



Cybersecurity Intelligence,
Protection, and Holistic
Enterprise Resilience

Annex 2 – Technical Requirements

Open Call 1

Nov 2026



Funded by
the European Union

Funded by the European Union's Digital Europe Programme under Grant Agreement No101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

Disclaimer

The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

Copyright Notice

© CIPHER

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732.

Contents

Technical Requirements	3
Knowledge	4
K1 — Regulatory capability gap assessment	4
K2 — Pentest methodology & T4.3 gap assessment	5
Testing	7
T1 — Vulnerability management validation	7
T2 — CIPHER XDR onboarding & data-collection validation	9
Range / Environment	11
R1 — Domain cyber-range contribution.....	11
P1 — DevSecOps & platform automation.....	13
Acronyms & terms	15

Technical Requirements

OC#1 is organised into contribution modes reflecting a capability lifecycle — **Knowledge** (identify gaps), **Development** (fill them), **Testing** (validate) — plus a **Range / Environment** mode that broadens the comparison baseline against which CIPHER forms its recommendations. Each mode targets a distinct applicant profile.

Development is carried by consortium partners during OC#1 and is deferred to OC#2; it is not opened to third parties in this call. OC#1 therefore opens five challenges across the Knowledge, Testing and Range / Environment modes:

- **Knowledge — K1:** Regulatory capability gap assessment (NIS2 auditor profile)
- **Knowledge — K2:** Pentest methodology & project gap assessment (offensive / OT profile)
- **Testing — T1:** Vulnerability management validation
- **Testing — T2:** CIPHER XDR onboarding & data-collection validation
- **Range / Environment — R1:** Domain cyber-range contribution
- **Platform / Enablement — P1:** DevSecOps & platform automation

Conventions common to all challenges. Eligible sectors are NIS2 Annex I/II, with OT prioritised. CIPHER owns all challenge outputs; applicants retain their pre-existing IP — the exception is R1, where a contributed range stays the applicant's property under a licence to CIPHER. All active techniques run only in the CIPHER cyber range, except where a challenge explicitly defines an applicant-environment scope that is governed separately. Programme phases, timeframe, budget ceiling and reporting are defined in the Annex 1 – Guide for Applicants and are not covered in this document.

Knowledge

K1 — Regulatory capability gap assessment

Challenge	<i>A certified NIS2 auditor assesses CIPHER's toolset against the Article 21(2) risk-management measures (OT-prioritised sectors), maps where the platform does and does not support each obligation and identifies prioritised gaps that scope of next project phases. Documentation only — no active testing. Output is owned by CIPHER.</i>
Expected applicant profile	Certified auditor (e.g. ISO 27001 Lead Auditor / IEC 62443 assessor) with demonstrable NIS2 compliance-assessment experience in critical sectors.
Objectives	(a) Map CIPHER capabilities against NIS2 Article 21(2)(a)–(j) and relevant IEC 62443 requirements; (b) identify and severity-rate compliance-coverage gaps; (c) translate gaps into scopeable next project phase requirement statements.
Scenario description	The auditor reviews CIPHER architecture and toolset inventory, assesses coverage of each Article 21(2) measure for an OT / critical-infrastructure operator, and flags obligations the platform leaves uncovered or partially covered. Applicants may propose an additional NIS2 Annex I/II sector focus.
Tool(s) / architecture	CIPHER provides: architecture documentation, toolset inventory, descriptions of compliance-relevant workflows, and sanitised sample outputs (read-only; no credentials, no range or live access). Applicant brings: their own audit framework and checklists as reference. No deployment, no integration.
Assessment scope — KPIs	1. Regulatory coverage — 100% of in-scope Article 21(2) measures assessed. 2. Gaps identified — count of distinct, severity-rated coverage gaps. 3. Actionability — each high/medium gap maps to at least one CIPHER next phase requirement. 4. Traceability — % of findings mapped to a specific Article 21(2) / IEC 62443 clause and CIPHER component.
Environment	Desk / documentation review; optional read-only walkthrough. No active testing against CIPHER infrastructure.
Requirements (HW/SW/data)	From CIPHER: documentation, architecture diagrams, toolset inventory, sanitised samples. From applicant: own audit tooling. No CIPHER compute provisioning.
Data provisions	Architecture documentation and toolset inventory (sanitised), under NDA. No real client or personal data.

Minimum deliverable framework	(1) Capability-vs-Article 21(2) coverage matrix; (2) severity-rated gap analysis; (3) CIPHER next phase requirement recommendations. Negative findings (areas with no gap) documented with rationale. Delivered to an agreed template.
Compliance boundaries	NDA on CIPHER internals; GDPR — no personal or sensitive data in any example or deliverable.
IP ownership	CIPHER owns outputs. Applicant retains pre-existing frameworks and checklists.
Consortium requirements	The overall selection should ensure access to independent and demonstrable expertise in NIS2 compliance assessment across critical sectors, with appropriate coverage of OT and critical-infrastructure environments. Applicants must be able to apply a structured and traceable audit methodology covering all in-scope NIS2 Article 21(2) measures and relevant IEC 62443 requirements. They must also be capable of translating identified compliance-coverage gaps into clear, prioritised and actionable requirements for next project phases. Where multiple applicants are selected, complementarity across NIS2 Annex I and Annex II sectors, regulatory perspectives and technical domains should be considered, while avoiding unnecessary duplication of sectoral coverage.

K2 — Pentest methodology & T4.3 gap assessment

Challenge	<i>An OT / critical-infrastructure offensive-security expert documents a best-practice identify-and-validate pentest methodology (EU-regulation-aware) and benchmarks CIPHER's activities automated pentesting against it, identifying prioritised technical gaps that scope next project phase. Documentation only — no active testing against CIPHER. Output is owned by CIPHER.</i>
Expected applicant profile	Offensive-security specialist with ICS / OT pentest experience (e.g. GICSP / OSCP-class, documented critical-infrastructure engagements).
Objectives	(a) Document a repeatable methodology — process, tools, techniques — for the pre-exploitation kill chain through safe validation of exploitable vulnerabilities in OT / critical infrastructure (exploitation confined to a controlled range); (b) benchmark CIPHER activity's current coverage against it; (c) severity-rate technical gaps and translate them into next project phase requirement statements; map the methodology to NIS2 Article 21(2)(e)/(f) and IEC 62443-3-3 / 4-2.
Scenario description	The expert documents reconnaissance → enumeration → vulnerability analysis → safe validation for an OT target class, then project gaps against

	it (technique coverage, automation, safe-execution controls, false-positive handling). Applicants may propose an additional OT / critical-infrastructure target class.
Tool(s) / architecture	CIPHER provides: CIPHER toolset inventory and current scope, architecture documentation, and sanitised sample findings (read-only; no credentials, no range or live access). Applicant brings: the tools and techniques their methodology relies on, as reference knowledge — not for deployment. Known limitations: CIPHER discloses project scope so effort targets gaps and may withhold its own gap hypotheses for independent validation.
Assessment scope — KPIs	1. Methodology completeness — covers process, tooling, techniques, and critical-infrastructure safe-execution constraints (checklist). 2. Technique coverage — breadth of documented techniques across the pre-exploitation and safe-validation phases. 3. T4.3 gaps identified — count of distinct, severity-rated technical gaps. 4. Actionability — each high/medium gap maps to at least one CIPHER next phase requirement. 5. Traceability — % of methodology elements mapped to a NIS2 / IEC 62443 clause.
Environment	Desk review of CIPHER documentation and samples; any methodology demonstration runs in the applicant's own lab. No active testing against CIPHER infrastructure.
Requirements (HW/SW/data)	From CIPHER: CIPHER inventory, architecture documentation, sanitised sample findings. From applicant: own lab and tooling for any demonstration. No CIPHER compute provisioning.
Data provisions	CIPHER tool inventory and configurations plus synthetic sample findings (sanitised), under NDA. No real client or personal data.
Minimum deliverable framework	(1) Documented methodology (process + tool inventory + techniques + critical-infrastructure safe-execution constraints); (2) regulatory mapping; (3) severity-rated project gap analysis; (4) CIPHER next phase requirement recommendations. Negative findings documented with rationale. Delivered to an agreed template.
Compliance boundaries	NDA on CIPHER internals; GDPR — no personal or sensitive data in any example or deliverable; no live CIPHER or client data handled.
IP ownership	CIPHER owns outputs. Applicant retains pre-existing methodology and knowledge.
Consortium requirements	The overall selection should ensure strong offensive-security and OT penetration-testing expertise, with sufficient coverage of critical-infrastructure target classes and safe-execution constraints. Applicants must be able to document a repeatable methodology covering reconnaissance, enumeration, vulnerability analysis and safe validation of exploitable vulnerabilities. They must also demonstrate the capacity to

benchmark CIPHER capabilities objectively against that methodology and translate identified technical gaps into prioritised and scopeable next project phase requirements.

Where multiple applicants are selected, the portfolio should seek complementary coverage of OT technologies, industrial protocols, target classes and critical-sector environments, while maintaining a consistent basis for comparing methodologies and gap findings.

Testing

T1 — Vulnerability management validation

Challenge	<i>A vulnerability-management practitioner exercises CIPHER's existing VM toolchain end-to-end across three views (SBOM, endpoint, network/host), pushes conformant scan proofs to project storage, validates the ingestion pipeline through to DefectDojo, and reports performance and integration friction. Active scanning runs only in the cyber range. Output is owned by CIPHER.</i>
Expected applicant profile	VM / security-engineering profile with hands-on experience operating scanners (OpenVAS / Trivy / Nmap / Nuclei-class) and aggregation platforms (DefectDojo / Dependency-Track-class).
Objectives	(a) Run the CIPHER baseline toolset against range targets across all three views; (b) push each scan as a reproducible bundle to WORM storage; (c) verify pipeline pickup from storage → Dependency-Track (SBOM) → DefectDojo aggregation and deduplication; (d) measure pipeline performance and surface integration friction; (e) map findings to NIS2 Article 21(2)(f) and CRA vulnerability-handling / SBOM obligations.
Scenario description	Sub-flows against range assets — SBOM / artifact (Trivy, two modes): (i) SBOM generation → storage → Dependency-Track → DefectDojo, (ii) vulnerability scan → storage → DefectDojo; Endpoint: Wazuh agents → internal pipeline → DefectDojo; Network/host: OpenVAS / Nmap / Nuclei → storage → DefectDojo. Applicants may propose additional NIS2 Annex I/II target classes (OT-prioritised).
Tool(s) / architecture	CIPHER provides: baseline scanners (OpenVAS, Aqua Trivy, Nmap, Wazuh agents, Nuclei / ProjectDiscovery), the range targets, the S3-

	compatible WORM storage bucket, the ingestion pipelines, Dependency-Track and DefectDojo. Applicant operates the scanners and validates the chain and may propose additional scanners provided outputs are pipeline-conformant. Integration touchpoints: storage push (S3 API), pipeline pickup, Dependency-Track ingest, DefectDojo import and deduplication. Accesses: dedicated range and scoped storage-bucket credentials — never live or production. Trivy runs in two modes: vulnerability scanner (→ storage → DefectDojo) and SBOM generator (→ storage → Dependency-Track → DefectDojo). All outputs, SBOM included land in WORM storage first as evidence; pipelines pick them up from there.
Testing scope — KPIs	1. Parse / ingestion success — % of pushed reports ingested to DefectDojo without manual fixup (spine metric; propose target). 2. Deduplication accuracy — the same vulnerability across scanners is merged, not double-counted. 3. Coverage — % of range assets scanned across all three views. 4. False-positive rate of surfaced findings. 5. Pipeline latency — scan-push to visible-in-DefectDojo. 6. Proof reproducibility — % of findings re-derivable from stored bundles (manifest and hash complete).
Testing environment	Cyber-range replica only; production-like OT and IT assets. OT-safe scan profiles mandatory. No live or production targets. Clean range per engagement; storage bucket scoped per engagement.
Requirements (HW/SW/data)	From CIPHER: range compute, baseline toolset, WORM storage, Dependency-Track and DefectDojo instances, scoped credentials. From applicant: scan expertise; any proposed additional scanner must emit a DefectDojo-parseable format.
Data provisions	Range targets (synthetic / emulated assets), deliberately vulnerable images and components for the SBOM flow, and synthetic endpoint telemetry. Under NDA. No real client or personal data.
Minimum testing framework	Run all three views; push each scan as native + normalized + JSON manifest (hashed) to WORM storage; confirm ingestion through to DefectDojo; document latency, false-positive, deduplication and friction results; provide regulatory mapping. Failure recovery: on pipeline or platform failure, proofs replay from storage — demonstrate at least one replay. Delivered to an agreed template.
Compliance boundaries	NDA on CIPHER internals; GDPR — no personal or sensitive data in targets or reports; findings / CVEs permissible; all active work confined to the range.

IP ownership	CIPHER owns outputs (scan proofs, bundles, performance reports). Applicant retains any pre-existing supplementary tooling or methodology.
Consortium requirements	The overall selection should seek coverage of multiple NIS2 critical-sector environments and a representative variety of IT, OT, endpoint, network, host and software-component contexts.
	Applicants must demonstrate the technical capacity to operate the relevant vulnerability-scanning tools, generate pipeline-conformant outputs and validate the complete evidence chain from scanning and WORM storage through Dependency-Track and DefectDojo. They must also be able to perform all active scanning within an isolated cyber-range environment using OT-safe scanning profiles where applicable. Where multiple applicants are selected, complementarity should be sought across target classes, scanner expertise and vulnerability-management use cases. Proposed supplementary scanners should broaden the assessment while preserving interoperability, reproducibility and comparability with the CIPHER baseline toolchain.

T2 — CIPHER XDR onboarding & data-collection validation

Challenge	<i>A detection / SOC practitioner onboards their environment to CIPHER XDR (Wazuh-based, CIPHER-hosted SaaS) by deploying the full range of agent types and SIEM inputs (EDR + IDS/IPS + OT security appliances), exercises the platform's data-collection and detection capabilities, and reports coverage, fidelity and integration friction. Output is owned by CIPHER. The activity validates whether CIPHER can ingest high-volume cybersecurity events, combine them with infrastructure- and application-level monitoring data, suppress low-impact alerts and generate higher-level risk alerts across organisational, network or geographical domains.</i>
Expected applicant profile Objectives	SOC / detection-engineering profile with Wazuh (or equivalent XDR) and SIEM-integration experience; controls a representative environment including IDS/IPS and/or OT security appliances.
	(a) Deploy agents across diverse host / OS types reporting to the CIPHER XDR SaaS; (b) integrate SIEM inputs from IDS/IPS and OT appliances; (c) exercise the full breadth of agent capabilities (FIM, SCA, inventory, log collection, vulnerability detection, rootcheck, active response) and collect security-event facts; (d) validate detection against known scenarios (range); (e) map to NIS2 Article 21(2)(b) incident handling and (f) effectiveness, and CRA monitoring / reporting obligations; (f) assess performance, integration effort, applicability across critical sectors and opportunities for extending CIPHER with applicant-provided risk-analysis capabilities.

Scenario description	Range (ground truth): Emulated OT / IT assets with injected attack scenarios → agents / inputs → CIPHER XDR, detection validated against known truth. Applicant environment: agents plus IDS/IPS / OT-appliance feeds deployed on a representative segment → CIPHER XDR SaaS. Applicants may propose a sector focus (OT-prioritised). Specifically, the applicant operates in a representative environment containing monitored information systems, endpoints or devices, and one or more existing cybersecurity data sources. The applicant deploys CIPHER tools and configures Wazuh/OpenSearch-compatible data collection Synthetic, real-time or replayed events are combined with infrastructure- and application-level monitoring data according to a CIPHER metric/risk model. The test verifies that relevant events are ingested, distributed processing operates as intended and higher-level risk alerts are generated. Multi-site, multi-network or multi-system scenarios are encouraged. Optionally, the applicant integrates its own risk analyser through the exposed interfaces.
Tool(s) / architecture	CIPHER provides: the XDR SaaS (Wazuh manager / indexer / dashboard), agent packages, pipeline components, and a scoped SaaS tenant with enrolment keys. Applicant deploys agents and configures SIEM inputs in their environment and enrolls them to the SaaS, using their own infrastructure and credentials. Integration touchpoints: agent → manager enrolment and communication (TLS), event and telemetry feeds, syslog / SIEM ingestion from appliances, applicant-side pipeline. Applicants may additionally integrate an open-source or proprietary risk-analysis tool that consumes data exposed through the testing environment and returns risk or alerting indicators to CIPHER XDR. Access conditions: dedicated and isolated credentials, API keys and test access only. Client production credentials and uncontrolled access to live systems are excluded.
Testing scope — KPIs	Agent-capability coverage — number of agent modules exercised vs available (core “leverage all capabilities” metric). Input-source breadth — number and types of SIEM inputs integrated (EDR + IDS/IPS + at least one OT appliance). Onboarding / connectivity success — % of deployed agents and collectors enrolled and reporting. Data-collection fidelity — completeness and correctness of collected events, no silent drops.

Testing environment Requirements (HW/SW/data) Data provisions Minimum testing framework Compliance boundaries IP ownership Consortium requirements	5. Detection coverage — % of injected range scenarios detected (ground truth). 6. MTTD — event-to-alert latency. 7. Each selected testing entity/use case should execute and document at least two distinct threat/risk scenarios or analysis cycles, using injected, replayed, synthetic or suitably controlled real-world data as appropriate. Multi-site, multi-network or multi-system scenarios are encouraged.
	CIPHER-hosted SaaS . Agents / pipelines to be deployed: range — emulated assets, injected scenarios, OT-safe; applicant environment — applicant-controlled representative segment, applicant infrastructure and credentials. CIPHER does not access applicant hosts directly; it receives the event data from the agents and inputs forward.
	From CIPHER: XDR SaaS tenant, agent packages, pipeline, range, scoped enrolment credentials. From applicant: compute and network capacity sufficient to host the required agents and interfaces; minimum sizing to be agreed during onboarding based on the selected scenario., host / OS diversity, IDS/IPS and/or OT appliances to feed, and operating data for the real-world half.
	Range: synthetic assets and injected scenarios (ground truth). Applicant environment: the applicant's own environment generates the data and the CIPHER XDR SaaS receives forwarded security events. Data-minimisation configured at the agent / pipeline (scoped hosts, modules, log sources). Governed by NDA + DPA. Representative / non-production segment recommended.
	Deploy agents across agreed host / OS types; integrate at least the agreed number of SIEM input types including at least one OT appliance; exercise the agreed agent-capability set; confirm data reaching the SaaS with fidelity; (range) run injected scenarios and report detection; document connectivity, fidelity and friction; provide regulatory mapping. Failure recovery: agent-side buffering and re-delivery on manager unavailability — demonstrate reconnection with no data loss. Delivered to an agreed template.
	CIPHER acts as processor of applicant security telemetry; the applicant is controller. DPA mandatory. Data-minimisation at collection; purpose and retention limited to OC#1 validation; aim to exclude special-category personal data from collected logs. Range: synthetic only. All appliance and credential handling stays applicant-side.
	CIPHER owns outputs (collected fact datasets, performance reports, configurations produced). Applicant retains its environment, source systems, raw operational data, and any pre-existing tooling or methodology.
	The overall selection should seek coverage of multiple critical-sector application domains and, where feasible, multi-site or multi-system environments.

Applicants must be able to host and test CIPHER's tools in an isolated environment, provide suitable (synthetic or real/replayed) data and grant the scoped technical access necessary for integration support.

Multi-site scenarios combining infrastructure, application and security-event data are particularly relevant.

Range / Environment

R1 — Domain cyber-range contribution

Challenge	<i>Invite partners to contribute a cyber-range / sector-emulation solution (open-source preferred) that enables NIS2 readiness assessment for a real operational domain, deployed into or federated with CIPHER so the consortium can run comparable assessments across competing solutions and produce evidence-based recommendations. Generic capture-the-flag ranges are out of scope — readiness value, not training alone.</i>
Expected applicant profile	Provider / maintainer of a cyber-range or sector-emulation platform (open-source preferred) with NIS2-relevant domain depth (OT, healthcare, energy, telco, etc.), able to grant deployment and extension rights.
Objectives	(a) Deploy / federate the range with CIPHER; (b) provide domain-realistic scenarios that assess NIS2 readiness (not CTF / training-only); (c) map scenarios and measurements to NIS2 Article 21(2) measures so readiness is assessable; (d) enable comparable evaluation against other CIPHER range environments to support consortium recommendations.
Scenario description	Applicant selects one NIS2 operational domain (any Annex I/II sector, applicant's choice — no CTF-style abstract challenges) and provisions a representative environment in which an operator's readiness against NIS2 measures can be exercised and assessed (realistic assets, threats, detection / response points).
Range description & architecture	Applicant provides: the range / emulation platform, domain scenarios, deployment artifacts (IaC / containers where applicable). CIPHER provides: hosting / integration environment, integration support, and an evaluation harness for comparable assessment. Integration touchpoints: deployment into CIPHER infrastructure or documented federation with the applicant-hosted range; scenario / measurement export. Open-source preferred (scoring weight); a sustainable deploy / extend / maintain licence is required regardless of model.
Evaluation scope — KPIs	1. NIS2 mapping — % of scenarios / measurements mapped to specific Article 21(2) measures.

	2. Domain realism — fidelity of assets / protocols / threats vs the real sector (rubric). 3. Readiness measurability — produces a quantifiable readiness signal (score / coverage), not pass/fail flags. 4. Deployability — successful deployment / federation with documented effort. 5. Interoperability — targets exercisable by CIPHER tooling (T4.3, XDR) where relevant. 6. Comparability — outputs expressible in a common form for cross-range recommendation.
Deployment environment	Contributed range deployed into CIPHER infrastructure (preferred) or federated with the applicant-hosted instance. Isolated from production; synthetic / emulated assets only. No live operator data.
Requirements (HW/SW/data)	From CIPHER: hosting / compute or federation connectivity, integration support, evaluation harness. From applicant: the range platform, domain scenarios, deployment documentation, and any licences / dependencies to run and extend it.
Data provisions	Synthetic / emulated sector environment supplied by the applicant's range. No real operator or personal data. Under NDA. Sample datasets must be synthetic or properly licensed.
Minimum deliverable framework	Deploy / federate one domain range with CIPHER; provide readiness-assessment scenarios mapped to NIS2 measures (not CTF); demonstrate at least one comparable readiness-assessment run; deliver deployment and extension documentation. Pure training / CTF content excluded. Delivered to an agreed template.
Compliance boundaries	NDA; synthetic data only; no live operator / personal data; licence must permit CIPHER deployment, operation, extension and post-project sustainability. Open-source licences preferred.
IP & licensing	Inverted from the other challenges. Applicant retains ownership of the contributed range and pre-existing scenarios, and grants CIPHER a licence to deploy, operate, extend and maintain it (project + sustainability). CIPHER owns only the integration artifacts, evaluation outputs, and any domain scenarios co-developed under the call.
Consortium requirements	The overall selection should seek complementary coverage of multiple NIS2 Annex I and Annex II operational domains, prioritising ranges that provide realistic and measurable readiness-assessment value for critical-sector and OT environments. Applicants must be able to deploy their cyber range within CIPHER infrastructure or federate it through documented interfaces. They must provide the platform, representative domain scenarios, deployment artefacts, required dependencies and a licence permitting CIPHER to deploy, operate, extend and maintain the contributed solution. The selected portfolio should support comparable readiness assessments across different range environments. Generic capture-the-flag or training-only solutions should not be considered sufficient. Open-source solutions

and sustainable licensing arrangements should be prioritised where they provide equivalent technical and operational value.

P1 — DevSecOps & platform automation

Challenge	<i>Partners deliver DevSecOps automation for technologies on a CIPHER-provided list that lack proper automation — e.g. porting a monolithic, Docker-Compose-only tool such as MISP to a maintainable Helm chart, or authoring IaC and CI/CD where none exists. Applicants select from the list; CIPHER defines what needs doing. Work lands in CIPHER repositories under review; execution against a non-production environment. Reusable output, OSS-preferred, licensed to CIPHER.</i>
Expected applicant profile	Platform / DevSecOps engineering profile with demonstrable IaC (Terraform / OpenTofu, Ansible), Kubernetes / Helm, and CI/CD (GitLab CI / GitHub Actions / Argo-class) experience; container and multi-arch build familiarity; experience taming monolithic or poorly-packaged applications a strong plus.
Objectives	(a) Codify deployment of a CIPHER-listed technology as idempotent, version-controlled IaC and/or a maintainable Helm chart; (b) build a CI/CD pipeline for build → test → deploy; (c) generate an SBOM, scan artifacts, and record a risk-management decision (accept / mitigate / compensating control) for findings in components CIPHER does not own — visibility and documented decision, not upstream remediation; (d) make the deployment portable / reproducible across ≥2 target environments (supporting proof-recreation independent of any single platform); (e) map pipeline supply-chain controls and risk decisions to NIS2 Article 21(2)(d)/(e) and CRA secure-development / SBOM obligations.
Scenario description	CIPHER publishes a list of technologies requiring automation (monolithic apps, tools without Helm charts, components lacking IaC), each with the gap and target platform noted. Applicants select one or more items and deliver the automation that stands them up reproducibly from a clean environment, with a documented portability demonstration (redeploy to a second target).
Scope & deliverables	CIPHER provides: the technology list with per-item gaps and targets, source repositories, a non-production target environment, container registry, secret store, and review capacity. Applicant delivers: IaC modules, Helm charts, CI/CD pipeline definitions, SBOM + scan + risk-decision record, and runbook / documentation, contributed to CIPHER repos via pull request. Integration touchpoints: Git (PR / review), container registry,

	Kubernetes / k3s API, secret store, pipeline runners. OSS-preferred for reusable deliverables.
Delivery scope — KPIs	1. Reproducibility — clean-environment rebuild succeeds unattended (documented one-command bootstrap). 2. Item coverage — listed items fully automated (IaC + chart + pipeline). 3. Portability — successful redeploy to ≥ 2 target environments. 4. Pipeline reliability — build / deploy success rate; mean deploy time. 5. Supply-chain visibility — SBOM produced and artifacts scanned per pipeline, with a recorded risk decision for unowned-component findings. 6. Idempotency & rollback — re-apply causes no drift; rollback path demonstrated.
Environment & access	Dedicated non-production CIPHER environment; least-privilege, time-boxed, scoped credentials; no production access . Changes land via pull request and consortium review / merge — no direct apply to shared infrastructure. Secrets via the platform secret store, never committed.
Requirements (HW/SW/data)	From CIPHER: technology list, repositories, non-prod environment / compute, container registry, secret store, review capacity. From applicant: DevSecOps toolchain and expertise; any pre-existing reusable modules under a licence permitting CIPHER use.
Configuration & secrets	No operational or personal data involved. Configuration is version-controlled; secrets and credentials are issued scoped and time-boxed, stored in the secret store, and never committed. Under NDA.
Minimum deliverable framework	For each selected listed item: deliver IaC and/or Helm + CI/CD; demonstrate clean-environment reproducible deploy and one portability redeploy; produce SBOM + scan + recorded risk decision; provide runbook / documentation. All contributed to CIPHER repositories. Delivered to an agreed template.
Compliance boundaries	NDA; non-production only; least-privilege scoped credentials; no production or live-data access; secrets never in repo. CIPHER's own deployment posture aligns to applicable legislation; applicants are not required to secure components they do not own — unowned-component risk is surfaced and decided, not remediated. Deliverables licensed for CIPHER use, OSS-preferred.
IP & licensing	Same posture as R1 (not the house-owns rule). Applicant retains ownership of the delivered automation and grants CIPHER a licence to use, deploy, extend and maintain it for the project (sustainability-preferred). Pre-existing generic modules the applicant reuses stay theirs, licensed to permit CIPHER use. Reusable deliverables OSS-preferred.

Acronyms & terms

Expansions of the acronyms, standards and project references used in this document.

CRA	Cyber Resilience Act — EU Regulation 2024/2847 on cybersecurity requirements for products with digital elements.
CTF	Capture The Flag — gamified security exercise; training value but no readiness signal (out of scope for R1).
CVE	Common Vulnerabilities and Exposures — standard identifier for a publicly known vulnerability.
DPA	Data Processing Agreement — GDPR contract between a data controller and a processor.
EDR	Endpoint Detection and Response.
FIM	File Integrity Monitoring — a Wazuh agent module.
GDPR	General Data Protection Regulation — EU Regulation 2016/679.
GICSP	Global Industrial Cyber Security Professional — ICS/OT security certification.
IaC	Infrastructure as Code — declarative provisioning (e.g. Terraform, containers).
ICS	Industrial Control System(s).
IDS / IPS	Intrusion Detection System / Intrusion Prevention System.
IEC 62443	IEC standard series for the security of industrial automation and control systems.
IP	Intellectual Property.
ISO 27001	ISO/IEC standard for information security management systems.
IT	Information Technology (contrasted with OT).
MTTD	Mean Time To Detect — latency from event to alert.
NDA	Non-Disclosure Agreement.
NIS2	Directive (EU) 2022/2555 on a high common level of cybersecurity — Network and Information Security Directive 2. Annex I/II list the covered sectors.
OC	Open Call — stage of cascade (financial-support-to-third-parties) funding. OC#1 is the first; OC#2 follows.
OpenVAS	Open Vulnerability Assessment System — network vulnerability scanner.
OSCP	Offensive Security Certified Professional — penetration-testing certification.
OT	Operational Technology — hardware/software controlling physical processes (contrasted with IT).
S3	Simple Storage Service — object-storage API; “S3-compatible” denotes any store exposing that API (e.g. MinIO).
SBOM	Software Bill of Materials — inventory of components in a software artifact.
SCA	Security Configuration Assessment — a Wazuh agent module.
SCADA	Supervisory Control And Data Acquisition — a class of industrial control system.

SIEM	Security Information and Event Management.
SOC	Security Operations Centre.
T4.3	CIPHER project task: Automated Penetration Testing.
T4.4	CIPHER project task: Cyber Range.
VM	Vulnerability Management.
WORM	Write Once, Read Many — immutable (tamper-evident) storage.
XDR	Extended Detection and Response.
EMS	Event Management System; the basis of CIPHER's federated risk-monitoring capability.
NBI	Northbound Security Interface.
KPI	Key Performance Indicator.
CTI	Cyber Threat Intelligence.
MISP	Malware Information Sharing Platform.
RMT	Risk Management Toolbox.
UEBA	User and Entity Behaviour Analytics.