



*Establishment of a FramewORk for Transforming current
EPES into a more resilient, reliable and secure system all
over its value chain*

D3.3 Reporting actions for IDS-SIEM and blockchain developments



Document details

Deliverable no	D3.3
Deliverable name	Reporting actions for IDS-SIEM and blockchain developments
Version	0.3
Release date	30/05/2025
Type	R
Dissemination level	SEN
Status	Final version (Draft / Final version)
Author	CIRCE – Esteban Gutierrez, Rafael Camarero CERTH – Giorgos Rizos, Paschalis Gkaidatzis, Nikolaos Tarsounas, Aris Mystakeidis, Anagnostis Mengidis, Dimosthenis Ioannidis TNO – Frank Fransen, Luca Morgese, Maarten de Kruijf, Reinder Wolthuis LINKS – Alessandro Mozzato, Fabio Caffaro, Xileny Seijas Portocarrero



DISCLAIMER OF WARRANTIES

This document has been prepared by eFORT project partners as an account of work carried out within the framework of the EC-GA contract no. 101075665.

Neither Project Coordinator, nor any signatory party of eFORT Project Consortium Agreement, nor any person acting on behalf of any of them:

- a) makes any warranty or representation whatsoever, expressed or implied,
 - I. with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or
 - II. that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or
 - III. that this document is suitable to any particular user's circumstance; or
- b) assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if the Project Coordinator or any representative of a signatory party of the eFORT Project Consortium Agreement has been informed of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

This work has been Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.



Document history

Version	Date of issue	Content and changes	Edited by
0.1	16/05/2025	First draft version	CIRCE
0.2	22/05/2025	Reviewed version	LINKS
0.3	29/05/2025	Final version	CIRCE



List of figures

Figure 1 Substation architecture	20
Figure 2 Testbeds used to generate attack traces	23
Figure 3: Operational Technology (OT) devices categories and types.	28
Figure 4: Data analysers layers	29
Figure 5: eFORT Pilots demonstrators, high level use case diagram	31
Figure 6: eSIEM monitor and control workflow diagram	33
Figure 7: eSIEM deployment diagram	35
Figure 8: eSIEM high-level component diagram.....	36
Figure 9: eSIEM Technology stack	38
Figure 10 - A-Bot's Use Cases.....	40
Figure 11 - A-Bot's first mock-up.....	40
Figure 12 - A-Bot's architecture.....	41
Figure 13 - Example of a tool called node_status that retrieves the voltage magnitude of a node of the electrical grid given its name	43
Figure 14 - A-Bot Alert messages	45
Figure 15 - A-Bot Notification API	45
Figure 16 - Example of interaction with the Intelligent Chatbot. The Intelligent Service v0 maps the user query to the most relevant backend function and reports directly the results providing limited conversational interaction capabilities.	46
Figure 17 - Interaction with A-Bot (Int. Serv. v1). User asks, in Italian, What is the status of node BELMONTE? A-Bot responds in Italian, that node BELMONTE has a vm_pu value of 0.99 and that this value indicates the node is in a safe state ($0.95 < vm_pu < 1.05$)	47
Figure 18 - Conversation with A-Bot v3. The user asks, "Which lines are connected to node BELMONTE?". A-Bot lists the connected lines, including their tags and bus IDs. In a follow-up, the user asks about the status of the connected lines. A-Bot responds with detailed information for each line, showing line IDs, tags, and load percentages and concludes that both lines are in a safe state, as their load percentages are well below the 50% limit.	47
Figure 19 - Supply Chain Channel Architecture	56
Figure 20 - Communication between components	59
Figure 21 - Authentication sequence diagram.....	59
Figure 22 - Supply Chain Data Model	61
Figure 23 Stability channel Architecture.....	64
Figure 24 - CISA Shareable SOAR Playbook: Detect – Process Internal FW Alert. Source CISA's github ⁵	68



Figure 25 - The visualization of a CACAO playbooks encoding CISA’s “Detect – Process Internal FW Alert playbook”, visualized on the Cymph platform.	70
Figure 26 - Conceptual overview of SOARCA.....	71
Figure 27 - Core component overview of SOARCA and integration with other tools ...	73
Figure 28 - Simplified overview of the internal flow between SOARCA components. ..	74
<i>Figure 29 - Reference Architecture for Electric Energy OT from SEI ETF (Martin, Chanoski, Granda, Kunsman, & Sachs, April 2022).</i>	<i>76</i>
Figure 30 - Initial reference architecture for EPES SOC enclaves.....	77
Figure 31. Conceptual distinction between the preventive and reactive actions.	79
Figure 32. Vulnerability response process for newly reported software vulnerabilities.	80
Figure 33. Incident response process with focus on containment step.....	82



List of tables

Table 1 Comparison of different machine learning models evaluating IEC104 on our dataset. The best results for each metric have been highlighted in bold with an orange background..... 25

Table 2 Comparison of different machine learning models evaluating IEC61850 on our dataset. The best results for each metric have been highlighted in bold with an orange background..... 26

Table 3: eSIEM Engine technology stack..... 37



Abbreviations and Acronyms

Acronym	Description
AI	Artificial Intelligence
API	Application Programming Interface
AUC	Area Under the Curve (a performance metric for classification models)
CACAO	Collaborative Automated Course of Action Operations (an OASIS Open standard for machine-readable security playbooks)
CISA	Cybersecurity and Infrastructure Security Agency (the U.S. federal agency responsible for cybersecurity and infrastructure protection)
CSV	Comma-Separated Values (a simple text format for tabular data)
CVSS	Common Vulnerability Scoring System (standard framework to rate severity of software vulnerabilities)
DLT	Distributed Ledger Technology (a decentralized database architecture, e.g. blockchain)
DSO	Distribution System Operator (entity that operates and maintains the power-distribution network)
EDR	Endpoint Detection and Response (security tools focused on monitoring and responding to threats on endpoints)
ENISA	European Union Agency for Cybersecurity
EPES	Electrical Power and Energy Systems
F1	F1 score (the harmonic mean of precision and recall in classification tasks)
HIDS	Host-based Intrusion Detection System (monitors and analyzes the internals of a host for signs of compromise)
HMI	Human-Machine Interface (the user interface to an automated or control system)
IDS	Intrusion Detection System (monitors network traffic and/or system activity for signs of intrusion)
IEC	International Electrotechnical Commission (body that publishes international electrical and electronic standards)
LLM	Large Language Model (a neural network trained on very large text corpora)
MCC	Motor Control Center (an assembly to control and protect electric motors)



Acronym	Description
MSP	Membership Service Provider (in Hyperledger Fabric, defines rules for identity validation and access)
MUI	Material Material UI (a React component library implementing Google's Material Design)
NIDS	Network-based Intrusion Detection System (an IDS that monitors and analyzes network traffic)
PLC	Programmable Logic Controller (an industrial computer for automation of electromechanical processes)
REST	Representational State Transfer (an architectural style for designing networked applications)
SCADA	Supervisory Control and Data Acquisition (industrial control system architecture)
SIEM	Security Information and Event Management (tools for real-time analysis of security alerts)
SOAR	Security Orchestration, Automation and Response (platforms that automate and orchestrate security workflows)
SOC	Security Operation Centre (facility for monitoring, detecting, and responding to security incidents)
SSH	Secure Shell (protocol for secure remote login and other secure network services)
SQL	Structured Query Language (standard language for managing relational databases)
SVM	Support Vector Machine (a supervised machine-learning algorithm)
TSO	Transmission System Operator (entity responsible for bulk-power transmission)



Contents

Contents	10
1 Executive Summary	14
2 Introduction	15
2.1 Background and Context	15
2.2 Vision / architecture	15
2.2.1 IDS – SIEM – SOAR	15
2.2.2 Blockchain	16
2.2.3 Chatbot	16
2.2.4 Integration and Deployment	16
2.3 Structure of the Deliverable	17
3 Intrusion Detection System (IDS)	18
3.1 Substation Structure	19
3.1.1 Station Level	19
3.1.2 Bay Level	19
3.1.3 Process Level	19
3.2 Substations Communication Protocols	20
3.2.1 IEC61850	20
3.2.2 IEC104	20
3.3 Overview of IDS Development	21
3.3.1 Step 1: Collecting a Proper Dataset	21
3.3.2 Step 2: Testing and Selecting the Most Suitable Algorithm	21
3.3.3 Step 3: Adapting the Algorithm for Real-Time Data Ingestion	21
3.4 Algorithm training and Datasets	22
3.4.1 Real Substation Traces	22
3.4.2 Testbed Traces for Attack Simulation	22
3.4.3 Preprocessing and Feature Extraction	23
3.4.4 Software Functionalities and Methodological Contributions	24
3.5 Machine Learning Algorithms for IDS	24
3.6 Real time ingestion of data	26



4	Security Information and Event Management (SIEM)	28
4.1	eSIEM	28
	4.1.1 SIEM Overview	28
	4.1.2 SIEM in Power Grid	29
	4.1.3 Our contribution	30
4.2	Information Gathering within agents in Power GridOT & IT Infrastructures	30
4.3	eSIEM Architecture	32
4.4	Submodules and Extensions	34
	4.4.1 Trust Management System	34
	4.4.2 Fast Mitigation System	34
4.5	Deployment Options	35
	4.5.1 Integration with visualization tool and hypothesis tool	36
	4.5.2 Technology Stack	37
5	Intelligent Chatbot.....	39
5.1	Design & User Interaction	39
	5.1.1 Objectives	39
	5.1.2 Use Case Scenarios	39
	5.1.3 Functional Requirements	40
	5.1.4 User Interface Mock-up	40
5.2	Overview of Chatbot Development	41
	5.2.1 Overview	41
	5.2.2 Purpose & Scope	41
5.3	System Architecture	41
	5.3.1 High-Level Overview	41
	5.3.2 Intelligent Service Integration	42
	5.3.3 Alert Mechanism	44
5.4	Core Functionalities	45
	5.4.1 Answering Grid Status Queries	45
	5.4.2 Real-time Alert Notification	48
5.5	Technical Implementation	49
	5.5.1 Frontend, Backend & Service Technologies	49
	5.5.2 API Integration & Data Handling	50



6	Grid Verification and Monitoring Layer by Blockchain Technology	52
6.1	Introduction	52
6.2	Overview of blockchain solutions	52
	6.2.1 Fundamentals of blockchain technology	52
	6.2.2 Benefits	52
6.3	Hyperledger fabric	53
	6.3.1 Peer nodes and identities	53
	6.3.2 Ordering service & orderers	53
	6.3.3 Certificate Authority	53
	6.3.4 Membership service providers (MSP)	53
	6.3.5 Channels	54
	6.3.6 Smart contracts	54
	6.3.7 Consensus mechanisms	54
6.4	Supply chain channel	54
	6.4.1 Purpose and objectives	55
	6.4.2 System architecture	56
	6.4.3 Security considerations	59
	6.4.4 Operational processes	61
6.5	Stability channel	61
	6.5.1 Purpose and objectives	61
	6.5.2 System Architecture	63
	6.5.3 Security considerations	65
	6.5.4 Operational processes	66
7	Reactive and Preventive Actions Issued to the Infrastructure.....	67
7.1	Introduction	67
7.2	CACAO playbooks	68
7.3	SOARCA	71
	7.3.1 Introduction	71
	7.3.2 Design	72
	7.3.3 Main application flow	73
	7.3.4 Considerations	74
7.4	EPES Security Operation Centre	75
7.5	Reactive & preventive cybersecurity actions in EPES environments	77



7.5.1 Vulnerability response process and preventive actions	79
7.5.2 Incident response process and reactive actions	81
8 Bibliography	83



1 Executive Summary

The eFORT deliverable presents a comprehensive, modular framework designed to enhance the cybersecurity, resilience, and operational transparency of electric power and energy systems (EPES). Building on the core requirements of real-time intrusion detection, event correlation, automated response, secure data sharing, and intuitive operator support, this document details the design and implementation of five tightly integrated components: a machine-learning-driven Intrusion Detection System (IDS); a rules-based Security Information and Event Management (SIEM) platform; a SOARCA automation engine powered by CACAO playbooks; a permissioned blockchain layer for immutable record-keeping and secure market transactions; and an Intelligent Chatbot interface underpinned by a large language model. Each component addresses specific attack surfaces and operational workflows, ensuring end-to-end protection from cyber threats, detailed traceability through blockchain records of maintenance and market activities, and streamlined human-machine interaction.

Chapters 3-7 elaborate on the architecture and implementation of these tools. Chapter 3 covers IDS algorithm selection, dataset curation, and integration into control-centre networks; Chapter 4 specifies the SIEM's logging infrastructure, event-correlation rules, and alerting pipelines; Chapter 5 describes the Intelligent Chatbot's conversational design, context-aware LLM integration, and notification services; Chapter 6 introduces the dual-channel blockchain layer-supporting both supply-chain provenance and battery-based energy-resiliency market transactions-and outlines smart-contract governance; and Chapter 7 details reactive and preventative cybersecurity workflows via CACAO playbooks and the SOARCA engine, culminating in the EPES SOC deployment model. Together, these elements form a unified security fabric that can detect, analyze, and remediate incidents while maintaining full auditability.

Collectively, this deliverable validates the eFORT framework's readiness for real-world EPES integration and lays the groundwork for broader adoption across the electric-grid sector.

