Request for Proposals
on
Security Operation Center
And
SIEM with Threat Intelligence platform
Call for Tender

Version 1.0
Date: 29 Sep 2026

Hong Kong Internet Registration Corporation Limited

Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong

IMPORTANT NOTICE

This communication contains information which is confidential and may also be privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any distribution, copying or use of this communication or the information in it is strictly prohibited. If you have received this communication in error, please notify the sender immediately and then destroy any copies of it.

Table of Contents

1. Summary 4
2. Definitions 5
3. Background 6
4. The Required Services 7
4.1. Part A – SOC service 7
4.2. Part B – SIEM platform with Threat Intelligence 16
5. Limitation of Liability and Indemnity 24
6. Information Security 26
7. Project Acceptance 26
8. Anti-collusion 27
9. Offering Advantages 27
10. Ethical Commitment 28
11. Schedule 30
12. Payment Schedule 30
13. Elements of a Strong Tender 31
14. Service Agreement Negotiation and Signature 31
15. HKIRC Contacts 32
Appendix A – Warranty 33
Appendix B – Declaration Form by Contractor on their compliance with the ethical commitment requirements 36
Appendix C – HKIRC Proposal Requirements 38
Appendix D – HKIRC Information Security Policy 39

1. Summary

HKIRC is going to commission an external Service Provider to provide Security Operation Center and SIEM with Threat Intelligence platform for the Company. The service shall provide 7 x24 Security Operation Center as well as "SOC" service and setup SIEM with Threat Intelligence platform support for company security operation. It shall also include all services required for the implementation of the Project.

HKIRC is looking for a service provider(s) ("the Contractor") to provide and setup for the above services. The contract period is valid for 12 months and include the option to extend the contract beyond one year in the original contract. The extension agreement will be same terms and price for other 24 months

The scope of service is detailed in section 4 of this document.

Parties interested in providing this service shall submit proposal (see Appendix C) to the Group no later than 23:59pm on 20th Oct 2026.

The Contractor should submit proposal by email to HKIRC contacts (refer to Appendix C - HKIRC Proposal Requirements, electronic copy). The Contractor must provide their information as required in the proposal cover page (Appendix C, 2 Cover Page).

2. Definitions

The following terms are defined as in this section unless otherwise specified.

“CFT” means this Call for Tender

“The Contractor” means the company who will provide the Services after award of contract.

“Critical Infrastructures (Computer Systems) Ordinance (Cap. 653)” or “CI Ordinance” means the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) of Hong Kong, including any applicable Codes of Practice, directions, amendments, and related regulatory requirements.

“Critical Computer System” or “CCS” means a computer system designated under the Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) or identified by HKIRC as supporting critical services, where compromise, disruption, or unavailability may adversely affect the operation of a critical infrastructure.

“HKIRC” means Hong Kong Internet Registration Corporation Limited.

“HKDNR” means Hong Kong Domain Name Registration Company Limited, a wholly-owned subsidiary of HKIRC, the company requesting the proposal for “The Services”.

“ISMS” means Information Security Management System. It consists of an information security organization and a set of policies, guidelines and procedures concerned with information security management.

“The Services” means the 7 x24 Security Operation Center with requirements stipulated in Section 4 of this document.

“Tenderer” means the company who will submit proposal to provide the Services

3. Background

About HKIRC

Hong Kong Internet Registration Corporation Limited (HKIRC) is a non-profit-distributing and non-statutory corporation responsible for the administration of Internet domain names under '.hk' and '.香港' country-code top level domains. HKIRC provides registration services through its registrars and its wholly-owned subsidiary, Hong Kong Domain Name Registration Company Limited (HKDNR), for domain names ending with '.com.hk', '.org.hk', '.gov.hk', '.edu.hk', '.net.hk', '.idv.hk', '.公司.香港', '.組織.香港', '.政府.香港', '.教育.香港', '.網絡.香港', '.個人.香港'. '.hk' and '.香港'.

HKIRC endeavours to be:

- Cost-conscious but not profit-orientated
- Customer-orientated
- Non-discriminatory
- Efficient and effective
- Proactive and forward-looking

More information about HKIRC can be found at http://www.hkirc.hk .

HKIRC and HKDNR are listed as public bodies under the Prevention of Bribery Ordinance (Cap 201).

4. The Required Services

The following defines the scope of service to be provided by the Contractor. There are two parts to the scope:

- Part A – SOC service
- Part B – SIEM platform with Threat Intelligence

Service Requirement

4.1. Part A – SOC service

4.1.1. Awarded Tenderer is required to conduct detail on-site understanding and knowledge transfer workshops with various teams internally to understand their roles and responsibilities and propose a target operating model on how to work together.
These include but are not limited to:

- HKIRC Information Security Team
- HKIRC System and DBA Team
- HKIRC Network Team

4.1.2. Awarded Tenderer is required to conduct an in-depth and holistic overall security architecture assessment as part of the understanding phase and provide a set of short-term and long-term recommendations for consideration, including but not limited to:

- Asset inventory completeness
- Log source quality and coverage
- Security Information and Event Management ("SIEM") and Endpoint Detection and Response ("EDR") use case coverage against MITRE ATT&CK Framework
- Security architecture design
- Operational efficiency (e.g., potential areas to improve response time via automation, process optimization, playbook etc.)

4.1.3. The Awarded Tenderer is expected to be able to bring their own SIEM stack to perform the SOC services, though in their proposal should also propose the end-to-end approaches and options for onboarding and offboarding their SIEM in the unlikely event that the contract does not extend beyond the pre-agreed contract length. The options include but are not limited to remove the SIEM, assisting to migrate to another SIEM or licensing the SIEM for a subscription based for contract period.

4.1.4. The Awarded Tenderer is expected to, in an ongoing manner (e.g., through monthly management meetings), highlight security and/or operational resilience pain points as a

result of lessons learnt from ongoing operations, and provide actionable recommendations on how to continuously improve the security posture from a governance, people, process, and technology perspective. These may be implemented by the various teams during business-as-usual operations, or by the Awarded Tenderer if it relates to SOC.

4.1.5. Awarded Tenderer is required to have in-depth experience in managing, configuring, and operating the following security tools:

- EDR
- Firewall
- DDoS mitigation platform
- Web Application Firewall
- Load Balancer
- Network Access Control system

Final detailed device list can be shared upon signed NDA with HKIRC.

4.1.6. Awarded Tenderer is required to be responsible for executing the incident management procedures comprising of the following (both onsite and offsite support) and consolidating the information into the IT Service Management tool for proper audit trail:

- 24x7x365 SOC hotline and email account to receive incident reporting by users, and to follow up accordingly with potential/actual incidents till closure;
- SOC shall support escalation of critical security incidents by phone, SMS or other instant messengers
- Alert monitoring in SIEM and EDR;
- Incident response execution with reference to playbooks and procedures that is proposed and developed by the Awarded Tenderer (up to 10 use cases per year)
- Root cause analysis of potential security incidents in the network;
- Updating and maintaining operational playbooks including but not limited to incident playbooks to reflect operational procedures, through consultation with relevant stakeholders;
- Service testing and tuning for SIEM and EDR upon onboarding of new devices;
- Provide support during their regular cyber incident response and recovery drills and/or security audits;
- Security operations reporting on a weekly and monthly basis to working group and management respectively.

4.1.7. Awarded Tenderer is required to provide consultation in the event of a potential security incident, including advice on incident containment, firewall rules changes, patch management, threat intelligence provision, and incident response.

4.1.8. Awarded Tenderer shall be capable of providing onsite incident response support in Hong Kong for major security incidents when requested by HKIRC.

4.1.9. Awarded Tenderer is required to evaluate the impact of onboarding additional business applications and supporting infrastructure, as well as security tools and devices, share insights on how it potentially impacts the security monitoring efficiency, and provide recommendations on how to integrate with existing practices to enhance security monitoring effectiveness.

4.1.10. Awarded Tenderer is required to leverage its industry expertise to provide best practice recommendations and demonstrate technical proficiency in implementing those practices, including but not limited to:

- Purple team simulation exercises;
- Threat hunting;
- Targeted cyber threat intelligence;
- New use case development for SIEM, EDR, and SOAR;
- API development between existing and/or future security devices;
- XML parser development; and
- Automation.

4.1.11. Awarded Tenderer shall perform at least one Purple Tem exercise during the onboarding period and provide recommendations to improve detection coverage, alert quality and incident response procedures.

4.1.12. Awarded Tenderer is required to provide 7x24 operations for all support levels without third party outsourcing.

4.1.13. The Awarded Tenderer shall be able to communicate with HKIRC in the following languages:

- Verbal communication: Cantonese and English
- Written communication: English

4.1.14. The Awarded Tenderer shall identify the number, roles, qualifications and working arrangements of its Hong Kong-based personnel in the proposal.

4.1.15. Awarded Tenderer and its staff are accredited with relevant security certifications, including but not limited to:

- Company accreditation: ISO/IEC 27001:2013 and CREST covering penetration testing, cyber incident response, threat intelligence and SOC services.
- Company accreditation: SOC 2 Type II report, or equivalent independent third-party assurance report, covering the systems, personnel, processes, locations and subcontractors used to deliver the proposed SOC and SIEM services.

- Staff accreditation: GCIH, GCFA, OSCP, CISSP, and CREST accredited consultants qualified to perform penetration testing, cyber incident response, threat intelligence and SOC services. Proposed SOC team structure and number of staff in each duty, the role and working experience of SOC.

4.1.16. Awarded Tenderer is required to have redundant SOC setup in Hong Kong.

4.1.17. Awarded Tenderer is required to have experience in providing similar scope of services to Hong Kong critical infrastructure providers.

4.1.18. Awarded Tenderer is required to provide and establish a secure remote access connection between the SOC and Data Centres throughout the service period.

4.1.19. Awarded Tenderer is required to assign a Project Manager to oversee all project management activities and have the relevant certification to drive the project to timely and quality completion (e.g., PMP, PSM1, etc.).

4.1.20. Service Level Agreement (SLA)

- SOC availability of at least 99.5% annually
- Escalation time to security alerts and incidents within 15 minutes
- Response time to on-site recovery requests (remote hand) within 2 hours

4.1.21. The Tenderer shall perform proactive threat hunting activities at least quarterly and additionally whenever significant new Threat Intelligence or Indicators of Compromise (IoCs) relevant to HKIRC are identified.

4.1.22. Security Incident Response

A first-line security incident response service is provided when SOC receives and confirms a security alert from the managed equipment. A Level-1 Security Analyst shall follow pre-defined incident response procedures to try classify the security alerts into malicious attacks, anomaly behaviors or botnet connections. It should be highlighted here that the "first-line security incident response" included in the Proposed Service is limited to initial handling and recommendations for reducing immediate impact in the ways of blocking accesses, isolating and relocating systems only.

Escalate to HKIRC team for response the incident response action related to the HKIRC's operation system, infrastructure, networking, databases and data backup restore.

Use case setup (SOP and playbook)

4.1.23. Awarded Tenderer needs to define the following possible use cases with recommendations and responsible to provide the implementation details for the related correlation rules setup in SIEM system:

- Monitor potential and unusual insider activities that could lead to data theft or destruction;
- Anomalous activities and other network and system alerts are correlated across business units to detect and prevent multi-faced attacks (e.g., simultaneous account takeover and DDoS attack);
- Monitor and analyse employee behaviour (e.g., network use patterns, non-work hours, and known devices) to alert anomalous activities;
- Detect unauthorised changes to firewalls, IPS, IDS, other security devices;

- Alert teams when the threat indicators indicate any potential external and internal threats.
- The use cases shall be continuously enhanced and updated for latest threats The use case should cover :
  * Malware infection
  * Password attack
  * Unauthorized privileged account
  * Watchlist activities
  * Suspicious traffic
  * Anomalous activity increase
  * Network reconnaissance
  * Critical asset/account tasks
  * Data exfiltration
  * CnC callback
  * Lateral movement
- The SOC shall allow customized use cases for security monitoring specific to HKIRC

4.1.24. Awarded Tenderer is required to deliver the documents of the use cases definition and description, playbook implementation setup details, test cases and test scripts; and assist to implement the SIEM and also perform UAT.

4.1.25. Awarded Tenderer needs to provide the proposal of the approach of the above use cases setup with samples to demonstrate the experience and quality of deliveries to meet our requirements.

4.1.26. The Tenderer shall be able to provide digital forensic investigation support including evidence preservation, log preservation, timeline analysis and incident investigation support upon request.

4.1.27. The Tenderer shall support HKIRC in preparing incident analysis and technical information required for regulatory reporting, security audits and compliance reviews.

4.1.28. Define cyber security incident handling and response procedure

- Awarded Tenderer will be responsible to help define and develop the cyber security incident handling and response procedure(s) including process workflow, security incident classification and agreed service level agreement (SLA), etc.
- Awarded Tenderer needs to provide the detailed methodology and solution approach description, how to develop the best-fit incident handling including the detection, and response processes and also integrate with internal procedure(s)

and system(s).

- Awarded Tenderer shall deliver cyber security incident handling and response procedure(s), and provide the different training sessions with training materials for second level support, IT operation teams and internal general staff.
- Awarded Tenderer will need to provide the proposed sample of cyber security incident handling and response procedure(s), illustrate the process flow with workflow diagram, security incident classification, and SLA, etc.
- Awarded Tenderer shall provide an incident report for each confirmed security incident containing:
  - Detection date and time
  - Affected systems
  - Investigation findings
  - Root cause analysis
  - Actions taken
  - Impact assessment
  - Recommendations

Critical Infrastructure Compliance

4.1.29. The Awarded Tenderer shall support HKIRC in complying with applicable requirements under the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653), its subsidiary requirements, applicable Codes of Practice, directions issued by the relevant regulating authority, and HKIRC's internal Critical Computer System security policies, procedures and plans.

4.1.30. The Awarded Tenderer shall promptly identify and notify HKIRC of any deficiency in the SOC, SIEM, incident-response or security-monitoring services that may affect HKIRC's ability to meet such requirements.

Critical Computer System Incident Escalation and Notification Support

4.1.31. Where an actual or suspected computer-system security incident may affect a Critical Computer System designated or identified by HKIRC, the Awarded Tenderer shall:

- immediately notify HKIRC through the agreed 24x7 escalation channels;
- provide sufficient information to enable HKIRC to determine whether the incident is serious or non-serious under the applicable CI requirements;
- provide the initial incident details required for regulatory notification, including:
  - affected Critical Computer System;
  - nature and seriousness of the incident;
  - earliest identifiable time of the incident;
  - time at which the incident was detected;
  - time at which the Awarded Tenderer and HKIRC became aware of the incident;
  - systems, functions and services affected;
  - actual or potential operational impact;
  - indicators of compromise;
  - containment and recovery actions taken or recommended; and
  - current incident status;

- provide updates at intervals agreed with HKIRC until closure; and
- support HKIRC in preparing the initial notification and subsequent written incident report required by the relevant regulating authority.

Post-Incident Regulatory Report

4.1.32. The Awarded Tenderer shall provide HKIRC with a detailed draft technical incident report and all supporting records in sufficient time for HKIRC to meet the applicable regulatory reporting deadline. The report shall include, where applicable:

- executive incident summary;
- detailed timeline;
- affected systems and critical functions;
- detection and investigation activities;
- attack vector and root cause;
- indicators of compromise;
- impact assessment;
- containment, eradication and recovery actions;
- evidence collected and preserved;
- residual risks;
- corrective and preventive actions;
- lessons learned; and
- recommendations for improving monitoring, correlation rules, playbooks and preventive controls.

CI Emergency Response Plan and Security Drills

4.1.33. The Awarded Tenderer shall support the development, maintenance, review, testing and implementation of HKIRC's computer-system security incident emergency response plan insofar as it relates to the SOC, SIEM, threat intelligence, incident investigation, containment and recovery services.

The Awarded Tenderer shall:

- participate in computer-system security drills, tabletop exercises and simulations requested by HKIRC;
- provide suitably qualified SOC and incident-response personnel;
- execute agreed incident scenarios and injects;
- record detection, escalation, decision and response times;
- provide relevant logs and evidence;
- prepare an after-action report; and
- track agreed improvement actions to closure.

CI Risk Assessment and Security Audit Support

4.1.34. The Awarded Tenderer shall provide HKIRC and its appointed assessors, auditors and regulating authorities with information, records, reports and reasonable technical assistance relating to the Services for computer-system security risk assessments, security audits and compliance reviews.

Upon request, the Awarded Tenderer shall provide:

- SOC operating procedures and playbooks;
- SIEM architecture and data-flow documentation;
- log-source inventory and coverage;

- detection-use-case inventory;
- incident and escalation records;
- user-access and privileged-activity records;
- service availability and SLA records;
- vulnerability and patching records for Tenderer-managed components;
- change records;
- evidence of testing and tuning;
- subcontractor and supply-chain information; and
- evidence supporting remediation of identified findings.

Notification of Material Changes

4.1.35. The Awarded Tenderer shall notify HKIRC in writing before implementing any proposed change that may materially affect the architecture, operation, security, location, ownership, support arrangement or resilience of services supporting HKIRC's Critical Computer Systems. The Awarded Tenderer shall provide an impact assessment and shall not implement the change without HKIRC's written approval.
Such changes include:

- replacement or relocation of the SIEM or SOC platform;
- change of SOC location;
- change of hosting or data-processing location;
- introduction or replacement of subcontractors;
- material change to log collection, retention or processing;
- material change to security architecture or remote connectivity;
- termination or replacement of a threat-intelligence source;
- product end-of-life or end-of-support;
- changes arising from sanctions or export restrictions; and
- changes that may reduce monitoring, detection, response or recovery capability.

Regulatory Cooperation and Urgent Directions

4.1.36. The Awarded Tenderer shall provide timely cooperation and technical assistance where HKIRC is required to respond to an inquiry, information request, investigation or direction issued by a relevant regulating authority concerning a Critical Computer System.

4.1.37. Where urgent action is required, the Awarded Tenderer shall make appropriately authorized technical and management personnel available on a 24x7 basis and shall implement actions approved or instructed by HKIRC, subject to agreed emergency change-control and evidence-preservation procedures.

4.2. Part B – SIEM platform with Threat Intelligence

Existing SIEM environment

4.2.1. HKIRC currently operates a SIEM platform with customized correlation rules, detection use cases, dashboards, parsers, decoders, alerting logic, and other monitoring content developed to support HKIRC's operational and security monitoring requirements.

4.2.2. The proposed SIEM platform must be able to support horizontal scaling by adding more servers to cater for growth when the demand increases, and providing the same search, report and alerting functionality from one instance to multiple instances

4.2.3. The proposed SIEM platform must provide out-of-the-box add-on apps to support the operational and security analytics of the following, but not limited to, technologies:

- AWS; Azure; Alicloud ,Vmware;
- Cisco; H3C; Checkpoint; Palo Alto; Symantec; FortiGate;
- Bluecoat; Forcepoint;
- Microsoft Office365 and Active Directory;
- Windows Infrastructure; Unix and Linux;
- Oracle/MS SQL/MySQL database etc.

Final detailed device list can be shared upon signed NDA with HKIRC.

4.2.4. The proposed SIEM platform must be able to support On-prem hardware, VM, Cloud or hybrid deployment approach, while still maintaining a single pane of glass visibility.

4.2.5. The proposed SIEM platform must be able to capture all information in the original and raw data, logs and alerts including payload information and redisplay them for purposes such as troubleshooting, analysis and other data processing needs. The proposed SIEM platform must be able to index all data from any network devices including logs, configurations, messages, traps and alerts, metrics and performance data without any custom adapters or connectors.

4.2.6. The proposed SIEM platform should incorporate Artificial Intelligence (AI), Machine Learning and advanced analytics capabilities to establish dynamic behavioral baselines, detect anomalous activities, identify potential security threats, reduce false positive and support predictive analysis for proactive threat detection and response.

4.2.7. The AI-enabled capabilities should include, but not be limited to, the following use cases and supporting controls:

- Alert enrichment with contextual information (e.g., asset criticality, business service mapping, identity context, recent change/activity, vulnerability posture, and threat intelligence);
- Correlation of multi-source alerts/events (SIEM, EDR, IAM, network, cloud, email, SaaS) to identify attack chains, reduce duplicates, and prioritize based on risk;
- Identification of anomalous behaviors and user/entity behavior analytics (UEBA) that may not be detectable through signature- or rule-based methods alone, with clear baselining and tuning approach;
- Automated triage and prioritization (e.g., grouping related alerts into incidents/cases, recommending next-best actions, and generating investigation hypotheses) with analyst-in-the-loop validation;
- Automated containment workflows that enable rapid threat mitigation, including IP address blocking, endpoint isolation through EDR controls, and real-time revocation of compromised user sessions via Microsoft Graph API, thereby reducing the window of exposure during security incidents.
- Leveraging threat intelligence workstream outputs, the solution shall automatically compile YARA rules and orchestrate agent-driven threat hunting activities to identify, investigate, and validate potential threats across the organization's environment.

4.2.8. The proposed SIEM platform must be able to correlate data from different repositories (e.g. Correlate Windows event log with EDR logs) for abnormal event detection, and trigger actions/alerts through scripts or API call with various solution vendors.

4.2.9. The proposed SIEM platform must be able to collect and index any of the data sources described below:

- Any machine data generated by applications, servers or network devices, TCP/UDP syslogs, including logs, configurations, messages, traps and alerts, performance data, data stored in Database without custom parsers or connectors for specific formats
- Flexible real-time and on-demand access to data from files, network ports, WMI, databases and custom APIs and interfaces
- Consumes archive files (such as gzip, tgz, zip, etc)
- Collecting real-time insights on mobile apps through Mobile SDKs
- Subscribes to message queues such as RabbitMQ , Redis, MQTT, JMS, Kafka

4.2.10. The proposed SIEM platform should also be able to

- Identify events in single line, multi-line and complex XML structures
- Recognize and normalize timestamps. Handles bad or missing timestamps through contextual inference
- Classify source formats dynamically

4.2.11. The proposed SIEM platform shall include a dashboard of security postures including threat activity trends, infected systems trend, access trend, traffic trend as well as showing the overall notable events.

4.2.12. The proposed SIEM platform should ensure all raw data collected by the onsite devices of the SIEM platform shall not leave HKIRC premises. Collected raw data should be kept for at least 180 days.

4.2.13. The proposed SIEM platform shall support STIX/TAXII and open IOC formats as threat intelligence source.

4.2.14. The proposed SIEM platform shall provide an incident review audit dashboard, to show reviewer activities; notable events by status; notable events by owner; and the incident closure information.

4.2.15. Awarded Tenderer shall deploy on-site security monitoring systems, including all necessary software, hardware, equipment, and communication links required for the successful delivery of the Security Monitoring and Managed Detection and Response (MDR) services. The Tenderer shall be responsible for all installation, configuration, integration, testing, and commissioning activities necessary for the operation of the services.

4.2.16. Awarded Tenderer should provide all necessary software, equipment and communication links required for the provision of the information security monitoring service. Which are expected to be owned, managed and maintained by the tenderer and configured in high availability infrastructure design.

4.2.17. Awarded Tenderer shall be responsible for applying the patches and software updates on the SIEM platform, and to work with HKIRC to provide advice on potential impacts of those security issues to the underlying technology stack provisioned by HKIRC to host those software and application, including but not limited to the operation system, infrastructure, networking and databases. The tenderer shall also at its own expense to upgrade the software, equipment and communication links where necessary.

4.2.18. Awarded Tenderer shall remove those software, equipment, and communication links provided by the tenderer and restore any necessary

system an network configuration upon termination or completion of SIEM and SOC contract.

4.2.19. The proposed SIEM licensing model shall not be constrained by Events Per Second (EPS) or similar ingestion-based licensing limits. The Tenderer shall clearly state any limitations, fair-use thresholds, storage limits or additional charges associated with log ingestion, indexing, retention or threat intelligence enrichment.

4.2.20. Awarded Tenderer shall disclose any technology, software, threat intelligence source or support dependency that may be affected by international sanctions, export restrictions or geopolitical restrictions.

4.2.21. The proposed SIEM shall provide extensive native log parsers and normalization capability covering international, local Hong Kong and Mainland China technologies. The Tenderer shall provide a list of available parsers and supported technologies.

4.2.22. Awarded Tenderer shall provide a documented process describing how SIEM correlation rules, detection logic and threat hunting content will be continuously updated using emerging cyber threat intelligence and lessons learned from incidents.

4.2.23. Awarded Tenderer shall provide onboarding support from new log sources, including log collection, parser development, normalization, testing, correlation rule development and operational handover.

SIEM Transition-in and Migration Requirements

4.2.24. The Awarded Tenderer shall be responsible for migrating all HKIRC-owned customized SIEM content from the existing environment to the proposed SIEM platform, regardless of the underlying technology platform selected by the Tenderer.

4.2.25. The Awarded Tenderer shall assess the compatibility of the existing customized content with the proposed SIEM platform and shall perform all necessary conversion, redevelopment, configuration, testing, tuning, documentation, and validation activities to ensure equivalent or improved monitoring, detection, correlation, alerting, reporting, and threat-hunting capabilities following migration.

4.2.26. The migration of existing customized SIEM content shall be included within the scope of the Services and shall not be treated as a separate chargeable change request.

4.2.27. The Tenderer shall submit a detailed transition plan for migration from the existing SOC and SIEM service provider to the proposed service. The plan shall include:

- transition governance, roles and responsibilities;
- detailed activities, milestones, dependencies and lead times;
- all one-off and recurring migration-related costs;
- migration of HKIRC-owned logs, correlation rules, detection use cases, dashboards, reports, parsers, decoders, playbooks, test cases, configurations and documentation;
- knowledge-transfer requirements;
- risk assessment and mitigation measures;
- service-continuity arrangements to prevent any monitoring or detection gap;
- parallel monitoring and validation arrangements;
- cutover, rollback and escalation procedures; and
- acceptance criteria and supporting evidence.

Critical Computer System Log Retention and Availability

4.2.28. Security logs and records relating to HKIRC's Critical Computer Systems shall be retained in searchable form for at least 180 days, or for a longer period where required by HKIRC, the applicable Code of Practice, a legal hold, an investigation, an audit or a direction from the relevant regulating authority.

4.2.29. The Awarded Tenderer shall ensure that:

- original timestamps and time zones are preserved;
- relevant systems use synchronized time sources;
- logs are protected from unauthorized modification or deletion;
- access to logs is recorded and auditable;
- logs and supporting evidence can be exported promptly in commonly readable formats; and
- relevant logs are placed under preservation hold immediately upon HKIRC's request or upon confirmation of a security incident.

Threat Intelligence

4.2.30. Threat Intelligence (TI) should be integrated and updated periodically (minimum once a day). For each collected piece of data (e.g., IP address, domain name, hash, etc.), there should be enrichment where applicable

4.2.31. Threat Intelligence must be gathered from various sources, ranging from public

sources, technical sources, dark web & deep web, Underground forums, special access sites, Code Repositories, Paste bin and human analyst. Collection of Threat intelligence from the various sources should be automated and fed into a centralized portal for investigation by analysts and escalation to HKIRC upon potential identification of true hits with supporting justification and screenshots where applicable.

4.2.32. Collect threat intelligence feeds that are related to the organisation's industry (e.g., domain name, ecommerce, hong kong dns etc.)

4.2.33. The proposed SIEM platform shall provide out-of-the-box support for integrating with over 10+ threat intelligence feeds IOC, including:

- Known malicious spyware and adware IP Address ranges;
- Malicious IP addresses;
- Bad DNS lookup;
- Bad IP reputation lookup;
- Tor lookups;

Remote access connectivity setup

4.2.34. Awarded Tenderer needs to provide the secure remote access solution between Awarded Tenderer's SOCs and client's DCs with redundancy setup:

- Dedicated leased lines with Virtual Private Network (VPN) IPsec tunnel and adequate bandwidths are required;
- All network equipment and leased lines at Awarded Tenderer's SOC together with the related setup, maintenance and insurance will be arranged and managed by Awarded Tenderer
- Awarded Tenderer should comply with network and security architecture standard and related policies.

4.2.35. Awarded Tenderer will be responsible for the management of the connectivity which includes (but not limited to) security controls, availability and stability monitoring, etc.

4.2.36. Awarded Tenderer will be responsible for the related setup and maintenance in Awarded Tenderer's SOC sites, and the delivery of the remote access connectivity design and operation document.

Note: Awarded Tenderer needs to submit the remote access solution proposal together with detailed architecture design and breakdown components, one-off / on-going costs and setup

lead-time information, as well as the on-going support and maintenance model in details.

Contractual Consideration

Contract should include all requirements from this CFT. Although the contract period is 12 + 24 months, in case the re-tendering process did not complete at the end of the current contract, HKIRC reserves the right to extend the current contracts for another 2 months, with the same terms and conditions. Also, if for any reason the contract is to be terminated before the completion of the contract period, the initiating party should give a 2-month notice in advance of the early termination date.

All vendors should propose for as many parts of the scope in the CFT as possible. HKIRC reserve the right to take up any part or parts of the each tender.

5. Limitation of Liability and Indemnity

The company submitting the tender agrees that if the company becomes the Contractor of the Project, it shall indemnify HKIRC and HKIRC against any claim, demand, loss, damage, cost, expense or liability which the company may suffer from.

Service Level Agreement (SLA), Service Credits and Contract Termination

All service provided by the Service Provider shall size and scaled to meet the agreed SLA. All equipment shall have redundancy to provide maximum uptime and service. All planned maintenance shall be notified and agreed with HKIRC four weeks in advance.

In case of the Service Provider's service level does not meet with the proposed SLA, the Service Provider shall, as part of the SLA, include a Service Credit scheme for compensation for the service which did not meet the SLA. Service Provider may propose detail scheme during the contractual negotiation stage, but will need to outline the proposed scheme within the tender for HKIRC to evaluate.

HKIRC also reserves the right to terminate the contract based on a "3-strike" principle; the Service Provider shall not break the SLA for more than three times per year. HKIRC also reserves the right to terminate the service if the service provided:

- Causes disruption and/or losses to HKIRC business and operation
- Causes service downtime without notices

Also, either party could terminate the contract, with 2-month notice, after 12th month of the contract.

Service Level Report and Review Meeting

Please provide a list of typical reports and their sample for daily and monthly reports, trend analysis report etc.

Monthly reports shall include but not limited to:

- Open incidents
- Resolved incidents
- Mean time to detect (MTTD)
- Mean time to respond (MTTR)
- Threat hunting findings
- Outstanding remediation items

Bi-monthly service review meetings should be arranged. The purpose of these is to:

Review the overall service level compliance
Technical review for the overall service performance

Service Location

The Services shall be provided in Hong Kong. The deliverables shall be delivered to the HKIRC's Data Centers and Office.

6. Information Security

The company submitting the proposal ("the company") shall acknowledge and agree that, if the company is selected as the Contractor, it shall be bounded by our Non-Disclosure Agreement (NDA) and Information Security Policy (highlights of the policies are illustrated in Appendix D). The company shall also comply with the obligations under the Personal Data (Privacy) Ordinance and any other obligations in relation to personal data.

The company shall be provided with a set of NDA after HKIRC received the company's Expression-of-Interest before the stipulated time. The NDA shall be signed and returned to HKIRC before the scheduled deadline. HKIRC will only consider proposals from companies which have signed the NDA.

The proposal should be marked "RESTRICTED" at the centre-top of each page in black colour. It must be encrypted if transmitted electronically.

Each proposal will be reviewed under the terms of non-disclosure by the HKIRC's staff and Board of Directors of HKIRC.

7. Project Acceptance

The overall project acceptance can be broken down into acceptances at various levels:-

- Completed the Setup for the SIEM and integration with HKIRC systems.
- On-boarding fort the 7X24 SOC – SOC with IR response service
- Confirmation of the UAT by HKIRC

8. Anti-collusion

(1) The Tenderer shall not communicate to any person other than HKIRC the amount of any tender, adjust the amount of any tender by arrangement with any other person, make any arrangement with any other person about whether or not he or that other person should or should not tender or otherwise collude with any other person in any manner whatsoever in the tendering process. Any breach of or non-compliance with this sub-clause by the Tenderer shall, without affecting the Tenderer's liability for such breach rules and laws or non-compliance, invalidate his tender.

(2) Sub-clause (1) of this Clause shall have no application to the Tenderer's communications in strict confidence with his own insurers or brokers to obtain an insurance quotation for computation of tender price and communications in strict confidence with his consultants/sub-contractors to solicit their assistance in preparation of tender submission.

(3) The Tenderer shall submit to the HKIRC a duly signed warranty in the form set out in Appendix A to the effect that he understands and will abide by these clauses. The warranty shall be signed by a person authorized to sign the contract on the Tenderer's behalf.

(4) Any breach of any of the representations and/or warranties by the Tenderer may prejudice the Tenderer's future standing as a HKIRC's contractor.

9. Offering Advantages

(1) The Tenderer shall not, and shall procure that his employees, agents and sub-contractors shall not, offer an advantage as defined in the Prevention of Bribery Ordinance, (Cap 201) in connection with the tendering and execution of this contract.

(2) Failure to so procure or any act of offering advantage referred to in (1) above committed by the Tenderer or by an employee, agent or sub-contractor of the Tenderer shall, without affecting the Tenderer's liability for such failure and act, result in his tender being invalidated.

10. Ethical Commitment

Prevention of bribery

(A) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, except with permission of Hong Kong Internet Registration Corporation Limited (hereafter referred to as the Organisation) solicit or accept any advantage as defined in the Prevention of Bribery Ordinance (Cap 201) in relation to the business of the Organisation. The Contractor shall also caution his directors, employees, agents and sub-contractors against soliciting or accepting any excessive hospitality, entertainment or inducements which would impair their impartiality in relation to the business of the Organisation. The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors are aware of the aforesaid prohibition and will not, except with permission of the Organisation, solicit or accept any advantage, excessive hospitality, etc. in relation to the business of the Organisation.

(B) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, offer any advantage to any Board member or staff in relation to the business of the Organisation.

Declaration of Interest

(C) The Contractor shall require his directors and employees to declare in writing to the Organisation any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract. In the event that such conflict or potential conflict is disclosed in a declaration, the Contractor shall forthwith take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(D) The Contractor shall prohibit his directors and employees who are involved in this Contract from engaging in any work or employment other than in the performance of this Contract, with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract.

The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(E) The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors who are involved in this Contract are aware of the provisions under the aforesaid sub-clauses (C) and (D).

Declaration of ethical commitment

(F) The Contractor shall submit a signed declaration in a form (see Appendix B) prescribed or approved by the Organisation to confirm compliance with the provisions in aforesaid sub-clauses (A) (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and confidentiality. If the Contractor fails to submit the declaration as required, the Organisation shall be entitled to withhold payment until such declaration is submitted and the Contractor shall not be entitled to interest in that period. To demonstrate compliance with the aforesaid sub-clauses (A), (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and handling of confidential information, the Contractor and the sub-contractors employed for the performance of duties under this Contract are required to deposit with the Organisation a copy of the internal guidelines issued to their staff.

11. Schedule

	Project schedule Tasks	To be Completed by	Remark
1	Publish of RFP	29/Sep/2026	
2	Deadline for vendors to submit proposal and quotation with Warranty Letter	20/Oct/2026 23:59pm	
3	Conclude final decision and appoint the vendor	4/Jan/2027	
4	Prepare contract and service agreement	7/Jan/2027	
5	Sign contract and service agreement with the appointed vendor	11/Jan/2027	
6	System implementation	5/Apr/2027	
7	Training	12/Apr/2027	
8	Nursing Period complete	12/May /2027	
9	Project completed with deliverables	19/May/2027	

12. Payment Schedule

The following payment schedule is recommended but interested vendors may propose their own in their tenders.

After the signed NDA, standard procurement agreement will disclose to bidder .
More detail payment terms and subject to the agreement.

	Item	Expected duration	Payment
1	SOC service	12 months	Monthly charge
2	SIEM platform with Threat Intelligence	6 weeks	One time setup charge

13. Elements of a Strong Tender

All submitted tender must follow the format as stated in Appendix C - HKIRC Proposal Requirements

Successful vendor is the one who submitted a clearly worded proposal that demonstrates the following attributes:

- a persuasive section on the company background
- international recognize certification for quality assurance
- a strong and flexible service and tools meeting HKIRC requirements with minimum customization
- high level of interaction between HKIRC and the vendor
- excellent fit with the capabilities and facilities of HKIRC
- strong company and project management team

14. Service Agreement Negotiation and Signature

The service agreement will be drawn up between the selected vendor and HKIRC, the wholly-owned subsidiary of HKIRC. HKIRC welcomes the vendor's proposal on a suitable service agreement for the project/service.

The service agreement must be signed by both parties within one week from the project/service award date. If the agreement is not signed within the said period, HKIRC will start the negotiation with the next qualified vendor on the selection list.

15. HKIRC Contacts

HKIRC Contacts information

Contacts	
Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong +852 23192303 – telephone +852 23192626 – fax http://www.hkirc.hk If you are not sure about the appropriate person to call, the receptionist can help you.	**Information Security Manager** Carter Lau +852 23193849 carter.lau@hkirc.hk **Senior IT Manager** Eddie Tse +852 23193811 eddie.tse@hkirc.hk

Appendix A – Warranty

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

Dear Sir/Madam,

Warranty

(1) By submitting a tender, the Tenderer represents and warrants that in relation to the tender of Security Operation Center and SIEM with Threat Intelligence platform:

(i) it has not communicated and will not communicate to any person other than the HKIRC the amount of any tender price;

(ii) it has not fixed and will not fix the amount of any tender price by arrangement with any person;

(iii) it has not made and will not make any arrangement with any person as to whether it or that other person will or will not submit a tender; and

(iv) it has not otherwise colluded and will not otherwise collude with any person in any manner whatsoever in the tendering process.

(2) In the event that the Tenderer is in breach of any of the representations and/or warranties in Clause (1) above, the HKIRC shall be entitled to, without compensation to any person or liability on the part of the HKIRC :

(i) reject the tender;

(ii) if the HKIRC has accepted the tender, withdraw its acceptance of the tender; and

(iii) if the HKIRC has entered into the contract with the Tenderer,

terminate the contract.

(3) The Tenderer shall indemnify and keep indemnified the HKIRC against all losses, damages, costs or expenses arising out of or in relation to any breach of any of the representations and/or warranties in Clause(1) above.

(4) Clause (1) shall have no application to the Tenderer's

communications in strict confidence with its own insurers or brokers to obtain an insurance quotation for computation of the tender price, or with its professional advisers, and consultants or sub-contractors to solicit their assistance in preparation of tender submission. For the avoidance of doubt, the making of a bid by a bidder to the HKIRC in public during an auction will not by itself be regarded as a breach of the representation and warranty in Clause (1)(i) above.

(5) The rights of HKIRC under Clauses (2) to (4) above are in addition to and without prejudice to any other rights or remedies available to it against the Tenderer.

Authorized Signature & Company Chop :

Name of Person Authorized to Sign (in Block Letters) :

Name of Tenderer in English (in Block Letters) :

Date :

Appendix B – Declaration Form by Contractor on their compliance with the ethical commitment requirements

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)
Contract No.:
Title:

In accordance with the Ethical Commitment clauses in the Contract:

1) We confirm that we have complied with the following provisions and have ensured that our directors, employees, agents and sub-contractors are aware of the following provisions:

   a) prohibiting our directors, employees, agents and sub-contractors who are involved in this Contract from offering, soliciting or accepting any advantage as defined in section 2 of the Prevention of Bribery Ordinance (Cap 201) in relation to the business of HKIRC except with the permission of HKIRC;

   b) requiring our directors, employees, agents and sub-contractors who are involved in this Contract to declare in writing to their respective company management any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract, and in the event that a conflict or potential conflict is disclosed, take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed;

   c) prohibiting our directors and employees who are involved in this Contract from engaging in any work or employment (other than in the performance of this Contract), with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract and requiring our agents and sub-contractors to do the same; and

   d) taking all measures as necessary to protect any confidential/privileged information or data entrusted to us by or on behalf of HKIRC from being divulged to a third party other than those allowed in this Contract.

Signature
(Name of the Contractor)
(Name of the Signatory)
(Position of the Signatory)
(Date)

Appendix C – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 11 - Schedule, item no. 4 for the proposal submission deadline.
Hard copies	No Hard Copy is required
Electronic copy	Electronic copy is mandatory. It shall be sent by email to **itprocurement@hkirc.hk** and **alvin.yip@hkirc.hk;** also cc eddie.tse@hkirc.hk and carter.lau@hkirc.hk
Proposal format	Specified in this document
Page count	40 pages or fewer
Font	Electronically published or typed. Times New Roman 12 point font.

1. **Proposal Content**

The proposal should contain the following:

- Cover Page
- Executive Summary
- Conflict of Interest Declaration
- Company Background
    - Financial Situation
    - Track Records
    - Organization and management team
    - Project team with credentials
    - Company credentials
    - Staff credentials
- Methodology
- Project management methodology
- Understanding of our requirements
- Knowledge and Advices on Projects/Services
- Deliverable and Services level
- Proposed Cost of Services and Payment Schedule
- Implementation Time Table
- Commercial and Payment Terms. e.g. Compensation for delay.

2. Cover Page

Prepare a non-confidential cover page with the following information in the order given.

Cover Page		
Project Title		
		HKIRC SOC and SIEM
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

Executive Summary

The executive summary provides a brief synopsis of the commercial and technical solution the vendor proposed for the project/service. This summary must be non-confidential. It should fit on a single page.

The executive summary should be constructed to reflect the merits of the proposal and its feasibility. It should also clearly specify the project/service's goals and resource requirements. It should include:

- Rationale for pursuing the project or service, the methodology/technology needed and the present state of the relevant methodology/technology.
- Brief description of the vendor's financial situation.
- Brief description of the vendor's facilities and experience on similar projects or services

Conflict of Interest Declaration

- Declare any conflict of interest in relation to the project and the '.hk' ccTLD registry HKIRC.

Company Background

- The vendor must describe its company background. Major activities, financial situation, organizational structure, management team and achievements in similar projects/services or service outsourcing of the company should be elaborated. Track records are preferred.
- List the key technical and management personnel in the proposal. Provide a summary of the qualifications and role of each key member.

Methodology

The vendor must describe the methods to be used, and briefly explains its advantage and disadvantage. Track records are preferred.

Project Management Methodology

The vendor must describe the methods to be used, and briefly explains its advantage and disadvantage. Track records are preferred.

Understanding of our requirements

The vendor shall describe their understanding of our requirements. With the use of a table, the vendor should clearly state their compliance on the requirements listed in the scope of service section; and briefly explain how they are achieved.

Knowledge and Advices on Projects/Services

The vendor should describe their knowledge and advices to ensure the success of this project/service or projects/services with similar nature.

Deliverable and Services level

The vendor should detail the project/service deliverables, and the services level of the proposed services. Tables of content of all reports included in the deliverables should be

provided in the proposal.

Proposed Costs of Service and Payment Schedule

The vendor should provide the breakdown of the cost of the whole project/service. The cost shall be broken down by milestone/phases. The payment shall be scheduled based on the milestones and/or deliverables.

Such costs should include, if applicable:

- Fixed setup cost (i.e. CAPEX on SOC & SIEM)
- Labour unit costs for additional services or requirements. They are typically quoted in unit man day. Quoted in normal working hour, non-working hour and in emergency.
- Equipment that is permanently placed or purchased for HKIRC to complete the project or service, if any.
- Subsequent support, maintenance or consultation service. (i.e. Monthly OPEX with reference 3 years TCO)
- Other direct costs including services, materials, supplies, postage, traveling, pocket money, etc .

Implementation Timetable

The vendor should present in this section the implementation schedule of the project/service. The schedule should be realistic and achievable by the vendor.

Commercial and Payment Terms

The vendor should describe the commercial and payment terms of the services e.g. compensation for the delay of the project/service.

Appendix D – HKIRC Information Security Policy

An Extract Relevant to Outsourcing

This document provides an extract of the HKIRC Information Security Policy (the "Policy") with the purposes of (a) introducing various measures and controls to be executed by HKIRC regarding outsourcing, and (b) setting the expectation of any potential contractors that their participation and conformance in these measures and controls are essential contractual obligations.
The original Policy applies to HKIRC's employees, contractors, and third-party users. However, a potential contractor may interpret the clauses up to their roles and responsibilities only. Nonetheless, the keyword "Contractors" hereby refer to all relevant staff of the contractor and of any other subcontractors under the contractor's purview.
Herein, HKIRC would also set the expectation of any potential contractors that upon their indication of interest to the project, they shall be required in the subsequent stages to sign off a non-disclosure agreement ("NDA") on all information to be provided.

**<->><->><->><

accordance with established policies and procedures of the Organization.

7.2.2 All employees of the Organization and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

7.3 TERMINATION AND CHANGE OF EMPLOYMENT

Security objective: To ensure that employees, contractors and third party users exit the Organization or change employment in an orderly manner.

7.3.2 All employees, contractors and third party users shall return all of the Organization's assets in their possession upon termination of their employment, contract or agreement.

7.3.3 The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

14. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

14.2.7 The organization shall supervise and monitor the activity of outsourced system development.

16. INFORMATION SECURITY INCIDENT MANAGEMENT

16.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

Security objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.3 Employees and contractors using the Organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or service.