wzbogacania źródeł logów dla rozwiązania SIEM GK ORLEN. Należy uzupełnić jedynie niebieskie pola, pozostawiając niezmienione indeksy (pola żółte).

Please fill in BLUE fields Don't edit Yellow fields											
(Device hostname)	(Device IP)	(WEP - Windows Event type logs RSYSLOG - Syslog type logs)	(Company Name - Plant Owner)	(Plant location - city name)	Plant / Process Name	(Network zone)	(Control System vendor)	(Device type)	(Log gathering mechanism)	(Log collector IP)	
ot_host_Name	ot_IP_address	ot_Mechanizm_pozykiwania_danych	ot_Spolka	ot_Lokalizacja	ot_Instalacja	ot_Strefa	ot_Vendor	ot_Rodzaj_Zrodla	ot_PobieranieIDanychPoprzez	ot_AdresKolektora	
mlouh-Drac	192.168.0.x	RSYSLOG	Company 1	Warsaw	Power Plant XYZ	OT	Control system vendor Name	Drac	Syslog collector	10.2.3.4	
mlouh-S	192.168.0.x	RSYSLOG	Company 1	Warsaw	Power Plant XYZ	OT	Control system vendor Name	Esxi	Syslog collector		
denasOS	192.168.0.x	RSYSLOG	Company 1	Warsaw	Power Plant XYZ	DMZ OT		NAS Synology	Syslog collector		
127NET11_SK	192.168.0.x	RSYSLOG	Company 1	Warsaw	Power Plant XYZ	IT		Switch Cisco	Syslog collector		
127NET21_SK	192.168.0.x	RSYSLOG	Company 2	Poznan	Distillation plant 1	IT		Switch HP	Syslog collector		
127FW1_SK	192.168.0.x	RSYSLOG				OT		Emerson Smart Firewall	Kivi syslog	192.168.0.150 (low OT IP) + 10.2.3.4 (low Central IP)	
6W4055	192.168.0.x	WEP				OT		Windows WEC		192.168.0.251	
650269	192.168.0.251	WEP				OT		Windows WEC		192.168.0.251	

7. Firewalls_Settings

Konfiguracja firewall-i dostępnych z poziomu systemu operacyjnego lub systemu antywirusowego tak, aby dostępne były jedynie usługi i porty, które są wykorzystywane w trakcie eksploatacji systemu ICS oraz systemów cyberbezpieczeństwa.

INDEX											
Host Name	Rule Name	Enabled	Direction	Profiles	Grouping	Local IP	Remote IP	Protocol	Edge traversal	Action	
Host Name 1	@(Microsoft.Windows.Apprep.ChxApp_1000.14393.0_0_neutral_neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.Apprep.ChxApp/resources/DisplayDisplayName)	Yes	Out	Domain,Private,Pu blic	SmartScreen	Any	Any	Any	No	Allow	
Host Name 1	@(Microsoft.LockApp_10.0.14393.0_neutral_cw5n1h2txyewy?ms-resource://Microsoft.LockApp/resources/AppDisplayN ame)	Yes	Out	Domain,Private,Pu blic	Windows Default Lock Screen	Any	Any	Any	No	Allow	
Host Name 1	@(Microsoft.AccountsControl_10.0.14393.187_neutr al_cw5n1h2txyewy?ms-resource://Microsoft.AccountsControl/Resources/Dis playName)	Yes	Out	Domain,Private,Pu blic	Email and accounts	Any	Any	Any	No	Allow	
Host Name 1	@(Microsoft.Windows.Cortana_1.7.0.14393_neutral_ neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.Cortana/resources/Pa ckageDisplayName)	Yes	In	Domain,Private,Pu blic	Cortana	Any	Any	Any	Yes	Allow	
Host Name 1	@(Microsoft.Windows.Cortana_1.7.0.14393_neutral_ neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.Cortana/resources/Pa ckageDisplayName)	Yes	Out	Domain,Private,Pu blic	Cortana	Any	Any	Any	No	Allow	
Host Name 1	SNAC Service	Yes	In	Domain		Any	Any	TCP	Any	Any	
Host Name 1	SMC Service	Yes	In	Domain		Any	Any	UDP	Any	Any	
Host Name 1	SMC Service	Yes	In	Domain		Any	Any	TCP	Any	Any	
Host Name 1	RM-RPC 135	Yes	In	Domain		Any	Any	TCP	135	Any	
Host Name 1	File and Printer Sharing (NB-Session-Out)	Yes	Out	Domain	File and Printer Sharing	Any	Any	TCP	Any	139	
Host Name 1	File and Printer Sharing (SMB-In)	Yes	In	Domain	File and Printer Sharing	Any	Any	TCP	445	Any	
Host Name 1	Acronis Storage Node Service	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 1	Acronis Backup Management Server	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 1	Acronis Api Gateway Service	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 1	Portmap service	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 1	Acronis Managed Machine Service	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 2	Acronis ZeroMQ Gateway Service	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 2	Acronis Monitoring Service	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 2	Acronis Active Protection Service	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 2	Acronis Service Manager Service	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 2	Acronis Remote Agent Service	Yes	In	Domain,Private,Pu blic		Any	Any	Any	No	Allow	
Host Name 2	acDNS (UDP Port)	Yes	Out	Domain,Private,Pu blic	acDNS	Any	Any	UDP	5353	Any	

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	8 / 13

8. Applications_List

Kompletna lista oprogramowania zainstalowanego na poszczególnych zasobach które są wykorzystywane w trakcie eksploatacji systemu ICS oraz systemów cyberbezpieczeństwa.

INDEX					
Host Name	Description	InstallDate	Name	Vendor	Version
Host Name 1	Acronis Backup	20180621	Acronis Backup	Acronis	12.5.8110
Host Name 1	VMware Tools	20180621	VMware Tools	VMware, Inc.	10.1.10.6082533
Host Name 1	Microsoft Visual C++2008 Redistributable-x64	20180621	Microsoft Visual C++2008 Redistributable-x64	Microsoft Corporation	9.0.30729.6161
Host Name 2	Symantec Endpoint Protection	20180716	Symantec Endpoint Protection	Symantec Corporation	14.0.3897.1101
Host Name 2	Microsoft Visual C++2008 Redistributable-x86	20180621	Microsoft Visual C++2008 Redistributable-x86	Microsoft Corporation	9.0.30729.6161
Host Name 2	Microsoft MonitoringAgent	20180627	Microsoft MonitoringAgent	Microsoft Corporation	8.0.10918.0

9. Systems Services

Kompletna lista usług, na poszczególnych zasobach, które są wykorzystywane w trakcie eksploatacji systemu ICS oraz systemów cyberbezpieczeństwa.

INDEX							System services		
Host Name	Caption	Name	PathName	ServiceType	StartMode	State			
Host Name 1	Microsoft Monitoring Agent Audi	AdtAgent	C:\Windows\system32\AdtAgent.exe	Own Process	Disabled	Stopped			
Host Name 1	Application XXXX	AeLookupSvc	C:\Windows\system32\svchost.exe#NAME?	Share Process	Manual	Stopped			
Host Name 1	Application Layer Gateway Servi	ALG	C:\Windows\System32\alg.exe	Own Process	Manual	Stopped			
Host Name 2	Application Identity	AppIDSvc	C:\Windows\system32\svchost.exe#NAME?	Share Process	Manual	Stopped			
Host Name 2	Application Information	AppInfo	C:\Windows\system32\svchost.exe#NAME?	Share Process	Manual	Running			
Host Name 2	Application Management	AppMgmt	C:\Windows\system32\svchost.exe#NAME?	Share Process	Manual	Stopped			
Host Name 2	App Readiness	AppReadiness	C:\Windows\System32\svchost.exe#NAME?	Share Process	Manual	Stopped			
Host Name 2	AppX Deployment Service (AppXSv	AppXSvc	C:\Windows\system32\svchost.exe#NAME?	Share Process	Manual	Stopped			

10. Local Accounts

Lista wszystkich kont lokalnych, wykorzystywanych we wdrażanych/modyfikowanych systemach ICS oraz w systemach cyberbezpieczeństwa

INDEX										
Host Name	Account name	Member of group	Description	Disabled	Local/Domain	LocalAccount	Lockout	PasswordChangeable	PasswordExpires	PasswordRequired
Host Name 1	Administrator	Administrators	Built-in account for administering the computer/domain	PRAWDA	Domain_name	PRAWDA	FALSZ	PRAWDA	PRAWDA	PRAWDA
Host Name 1	kowalskia	Users	Adam Kowalski	FALSZ	Domain_name	PRAWDA	FALSZ	PRAWDA	PRAWDA	PRAWDA
Host Name 1	Guest	Guest	Built-in account for guest access to the computer/domain	PRAWDA	Domain_name	PRAWDA	FALSZ	FALSZ	PRAWDA	FALSZ
Host Name 2	Administrator	Administrator	Built-in account for administering the computer/domain	PRAWDA	Domain_name	PRAWDA	FALSZ	PRAWDA	PRAWDA	PRAWDA
Host Name 2	kowalskia	Users	Adam Kowalski	FALSZ	Domain_name	PRAWDA	FALSZ	PRAWDA	PRAWDA	PRAWDA
Host Name 2	Guest	Guest	Built-in account for guest access to the computer/domain	PRAWDA	Domain_name	PRAWDA	FALSZ	FALSZ	PRAWDA	FALSZ

11. Domain Account

Lista wszystkich kont domenowych, wykorzystywanych we wdrażanych/modyfikowanych systemach ICS oraz w systemach cyberbezpieczeństwa.

INDEX						
Domain Name	User account	Member of	OU	GPO Name	Domain Group	Description
name.local	kowalskij	Domain Admin	Name_Users	Domain Users	DCS Admin	Members in this group can have their passwords replicated to all r
name.local	kowalskij	Domain Admin	Name_Users	Domain Users	APC Administrators	APC System Administrators
name.local	kowalskij	Domain Admin	Name_Users	Domain Users	Enterprise Admins	Designated administrators of the enterprise

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	9 / 13

12. AD_OU

Lista wszystkich jednostek organizacyjnych w domenie wykorzystywanych we wdrażanych/modyfikowanych systemach ICS oraz w systemach cyberbezpieczeństwa. Wraz z nazwą OU należy zamieścić pełną ścieżkę dla każdej z jednostek organizacyjnych oraz ilość elementów w każdej z nich (np. ilość kont użytkowników czy kont komputerów).

INDEX				
Domain Name	OU_Name	full patch of OU	Count (CN)	Description
name.local	Users	OU=Users,DC=name,DC=local		All Users
name.local	Admins	OU=Admins, OU=Users,DC=name,DC=local	4	Admintrator
name.local	PowerUsers	OU=PowerUsers, OU=Users,DC=name,DC=local	20	Power Users
name.local	Groups	OU=Groups, DC=name,DC=local		All groups
name.local	Security Groups	OU=Security Groups,OU=Groups, DC=name,DC=local		
name.local	FileShare Groups	OU=FileShare Groups,OU=Groups, DC=name,DC=local		
name.local	Computers	OU=Computers,DC=name,DC=local		All computers
name.local	Servers	OU=Servers,OU=Computers,DC=name,DC=local	3	All Servers
name.local	Workstations	OU=Workstations,OU=Computers,DC=name,DC=local	10	All workstations
name.local	VMs	OU=VMs,OU=Computers,DC=name,DC=local	5	All Virtual Machines

13. GPO

W arkuszu GPO należy zamieścić Eksport polityk GPO wykorzystywanych we wdrażanych/modyfikowanych systemach ICS oraz w systemach cyberbezpieczeństwa

INDEX				
Default Domain Controllers Policy				
Computer Configuration (Enabled)				
Policies				
Windows Settings				
Security Settings				
Local Policies/User Rights Assignment				
Policy	Setting			
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone			
Add workstations to domain	NT AUTHORITY\Authenticated Users			
Adjust memory quotas for a process	IIS APPPOOL\DefaultAppPool, IIS APPPOOL\NET v4.5 Classic, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, IIS APPPOOL\NET v4.5			
Allow log on locally	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators			
Back up files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators			
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone			
Change the system time	BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE			
Create a pagefile	BUILTIN\Administrators			
Debug programs	BUILTIN\Administrators			
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators			
Force shutdown from a remote system	BUILTIN\Server Operators, BUILTIN\Administrators			
Generate security audits	IIS APPPOOL\DefaultAppPool, IIS APPPOOL\NET v4.5 Classic, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, IIS APPPOOL\NET v4.5			
Increase scheduling priority	BUILTIN\Administrators			
Load and unload device drivers	BUILTIN\Print Operators, BUILTIN\Administrators			
Log on as a batch job	BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators, BUILTIN\IIS_IUSRS			

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	10 / 13

14.Name_of_device_L2

Pełna konfiguracja urządzenia sieciowego (dla warstwy L2). W pole Runing Config należy zamieścić zrzut konfiguracji z urządzenia. W przypadku wykorzystania kolejnych urządzeń – należy dodać odpowiednie arkusze z danymi (Wraz z uzupełnieniem i powiązaniem na arkuszu INDEX).

INDEX	
Hostname:	
Manufacturer:	Cisco
Model:	WS-C2960XR
Software ver.:	15.2(2)E7
SW Image:	C2960X-
IP Address:	xx.xx.xx.xx
Port Desc.:	Gi1/0/1 HSRP UPLINK Gi1/0/2 UPLINK TO L35 Gi1/0/3 Gi1/0/4 Host_name_2 Gi1/0/5 Gi1/0/6 Host_name_3 Gi1/0/7 Gi1/0/8 Gi1/0/9 Gi1/0/10 NAS Gi1/0/11 Gi1/0/12 Gi1/0/13 Host_name_7 Gi1/0/14 Host_name_8 Gi1/0/15 SPARE Gi1/0/16 SPARE Gi1/0/17 Gi1/0/18 Gi1/0/19 Gi1/0/20 SPARE Gi1/0/21 SPAN int L2 Gi1/0/22 SPAN Vlan L3 Gi1/0/23 SPAN External Gi1/0/24 SPARE
Running Config:	

15.Name_of_device_L3

Pełna konfiguracja urządzenia sieciowego (dla warstwy L3).). W pole Runing Config należy zamieścić zrzut konfiguracji z urządzenia. W przypadku wykorzystania kolejnych urządzeń – należy dodać odpowiednie arkusze z danymi (Wraz z uzupełnieniem i powiązaniem na arkuszu INDEX).

INDEX	
Hostname:	
Manufacturer:	Cisco
Model:	WS-C2960XR
Software ver.:	15.2(2)E7
SW Image:	C2960X-
IP Address:	xx.xx.xx.xx
Port Desc.:	Gi1/0/1 HSRP UPLINK Gi1/0/2 UPLINK TO L35 Gi1/0/3 Gi1/0/4 Host_name_2 Gi1/0/5 Gi1/0/6 Host_name_3 Gi1/0/7 Gi1/0/8 Gi1/0/9 Gi1/0/10 NAS Gi1/0/11 Gi1/0/12 Gi1/0/13 Host_name_7 Gi1/0/14 Host_name_8 Gi1/0/15 SPARE Gi1/0/16 SPARE Gi1/0/17 Gi1/0/18 Gi1/0/19 Gi1/0/20 SPARE Gi1/0/21 SPAN int L2 Gi1/0/22 SPAN Vlan L3 Gi1/0/23 SPAN External Gi1/0/24 SPARE
Running Config:	

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	11 / 13

16. TLS certificate

Szczegóły wykorzystywanych certyfikatów

INDEX	
RM Agent in multidomain environment use certificates for autentication needs. details are presented below.	
Issuer	Name-CA-Vxx.name.local
Issued to:	Name-CA-Vxx
Issued by:	Name-CA-Vxx
Valid from	xx.xx.20xx
Version	Vx
Serial number	
Protocol	TLS 1.x
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Subject	name.local
Public key	(RSA xxxxx Bits)
Public key parameters	xx xx
Certificate Template Name	Name
Subject Key Identifier	
CA Version	V0.0
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constraints	Subject Type=CA; Path Length Constraint=None
Thumbprint algorithm	sha1
Thumbprint	

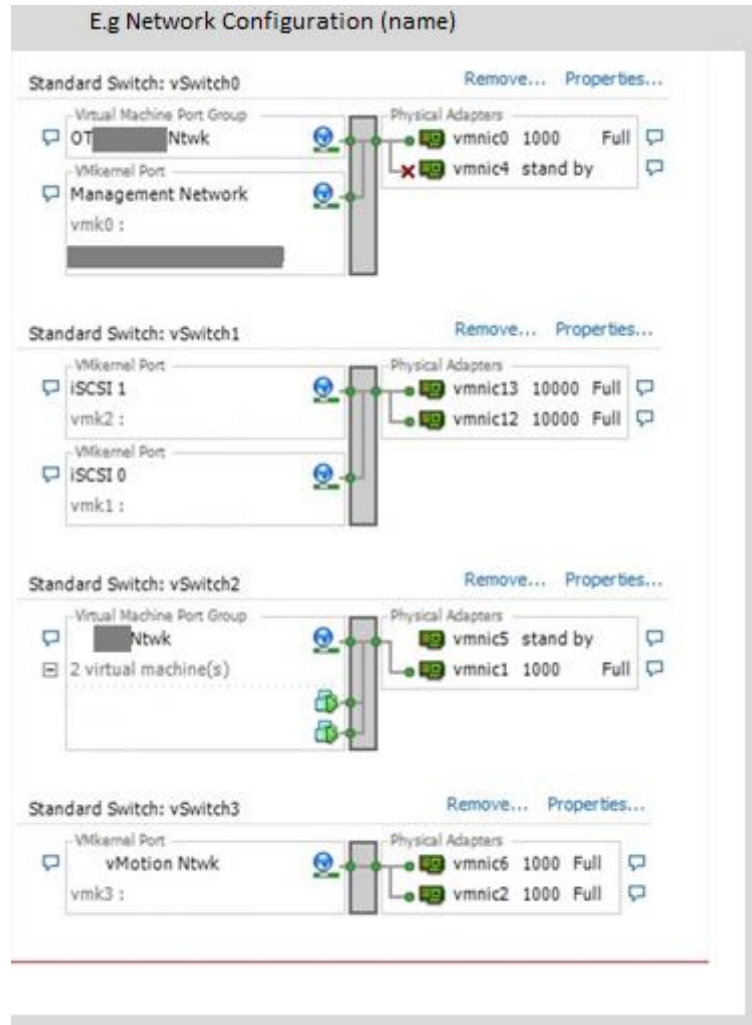
17. vSphere Host configuration

Arkusz zawierający pełną konfigurację wirtualizatorów

INDEX	
vSphere Hosts	
Hostname	name
Active Policy	High Performance
BIOS hardening	
Access Password Protection	√
Boot only from Hard Drive	√
Hardware configuration	
Product Name	ProLiant DLxxx Genx
System ROM	Pxx vx.xx (0x/xx/20xx)
iLO License Type	iLO Advanced
iLO Host Name	name.local
Product ID	xxxxxx_xxx
Power Management Controller FW	x.x.x
High Efficiency Mode	Balanced
Processor Socket 1	Intel(R) Xeon(R) CPU E5-xxxx W vx @ x.00GHz
Processor Socket 2	Intel(R) Xeon(R) CPU E5-xxxW vx @ x.00GHz
Memory Socket 1/9	DIMM DDR4 xxxxx MB Maximum Freq. xx00 MHz
Memory Sockt 1/12	DIMM DDR4 xxxxx MB Maximum Freq. xx00 MHz
Memory Socket 2/9	DIMM DDR4 xxxxx MB Maximum Freq. xx00 MHz
Memory Sockt 2/12	DIMM DDR4 xxxxx MB Maximum Freq. xx00 MHz
Device Inventory	
HP Ethernet 1 Gb 4 port 331i	Embedded
HP Ethernet 1 Gb 4 port 366FLR	Embedded
Smart Array P440ar Controller	Embedded
HPE Smart Storage Battery	Embedded
HP Ethernet 1Gb 4-port 366T	PCI-E Slot 1
HPE Ethernet 10Gb 2-port 562SFP+	PCI-E Slot 4
3x SSD 400GB MO000400JWDKU	N/A

Wraz z konfiguracją połączeń sieciowych:

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	12 / 13



18. VM list and resources

Arkusz z pełną listą maszyn wirtualnych oraz ich konfiguracją sprzętową.

INDEX										
VM resource requirement estimation										
	CPU Allocation (MHz)	CPU Quantity	Virtual Memory (GB)	Disk Avg (IOPs)	Disk Max (IOPs)	Network (Mbps)	Disk Size (GB)	Network assignment	Hot-plug resources	
Backup	x000	3	x	xx	xx	xx	xx	L3 Name	Enabled	
Service AV (Symantec)	x000	2	xx	xx	xx	xx	xx	L3 Name	Enabled	
WSUS	x000	2	xx	xx	xx	xx	xx	L3 Name	Enabled	
AWL	x000	2	x	xx	xx	xx	xx	L3 Name	Enabled	
Domain Controller 1	xx0	2	x	xx	xx	xx	xx	L3 Name	Enabled	
Domain Controller 2	xx0	2	x	xx	xx	xx	xx	L3 Name	Enabled	
vCenter Server 6.0	x000	4	x	xx	xx	xx	xx	L3 Name	Enabled	
Relay Node RDP	\	1	x	xx	xx	xx	xx	L3 Name	Enabled	
PI Collector (pri)	x000	2	x	xx	xx	xx	xx	L3 Name	Disabled	
PI Collector(sec)	x000	2	x	xx	xx	xx	xx	L3 Name	Disabled	
APC	x000	4	x	xx	xx	xx	xx	L3 Name	Enabled	
AMS	x000	2	x	xx	xx	xx	xx	L3 Name		

19. Labels

Etykiety dla okablowania

	Standard Cyberbezpieczeństwa OT Dokumentacja konfiguracyjna cyberbezpieczeństwa OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	13 / 13

INDEX						
Cable name	Network device			Other infrastructure device		
	Host Name	Port No.	Label	Host Name	Port No.	Label
Network device (for example: switch) <- -> Other device (for example: computer, server, disc array)						
W01	Switch_L1	0	W01/Switch_L1/0	Server_Name_1	1	W01/Server_Name_1/1
W02	Switch_L1	1	W02/Switch_L1/1	Server_Name_1	2	W02/Server_Name_1/2
W03	Switch_L1	2	W03/Switch_L1/2	Server_Name_1	3	W03/Server_Name_1/3
W04	Switch_L1	3	W04/Switch_L1/3	Server_Name_2	1	W04/Server_Name_2/1
W05	Switch_L1	4	W05/Switch_L1/4	Server_Name_2	2	W05/Server_Name_2/2
W06	Switch_L1	5	W06/Switch_L1/5	Server_Name_2	3	W06/Server_Name_2/3
W07	Switch_L1	6	W07/Switch_L1/6	Server_Name_3	1	W07/Server_Name_3/1
W08	Switch_L1	7	W08/Switch_L1/7	Server_Name_3	2	W08/Server_Name_3/2
W09	Switch_L1	8	W09/Switch_L1/8	Server_Name_3	3	W09/Server_Name_3/3
W10	Switch_L2	1	W10/Switch_L2/1	Server_Name_4	1	W10/Server_Name_4/1
W11	Switch_L2	2	W11/Switch_L2/2	Server_Name_4	2	W11/Server_Name_4/2
W12	Switch_L2	3	W12/Switch_L2/3	Server_Name_4	3	W12/Server_Name_4/3
W13	Switch_L2	4	W13/Switch_L2/4	Server_Name_5	1	W13/Server_Name_5/1
W14	Switch_L2	5	W14/Switch_L2/5	Server_Name_5	2	W14/Server_Name_5/2
W15	Switch_L2	6	W15/Switch_L2/6	Server_Name_5	3	W15/Server_Name_5/3
W16	Switch_L2	7	W16/Switch_L2/7	other_device_name_1	1	W16/other_device_name_1/1
W17	Switch_L2	8	W17/Switch_L2/8	other_device_name_2	2	W17/other_device_name_2/2
S1	Switch_L1	9	S1/Switch_L1/9			
S1	Switch_L2	9	S1/Switch_L2/9			
S2	Switch_L3	1	S3/Switch_L2/9			
S2	Switch_L4	2	S3/Switch_L2/9			
C1				Server_Name_1	4	C1/Server_Name_1/4
C1				Server_Name_2	5	C1/Server_Name_2/5
C2				Server_Name_3	5	C2/Server_Name_3/5
C2				Server_Name_4	5	C2/Server_Name_4/5

XX/YYYY/ZZZ

WXX number (common for both ends)

WXX- connection between switches and other devices

SXX- direct connection between two switches

COX- direct connection between two servers or computers

YYYY – device name (assigned to plug)

ZZZ – port number (assigned to plug)

20. Postanowienia końcowe

Właścicielem niniejszego standardu jest Obszar Cyberbezpieczeństwa OT ORLEN S.A. Jakikolwiek zmiany lub aktualizacje w dokumencie muszą być realizowane za zgodą i przez Obszar Cyberbezpieczeństwa OT ORLEN S.A. Każda aktualizacja dokumentu musi być zaakceptowana przez osobę kierownika Obszar Cyberbezpieczeństwa OT ORLEN S.A.

21. Załączniki

1. Zał. 1.1.5. Dokumentacja konfiguracyjna cyberbezpieczeństwa – Arkusz z danymi