Harmonizing People, Processes, and Technology for Robust Cybersecurity

D4.4 Automated Response Toolkit v2

Document Summary Information

Grant Agreement No	101158555	**Acronym**	CYberSynchrony
Full Title	Harmonizing People, Processes, and Technology for Robust Cybersecurity		
Start Date	01/06/2024	**Duration**	36 months
Project URL	https://www.cybersynchrony.eu/		
Deliverable	D4.4 Automated Response Toolkit v2		
Work Package	WP4 Advanced Proactive Cyber Risk Monitoring and Rapid Response (CYBRITE)		
Contractual due date		**Actual submission date**	
Type	OTHER	**Dissemination Level**	Public
Lead Beneficiary	Focal Point (FP)		
Responsible Author	Koutras Dimitris (FP), Malamas Vangelis (FP)		
Contributions from			

Funded by the European Union

Funded by the European Union under Grant Agreement no. 101158555. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Revision history

Version	Issue Date	Changes	Contributor(s)
0.1	27.03.2026	Initial Deliverable structure	Koutras Dimitris (FP)
0.2	02.04.2026	Deliverable Structure Finalization	Malamas Evangelos (FP)
0.3	09.05.2026	First contribution	Koutras Dimitris, Malamas Evangelos (FP)
0.4	22.05.2026	Contribution	Malamas Evangelos, Koutras DImitris (FP)
0.5	29.05.2026	Final draft	Koutras Dimitris, Malamas Evangelos (FP)
0.6	10.06.2026	New contribution	Koutras Dimitris, Malamas Evangelos (FP)
0.6	17.06.2026	Peer review no 1	Laskarina Mavropoulou (MER)
0.7	19.06.2026	Peer review no 2	Spyridon Papagiannopoulos (UPRC)
1.0	22.06.2026	Final changes	Koutras Dimitris, Malamas Evangelos (FP)

Disclaimer

The content of the document herein is the sole responsibility of the publishers, and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CYberSynchrony consortium make no warranty of any kind with regard to this material including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© CYberSynchrony Consortium This Deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

[1] According to CYberSynchrony's Quality Assurance Process for reports:

- 3 months before Deliverable's Due Date: Table of Contents ready to be reviewed by WP leader/ Technical Manager/ Quality Manager
- 2 months before Deliverable's Due Date: 50% should be complete. Review by the Quality Manager (& Technical Manager for software).
- 1 month before Deliverable's Due Date:100% should be complete. Review by the Quality Manager and Peer Reviewers.
- M: Sent to PC for Submission to the EC after addressing all comments by Quality Manager and Peer Reviewers

Table of Contents

Executive Summary 6
1 Introduction 8
1.1 Mapping CYberSynchrony Outputs 8
1.2 Linkage to other project outputs 10
1.3 Deliverable Structure 11
2 Position in CYberSynchrony Architecture 12
3 Defensive Cyber Operations (DCO) 15
3.1 Component Description 15
3.2 Architecture 16
3.3 Technologies Used 18
3.4 Updates since v1 19
3.5 Integration, interoperability and deployment 21
3.5.1 Integration with Wazuh 21
3.5.2 Integration with Neo4j 22
3.5.3 Integration with LLM services 22
3.5.4 Integration with the CyberSynchrony dashboard 22
3.5.5 Integration with CSPA 23
3.5.6 Integration with ASA 24
3.5.7 Integration with PTA 24
3.5.8 Kubernetes deployment 24
4 Conclusions 28

List of Figures

Figure 1 - CYBERRA dashboard entry point for Defensive Cyber Operations. The figure shows the CYBERRA landing page and the Defensive Cyber Operations card through which the DCO demo and dashboard can be accessed 12

Figure 2 - DCO dashboard with MITRE ATT&CK-mapped incidents, alerts, and playbooks. The figure shows technique tabs, incident counters, alert details, and a rendered defensive playbook 13

Figure 3: DCO high-level architecture. The diagram shows the CyberSynchrony dashboard communicating with DCO over HTTP, while DCO retrieves alerts from Wazuh Indexer, agent information from Wazuh Manager, and defensive playbooks from Neo4j. 17

Figure 4: Kubernetes deployment positioning of focalpoint-dco. The figure should show the GitLab registry secret, ConfigMap, Secrets, DCO deployment, ClusterIP service, and NetworkPolicy 26

List of Tables

Table 1: Adherence to CYberSynchrony's GA 8

Table 2: Links to other Project Outputs/Work 10

Table 3: DCO main components 16

Table 4: DCO API endpoint 18

Table 5: Technologies 19

Table 6: Main differences between D4.2 v1 and D4.4 advanced version 21

© CYberSynchorny, 2024

Table 7: : CSPA posture-assessment flow and its relation to DCO enrichment. The figure should show how inventory data is processed by CSPA and mapped to CPE, D3FEND, ATT&CK, detection strategies, and mitigations. 24

Table 8: Deployment configuration elements 25

© CYberSynchorny, 2024

Acronyms and abbreviations

Abbreviation / Term	Description
AD	Active Directory
API	Application Programming Interface
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
CI/CD	Continuous Integration / Continuous Deployment
C&C	Command and Control
CSPA	**Cyber Security Posture Assessment**
CVE	**Common Vulnerabilities and Exposures**
CWE	**Common Weakness Enumeration**
CYBERRA	**CYberSynchrony module for Threat Intelligence and Risk Assessment**
CYBRITE	**CYberSynchrony module for Advanced Proactive Cyber Risk Monitoring and Rapid Response**
CYRESCUE	**CYberSynchrony module for Cybersecurity Resilience and Incident Response Enhancement**
D3FEND	**MITRE D3FEND defensive cybersecurity ontology**
DCO	**Defensive Cyber Operations**
EDR	**Endpoint Detection and Response**
FIM	**File Integrity Monitoring**
HTTP	**Hypertext Transfer Protocol**
IOC	**Indicator of Compromise**
JSON	**JavaScript Object Notation**
K8s	**Kubernetes**
LLM	**Large Language Model**
MITRE	**MITRE Corporation**
Neo4j	**Graph database used for entity, technique, and playbook relationships**
PTA	**Purple Team Assessment**
REST	**Representational State Transfer**
D3FEND	**MITRE D3FEND defensive cybersecurity ontology**
SIEM	**Security Information and Event Management**
SOAR	**Security Orchestration, Automation and Response**

© CYberSynchorny, 2024

Executive Summary

Deliverable D4.4, titled "Advanced Automated Response Toolkit", is developed under Work Package 4 (WP4) of the CYberSynchrony project, which focuses on Advanced Proactive Cyber Risk Monitoring and Rapid Response. This deliverable builds upon D4.2 "Automated Response Toolkit v1" and presents the advanced, platform-integrated version of the automated response capability, centred on the Defensive Cyber Operations (DCO) tool.

D4.2 established the foundation of the Automated Response Toolkit by introducing the concept of automated response playbooks, SIEM/SOAR integration, and structured incident response workflows. It focused on the design of playbook logic, the use of SIEM alerts as triggers, and the role of response automation in improving cyber resilience. However, D4.2 remained closer to a first implementation and methodology-oriented version. It included a limited set of representative playbooks and focused mainly on demonstrating how automated response could be structured for selected cyber incidents.

D4.4 advances this work substantially. The new version documents DCO as an implemented, scalable, and integrated platform capability. The main difference from v1 is that DCO is no longer limited to a small catalogue of manually prepared or representative playbooks. The advanced version introduces a playbook-generation and management approach capable of producing and maintaining more than 1,000 defensive playbooks, covering almost all cases that can be extracted and mapped from Wazuh alerts and MITRE ATT&CK-oriented detection information. This represents a major expansion in coverage: from an initial limited playbook set in v1, to a broad, scalable, knowledge-driven response capability in D4.4.

The advanced DCO tool is implemented as a Go-based security orchestration and response application. It integrates with Wazuh for threat detection, alert retrieval, and agent inventory; with Neo4j for storing and retrieving defensive playbooks and relationships; and with LLM providers for generating or enriching incident response playbooks. The DCO platform contains two main backend applications: the API service, which manages interaction with Wazuh, Neo4j, and the LLM layer, and the playbook-generator, which automatically creates incident response playbooks by extracting data from Wazuh and Neo4j, processing it through an LLM, and storing the generated results for operational use.

The DCO dashboard is integrated into the CyberSynchrony platform interface. It allows analysts to navigate incidents through MITRE ATT&CK technique identifiers, review summary indicators, expand alert details, inspect Wazuh event information, and read defensive playbooks rendered in Markdown. The dashboard supports both live and demo modes. In live mode, the frontend communicates with the focalpoint-dco backend API. In demo mode, a static dataset is used to demonstrate the behaviour of the interface without requiring backend availability.

The deliverable also explains the integration of DCO with the wider CYberSynchrony ecosystem. CYberSynchrony is designed as a holistic modular framework that integrates technology, processes, and human capabilities to strengthen preparedness, rapid incident response, and coordinated cybersecurity operations. DCO contributes to this vision by providing the response layer that connects detection evidence with operational guidance. In this framework, DCO is not an isolated tool. It is designed to benefit from and contribute to the whole CyberSynchrony platform.

A key integration point is the Cyber Security Posture Assessment (CSPA) component. CSPA allows users to upload system inventory data and receive a comprehensive analysis of hardware, software, and services. It maps these artifacts to CPE identifiers, MITRE D3FEND digital artifacts, MITRE ATT&CK techniques, and related detection and mitigation strategies. This is highly relevant to DCO because CSPA can enrich incident response playbooks with asset-specific defensive context. While MITRE ATT&CK explains what the adversary does, MITRE D3FEND

© CYberSynchorny, 2024

explains what defenders can protect, detect, and mitigate. As a result, DCO can use CSPA outputs to make playbooks more precise and better aligned with the affected digital artifacts.

DCO can also interoperate with the Attack Surface Assessment (ASA) and Purple Team Assessment (PTA) components. ASA can provide vulnerability and exposure information through CVE and CWE mappings, helping DCO prioritise incidents that affect vulnerable systems. PTA can provide validation evidence by showing whether detection and response logic worked during purple-team exercises. Together, CSPA, ASA, and PTA create a strong enrichment and feedback loop around DCO: CSPA explains the posture, ASA explains the exposure, PTA validates the response, and DCO operationalises the defensive action.

The advanced toolkit is also designed for operational deployment. The focalpoint-dco application can be deployed into production or staging Kubernetes environments. Deployment requires configuration of Wazuh and Neo4j endpoints, secure management of credentials through Kubernetes Secrets, creation of a GitLab registry secret for pulling the private container image, and application of ConfigMap, Secret, Deployment, Service, and NetworkPolicy manifests. The DCO service is exposed internally as a hardened ClusterIP service and restricted by a NetworkPolicy on port 8443, supporting secure deployment in controlled environments.

Overall, D4.4 demonstrates that the Automated Response Toolkit has matured from an initial response-playbook concept into an advanced, integrated, and deployable Defensive Cyber Operations capability. The main improvements are the large-scale playbook-generation capacity, the integration with Wazuh and Neo4j, the use of LLMs, the connection with the CyberSynchrony dashboard, and the ability to interoperate with CSPA, ASA, and PTA. These improvements directly support the CYberSynchrony objective of harmonising people, processes, and technology for robust cybersecurity.

© CYberSynchorny, 2024

1 Introduction

The CYberSynchrony project introduces a modular and holistic cybersecurity framework that combines technological capabilities, operational processes, human expertise, and a security-centric culture. The project places strong emphasis on rapid incident response, improved preparedness, mutual assistance, enhanced threat assessment, risk monitoring, early incident detection, and coordinated information exchange between stakeholders.

D4.4 "Advanced Automated Response Toolkit" contributes directly to this vision by presenting the advanced version of the automated response capability developed in WP4. The deliverable focuses on the Defensive Cyber Operations (DCO) tool, which is the central response-oriented component described in this document. DCO provides a bridge between security monitoring and operational response by connecting Wazuh alerts, MITRE ATT&CK mappings, Neo4j-based playbook knowledge, and LLM-assisted playbook generation.

The first version of the Automated Response Toolkit, documented in D4.2, established the conceptual foundation for automated playbooks, SIEM/SOAR integration, and rapid response workflows. It showed how selected cyber incidents could be addressed through structured playbooks and how alerts could trigger response actions. This was an important first step, but its coverage was intentionally limited. The v1 version relied on a small set of representative playbooks, approximately ten, which were sufficient to demonstrate the methodology but not sufficient to cover the broad operational reality of a live security monitoring environment.

D4.4 extends this work by documenting the concrete implementation of the advanced DCO capability. The DCO tool is now positioned as a platform component that supports alert navigation, technique-based grouping, playbook retrieval, LLM-assisted playbook generation, analyst review, and Kubernetes-based deployment. Most importantly, the advanced version can generate and maintain more than 1,000 playbooks. These playbooks are derived from Wazuh-extracted alert and technique information and are designed to cover almost all operational cases that can be mapped from the detection layer. This is the central improvement of the new version.

The deliverable follows the structural logic used in D3.4. It begins by mapping the deliverable to CYberSynchrony outputs and explaining its relationship with other project components. It then describes the position of DCO in the CYberSynchrony architecture, presents the DCO tool, explains updates since v1, and documents integration, interoperability, and deployment aspects. This structure allows the deliverable to focus on the actual tool while also showing its contribution to the wider CyberSynchrony platform.

1.1 Mapping CYberSynchrony Outputs

This section presents the CYberSynchrony Grant Agreement commitments and project objectives addressed by D4.4. The deliverable contributes to the implementation of the WP4 advanced response capability and to the overall platform objective of improving preparedness, coordinated response, and resilience against cyber threats.

Table 1: Adherence to CYberSynchrony's GA

Component no	Component title	Respective Document Chapter(s)	Justification
DELIVERABLE			
D4.4	Advanced Automated Response Toolkit	Chapters 2, 3, 4	D4.4 documents the advanced version of the automated response capability, focusing on DCO as the implemented tool for connecting alerts, MITRE

© CYberSynchorny, 2024

			ATT&CK techniques, defensive playbooks, Wazuh telemetry, Neo4j knowledge representation, and LLM-assisted response guidance.
TASKS			
WP4	Advanced Proactive Cyber Risk Monitoring and Rapid Response	Chapters 2, 3	DCO contributes to proactive monitoring and rapid response by consuming Wazuh alerts, organising them by technique, and associating them with defensive playbooks for analyst review and response support.
T4.1	SIEM and Traffic Analysis Deployment	Chapter 3	DCO builds on the SIEM layer by retrieving alerts and agent information from Wazuh. This allows the platform to connect detection outputs with response-oriented playbook guidance.
T4.3	Application of Incident Response Automation Playbooks	Chapters 3, 4	DCO operationalises playbook-driven incident response through API endpoints, dashboard views, and automatically generated or retrieved playbooks.
T4.3.1	Design of Playbooks for Cyber Incident Response	Chapter 3.1	The advanced version significantly expands the playbook catalogue from a limited v1 set to more than 1,000 generated playbooks, covering a much broader range of ATT&CK-mapped cases extracted from Wazuh.
T4.3.2	Integration with SIEM and Response Automation	Chapters 3, 3.2	DCO integrates with Wazuh Manager and Wazuh Indexer and exposes REST API endpoints for agents and playbooks. It supports a response-oriented workflow through the CyberSynchrony dashboard.
Platform integration objective	Interoperability across CYberSynchrony modules	Chapters 2, 3.2	The deliverable explains how DCO can interact with CSPA, ASA, and PTA, supporting a unified risk-to-response workflow.
Project-level rapid response objective	Enhanced preparedness and efficient response to cyber threats	Executive Summary, Chapters 2–4	DCO supports the project's objective of reducing response time and improving defensive coordination by transforming alerts into structured defensive guidance.

© CYberSynchorny, 2024

1.2 Linkage to other project outputs

D4.4 is directly linked to previous and parallel project outputs. Its main predecessor is D4.2, which established the first version of the Automated Response Toolkit. D4.4 advances that foundation by presenting DCO as a concrete, scalable, platform-integrated capability.

It is also linked to D3.4, which documents the Risk Scenario Analysis Toolkit V2. D3.4 includes components such as CSPA, ASA, and PTA, each of which provides inputs that can improve DCO's response logic. CSPA provides posture and defensive-mapping context. ASA provides exposure and vulnerability context. PTA provides validation evidence for detection and response performance.

Table 2: Links to other Project Outputs/Work

WP Number	Task Number	Deliverable Number related
WP3	D3.4 Risk Scenario Analysis Toolkit V2	D3.4 provides risk assessment, posture assessment, vulnerability assessment, and validation capabilities that can support DCO's response prioritisation and playbook enrichment.
WP3 / CYRESCUE	CSPA	CSPA analyses system inventories, maps assets to CPE identifiers, projects them to MITRE D3FEND digital artifacts, and associates them with MITRE ATT&CK techniques, detection strategies, and mitigations. This can enrich DCO playbooks with precise defensive context.
WP3 / CYBERGOPLUS	ASA	ASA identifies assets, correlates them with CVEs and CWEs, and provides vulnerability and exposure context. This can help DCO prioritise incidents affecting vulnerable or exposed assets.
WP3 / CYRESCUE	PTA	PTA validates detection and response capabilities through purple-team assessment workflows. Its outcomes can inform whether DCO playbooks and detection mappings require improvement.
WP4	D4.2 Automated Response Toolkit v1	D4.2 introduced the first version of the automated response toolkit, including a limited number of representative playbooks and the conceptual design of SIEM/SOAR response automation. D4.4 expands this into a scalable DCO implementation capable of generating more than 1,000 playbooks.
WP5	Incident response collaboration	DCO outputs, including technique-mapped incidents and structured playbooks, can support common operational understanding and coordinated response between entities.
WP6	Cybersecurity awareness and training	DCO playbooks and dashboard workflows can be used as structured training material for analysts and cybersecurity staff.

Contribution to the integrated CYberSynchrony platform

© CYberSynchorny, 2024

The contribution of D4.4 is not limited to the delivery of a standalone response tool. DCO is designed as an integration point within the CYberSynchrony ecosystem. It contributes to the platform by connecting detection, risk intelligence, asset posture, vulnerability exposure, validation evidence, and operational response.

At the platform level, DCO contributes to the following integration chain:

1. Detection and monitoring: Wazuh agents and Wazuh rules generate security alerts from monitored endpoints and infrastructure.
2. Technique mapping: Alerts are correlated with MITRE ATT&CK techniques, enabling analysts to understand the adversarial behaviour behind the event.
3. Response knowledge: Neo4j stores defensive playbooks and relationships, allowing DCO to retrieve the relevant response guidance.
4. Playbook generation: The LLM-enabled playbook-generator can create structured response playbooks from Wazuh and Neo4j data.
5. Posture enrichment: CSPA can add asset-specific D3FEND, detection, and mitigation context.
6. Exposure enrichment: ASA can add CVE and CWE context for affected assets.
7. Validation feedback: PTA can provide evidence about whether the detection and response logic worked during controlled assessment activities.
8. Analyst decision support: The DCO dashboard presents incidents, alerts, and playbooks in a readable operational interface.

This integration supports the CYberSynchrony vision of harmonising people, processes, and technology. People are supported through analyst-facing guidance and training value. Processes are supported through structured playbook workflows and repeatable response logic. Technology is supported through the integration of Wazuh, Neo4j, LLM services, Kubernetes deployment, and the wider CyberSynchrony platform modules.

1.3 Deliverable Structure

The deliverable is structured as follows:

Chapter 1 – Introduction presents the scope of D4.4, its relation to D4.2, its mapping to CYberSynchrony outputs, and its linkage with other project components.

Chapter 2 – Position in CYberSynchrony Architecture describes the positioning of DCO within the wider CYberSynchrony platform and explains how it contributes to the integrated cybersecurity workflow.

Chapter 3 – Defensive Cyber Operations (DCO) presents the DCO tool, including its component description, architecture, main features, dashboard logic, backend implementation, and operational workflow.

Chapter 3.1 – Updates since v1 explains the evolution from D4.2 to D4.4, highlighting the shift from a limited v1 playbook catalogue to a scalable DCO capability able to generate more than 1,000 playbooks.

Chapter 3.2 – Integration, interoperability and deployment presents the integration of DCO with Wazuh, Neo4j, the dashboard, LLM services, Kubernetes, and related CYberSynchrony tools such as CSPA, ASA, and PTA.

Chapter 4 – Conclusions summarises the outcomes of the deliverable and the role of DCO in improving preparedness, rapid response, and platform interoperability.

© CYberSynchorny, 2024

2 Position in CYberSynchrony Architecture

The DCO tool is positioned as the advanced response capability within the CYberSynchrony architecture. While several CYberSynchrony components focus on risk identification, threat intelligence, posture analysis, exposure assessment, or validation, DCO focuses on operationalising the response layer. It transforms monitored security events into structured incidents and connects them with defensive playbooks.

In the overall CYberSynchrony architecture, DCO interacts with three main categories of components:

- Detection and monitoring components, which provide alerts and security telemetry.
- Knowledge and assessment components, which provide risk, posture, vulnerability, and validation context.
- Platform and dashboard components, which provide the interface through which analysts access the results.

DCO is exposed through the CyberSynchrony user interface and is accessible from the CYBERRA dashboard entry point. Although the tool contributes functionally to WP4 rapid response objectives, its dashboard presentation inside the platform supports integrated access to threat intelligence, risk assessment, and defensive operations. This is consistent with the project's modular architecture, where components are autonomous but connected through APIs, shared data models, and platform-level workflows.

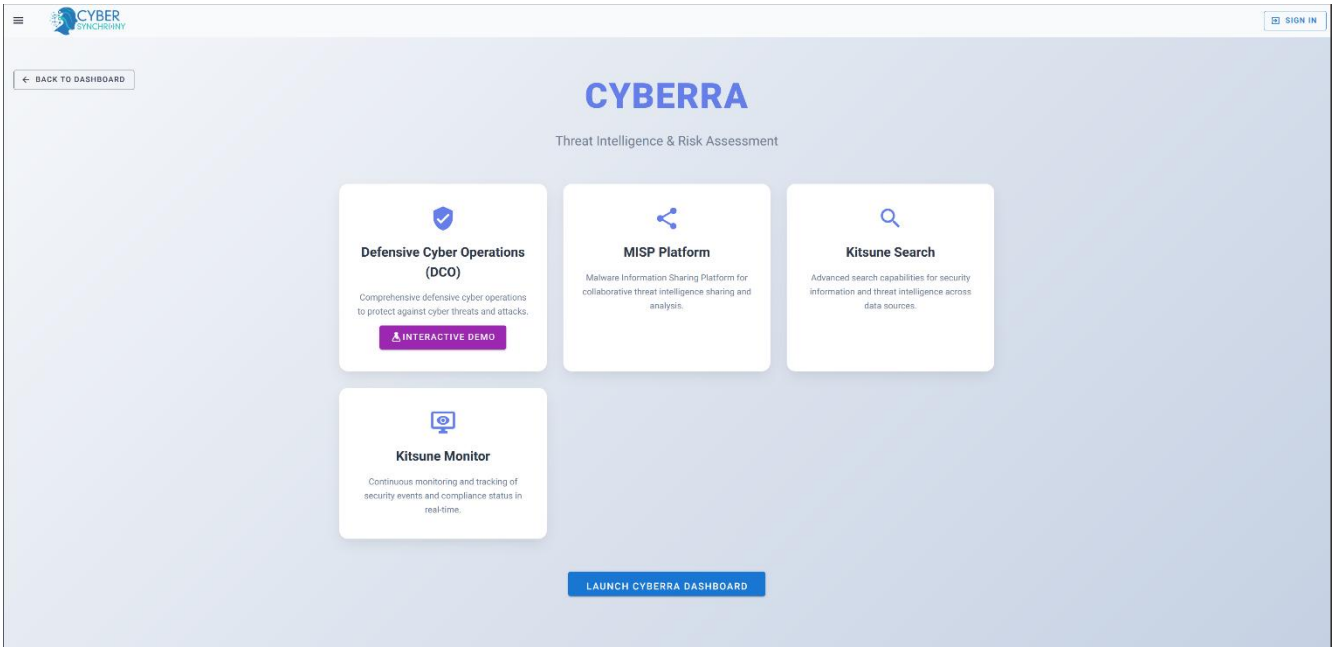

Figure 1 - CYBERRA dashboard entry point for Defensive Cyber Operations. The figure shows the CYBERRA landing page and the Defensive Cyber Operations card through which the DCO demo and dashboard can be accessed

The DCO dashboard presents incidents as MITRE ATT&CK technique-oriented tabs. This design allows analysts to view security events according to adversarial behaviour rather than only as isolated alerts. The interface also provides summary indicators for incidents, alerts, and playbooks, supporting quick situational awareness.

© CYberSynchorny, 2024

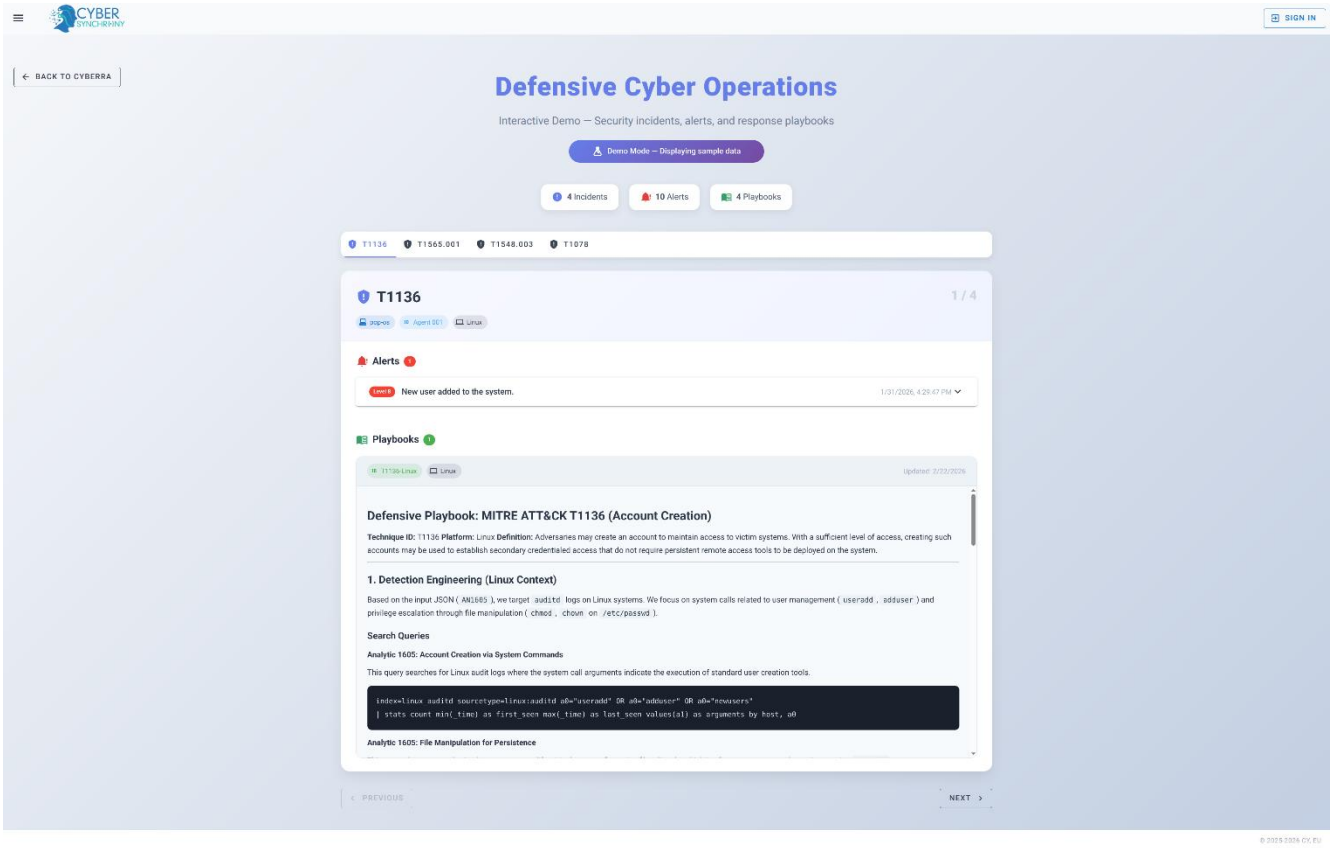

Figure 2 - DCO dashboard with MITRE ATT&CK-mapped incidents, alerts, and playbooks. The figure shows technique tabs, incident counters, alert details, and a rendered defensive playbook

At the platform level, DCO supports the following architectural role:

- It consumes Wazuh alerts and agent information as detection evidence.
- It maps incidents to MITRE ATT&CK techniques.
- It retrieves defensive playbooks from Neo4j.
- It can use LLM-assisted generation to produce structured playbooks.
- It renders playbooks in the dashboard in a human-readable format.
- It can be enriched by CSPA, ASA, and PTA outputs.

The relation between DCO and the other relevant CyberSynchrony components can be described as follows.

CSPA provides posture and defensive context. It receives system inventories, resolves assets to CPEs, maps them to MITRE D3FEND digital artifacts, and associates them with ATT&CK techniques, detection strategies, and mitigations. In relation to DCO, CSPA can help explain what is being defended and which countermeasures are relevant to the affected asset.

ASA provides attack surface and vulnerability context. It can identify which assets are associated with known CVEs and CWEs. In relation to DCO, ASA can help prioritise incidents that affect vulnerable assets or systems with exploitable weaknesses.

PTA provides validation context. It can assess whether detection and response mechanisms are working in practice and can provide feedback on whether the corresponding DCO playbooks are sufficient, incomplete, or require improvement.

© CYberSynchorny, 2024

Therefore, DCO contributes to the platform as the response activation layer. It consumes detection and contextual intelligence and provides analysts with structured response guidance. This supports the CYberSynchrony objective of improving rapid incident response, operational efficiency, resilience, and cross-organisational cybersecurity readiness.

© CYberSynchorny, 2024

3 Defensive Cyber Operations (DCO)

Defensive Cyber Operations (DCO) is the main tool described in D4.4. It is a Go-based security orchestration and response application that integrates Wazuh, Neo4j, LLM services, and the CyberSynchrony dashboard. Its purpose is to support proactive detection and response to cyber threats by combining Wazuh SIEM alerts with MITRE ATT&CK-mapped defensive playbooks.

The DCO tool addresses a central challenge in modern security operations: security teams often receive large numbers of alerts, but response knowledge is distributed across documents, procedures, tools, and analyst experience. DCO reduces this gap by grouping alerts into technique-based incidents and presenting the corresponding response playbooks directly inside the dashboard.

In D4.2, the first version of the toolkit demonstrated the response-playbook methodology using a limited number of playbooks. These were useful for showing the response concept, but they could not cover the broad range of events and techniques that can be extracted from a real monitoring system. D4.4 introduces the advanced DCO implementation, where the playbook-generation process is connected to Wazuh and Neo4j and can scale to more than 1,000 generated playbooks. This allows the platform to cover almost all Wazuh-extractable cases mapped to MITRE ATT&CK techniques, rather than focusing only on a small number of manually selected scenarios.

3.1 Component Description

The DCO platform is composed of two main backend applications:

wazuh-mitre: the API service that provides endpoints for interacting with the platform. It handles connections to Wazuh, Neo4j, and the LLM service. It is the main entry point for managing playbooks, alerts, and related information.

playbook-generator: a standalone service or tool designed to automatically generate incident response playbooks. It extracts data from Wazuh and Neo4j, processes it through an LLM, and stores the generated results.

The DCO repository is organised into several key directories. The cmd directory contains the main applications. The internal directory contains the core domain logic. The api package contains the HTTP REST API server using Huma and Chi. The config package manages configuration through Viper. The database package manages interaction with Neo4j. The llm package integrates LLM providers such as Ollama and Google GenAI. The playbook package contains the business logic for generating and managing playbooks. The wazuh package provides the client for interacting with Wazuh Manager and Wazuh Indexer. The logger package manages logging through Zerolog. Docker and Kubernetes directories provide material for local development, testing, and production deployment.

The DCO dashboard includes the following core capabilities:

- Incident navigation through MITRE ATT&CK technique tabs.
- Summary dashboard showing the number of incidents, alerts, and playbooks.
- Expandable alert details with rule information, MITRE tactics, agent information, event data, and full logs.
- Rendered Markdown playbooks with headings, tables, lists, and code blocks.
- Live and demo modes, supporting both backend-driven operation and standalone demonstration.

DCO playbooks provide structured response guidance for each detected technique. They can include detection strategies, investigation steps, containment actions, eradication guidance, recovery actions, and hardening recommendations. The advanced version expands the role of playbooks from a small demonstration set into a broad operational knowledge base.

© CYberSynchorny, 2024

3.2 Architecture

The high-level DCO architecture consists of the following layers:

DCO high-level architecture. The diagram shows the CyberSynchrony dashboard

Layer / Component	Responsibility
CyberSynchrony Dashboard	Provides the analyst-facing interface for viewing incidents, alerts, and playbooks.
DCO API	Exposes REST endpoints for health checks, agents, playbooks, and technique-specific playbook retrieval.
Wazuh Indexer	Provides indexed security alerts generated from monitored endpoints.
Wazuh Manager	Provides agent and endpoint information.
Neo4j Database	Stores defensive playbooks, entities, and relationships.
LLM Service	Supports automatic generation or enrichment of incident response playbooks.
Playbook Generator	Extracts Wazuh and Neo4j information, processes it through an LLM, and stores generated playbooks.
Kubernetes Deployment	Provides the production or staging deployment model for focalpoint-dco.

Table 3: DCO main components

© CYberSynchorny, 2024

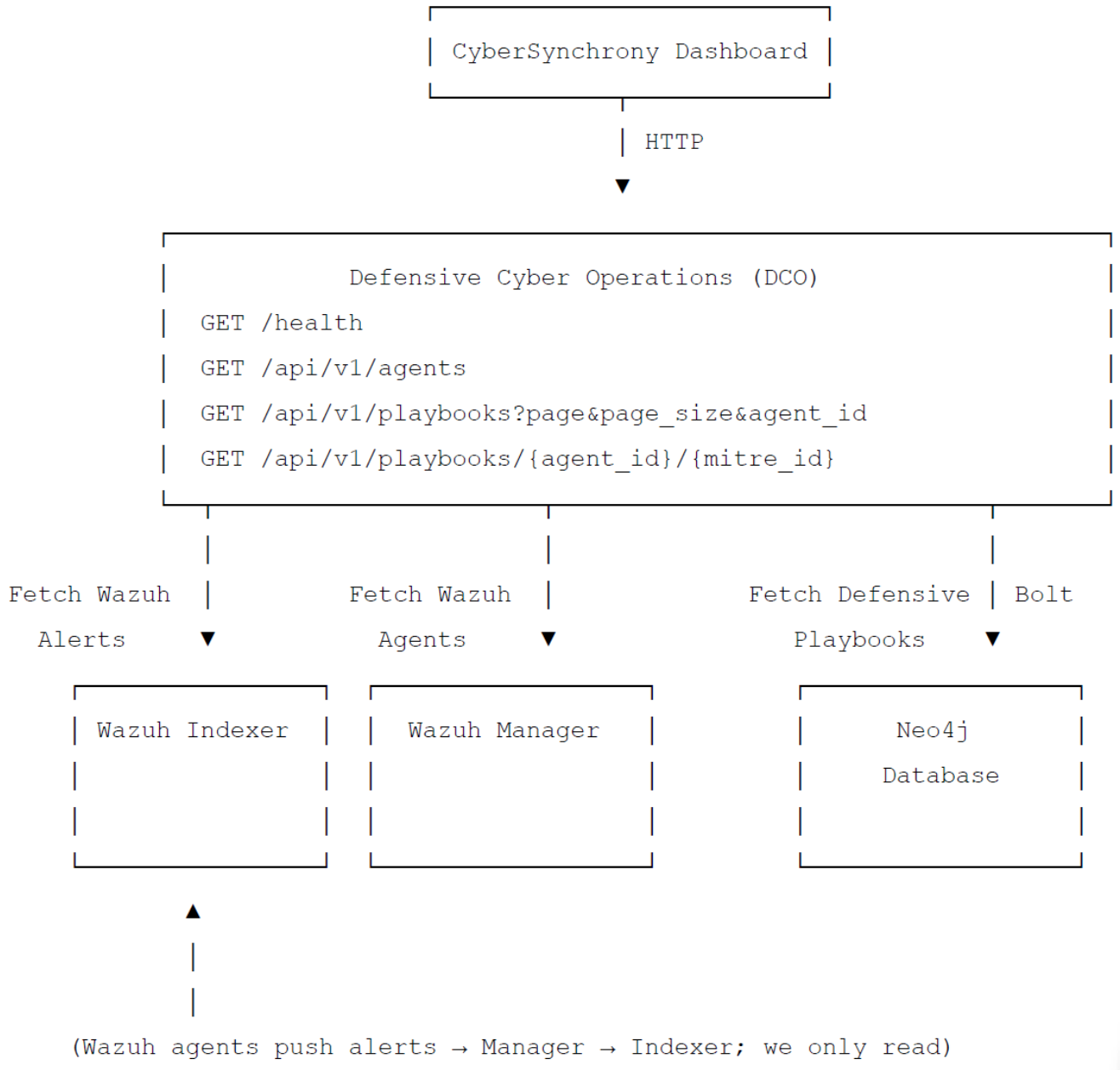

Figure 3: DCO high-level architecture. The diagram shows the CyberSynchrony dashboard communicating with DCO over HTTP, while DCO retrieves alerts from Wazuh Indexer, agent information from Wazuh Manager, and defensive playbooks from Neo4j.

The DCO backend reads from Wazuh rather than replacing Wazuh's detection function. Wazuh agents push alerts to Wazuh Manager and Indexer. DCO retrieves alerts from the Indexer, retrieves agent information from the Manager, and retrieves playbooks from Neo4j. This architecture keeps detection, knowledge representation, and response guidance separated but connected.

The main DCO API endpoints are:

© CYberSynchorny, 2024

Endpoint	Description
GET /health	Verifies that the DCO service is running.
GET /api/v1/agents	Retrieves Wazuh agent information.
GET /api/v1/playbooks?page&page_size&agent_id	Retrieves defensive playbooks with pagination and optional agent filtering.
GET /api/v1/playbooks/{agent_id}/{mitre_id}	Retrieves a defensive playbook associated with a specific agent and MITRE ATT&CK technique.

Table 4: DCO API endpoint

The frontend architecture includes three main pages:

- cyberra.vue: the CYBERRA module landing page.
- cyberra-dco.vue: the live DCO page connected to the backend API.
- cyberra-dco-demo.vue: the demo DCO page using static sample data.

The frontend also includes a DCO API client, TypeScript interfaces for DCO data, and shared navigation composables.

3.3 Technologies Used

The DCO implementation uses the following main technologies:

Technology / Stack	Purpose
Go	Backend implementation language for the DCO API and playbook generator.
Huma v2	API framework for OpenAPI-oriented REST endpoint definition.
Chi router	HTTP router used by the backend API.
Viper	Configuration management.
Zerolog	Structured logging.
Wazuh Manager	Agent and endpoint management information.
Wazuh Indexer	Alert retrieval and security event data source.
Neo4j	Graph database for playbooks, entities, and relationships.
Ollama / Google GenAI	LLM providers for playbook generation or enrichment.

© CYberSynchorny, 2024

Vue 3	Frontend dashboard framework.
TypeScript	Type-safe frontend implementation.
Vite	Frontend build and development environment.
Vuetify	UI components for dashboard presentation.
Kubernetes	Deployment environment for focalpoint-dco.
GitLab Container Registry	Container image hosting for DCO.

Table 5: Technologies

3.4 Updates since v1

D4.4 represents a substantial evolution from D4.2. While D4.2 described the first version of the Automated Response Toolkit and focused mainly on the design of automated incident response playbooks and SIEM/SOAR concepts, D4.4 documents the implemented, integrated, scalable, and deployable DCO capability.

The most important difference is the scale and automation of playbook production. In v1, the toolkit included a limited number of representative playbooks, around ten. These playbooks were valuable for demonstrating the methodology and proving that automated response logic could be structured around security alerts and incident categories. However, the limited catalogue meant that v1 could not provide broad operational coverage across the many different alerts, agents, and MITRE ATT&CK techniques that a real SIEM environment can produce.

In D4.4, the new DCO version introduces a playbook-generation pipeline capable of producing more than 1,000 playbooks. These playbooks are generated from information extracted from Wazuh and Neo4j and processed through an LLM. This means the toolkit is no longer dependent only on a small manually prepared set of examples. Instead, it can scale towards wide operational coverage, covering almost all cases that can be extracted from Wazuh and mapped to MITRE ATT&CK techniques.

The updates since v1 are summarised below.

1. From limited manual playbooks to large-scale playbook generation

The v1 toolkit demonstrated the playbook concept through a small number of selected examples. The advanced version introduces the playbook-generator component, which can automatically create a much larger catalogue of playbooks. The number of supported playbooks increases from approximately ten in v1 to more than 1,000 in the advanced version. This is a major functional improvement because it transforms the toolkit from a proof-of-concept response library into a scalable operational response knowledge base.

2. From selected scenarios to broad Wazuh-extracted coverage

In v1, the playbooks were based on selected response scenarios. In D4.4, the system extracts alert and technique information from Wazuh, connects it with Neo4j knowledge, and generates playbooks for a much broader range of detected behaviours. This allows DCO to cover most of the cases that Wazuh can expose through alerts and MITRE mappings, rather than focusing only on a few representative incidents.

3. From static response documentation to dynamic playbook generation

The v1 approach relied mostly on static playbook descriptions. The advanced version supports dynamic generation and enrichment using LLM services. This allows playbooks to be created or improved based on the

© CYberSynchorny, 2024

available alert data, entity information, and graph relationships. The playbooks remain analyst-readable but are generated at a scale that would be difficult to maintain manually.

4. From conceptual SIEM/SOAR integration to implemented Wazuh integration

D4.2 described the use of SIEM alerts as triggers for response workflows. D4.4 implements this through Wazuh. DCO retrieves alerts from Wazuh Indexer and agent information from Wazuh Manager. This creates a concrete bridge between monitoring and response.

5. From general incident categories to MITRE ATT&CK technique-based navigation

The v1 toolkit discussed incident categories such as phishing, malware, ransomware, and anomalous behaviour. The advanced version organises incidents through MITRE ATT&CK technique IDs. This is more precise because it connects alerts to adversarial behaviours. Analysts can navigate incidents by technique, review related alerts, and read the corresponding playbook.

6. From independent playbook logic to Neo4j-based knowledge representation

In v1, the playbook logic was mainly document- or workflow-oriented. In D4.4, playbooks and related entities are stored in Neo4j. This enables relationships between agents, techniques, playbooks, detections, and mitigations to be represented as a graph. The result is more flexible retrieval and better support for future enrichment.

7. From isolated toolkit to integrated platform component

D4.2 described the toolkit as part of WP4 response automation. D4.4 positions DCO as an integrated CyberSynchrony platform capability. It is accessible through the platform dashboard and can interoperate with other modules, especially CSPA, ASA, and PTA.

8. From response guidance only to posture- and exposure-aware response

The advanced version can be enriched by CSPA and ASA. CSPA can provide D3FEND-based defensive posture information, while ASA can provide CVE/CWE exposure information. This means DCO playbooks can become more context-aware, considering not only the alert but also the defensive posture and vulnerability exposure of the affected asset.

9. From unvalidated playbooks to feedback-driven improvement

Through PTA integration, DCO can be improved using validation outcomes. PTA can indicate which techniques were prevented, alerted, logged, or missed. This feedback can be used to refine DCO playbooks and improve response guidance over time.

10. From local or conceptual deployment to Kubernetes-ready deployment

D4.4 documents a Kubernetes deployment model for focalpoint-dco. This includes ConfigMaps, Secrets, deployment manifests, service exposure, NetworkPolicy, GitLab registry authentication, verification commands, and controlled access. The result is a tool that can be deployed in staging or production environments.

Area	D4.2 Automated Response Toolkit v1	D4.4 Advanced Automated Response Toolkit

© CYberSynchorny, 2024

Playbook scale	Limited representative catalogue of approximately ten playbooks	More than 1,000 generated playbooks covering almost all Wazuh-extractable ATT&CK-mapped cases
Playbook creation	Mostly manual or predefined examples	LLM-assisted generation using Wazuh and Neo4j data
Detection source	Conceptual SIEM/SOAR integration	Concrete integration with Wazuh Indexer and Wazuh Manager
Knowledge storage	Playbook logic described as workflows	Neo4j graph database stores playbooks, entities, and relationships
Incident organisation	General incident categories	MITRE ATT&CK technique-based incident navigation
Dashboard	Initial implementation and response concept	Integrated CyberSynchrony dashboard with live and demo DCO pages
Platform integration	Mainly WP4-focused	Integrated with the wider platform, including CSPA, ASA, and PTA
Posture enrichment	Not fully available	CSPA can provide D3FEND, detection, and mitigation context
Vulnerability enrichment	Not fully available	ASA can provide CVE/CWE exposure context
Validation feedback	Limited	PTA can provide validation evidence and feedback for playbook improvement
Deployment maturity	Early-stage deployment logic	Kubernetes-ready deployment with ConfigMaps, Secrets, Service, and NetworkPolicy

Table 6: Main differences between D4.2 v1 and D4.4 advanced version

3.5 Integration, interoperability and deployment

The DCO tool is designed to interoperate with several internal and external components. Its main integrations are with Wazuh, Neo4j, LLM services, the CyberSynchrony dashboard, and related CYberSynchrony modules such as CSPA, ASA, and PTA.

3.5.1 Integration with Wazuh

Wazuh provides the security monitoring and detection foundation for DCO. Wazuh agents monitor endpoints and infrastructure for suspicious activity. Rules trigger alerts that may be correlated with MITRE ATT&CK techniques. DCO retrieves these alerts from Wazuh Indexer and retrieves agent information from Wazuh Manager.

Through this integration, DCO can display:

© CYberSynchorny, 2024

- alert rule information,
- severity levels,
- alert location and index,
- mapped MITRE ATT&CK tactics,
- agent name, IP, and manager details,
- event data,
- full raw log entries.

This allows DCO to act as the response layer on top of Wazuh's detection capability. Wazuh detects and structures the alert data, while DCO translates this alert data into defensive response guidance.

3.5.2 Integration with Neo4j

Neo4j is used as the graph-based knowledge layer. It stores defensive playbooks, entities, and relationships. DCO retrieves playbooks from Neo4j based on the relevant agent and MITRE ATT&CK technique.

This graph-based design is important because defensive knowledge is relational. A single technique may be linked to multiple affected assets, detections, mitigations, and response actions. Neo4j allows these relationships to be stored and queried flexibly.

In the advanced version, Neo4j is also essential for scaling playbook generation. The playbook-generator can extract graph-based context and use it to produce more complete and technique-specific response guidance. This is one of the reasons why D4.4 can support more than 1,000 playbooks, while v1 was limited to a much smaller number.

3.5.3 Integration with LLM services

DCO integrates with LLM providers through the llm package. The configuration supports providers such as Ollama and Google GenAI. The playbook-generator uses this integration to process information extracted from Wazuh and Neo4j and produce structured incident response playbooks.

LLM-assisted generation can support:

- generation of detection guidance,
- response tier creation,
- containment recommendations,
- eradication and recovery guidance,
- hardening recommendations,
- analyst-readable playbook formatting.

The use of LLMs supports scalability while preserving the need for analyst review and validation. The LLM does not replace the analyst; it accelerates the creation and enrichment of playbooks so that the platform can provide broader coverage.

3.5.4 Integration with the CyberSynchrony dashboard

The DCO frontend is integrated into the CyberSynchrony dashboard. The dashboard includes a live DCO page and a demo DCO page. In live mode, API requests are proxied to the focalpoint-dco backend. In demo mode, static JSON data is used.

The frontend provides:

© CYberSynchorny, 2024

- incident navigation tabs,
- summary chips,
- expandable alert panels,
- rendered Markdown playbooks,
- previous and next navigation,
- technique-oriented presentation.

This integration ensures that DCO is accessible to users through the same platform environment as the other CYberSynchrony components. It also means that response guidance is not hidden in backend systems or separate documentation. It is displayed directly next to the alert evidence.

3.5.5 Integration with CSPA

CSPA is one of the most important integration points for DCO because it provides posture-oriented defensive context. CSPA ingests a JSON inventory containing hardware, applications, services, and optional host metadata. It resolves each asset to a normalised CPE identifier and maps it to MITRE D3FEND digital artifacts, MITRE ATT&CK techniques, detection strategies, and mitigations.

The value of CSPA for DCO is that it explains what the organisation is defending. Wazuh can show that something happened. DCO can show how to respond. CSPA can add context about the asset itself, the digital artifact involved, the relevant D3FEND concepts, and the defensive strategies that apply to that artifact.

For example, if DCO receives an alert mapped to a technique involving remote services, CSPA can help identify whether the affected host contains SSH, RDP, or another exposed service. It can then provide D3FEND mappings and mitigation suggestions such as network segmentation, multi-factor authentication, or monitoring of remote service activity. This makes the DCO playbook more precise because it is not only technique-based but also asset-aware.

CSPA can enrich DCO in several ways:

- Asset-specific response: DCO can adapt playbook guidance according to the actual hardware, software, and services present on the affected host.
- D3FEND-based defensive mapping: DCO can include defensive concepts and countermeasures linked to the relevant digital artifacts.
- Detection improvement: DCO playbooks can include more precise detection logic based on the CSPA detection strategies.
- Mitigation improvement: DCO playbooks can include mitigation actions derived from CSPA's D3FEND and ATT&CK mappings.
- Post-incident hardening: After the immediate response, CSPA can support longer-term remediation by identifying which defensive controls should be improved.

© CYberSynchorny, 2024

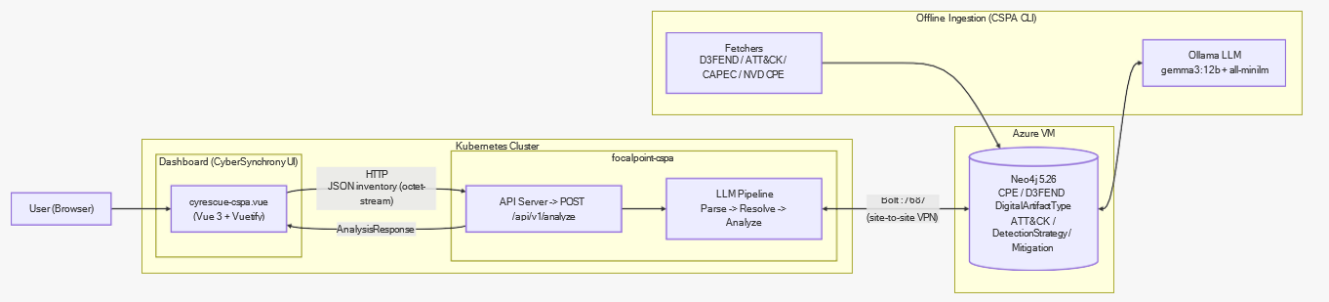

Table 7: : CSPA posture-assessment flow and its relation to DCO enrichment. The figure should show how inventory data is processed by CSPA and mapped to CPE, D3FEND, ATT&CK, detection strategies, and mitigations.

This integration is important because it connects two perspectives. DCO is incident-response oriented, while CSPA is posture-oriented. When combined, they support both immediate response and longer-term defensive improvement. This is aligned with the CYberSynchrony objective of harmonising people, processes, and technology: analysts receive better guidance, response processes become more context-aware, and the platform connects multiple technical modules into a unified workflow.

3.5.6 Integration with ASA

ASA provides vulnerability and exposure information. It resolves assets to CPE identifiers and correlates them with vulnerability data such as CVEs and CWEs. This can support DCO by helping analysts understand whether an alert affects an asset with known vulnerabilities.

For example, when DCO receives an alert for a particular system, ASA information can help answer whether the system runs vulnerable software, whether the affected component is associated with critical CVEs, and whether remediation should include patching or compensating controls.

This creates a risk-informed response process. DCO handles the operational response, while ASA contributes exposure intelligence. In practice, this means that the same type of alert can be prioritised differently depending on whether the affected asset is exposed, outdated, or linked to known high-severity vulnerabilities.

3.5.7 Integration with PTA

PTA provides validation information. It supports structured assessment of detection and response capabilities through ATT&CK-mapped exercises and outcome recording. PTA can show whether a technique was prevented, alerted, logged, or missed.

This information can be used to improve DCO playbooks. If PTA results show that a technique is frequently missed or only partially detected, the related DCO playbook can be revised. If a detection works but the response is weak, the playbook can be enriched with clearer containment and recovery steps.

PTA therefore supports continuous improvement of DCO by providing feedback from controlled defensive assessment activities. This closes the loop between response design and response validation.

3.5.8 Kubernetes deployment

DCO is deployable in Kubernetes through the focalpoint-dco application. Deployment requires:

- a running Kubernetes cluster,
- kubectl configured to communicate with the cluster,

© CYberSynchorny, 2024

- access to the GitLab Container Registry where the focalpoint-dco image is hosted,
- updated ConfigMap values for Wazuh endpoints,
- updated Secrets for Wazuh and Neo4j credentials,
- a registry secret to pull the private image.

Configuration element	Purpose
APP_WAZUH_INDEXER_URL	Defines the endpoint of Wazuh Indexer.
APP_WAZUH_MANAGER_URL	Defines the endpoint of Wazuh Manager.
WAZUH_INDEXER_USERNAME	Username for Wazuh Indexer authentication.
WAZUH_INDEXER_PASSWORD	Password for Wazuh Indexer authentication.
WAZUH_MANAGER_USERNAME	Username for Wazuh Manager authentication.
WAZUH_MANAGER_PASSWORD	Password for Wazuh Manager authentication.
NEO4J_URI	Neo4j database URI.
NEO4J_USERNAME	Neo4j username.
NEO4J_PASSWORD	Neo4j password.
gitlab-registry secret	Allows the Kubernetes cluster to pull the private focalpoint-dco image.

Table 8: Deployment configuration elements

The manifests should be applied in the following order:

1. k8s/configmap.yaml 2. k8s/secrets.yaml 3. k8s/dco.yaml 4. k8s/service.yaml 5. k8s/networkpolicy.yaml

After deployment, the pod status can be verified with:

```
kubectl get pods -l app=focalpoint-dco
```

Application logs can be inspected with:

```
kubectl logs deployment/focalpoint-dco -f
```

The service is configured as a hardened ClusterIP and restricted by NetworkPolicy on port 8443. This means that, by default, it is only accessible from within the cluster. For debugging, port-forwarding may be used:

```
kubectl port-forward svc/focalpoint-dco 8443:8443
```

Then the API documentation can be accessed locally through:

https://localhost:8443/docs

For production access, an Ingress resource or LoadBalancer may be configured depending on the cloud provider and deployment requirements. TLS termination and access control must be handled according to the security policy of the deployment environment.

© CYberSynchorny, 2024

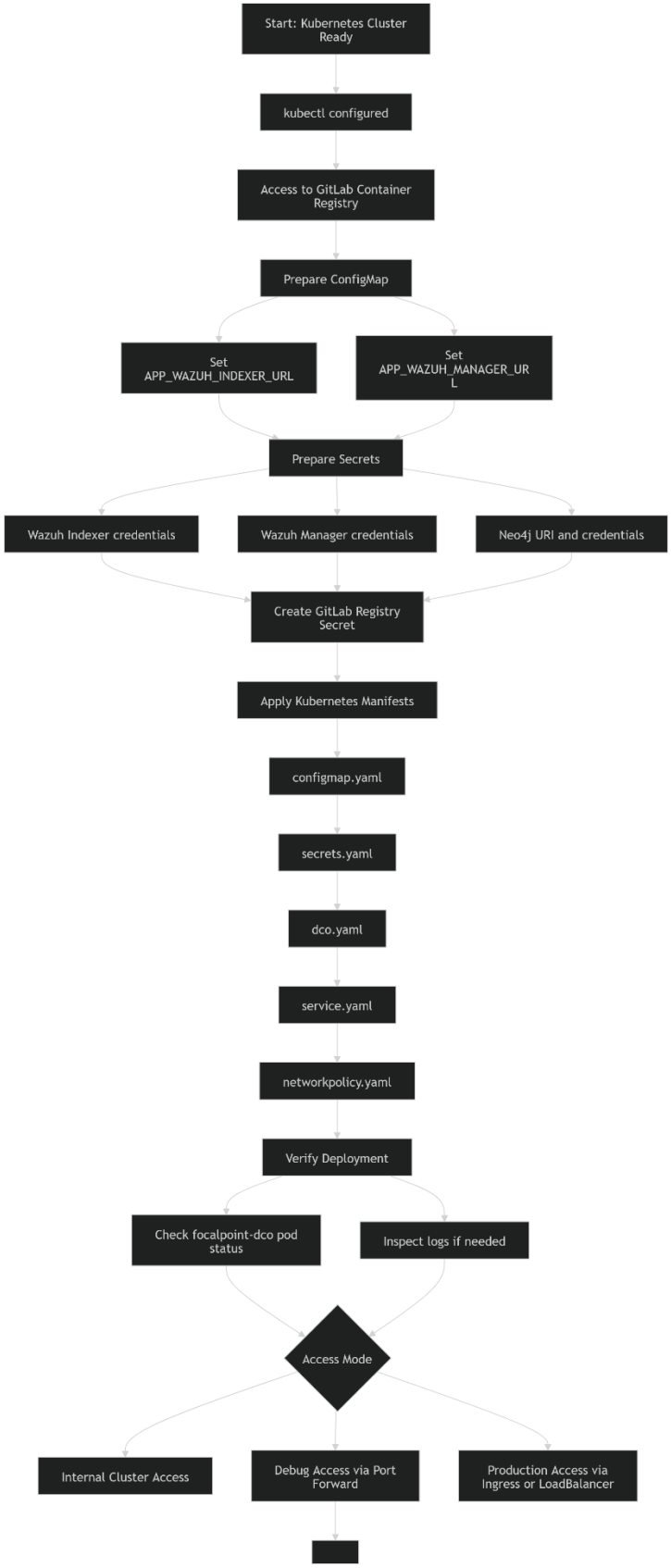

Figure 4: Kubernetes deployment positioning of focalpoint-dco. The figure should show the GitLab registry secret, ConfigMap, Secrets, DCO deployment, ClusterIP service, and NetworkPolicy

© CYberSynchorny, 2024

4 Connection of the Integrated DCO Framework with KPI1.6 Measurement

The integrated DCO framework described in the previous chapters provides the operational basis for measuring KPI1.6 during the pilot validation activities. The KPI is not treated as an isolated reporting exercise, but as a direct outcome of the platform workflow connecting threat intelligence, alert validation, response guidance, and evidence preservation.

Within the integrated CYberSynchrony environment, the pilots provide the operational context in which simulated or real security incidents can be observed. The Threat Intelligence Platform, including MISP, contributes the enrichment and classification layer by providing IoCs, threat context, tags, CVEs, and zero-day-type indicators where relevant. This information supports the interpretation of the detected event and helps distinguish between zero-day-type scenarios and other threats.

The DCO component, described in the previous chapters as the response-oriented layer of the platform, provides the main link between detection and response. Alerts or validated incident signals are connected with DCO playbooks, which generate or select the appropriate response workflow. Therefore, the DCO integration becomes the practical point where the platform demonstrates that a detected incident has moved into an actionable response process.

The integration with the wider platform also supports the quality of the KPI evidence. Where relevant, tools from the CyberSynchrony platform like MISP will provide additional context while all of theam can support validation of response effectiveness through structured assessment results. These components do not replace the KPI measurement process, but they enrich the interpretation of incidents and help ensure that the response is linked to the actual risk and technical context of the pilot environment.

In this way, the current value of KPI1.6 will be derived from the response performance observed during pilot activities using the integrated workflow described in this deliverable. The target value will be assessed against the expected response thresholds defined for the KPI. The secure exchange / integrity layer can then support the traceability of the evidence generated across the workflow, ensuring that the reported KPI values are linked to verifiable platform outputs rather than manual declarations alone.

© CYberSynchorny, 2024

5 Conclusions

D4.4 presents the advanced version of the Automated Response Toolkit developed in CYberSynchrony, focusing on the Defensive Cyber Operations tool. The deliverable demonstrates the evolution from the initial playbook and SIEM/SOAR concepts of D4.2 to a concrete, integrated, scalable, and deployable DCO capability.

The main improvement of D4.4 is the expansion of playbook coverage. The v1 toolkit included a limited number of representative playbooks, approximately ten, mainly to demonstrate the methodology. The advanced version introduces an LLM-assisted playbook-generation pipeline connected with Wazuh and Neo4j, enabling the generation and management of more than 1,000 playbooks. This allows DCO to cover almost all cases that can be extracted from Wazuh and mapped to MITRE ATT&CK techniques.

DCO contributes to the CYberSynchrony objective of improving preparedness, rapid response, and cybersecurity resilience. It enables analysts to move from Wazuh alerts to MITRE ATT&CK-mapped incidents and from incidents to structured defensive playbooks. By combining detection evidence, graph-based knowledge, and LLM-assisted playbook generation, DCO provides a practical mechanism for improving response consistency and reducing manual effort.

The advanced toolkit also strengthens platform interoperability. It is integrated with the CyberSynchrony dashboard and can interact with CSPA, ASA, and PTA. CSPA contributes posture and defensive-mapping context. ASA contributes vulnerability and exposure context. PTA contributes validation evidence. Together, these integrations support an end-to-end risk-to-response workflow.

The deployment model further demonstrates the operational maturity of the tool. focalpoint-dco can be deployed into Kubernetes using ConfigMaps, Secrets, service definitions, NetworkPolicies, and GitLab registry authentication. This makes the component suitable for controlled staging and production environments.

Overall, D4.4 confirms that the Automated Response Toolkit has matured into a central operational capability for CYberSynchrony. DCO provides the platform with a structured response layer that connects people, processes, and technology: people through analyst guidance, processes through repeatable playbooks, and technology through integrated Wazuh, Neo4j, LLM, dashboard, CSPA, ASA, PTA, and Kubernetes components.

© CYberSynchorny, 2024

6 KPIs Mapping

KPI ID	KPI Name	Owner
KPI1.6	Threat Intelligence Platform Security Incident Response Time	MAG
Target		
Reduce response time to 4 hours for zero-day-type threats and 8 hours for other threats, compared to the previous year.		
Measurement Methodology		
Components involved	**Participating partners & Role in KPI Measurement**	**Evidence collection process & validation approach**
Threat Intelligence Platform – MISP - DCO-Playbooks - secure exchange integrity layer - Incident Response Register.	IANUS will support incident enrichment and classification through MISP, including IoCs, tags, CVEs, threat context and zero-day-type indicators. FP will support the response workflow through DCO Playbooks, including playbook generation or selection. BYTE will support evidence integrity through the secure exchange integrity layer. MAG will coordinate KPI ownership, monitoring and reporting.	Evidence will be collected through an Incident Response Register in Excel. Each row will represent one simulated or real platform security incident. Evidence may include MISP event/export, IoC analysis, Wazuh or DCO alert ID, DCO playbook output, analyst acknowledgement, escalation note, containment recommendation, screenshot, report, or integrity/hash reference from the secure exchange layer. Evidence will be considered valid when detection time, response start time, responsible partner, tool involved and evidence link are recorded.
Methodology Description		
KPI1.6 will be measured by recording the time between incident detection and the first documented response action. Response time is calculated as: Response Time = Response Start Time − Detection Time. The response start time may be analyst acknowledgement, escalation, containment recommendation, or DCO playbook generation/selection. Results will be reported separately for zero-day-type incidents against the 4-hour target and other threats against the 8-hour target. The KPI will be measured using simulated Threat Intelligence Platform security incidents, or real incidents if they occur.		
KPI Progress Status		
Current Value/Target	**Date of Measurement**	**Status**	**Next Actions** (if required)
Current Value : measured without the use of CS platform./Target: ≤4h for zero-day-	To be populated after execution of simulated or real platform security incident scenarios.	ON Track	Prepare the Incident Response Register, define simulated Threat Intelligence Platform security incident scenarios, agree evidence fields with IANUS, FP, BYTE and MAG, execute the first

© CYberSynchorny, 2024

type incidents and ≤8h for other threats.			measurement scenarios, and record response-time results.
Challenges, Deviations and Corrective Actions			
It will be addressed through simulated platform security incidents, or real incidents through pilot use cases and tests. If no real incident occurs during the reporting period, controlled simulations will be used(before and after the use of the CyberSynchrony platform).			

© CYberSynchorny, 2024