INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

ANNEX B

TERMS OF REFERENCE

Tender reference No: 2026-07-095

Assignment Name: **Procurement and Delivery of IBM QRadar SIEM Configuration Services and IBM QRadar SOAR Implementation Services for the Central Election Commission of Ukraine**

1. Background

As Ukraine prepares for post-war elections, its Central Election Commission of Ukraine (CEC) faces significant technical challenges, including cyber threats, outdated infrastructure, and gaps in ICT systems.

In modern hybrid-threat environments, the timely detection of, and rapid, coordinated response to, cybersecurity incidents has become an essential capability of any critical-information-infrastructure operator. Achieving these capabilities requires a centralized platform to collect, normalize, correlate, and act upon security telemetry. Without such a capability, organizations may be unable to meet contemporary cyber resilience requirements, comply with regulatory expectations, or safeguard the integrity of electoral processes.

Security Information and Event Management (SIEM) is a class of cybersecurity solutions that aggregates and correlates security-relevant events across an organization's IT environment. These may include servers, network devices, security controls, endpoints, applications, identity providers, cloud workloads, and other technology assets. SIEM solutions apply analytics and correlation rules to identify and prioritise security events for investigation by security analysts. A properly tuned SIEM is a cornerstone of operational visibility and effective threat detection.

Security Orchestration, Automation and Response (SOAR) extends SIEM capabilities by providing a case-management platform and an automation engine for incident response.
SOAR consumes detections from SIEM and other security tools, enriches them with contextual data (threat intelligence, asset/identity data, CMDB), executes automated playbooks (notification, containment, evidence collection, ticketing), and maintains a full audit trail of every response action.

The Beneficiary has an existing deployment of **IBM QRadar SIEM** that requires comprehensive tuning, optimization, and extension to deliver its full operational value. In parallel, the Beneficiary intends to introduce **IBM QRadar SOAR** to centralize and automate incident-response workflows. Together, the enhancement of QRadar SIEM and the implementation of QRadar SOAR — supported by a curated set of cybersecurity incident response scenarios, response playbooks and operational regulations — constitute **a key element of building a modern security process**.

Accordingly, this procurement is limited to configuration, tuning, integration and implementation services for the existing IBM QRadar SIEM environment and the IBM QRadar SOAR environment to be licensed separately by the Beneficiary. Replacement of the SIEM/SOAR platform or proposal of an alternative SIEM/SOAR product is outside the scope of this tender. **Software licensing is out of scope of this tender.** Licenses for IBM QRadar SIEM (existing) and IBM QRadar SOAR (to be acquired by the Beneficiary) shall be the responsibility of the Beneficiary. Accordingly, this tender is limited to the procurement of Deployment Services comprising configuration, tuning, integration and implementation of the existing IBM QRadar SIEM environment and the IBM QRadar SOAR environment.

2. Objectives of the Assignment

The CEC customer requires a reliable Bidder to deliver effective, secure, and compliant Configuration Services for the enhancement of the existing IBM QRadar SIEM and Implementation Services for IBM QRadar SOAR at the Central Election Commission of Ukraine in preparation for post-war elections.

The key objectives of this assignment are:

- To increase the operational maturity of the Beneficiary's Security Operations Center.
- To improve the accuracy and coverage of cybersecurity incident detection through optimization and extension of IBM QRadar SIEM correlation rules and log-source coverage.
- To centralize monitoring and response by establishing a full bi-directional integration between IBM QRadar SIEM and IBM QRadar SOAR.
- To automate routine incident-response scenarios through IBM QRadar SOAR playbooks.
- To standardize cybersecurity processes through the development of cybersecurity incident response scenarios, operational regulations, and supporting documentation.

3. Scope of Work

3.1 The selected Bidder will be expected to deliver configuration services for IBM QRadar SIEM and implementation services for IBM QRadar SOAR as further specified in this ToR and in Annex 2.2. Any other software or hardware products or related services that may be required by the Central Election Commission of Ukraine in the future and are relevant to this procurement may be procured under a Framework Contract to be concluded as an outcome of this tender based on a separate quotation.

3.2 General architecture and deployment principles:

- All IBM QRadar SOAR components shall be deployed on premises on infrastructure prepared by the Beneficiary in accordance with IBM system requirements.
- The existing IBM QRadar SIEM deployment shall be enhanced in place; no replacement of the SIEM platform is foreseen under this tender.
- Bi-directional integration between IBM QRadar SIEM and IBM QRadar SOAR shall be configured so that QRadar offenses automatically generate cases in QRadar SOAR.

- Integration with the Beneficiary's corporate services (SMTP/IMAP, Active Directory / LDAP, ticketing system) shall be configured.
- The Bidder shall not require third-party software or hardware that is not part of the standard IBM QRadar SIEM / SOAR distribution, except where explicitly agreed with the Beneficiary.

3.3 Scope of services to be delivered. The Deployment Services consist of four interrelated work-streams, each of which shall be planned, executed, documented and accepted as defined in Annex 2.2.

3.3.1 IBM QRadar SIEM — tuning and enhancement of the existing deployment

- Analysis of the current configuration: deployment architecture, component health, licensing coverage, and software versions.
- Architecture optimization: capacity analysis of SIEM components (Console, Event Processor, Flow Processor, Data Nodes, WinCollect, etc.), scaling recommendations.
- Logging audit and tuning: review of connected log sources, elimination of duplicates, gaps and incorrect parsers (DSMs).
- Integration of additional log sources in accordance with an agreed inventory; configuration or refinement of DSM parsers as required.
- Retention and storage review: audit of event/flow retention settings (EPS/FPS), alignment with regulatory and internal policy requirements.
- Documented recommendations: formalized findings and proposals for further development of the SIEM platform.

3.3.2 IBM QRadar SOAR — implementation and configuration

- On-premises installation of IBM QRadar SOAR on Beneficiary-provided infrastructure in accordance with IBM system requirements.
- Base configuration: system parameters, incident categories, artifact types, custom fields.
- Bi-directional integration with IBM QRadar SIEM to enable automatic case creation from QRadar offenses.
- Configuration of role-based access control (RBAC) aligned with the organizational structure of the Beneficiary’s cybersecurity incident response team.
- Integration with corporate systems: e-mail (SMTP/IMAP), Active Directory / LDAP, and the ticketing system.

3.3.3 Development and implementation of cybersecurity incident response scenarios

The Bidder shall develop and implement an agreed set of **20 cybersecurity incident response scenarios** covering the threat landscape relevant to the Beneficiary. The type of controls to be implemented will be defined jointly with the Beneficiary at the project's initiation phase and may include controls from the Bidder's existing library as well as entirely new controls specific to the Beneficiary's environment. A review of existing correlation rules and offenses shall be performed prior to the development of new cybersecurity incident response scenarios, with corrective actions taken where required.

One cybersecurity incident response scenario may comprise from 1 up to 10 IBM QRadar correlation rules targeting a single threat. The scope and complexity of the 20 cybersecurity incident response scenarios shall be agreed during the inception phase and reflected in the approved project plan. Any material changes after approval shall require a separate agreement between the Customer and the Bidder. Each cybersecurity incident response scenario shall include:

- Identification of key assets, processes, and IT-infrastructure functions of the Beneficiary.

- Optimization of existing correlation rules: review of active Custom Rules, elimination of excessive triggering, prioritization by criticality.
- Formalized specification: documented description of the threat model, detection logic and required technical prerequisites; specification approval by the Beneficiary.
- MITRE ATT&CK mapping: each cybersecurity incident response scenario mapped to the corresponding techniques and tactics of the MITRE ATT&CK framework for structured coverage.
- Configuration of correlation rules in IBM QRadar SIEM in accordance with the approved specification, including the connection of new log sources where required.
- Response automation through SOAR: for each cybersecurity incident response scenario, a corresponding playbook or response procedure in IBM QRadar SOAR shall be developed.
- Enrichment integration: connection of external and internal enrichment sources (IP reputation, geolocation, Active Directory data, CMDB).
- Automatic creation of incidents in IBM QRadar SOAR and of tickets in the Beneficiary's ticketing system on rule triggering where suitable.
- Tuning and optimization after the test runs: adjustment of rules, thresholds and playbook logic based on real Beneficiary data.

3.3.4 Documentation and operational regulations

On completion of the works the Bidder shall deliver the following package of technical and operational documentation:

- Administrative documentation of IBM QRadar SIEM and SOAR: deployment architecture, components, network configuration and backup setup.
- Operational documentation: administrator manuals for SIEM and SOAR, including maintenance, upgrade and troubleshooting procedures.
- cybersecurity incident response scenarios documentation: formalized description of the threats detected by each cybersecurity incident response scenario, detection logic, exclusions, MITRE ATT&CK categorization.
- Incident-response regulations: incident-handling procedures, escalation and responsibility rules, response to SLAs.
- Monitoring and response regulation for incidents detected by IBM QRadar SIEM and IBM QRadar SOAR: shift composition and rotation, information flow, reporting.
- IBM QRadar SOAR playbooks: full description of automated response processes with execution flow diagrams and operating instructions.
- Integration schema: an up-to-date diagram of connections between IBM QRadar SIEM, IBM QRadar SOAR and adjacent systems of the Beneficiary.
- Recommendations for further development: prioritized roadmap of functional extensions for the following 12–18 months.

3.4 Licensing. No software licenses are provided under this tender. Licenses for IBM QRadar SIEM (existing deployment) and IBM QRadar SOAR (to be acquired separately by the Beneficiary) shall be in force throughout the project. The Bidder shall verify license validity at project kick-off and shall flag any licensing gaps to the Beneficiary in writing.

3.5 The general list of Deployment Services to be procured and delivered is provided below in Table 1.

Table 1. Deployment Services

#	Item	Q-ty
1	IBM QRadar SIEM & SOAR Deployment Services (configuration enhancement of the existing IBM QRadar SIEM, on-premises deployment and configuration of IBM QRadar SOAR, development and implementation of 20 cybersecurity incident response scenarios with associated playbooks, knowledge transfer, and full project documentation)	1

3.6 Additional services may be procured from the successful Bidder if needed, and this (should the need arise) will be the subject of a separate quotation. As an outcome of this tender, a Framework Contract will be concluded with the Bidder.

3.7 The detailed technical requirements for the Deployment Services to be procured are provided in Annex 2.2 (the specification in Annex 2.2 takes precedence over the general list in Table 1 above).

4. Timing and Work Plan

Project implementation shall not exceed 120 calendar days from the date of contract signature. The indicative phased schedule is summarized below; a detailed timeline of deliverables will be developed and agreed with the selected Bidder during the inception phase.

- Phase 1 — Inception: contract signature, project-team appointment, collection of input data, agreement on log-source inventory and cybersecurity incident response scenarios, infrastructure-readiness verification for SOAR (1–2 weeks).
- Phase 2 — SIEM audit: full analysis of IBM QRadar SIEM configuration; audit report and tuning plan (1–2 weeks).
- Phase 3 — SIEM tuning: remediation of findings; connection of new log sources; DSM parser refinement (1–2 weeks).
- Phase 4 — SOAR deployment: installation, base configuration, integration with SIEM, AD, e-mail and ticketing; RBAC (2 weeks).
- Phase 5 — cybersecurity incident response scenarios & playbooks: correlation rules, SOAR playbooks, MITRE ATT&CK mapping, enrichment (3–4 weeks).
- Phase 6 — Testing: functional and end-to-end testing (SIEM → SOAR → ticketing), tuning (1–2 weeks).
- Phase 7 — Documentation and handover: documentation package, knowledge-transfer sessions, acceptance act (1–2 weeks).

Indicative total project duration: 10–16 weeks.

5. Deliverables and Reporting Requirements

5.1 The deliverables for this assignment shall include:

- Deployment Services for IBM QRadar SIEM and IBM QRadar SOAR delivered in accordance with Annex 2.2.

- Central Election Commission of Ukraine Acceptance Letter confirming the acceptance of the Deployment Services.
- Full documentation package as defined in section 3.3.4 of this ToR and in Annex 2.2.

5.2 As part of the reporting the Bidder must submit:

- An initial delivery plan within 3 working days of contract signature.
- Biweekly progress reports highlighting technical tasks completed, blockers, and next steps.
- A final delivery report shall include a list of delivered services and cybersecurity incident response scenarios, together with the documentation package defined in Section 3.3.4 of this ToR.

The technical documentation supporting acceptance testing is to be provided for approval in electronic (PDF) and paper form in the Ukrainian language.

6. Management and Organization

From **Customer (IDEA)**, a relevant Project Manager will be designated to provide relevant guidance for the achievement of the overall objective of the assignment and deliverables. All Bidder communications shall be directed to the designated **Customer** Project Manager. Final deliverables must be jointly confirmed by **Customer** and the designated Central Election Commission of Ukraine technical contact.

All questions arising during the course of the project should be coordinated with Tetiana Bibik, **Customer** Project Manager (e-mail: t.bibik@idea.int).

7. Monitoring and Evaluation

This Monitoring and Evaluation section defines how **Customer** will track the progress, quality, and outcomes of the delivery of Deployment Services for IBM QRadar SIEM and IBM QRadar SOAR for the Central Election Commission of Ukraine. The aim is to ensure timely, secure, and high-quality delivery of services in compliance with technical specifications.

7.1 Key Performance Indicators (KPIs)

- Completion of the SIEM audit and tuning phase within 35 calendar days of contract signature.
- On-premises deployment of IBM QRadar SOAR with base integrations (SIEM, AD/LDAP, e-mail, ticketing) completed within 70 calendar days of contract signature.
- All 20 cybersecurity incident response scenarios and corresponding SOAR playbooks delivered, tested and tuned within 100 calendar days of contract signature.
- Final documentation handover and operational acceptance within 120 calendar days of contract signature.
- Full compliance with the technical requirements outlined in Annex 2.2.
- Delivery of a valid Acceptance Letter from the Central Election Commission of Ukraine.

7.2 Monitoring Activities

- Biweekly check-ins with the Bidder to track progress against the delivery timeline.
- Document verification: review of progress reports, test protocols, and delivery documentation.
- Confirmation with the Central Election Commission of Ukraine of the functional acceptance of the tuned IBM QRadar SIEM, the new IBM QRadar SOAR deployment and the implemented cybersecurity incident response scenarios.

7.3 Evaluation Framework

Evaluation Criteria:

- Adherence to timeline milestones.
- Full compliance with the architecture and integration requirements set out in Annex 2.2.
- Absence of critical errors in the tuned IBM QRadar SIEM and in the newly deployed IBM QRadar SOAR.
- Quality and completeness of documentation (High-Level Design, Low-Level Design, cybersecurity incident response scenarios specifications with MITRE ATT&CK mapping, SOAR playbook documentation, operational regulations, test protocols).

Evaluation Process:

- Baseline technical assessment at project launch (SIEM audit results).
- Mid-term evaluation at completion of SOAR deployment and SIEM tuning.
- Final evaluation after testing, cybersecurity incident response scenarios implementation and documentation handover.
- Feedback survey from Central Election Commission of Ukraine technical staff and **Security** analysts.

Annexes (to be provided)

Annex 2.2. Technical requirements for IBM QRadar SIEM and IBM QRadar SOAR deployment services for the Central Election Commission of Ukraine.