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

This Annex defines the technical requirements for the Deployment Services to be delivered by the Bidder for the enhancement of the existing IBM QRadar SIEM and for the implementation of IBM QRadar SOAR at the Beneficiary's premises. The scope is structured into six phases that are sequential at the macro level but may be executed with partial overlap as agreed in the project plan.

1. Preparations

- Analyze the existing IT and security infrastructure of the Beneficiary and document the configuration of the relevant components (virtual machines, services, network connectivity, hardware and software versions).
- Conduct an audit of the existing IBM QRadar SIEM deployment, covering:
    - Deployment architecture, component health and software versions (Console, Event Processor, Flow Processor, Data Nodes, WinCollect, etc.).
    - Licensing coverage (EPS/FPS allocation versus actual consumption).
    - Connected log sources: inventory, parser correctness (DSMs), duplicates, and gaps.
    - Event/flow retention configuration; alignment with regulatory and internal policy requirements.
    - Active correlation of rules, building blocks, reference sets, and active offenses.
- Assess the readiness of the on-premises infrastructure provided by the Beneficiary for the deployment of IBM QRadar SOAR (CPU/RAM/storage, network connectivity, OS prerequisites) against IBM system requirements.
- Verify network connectivity between IBM QRadar SIEM, the planned IBM QRadar SOAR deployment and the relevant log sources, corporate services and integration targets.
- Produce a SIEM audit report and a tuning plan; obtain Beneficiary approval before proceeding to the tuning phase.

2. IBM QRadar SIEM — tuning and enhancement of the existing deployment

- Configuration review: deployment architecture, component health, licensing coverage and software versions.
- Architecture optimization: capacity analysis of SIEM components; documented scaling recommendations.
- Log source audit and tuning:
    - Review of connected log sources; elimination of duplicates and gaps.
    - Identification and remediation of incorrect or missing DSM parsers.
    - Integration of additional log sources in accordance with an agreed inventory.
- Configuration or development of DSM parsers where required (custom DSMs for non-standard sources).

- Retention and storage review: audit of event/flow retention settings (EPS/FPS), with adjustments to align with regulatory and internal policy requirements.
- Tuning of existing correlation rules: review of active Custom Rules, elimination of excessive triggering, prioritization by criticality.
- Documented set of recommendations for the further development of the SIEM platform, covering scalability, additional log sources and operational improvements.

3. IBM QRadar SOAR — installation and configuration

- On-premises installation of IBM QRadar SOAR on the Beneficiary's infrastructure in accordance with IBM system requirements.
- Base configuration:
    - System parameters and platform settings.
    - Incident categorization (severity, type, status), artifact types and custom fields aligned with the Beneficiary's incident-management practice.
- Bi-directional integration with IBM QRadar SIEM:
    - Automatic case creation in IBM QRadar SOAR from QRadar SIEM offenses.
    - Bi-directional update of case/offense status between SIEM and SOAR.
- Role-based access control (RBAC) configuration aligned with the organizational structure of the Beneficiary’s cybersecurity incident response team (analyst tiers, lead analysts, administrators, auditors).
- Integration with corporate systems:
    - E-mail (SMTP for outbound notifications; IMAP for inbound case creation where required).
    - Active Directory / LDAP for authentication and analyst identity.
    - Ticketing system of the Beneficiary for automatic ticket creation and bi-directional status updates.

4. Development and implementation of cybersecurity incident response scenarios (20 cybersecurity incident response scenarios)

The Bidder shall develop and implement 20 cybersecurity incident response scenarios (security controls). The set of cybersecurity incident response scenarios shall 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. Each 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, including required data sources, estimated number of correlation rules, SOAR playbook scope, enrichment requirements and acceptance criteria. Any material changes after approval shall require a separate agreement between the Customer and the Bidder.

For each cybersecurity incident response scenario, the following steps shall be performed:

- Identification of key assets, processes, and IT-infrastructure functions of the Beneficiary that the cybersecurity incident response scenario is intended to protect.
- Threat-model definition: the threat being detected, attack vector(s) and prerequisites.
- Detection-logic specification: data sources, fields, correlation logic, thresholds, exceptions.
- MITRE ATT&CK mapping: explicit linkage of the cybersecurity incident response scenarios to the corresponding techniques and tactics.
- Feasibility assessment: only cybersecurity incident response scenarios that can be implemented in IBM QRadar SIEM using available data (or data that can be onboarded under this project) are accepted for implementation.
- Beneficiary approval of the cybersecurity incident response scenarios specification before implementation.
- Configuration of correlation rules in IBM QRadar SIEM in accordance with the approved specification, including connection of new log sources where required.
- Response automation through IBM QRadar SOAR: a corresponding playbook or response procedure shall be developed for every cybersecurity incident response scenario.
- Enrichment integration – where suitable:
    - IP reputation and threat-intelligence enrichment.
    - Geolocation enrichment.
    - Active Directory enrichment (user attributes, group membership).
    - CMDB / asset enrichment where a source is available.
- 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 run: adjustment of rules, thresholds and playbook logic based on real Beneficiary data.

5. Testing

- Development of a comprehensive Acceptance Test Plan covering:
    - Functional tests for each tuned and newly implemented IBM QRadar SIEM correlation rule (positive and negative scenarios).
    - Functional tests for each IBM QRadar SOAR playbook (decision branches, enrichment calls, notifications, ticket creation).
    - End-to-end tests covering the flow of SIEM offense → SOAR case → enrichment → ticket → closure.
    - Integration tests for SMTP/IMAP, Active Directory / LDAP, and the ticketing system.
    - RBAC tests confirming that each role has the expected privileges and no excessive access.
- Execution of the Acceptance Test Plan jointly with the Beneficiary's technical team.
- Tuning rules, playbooks, and thresholds based on the test results, until success criteria are met.

- Production of a final test report documenting the executed test cases, results, observed defects, and their resolution.

6. Documentation

The Bidder shall deliver the following documentation as part of the project handover. All documents shall be provided in electronic (PDF) and editable (DOCX) formats; final acceptance documentation shall additionally be provided in paper form in the Ukrainian language.

- High-Level Design (HLD) covering IBM QRadar SIEM (as-built, post-tuning) and IBM QRadar SOAR (as deployed).
- Low-Level Design (LLD) includes network connectivity diagrams, integration points, RBAC matrix, backup, and recovery configuration.
- Administrative documentation of IBM QRadar SIEM and IBM QRadar SOAR: deployment architecture, components, network configuration, 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 regulation: incident-handling procedures, escalation and responsibility rules, response of SLAs.
- Monitoring and response regulation for incidents detected by IBM QRadar SIEM and IBM QRadar SOAR, defining shift composition and rotation, information flow and reporting.
- IBM QRadar SOAR playbook documentation: full description of each automated response process, 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.
- Operational Acceptance Document (Testing Report) summarizing the results of the Acceptance Test Plan execution.
- Recommendations for further development: prioritized roadmap of functional extensions for the following 12–18 months.

7. Knowledge transfer

- Knowledge-transfer sessions for the Beneficiary's administrators of IBM QRadar SIEM and IBM QRadar SOAR, covering the tuned/deployed configuration, day-to-day operations and the most common troubleshooting scenarios.
- Knowledge-transfer sessions for security analysts, covering the implemented cybersecurity incident response scenarios, SOAR playbooks, dashboards, and the agreed incident-handling workflow.
- All knowledge-transfer sessions shall be supported by the documentation produced in section 6 above; session recordings or session minutes shall be provided to the Beneficiary.

8. Assumptions and dependencies

- The Beneficiary provides the Bidder with administrative access to IBM QRadar SIEM and to the server infrastructure required for the deployment of IBM QRadar SOAR. The Bidder shall treat all logs, configuration data, network information, incident data, credentials, access tokens and any other information obtained during the provision of the Deployment Services as confidential information. The Bidder shall not copy, export, disclose, transfer or process the Beneficiary's data outside the approved environment without the Beneficiary's prior written approval. All administrative actions performed by the Bidder in the Beneficiary's systems shall be logged where technically possible. All temporary accounts, credentials, access tokens and integration keys used by the Bidder shall be revoked, transferred to the Beneficiary or otherwise handled in accordance with the agreed handover procedure upon completion of the project.
- The Beneficiary appoints a responsible technical representative (SIEM / SOAR administrator) who participates in technical sessions and takes decisions in a timely manner.
- Servers for the deployment of IBM QRadar SOAR (on premises) are prepared by the Beneficiary in accordance with IBM system requirements prior to the start of the installation phase.
- Network connectivity between IBM QRadar SIEM, IBM QRadar SOAR and the log sources is provided and verified by the Beneficiary prior to the start of the works.
- The scope of integrations with corporate systems (ticketing, CMDB, threat intelligence, etc.) is fixed at the technical-requirements approval stage; additional integrations shall be agreed and priced separately.
- The set of cybersecurity incident response scenarios (count and types) is fixed jointly with the Beneficiary at the inception phase; any changes after the start of development require additional agreement.
- The licensing of IBM QRadar SIEM and IBM QRadar SOAR (existence of valid active licenses) is the responsibility of the Beneficiary, as stated in Annex 2.1 (section 3.4) and Annex 2.2.