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

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

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

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

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

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

List of figures

This project has received funding from the European Union’s Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

List of tables

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

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)

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

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)

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Contents

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

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.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.