Request for Proposal

No. EA/02-28-2024

For Supply of Security Information and Event Management (SIEM) Solution

1. Bids are invited from potential Companies for supply of Security Information and Event Management (SIEM) Solution as per RFP Annexure. This bid Document is also available in Etisalat website (www.etisalat.af, Tenders).

2. RFP Deadline is **26-September-2024**. The bids shall be submitted though email (snabizada@etisalat.af) and marked clearly with **RFP name, number.**

Note: If you submit your commercial part of proposal by email, please provide it in **password protected document/format**. We will request the password once here the concerned committee started the bid's commercial evaluation.

3. Bid received after the above deadline shall not be accepted.

4. Local and international firms can send their offer via email to snabizada@etisalat.af and copy Ihsanullah@etisalat.af.

5. Etisalat Afghanistan reserves the right to accept or reject any or all bids and to annul the bidding process at any time, without thereby incurring any liability to the affected bidder(s) or any obligations to inform the affected bidder(s) of the grounds for Etisalat Afghanistan action.

6. Bidder should be registered with Etisalat Afghanistan in Vendor Registration List. If any interested bidder **is not registered**, first they should fill the attached Vendor Registration Form and provide following documents before tender deadline and submission of bid. Bidder's offer will not be considered without registration process**.**

1- Company Profile
2- Business License
3- President and Vice President ID Cards/Tazkira Copies
4- Article of Association (اساسنامه)
5- Past Performance:

Firm must describe past performance on similar public and or private agency contracts, including past performance on similar works for any other telecom company.

7. All correspondence on the subject may address to Shoaib Nabizada, Sr. Analyst Procurement & Contracts, and Etisalat Afghanistan. Email snabizada@etisalat.af and Phone No. 0781204113.

Ihsanullah Zirak
Director Procurement and Supply Chain
Ihsan Plaza, Shar-e-Naw, Kabul, Etisalat Afghanistan
E-mail**:** ihsanullah@etisalat.af

Request for Proposal

(RFP)

For

Security Information and Event Management (SIEM) Solution

1. DEFINITIONS

In this document, the following terms and meanings shall be interpreted as indicated:

1.1 Terms.

"Acceptance Test(s) "means the test(s) specified in the Technical Specifications to be carried out to ascertain whether the Goods, Equipment, System, Material, Items or a specified part thereof is able to attain the Performance Level specified in the Technical Specifications in accordance with the provisions of the Contract.

"Acceptance Test Procedures" means test procedures specified in the technical specifications and/or by the supplier and approved by EA as it is or with modifications.

"Approved" or "approval" means approved in writing.

"BoQ " stands for Bill of Quantities of each job/work as mentioned in this contract and its annexes according to which the contractor shall supply equipment & services and subject to change by agreement of both parties.

"Bidding" means a formal procurement procedure under which sealed bids are invited, received, opened, examined and evaluated for the purpose of awarding a contract.

"Bid/Tender Document" means the Bid/Tender documents issued by EA for invitation of Bids/Offers along with subsequent amendments and clarifications.
"CIF" means "Cost Insurance Freight" as specified in INCOTERM 2010.

"Competent Authority" means the staff or functionary authorized by EA to deal finally with the matter in issue.

"Completion Date" means the date by which the Contractor is required to complete the Contract.

"Country of Origin" means the countries and territories eligible under the rules elaborated in the "Instruction to Bidders ".

"Contract" means the Contract between Etisalat Afghanistan (EA) and the Contractor and comprising documents.

"Contractor" means the individual or firm(s) ultimately responsible for supplying all the Goods/Equipment/Systems/Material/Items on time and to cost under this contract to EA.

"Contractor's Representative" means the person nominated by the contractor and named as such in the contract and approved by EA in the manner provided in the contract.

"Contract Documents" means the documents listed in Article (Contract Documents) of the Form of Contract (including any amendments thereto) or in any other article in this contract.

"Contract Price" means the price payable to the Contractor under the Contract for the full and proper performance of its contractual obligations.

"Day" means calendar day of the Gregorian calendar.

"Delivery charges" means local transportation, handling, insurance and other charges incidental to the delivery of Goods to their final destination.

"D.D.P" means Delivered Duty Paid as defined in the Incoterms 2010 including the unloading responsibility of bidder/seller.

"Effective Date" means the date the Contract shall take effect as mentioned in the Contract.

"Etisalat Afghanistan (EA)" means the company registered under the Laws of Islamic republic of Afghanistan and having office at Ihsan Plaza Charahi Shaheed Kabul in person or any person dully authorised by it for the specific purpose for the specific task within the Contract and notified to contractor in writing.

"Final Acceptance Certificate" means the certificate issued by EA after successful completion of warranty and removal of defects as intimated by EA.

"Force Majeure" means Acts of God, Government restrictions, financial hardships, war and hostilities, invasion, act of foreign enemies, rebellion, revolution, riot, industrial disputes, commotion, natural disasters and other similar risks that are outside of Contractor's and EA's control.

"Goods Receipt Certificate" means certificate issued by the consignee certifying receipt of Goods in good order and condition.

"Liquidated Damages" mean the monetary damages imposed upon the contractor and the money payable to EA by the contractor on account of late delivery of the whole or part of the Goods.

"**L.o.A**" means Letter of Award issued by EA to successful bidder with regard to the award of tender.

"Month" means calendar month of the Gregorian calendar.

"Offer" means the quotation/bid and all subsequent clarifications submitted by the Bidder and accepted by EA in response to and in relation with the Bid Documents.

"Origin" means the place where the Goods are mined, grown or produced from which the ancillary services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembling of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

"EA's Representative" shall mean the representative to be appointed by EA to act for and on behalf of EA with respect to this Contract.

"Specifications" means the specifications, provided in the Contract and its annexure and in EA Tender Specifications and where the Contract is silent and in cases of conflicting specifications appearing in the documents, based on the latest version of ITU-T recommendations.

"Supplier/Vendor" (used interchangeably) means the individual or firm ultimately responsible

for supplying all the Goods on time and to cost under this Contract acting individually alone or as a "prime contractor" for a consortium.

"Supplier's Representative" means the person nominated by the Contractor and named as such in the Contract and approved by EA in the manner provided in the Contract.

"Warranty Period" shall mean the period of 12 months or any extended period starting from the acceptance of the delivered Goods in good order and conditions at consignee's certified by EA authorized representative (s).

2. INTRODUCTION TO WORK.

2.1 Bids are invited for Supply of Security Information and Event Management (**SIEM**) Solution in accordance with Etisalat specifications as per Annexure A.

3. Scope of Work

As per Annexure –A

4. Validity of Offers

The Tenders must be valid for a minimum of 90 days from the Tender closing date, or as may be specified by Purchaser in the Tender documents.

5. Price:

5.1 International Bidders can quote CIP Kabul and Local Bidders shall quote DDP Kabul prices accordingly.
5.2 DDP Prices shall be inclusive of Custom Duties and all Taxes as applicable in Afghanistan as per Islamic Republic of Afghanistan Tax Laws.

6. Payment Terms.

6.1 Payment mode:
6.1.1 License/Software Part: 100% of payment after delivery.
6.1.2 Professional Services/Implementation Part: 100% of payment after completion of project and RFS.
6.2 Payment shall be made by bank transfer after receipt of original Hardcopy of invoice.
6.3 Advance payment will be not made to contractor.
6.4 EA shall make prompt payment, within thirty days of submission of an invoice/claim by the contractor subject to availability of pre requisite documents specified under the contract and adjustment of penalty (if any) on account of late delivery and/or defective Goods replacement after confirmation from Project Director.
6.5 Payments are subject to deduction of income tax at prevalent rate from the relevant invoices of the contractor and paid to the Tax Authorities, except those especially exempted by the authorities. EA will issue certificate of deductions to the contractor to enable him to settle tax returns with the concerned authorities.

6.6 "Etisalat Afghanistan has full right to issue the PO/Contract payments via mHawala (mobile financial services) system to your mHawala account".

7. Construction of Contract:

The Contract shall he deemed to have been concluded in the Islamic Republic of Afghanistan and shall be governed by and construed in accordance with Islamic Republic Afghanistan Law.

8. Termination of the Contract:

9.1 If during the course of the Contract, the Contractor shall be in breach of the Contract and the Purchaser shall so inform the Contractor by notice in writing, and should the breach continue for more than seven days (or such longer period as may be specified by the Purchaser) after such notice then the Purchaser may immediately terminate the Contract by notice in writing to the Contractor.

8.2 Upon termination of the Contract the Purchaser may at his option continue work either by himself or by sub-contracting to a third party. The Contractor shall if so required by the Purchaser within 14 days of the date of termination assign to the Purchaser without payment the benefit to any agreement for services and/or the execution of any work for the purposes of this Contract. In the event of the services/jobs being completed and ready for utilization by the Purchaser or a third party and the total cost incurred by the Purchaser in so completing the required services/jobs being greater than which would have been incurred had the Contract not been terminated then the Contractor shall pay such excess to the Purchaser.

8.3 The Contractor shall not have the right to terminate or abandon the Contract except for reasons of force majeure.

9. Local Taxes, Dues and Levies:

9.1 The Contractor shall be responsible for all government related taxes, dues and levies, including personal income tax, which may be payable in the Afghanistan or elsewhere.

9.2 Withholding tax (if applicable) shall be deducted on local portion only as per prevailing rates as notified Islamic republic of Afghanistan. The amount of withholding Tax(s) is 2% of all project cost for local/registered companies who have Afghanistan Government Official Work License and 7% for International/ nonregistered companies.

Annexure-A

Implementation of New SIEM Solution
Security Information and Event Management

Scope of Work for SIEM Solution:

1.0 Introduction:

Etisalat Afghanistan is committed to enhancing its security infrastructure to safeguard critical assets and ensure the highest levels of data protection and threat management. As part of this commitment, we are seeking a qualified supplier to provide a comprehensive Security Information and Event Management (SIEM) solution. This SIEM solution will play a pivotal role in monitoring, detecting, and responding to security threats across our diverse IT & Telecom environments.

2.0 Objective

Etisalat Afghanistan is seeking a qualified supplier who can supply, install, commission and maintain security information and event management (SIEM) tool that meet the following objectives.

1) Windows Domain Controller
2) Windows and Linux Servers
3) Customize OS (CGSL)
4) Windows Endpoints
5) Exchange Servers
6) Web, DNS and DHCP Servers
7) VMware
8) Databases (SQL Server, mySQL, Mongo DB, Postgre SQL & Oracle database)
9) Application Servers
10) Vulnerability Scanners
11) Load Balancers
12) WLAN Controller
13) Next Gen Firewalls
14) Web Application Firewalls
15) Web Proxies
16) Network Switches
17) Cisco Routers & Switches
18) ZTE Routers & Switches
19) Huawei Routers & Switches
20) Dell Switches
22) EMC Networker Backup Solution
23) Endpoint Detection & Response (EDR)
24) Network Detection & Response (NDR)
25) PAM
26) IAM
27) NAC
28) MFA

29) ZTNA
30) Firewall Analyzer
31) Firewall Manager
32) AD security tools
33) Service Desk solution
34) In-house web applications
35) Any network device with non-standard log format like telecom devices.
36) We would require scalability for integration with different platforms for the future.

3.0 Scope of Work

1) Supply, installation and commissioning of security information and event management (SIEM)tools as per requirements specification provided in section 2.0.
2) Supply and Installation of security information and event management (SIEM) tool Licenses and related software utilities / add-ons.
3) The bidder should ensure the license deliver to Afghanistan and there should be no restrictions on.
4) The bidder should confirm the type of license (Perpetual, Term or subscription) and ensure the license is cost-effective.
5) The bidder should include overseas/online training for 6 engineers. and confirm both type of training (overseas and online).
6) End to end Documentation of SIEM solution.
7) OEM Professional Services for end-to-end integration, creating use cases, fine tuning and creating rules based on requirements.
8) The solution should be on-premises.
9) The solution should support redundancy and high availability (HA).
10) The event per second (EPS) should be at least 150,000 or 200,000. And can handle the required traffic load.
11) The bidder should provide hardware requirements for the solution.
12) The solution firmware and software should be patched to the latest stable version released by OEM.
13) The Solution implementer must ensure the security patches applied before placing them in the production environment.
14) Any proposed solution should have 3 years standard warranty with support for up to 7 years extended life, and it should not be marked as end of sales.
15) Cloud security measurements (if any) should be applied and validated by the solution implementer (vendor).
16) The solution should support the MFA for system URL console access.
17) The vendor should clearly specify the timeline for implementation.
18) The vendor should provide a detailed Service Level Agreement (SLA) that outlines response times, resolution times, and penalties for not meeting the agreed-upon service levels.

4.0 SIEM Tool General Technical Requirements

SIEM should meet the following requirements:

1) Log collection.
2) Log aggregation and normalization.
3) Log archival.
4) Alert generation.
5) Log and Event correlation.
6) File integrity monitoring
7) User activity monitoring.
8) Log forensics, Analysis and Auditing.
9) Compliance reporting.
10) Dashboard and Reports.
11) Incident management.
12) Database activity monitoring features.
13) Vulnerability assessment and management.
14) Integration with the devices and applications.
15) The solution agent should support centralized deployment
16) Proof of concept testing of the SIEM solution.

4.1 SIEM Detailed Technical Specifications

Bidders shall use the following options to indicate the "DEGREE OF SUPPORTOF COMPLIANCE" their solution provides for each of requirements given in table below:

a. **FS - (Fully Supported)** the application fully supports the requirement without any modifications.
b. **PS - (Partially Supported)** the application supports the requirement with use of a system or workflow workaround.
c. **NS - (Not Supported)** the system is not capable of supporting the requirement and cannot be modified to accommodate the requirement.

Table 1: Detailed technical specifications:

#	Requirements	FS	PS	NS	Comments
1.	**SIEM Architecture and Deployment**				
1.1	Software-as-a-service (SaaS) deployment model to keep costs low and simplify upgrades.				
1.2	The solution should be on-premises and VM base.				
1.3	Multi-tenancy deployment options for complex and geographically spread Etisalat 5 hops.				
1.4	Granular role-based access control (RBAC) to restrict permissions and access.				
1.5	Smooth migration process with reasonable timeline, clear expectations and customized configuration options.				

1.6	Flexible training options to help your team ramp up, gain confidence and achieve mastery to operate your new SIEM deployment.				
1.7	Effortless maintenance and timely updates to protect against emerging threats and address any issues.				
1.8	Reliable support services with skilled personnel and service-level agreement (SLA) terms.				
1.9	Regular cadence of new product releases that prioritize efficiency and user experience.				
2. Data Onboarding, Processing & Management					
2.1	Built upon existing high-fidelity endpoint data and extended to third-party data for full visibility.				
2.2	Variety of data connectors available out-of-the-box across IT and security domains.				
2.3	Readily available data parsers to ensure access and readability for faster analysis.				
2.4	HTTP event collector (HEC) to easily onboard custom data sources and leverage parsers to normalize data ingest.				
2.5	Unified fleet management for log collectors to easily monitor data ingest and health.				
2.6	Robust API capabilities to ensure secure, easy data sharing with applications.				
2.7	Support for data pipelines to move data efficiently and route it into your SIEM.				
2.8	Petabyte-scale data ingestion to onboard new data into your SIEM fast.				
2.9	Index-free ingestion to speed up data retrieval and efficiently use available resources.				
2.10	Data normalization for different information fields and data formats for faster analysis.				
2.11	Out-of-the-box parsers to convert data into a suitable format to structure data.				
Native ecosystem components to reduce interoperability friction across siloed tools, such as:					
2.12.1	Extended detection and response (XDR).				
2.12.2	Endpoint detection and response (EDR).				
2.12.3	Threat intelligence.				
2.12.4	Cloud-native application protection platform (CNAPP).				
2.12.5	Identity threat detection and response (ITDR).				
2.12.6	Next-generation antivirus (NGAV)				
2.12.7	Next-generation Firewall				
2.12.8	Data protection				

2.12.9	Exposure management				
2.13	Sub-second latency to process logs, alert on threats and make data actionable in real time				
2.14	Freedom to access your data whenever, wherever and in any way, you need it.				
2.15	Multiple search options, from free-text search to advanced RegEx search for patterns.				
2.16	Lightning-fast, scalable search across large datasets and growing data volumes.				
2.17	Single, cross-platform query language that is user-friendly to overcome the entry barrier				
2.18	Metrics dashboard to assess system health, manage data and predict usage				
	Dashboard:				
2.19	Solution should provide web-based facility to view security events and security posture of the Organization				
2.20	Solution should have drill down capability to view deep inside the attack and analyze the attack pattern.				
2.21	Should be able to configure custom alerts and notifications?				
2.22	Dashboard should support export of data to multiple formats including CSV, XML, Excel, PDF, word formats.				
3.	**Analytics**				
3.1	Sensible, high-fidelity correlation rules — available out-of-the-box — that are continuously tested and easy to tune.				
3.2	Wide range of ready-to-use detections across various security domains, such as: (**Endpoint, Cloud, Identity, Network, Email & Application**)				
3.3	Support for open detection sharing, such as Sigma, YARA and Snort rules				
3.4	Use of generative AI (GenAI) to allow analysts of all skill levels to do more with less by answering analyst questions in plain language				
3.5	GenAI-powered analysis to sift through large data volumes and detect anomalies.				
3.6	Behavioral analytics that leverage statistical analysis and machine learning (ML) like user and entity behavior analytics (UEBA).				
3.7	AI-driven anomaly detection to identify abnormal users by creating dynamic peer groups				
3.8	Contextual enrichment with techniques and				

	tactics from the MITRE ATT&CK® framework				
3.9	Ability to tag and enrich parsed data with high-quality threat intelligence that provides confidence-rated indicators of compromise (IOCs), malware context, campaign information and adversarial names.				
3.10	Detection coverage mapping against the MITRE ATT&CK framework for quick action.				
3.11	Out-of-the-box popular use case dashboard visualizations for at-a-glance visibility				
3.12	Customizable dashboards and preferential views that can build on any query to analyze and display your data.				
3.13	Inclusion of documented threat hunting queries — regularly updated and extracted from the latest threat intelligence insights — to discover the most advanced adversaries.				
3.14	Analytics workflow to operationalize threat hunting processes and reduce the manual effort needed to create, validate, tune and operationalize threat queries.				
3.15	Third-party testing of detection and protection capabilities, such as MITRE Engenuity ATT&CK and SE Labs evaluations, with superior results.				
4.	**Incident Investigation and Response**				
4.1	Alert prioritization based on severity and grouping to sift through the noise faster.				
	Comprehensive incident management that enables incident creation from a detection — or a group of related detections — to keep incident information organized.				
4.2	Fully integrated security orchestration, automation and response (SOAR) capabilities included standard.				
4.3	Intuitive, no-code workflow builder to automate any use case and carry out any task.				
4.4	Many out-of-the-box workflow templates for popular use cases with customizable options.				
4.5	Workflow automation triggered based on events or detections, scheduled or on demand				
4.6	Broad integrations ecosystem across security domains and IT tools, such as IT service management (ITSM) tools.				
4.7	Bidirectional integration between SIEM and SOAR to ensure information sharing.				

4.8	Ability to automate routine investigative tasks such as correlations and data collection.				
4.9	Integration with industry-leading, adversary-focused threat intelligence for threat reports, threat profiles, technical reports, malware sandbox and daily IOC reports on emerging threats.				
4.10	Threat intelligence spanning over 230 distinct adversaries based on analysis of trillions of endpoint-related events per week.				
4.11	Advanced investigation visualizations, such as graph views to understand entity relationships and attacker paths, and timeline views to understand the progression of an attack.				
4.12	Real-time collaboration for analysts to share and document findings.				
4.13	Ability to send notifications via your preferred communication method, such as email or others.				
4.14	Flexibility to automate any use case with numerous prebuilt response actions.				
4.15	Tight EDR agent integration to execute any action on the endpoint, such as network isolation, quarantine, real-time response and more.				
4.16	Integration with any HTTP-based API to create actions in low-code or full-code.				
4.17	Historical data access to enable threat hunting use cases across large volumes of data.				
4.18	Ability to create custom applications to deploy more use cases and bridge product gaps				
4.19	Ability to customize your existing security operations platform with a purpose-built, integrated low-code application platform (LCAP).				
4.20	GenAI-powered investigation engine that allows analysts to generate summaries of incidents in plain language with recommended next steps.				
5.	**Security Orchestration, Automation, and Response (SOAR)**				
	Automation:				
5.1	Automated Playbooks: Must implement automated response actions for common security incidents like blocking IP addresses, isolating endpoints & disabling user accounts.				
5.2	Task Automation: Should automate repetitive tasks such as log analysis, threat intelligence enrichment, and incident ticket creation				

5.3	Automated Remediation: Must automatically execute predefined remediation steps for detected threats.				
5.4	**Orchestration:**				
5.5	Integration with Security Tools: Must orchestrate workflows across various security tools and platforms, including firewalls, endpoint protection, intrusion detection/prevention systems (IDS/IPS), and cloud security solutions.				
5.6	Unified Incident Management: Must provide a unified incident management interface that consolidates alerts and events from multiple sources, enabling a cohesive response strategy.				
5.7	**Playbooks:**				
5.8	Predefined Playbooks: Must include predefined incident response playbooks for common attack scenarios, such as phishing attacks, malware infections, and data breaches.				
5.9	Customizable Playbooks: Should allow customization of playbooks to tailor incident response processes to the organization's specific requirements and procedures.				
5.10	Interactive Playbooks: Should support interactive playbooks that guide analysts through manual and automated steps during incident response.				
6.	**Threat Intelligence**				
6.1	**Real-Time Threat Intelligence:**				
6.2	Integration with Multiple Feeds: Should integrate with multiple external threat intelligence feeds, such as commercial providers, open-source feeds, and industry-specific feeds.				
6.3	Dynamic Threat Database: Should maintain an up-to-date threat database that includes information on known indicators of compromise (IOCs), such as IP addresses, domain names, URLs, file hashes, and malware signatures.				
6.4	Automated Threat Updates: Should automatically update threat intelligence data to ensure the SIEM is always armed with the latest threat information.				
6.5	**Threat Enrichment:**				
6.6	Contextual Data: Should enrich security events with additional contextual information from				

	threat intelligence feeds, such as the severity of a threat, associated threat actors, attack methods, and targeted industries.				
6.7	Automated Enrichment: Should automatically add threat intelligence data to incoming security events, enabling faster and more informed decision-making by security analysts.				
6.8	**Threat Hunting**				
6.9	Advanced Search Capabilities: Should provide advanced search capabilities to allow analysts to proactively search for threats within the environment based on IOCs and other threat intelligence data.				
6.10	Hunting Playbooks: Should include predefined threat hunting playbooks that guide analysts through the process of identifying and investigating potential threats.				
6.11	Hypothesis-Driven Hunts: Should allow analysts to create and test hypotheses about potential threats based on emerging threat intelligence.				
7.	**Cloud Security Monitoring**				
	Cloud Log Collection:				
7.1	Multi-Cloud Support: Should collect logs from multiple cloud-based applications such as EDR, Adobe Sign, Azure AD, Microsoft 365 and so on				
7.2	API Integration: Should use APIs to collect logs and events from cloud services and applications.				
	Cloud Threat Detection:				
7.3	Cloud-Specific Rules: Should implement threat detection rules specific to cloud environments to identify unauthorized access, and other cloud-specific threats.				
7.4	Cloud Activity Monitoring: Should monitor cloud activities such as user logins, file access, and configuration changes				
8.	**Data Retention, Privacy and Compliance**				
8.1	flexible long-term data retention options for data that is always accessible and always high-speed				
8.2	Scheduled on-demand reporting capabilities for audits and compliance and the ability to keep a security system of record				
8.3	Masking and obfuscation capabilities to meet privacy and protection requirements				
8.4	Online retention logs should be for the 6 months				
8.5	Offline archived retention logs should be for the				

	12 months				
9.	**Services**				
9.1	24/7 expert-led managed detection and response (MDR) coverage across critical attack vectors: endpoint, cloud, identity and third-party data, such as email, network detection and response (NDR), firewall and more.				
9.2	Certified security analyst team with in-depth technology knowledge.				
9.3	Integrated threat intelligence for full attack context and the latest IOCs.				
9.4	Proactive human-led threat hunting to uncover sophisticated adversary tradecraft.				
9.5	Surgical threat remediation in true end-to-end fashion, including full cleanup to original state without costly reimaging or downtime.				
9.6	Breach prevention warranty without red tape to cover the costs of a breach should one ever occur within a protected environment				
9.7	Efficacy of attack detection coverage as denoted by MITRE ATT&CK evaluations.				
9.8	Industry and analyst recognition to validate expert-driven protection through services.				
9.9	Implementation and operational services to accelerate configuration and tuning.				
9.10	Wide ecosystem of service providers for additional strategic support				

5.0 Current infrastructure:

Table 2: Current environment in Etisalat Afghanistan.

#	Environments	Description	FS	PS	NS	Comments
1.1	Windows Server	Windows 2012, 2016, 2019,2022,2023,2024, Standard Editions and customized windows OS.				
1.2	Linux	Redhat 6, Redhat 7 and higher version, SUSE 9, SUSE 10, SUSE 11 and higher version, CentOS 7 & Customize CGSL V3 & V4, Solaries 5.9 version 2.1, and all customized based OS.				
1.3	Unix	AIX 5, AIX 6 and higher version, Solaris 10, Solaris 9 and higher version, Oracle Linux and customized based UNIX OS.				
1.4	Ubuntu	Ubuntu 22.04 LTS, Ubuntu 18.04.5, Ubuntu 20.04.5 & CentOS 7.9.2009.				

1.5	Customized OS	Euler OS, NewStart CGS Linux, Red Hat Enterprise Linux AS realse 4 & Dopralinux				
1.6	Virtualization	VMware (ESXI & Vecenter), vSphere & RHVH, Open Stack and Oracle Linux Virtualization.				
1.7	Database Server	Unified audit log option should support for SQL Server, SQLite, mySQL, Mongo DB, Postgre SQL & Oracle database.				
1.8	Application Logs	IIS, Apache, Tomcat, OpenJDK, Web Servers (Apache, Nginx), Application Servers (Tomcat, WebLogic), Email Servers (Microsoft Exchange).				
1.9	Software Applications	Office applications, Office365, D365 ERP, Active Directory, SAP, BI & DLP, NewStart HA Cluster, NEC Cluster, Active Directory & DNS.				
1.10	Security Environments	Firewalls, EDR, NDR, ZTNA, PAM, IAM, NAC, MFA, Analyzer, Manager, WAF, DLP, appliance DNS Box & vulnerability Scanner.				
	Huawei Devices	**OS Type**				
1.11	ATN 910C-G	Huawei VRP V800R021C10SPC600				
1.12	ATN 980B	Huawei VRP V300R005C10SPC100B730 (V300R005SPH380)				
1.13	ATN 980C	Huawei VRP V800R022C00SPC600B828 (V800R022SPH120)				
1.14	NE40E-X8A	Huawei VRP V800R022C10SPC500B663 (V800R022SPH226)				
1.15	Huawei CE6863E-48S6CQ	Huawei VRP V200R022C00SPC500B123 (V200R022SPH010)				
1.16	Could Engine S12700E-8					
1.17	Huawei NetEngine 8000 M14	Huawei VRP V800R012C00SPC300B887 (V800R012SPH021)				
	Dell Devices	**OS Type**				
1.18	Dell EMC S4148F-ON	Dell OS10 10.5.4.7				
1.19	Dell EMC	Dell OS10 10.5.4.3				

	S5248F-ON					
	ZTE Devices	**OS Type**				
1.20	5950-60TM	ZTE ZXR10 3.03.10.B45				
1.21	5950-60TM-E	ZTE ZXR10 3.07.02.01B6				
1.22	5952E	ZTE ZXR10 3.01.10.B31P02				
1.23	5960	ZTE ZXR10 5.00.00R6P150				
1.24	5960 STACK	ZTE ZXR10 5.00.00R6P80				
1.25	5960-4M-HC	ZTE ZXR10 5.00.00R6P150				
1.26	5960X-54DU-HF	V6.00.00.84P01				
1.27	8902E	ZTE ZXR10 3.05.00R4B40				
1.28	9904-S	ZTE ZXR10 2.00.00R8P16				
1.29	5960X-56QU-HF	V6.00.00.84P01				
1.30	M6000-3S	ZTE ZXR10 00				
1.31	ZXR10_5952E	ZTE ZXR10 2.8.23.C.16.P17, ROS 4.08.24R2				
1.32	ZXR10_GAR	ZTE ZXR10 2.6.02, ROS 4.6.02				
	Cisco Devices	**OS Type**				
1.33	Cisco AIR-CT5520-K9	Cisco IOS 12.2(46)SE (LANLITEK9)				
1.34	Cisco C9200L-24P-4X	Cisco IOS-XE Amsterdam 17.03.04				
1.35	Cisco C9200L-24T-4X	Cisco IOS-XE Amsterdam 17.03.03				
1.36	Cisco C9200L-48T-4X	Cisco IOS-XE Amsterdam 17.03.04				
1.37	Cisco C9500-48Y4C	Cisco IOS-XE 17.03.04				
1.38	WS-C2960					
1.39	WS-C3560-24TS-S					
1.40	WS-C3560V2-24PS-S					
1.41	WS-C3560V2-24TS-SD					
1.42	WS-C3560V2-48PS-E					
1.43	WS-C3560V2-PS-S					
1.44	WS-C3560X-48T-E					
1.45	WS-C3750-48PS-E					
1.46	WS-C3750-					

	48TS-S					
1.47	IDRACs	All Servers IDRACs & ESXI Management.				
1.48	Backup & Storage Logs	Backup Solutions (EMC Networker)				
1.49	Data Centers	7 hops (Kabul: 3 DC, Regional: 4)				
1.50	Additional Logs for future scalability	Ensure scalability for integration with additional platforms and services				
Note: The bidder should verify and confirm the SIEM solution should support all the existing environments as outlined in this table. Compatibility and support for each environment are essential.						

Annexure – B

General Security Requirements:

1. Vendor must ensure their operating systems are up to date and is not End of Life/End of Support.
2. Vendor must ensure proper patch management of their servers in alignment with EA IT and Cybersecurity policies.
3. Vendor must ensure a licensed and standard AV solution is installed in all of their operating systems.
4. Vendor must ensure full cooperation and coordination with EA Cybersecurity team whenever required.
5. Vendor must not install any application without proper coordination and agreement of EA SOC Team.
6. The use of insecure cryptographic algorithms and protocols are strictly prohibited and all integrations and system communication must be based on secure and strong cryptographic algorithms.
7. Vendor must ensure strong protection of EA data stored on vendor's cloud.
8. Vendor must align all of their services and configurations in accordance to EA Information Security policies and standards.
9. Vendor must use and install only licensed applications.
10. The installation and Integration of servers must be aligned with IT and Cybersecurity requirements.
11. Vendor must not use/install any application/service that is not required.
12. Vendor must communicate any software installation with EA Cybersecurity team in advance.
13. Vendor must align their changes according to EA Change Management Policy.
14. Vendor must ensure all their operating systems are fully patched with the latest OS/Software updates.
15. Vendor must not use any OS that is/will be End of Life / End of Support in less than 3 year.
16. Only secure and strong cryptographic algorithms are allowed to be used in the vendor platforms.
17. System must support Role Based Access Control, and Rule Based Access Control
18. System must provide Strong authentication and authorization mechanisms
19. System must be capable of advanced logging mechanisms to ensure user activities are logged for audit and security purposes and the log must include all of the following at minimum.
    - Failed and successful logins
    - Modification of security settings
    - Privileged use or escalation of privileges

- System events
- Modification of system-level objects
- Session activity
- Account management activities including password changes, account creation, modification…
- Event logs must contain the following details:
- Date and time of activity
- Source and Destination IP for the related activity
- Identification of user performing activity
- Description of an attempted or completed activity.

20. The system must support live log retention of 1 Year and backup up to 3 years.
21. System must be capable of encrypting the log files to ensure user does not modify or change the logs.
22. System must provide cryptographic algorithms such as AES 128/256 Bit, SHA 256/384/512 bits.
23. System must be secure against well-known attacks including but not limited to SQL Injection, XSS, CSRF, SSRF, Code Execution and other attacks.
24. Vendor system's password configuration must be aligned with EA Information security policies.
25. System must support integration with LDAP, IAM "Identity and Access Management" and PAM "Privileged Access Management" Solutions.
26. System must support external log synchronization mechanisms to push logs to another system for analysis such as SIEM and centralized log server.
27. The database must support the encryption of admin user's information with algorithms such as PBKDF2 and SHA256/384/512 bits.
28. The database platforms "if any" must support the encryption of data in-transit and at rest.

Important Note:

Bidders, vendors, and any concerned party shall fill all the fields in the below table, any missing or non-compliant item may cause disqualifying the proposed system from the Etisalat Security side.

S. No.	Description	Compliance (YES/NO/NA)	Comments
1	**Etisalat Security Requirements**		
1.1	The Contractor/Supplier/vendor to sign Non-Disclosure Agreement (NDA) with Etisalat before finalizing RFx/contract/POC agreement as per Etisalat NDA process.		
1.2	Contractor/Supplier/vendor equipment's (e.g. Servers, PCs, etc.) that are connected to Etisalat network must be securely wiped before taking out of		

	Etisalat premises.		
1.3	The proposed/contracted system shall pass Etisalat Security Audit (Vulnerability Assessment/Penetration Testing) before go-live/service acceptance by Etisalat. Contractor/Supplier/vendor shall provide SLA for fixing Security gaps based on severity.		
1.4	Contractor/Supplier/vendor shall fix all security issues identified and reported by ETISALAT and/or Third Party Contracted to do the testing, with no additional cost		
1.5	Contractor/Supplier/vendor confirms that its products/solution are tested for weaknesses via methods such as Vulnerability Assessment, penetration testing, red teaming exercises and scans that check for compliance against the baseline security standards or security best practices, before the new product or any of its releases is delivered to ETISALAT. The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution.		
2	**Security Architecture**		
2.1	The Contractor/Supplier/vendor shall ensure that proposed solution shall comply with the applicable IT and Telecom Security standards (such as Afg. NESA (SIA) IA V2, Afg. DESC (ISR), Afg. TRA, 3GPP, ETSI, ENISA, CSA, NIST, PCI, ISO, GDPR etc.) The Contractor/Supplier/vendor shall confirm the applicable standard.		
2.2	The proposed solution shall support the latest operating systems and application versions. Contractor/Supplier/vendor to ensure proposed solutions will run the latest stable software, operating system, and firmware.		
2.3	The solution shall be designed with multi-tier architecture, (Demilitarized Zone (DMZ), middleware, and private network). Any system accessible from the Internet shall be on the DMZ and access to internal sensitive data shall be secured through the middle tier application proxy.		

2.4	The proposed solution shall not impact or relax existing Etisalat security control or posture.		
2.5	The performance of the proposed system shall meet the business requirements without disabling or removing any existing security control		
2.6	The Contractor/Supplier/vendor shall provide only secure methods of communication such as HTTPS, SFTP, SCP, TLS1.3, IPSEC, SRTP, SSH v2, SNMPv3 between the proposed nodes. Non-secure protocols such as Telnet, HTTP and FTP shall not be used.		
3	**Password Security**		
3.1	All Operating Systems (e.g. Linux and Windows) shall be hardened according to well-known standards such as, but not limited to NIST, CIS security benchmark, and NSA.		
3.2	The proposed system includes password management module that supports the following features:		
3.3	Setting the minimum password length		
3.4	Password complexity, and not accepting blank passwords		
3.5	Maximum password age and password history		
3.6	Account lockout		
3.7	Enforce changing password after first login		
3.8	Prompt / notify for the old password on password changes		
3.9	The password shall be saved in hashed format (i.e. irreversible encryption)		
3.10	Forgetting or resetting password function shall support using OTP or email for verification		
4	**Authentication**		
4.1	The proposed system shall not provide access without valid username and password.		
4.2	All user access to the proposed system shall support Privilege account Management (PAM) integration.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent password dictionary attacks		
4.4	For mobile applications, the proposed system shall support and uses fingerprint authentication method		

4.5	The proposed system supports and uses secure authentication protocols, like Kerberos, LDAP-S, NTLM V2 and above, HTTPs (for web applications)		
4.6	The proposed system will not use insecure authentication protocols, like NTLM v1, HTTP (for web applications)		
4.7	The proposed system shall support session timeout settings		
4.8	The proposed solution shall support secure API architecture to integrate systems to exchange data where deemed necessary.		
5	**Authorization**		
5.1	The proposed solution shall support role-based access controls that includes access profiles or security matrix (i.e. Role Name VS. Access Permissions)		
5.2	The proposed system supports role-based access permissions, i.e. Administrator, Operator, Viewer, User…		
6	**Software Security**		
6.1	The software development and testing will not run on the production systems, and will be running in an isolated environment		
6.2	The software source code will not include clear-text passwords		
6.3	The software code will not include insecure protocols, like FTP, telnet ...etc.		
6.4	The software testing will not use live/production sensitive or PII data unless it's masked as Etisalat security policy		
6.5	The proposed system enforces input and output validation to prevent security attacks, like SQL Injection, Buffer Overflow…etc.		
6.6	For web portals, the proposed system includes all security controls to prevent / protect from OWASP Top 10 security attacks and risks		
6.7	For mobile application, the proposed system shall include security checks / controls to protect from mobile attacks, like SSL Pinning, Jailbreak, Anti-debug, Anti-hooking, and Advanced Obfuscation…		

S. No.	Description	Compliance (YES/NO/NA)	Comments
7	**Security Event Logging**		
7.1	Proposed systems shall support standard logging protocols such as CIFS/Syslog/CSV logs files		
7.2	The system shall generate and support audit logs that contain the following fields (as a minimum): a) Username b) Timestamp (Date & Time). c) Client IP Address d) Transaction ID & session information		
7.3	The proposed solution shall support the integration with Etisalat NTP for time synchronization and accurate logging.		
8	**Public Cloud Security**		
8.1	Etisalat customers' and staff personal data (PII: name, contacts, address, Emirates ID, Passport number, Nationality …) is encrypted at rest and in transit using a strong industry-standard encryption protocol		
8.2	The Public Cloud setup that stores PII information shall be hosted in the Afghanistan		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat (i.e. not shared)		
8.4	The Public Cloud data Center shall not be moved to another country or location without prior coordination and approval from Etisalat		
8.5	All Etisalat data will be permanently erased from the Public Cloud on termination of the service or support agreement		
8.6	The proposed Cloud system supports Etisalat Cloud Access Security Broker (such as Microsoft MCAS, Netskope CASB)		
9	**Virtualization and Container Security**		
9.1	If applicable, Bidder shall ensure the proposed virtualized infrastructure, service based and micro services architecture to support multi tenancy, zoning & micro-segmentation, security visibility, secure virtualization (sVirt), trusted image signing, virtual Firewalls, DoS protection, Trusted platform		

	module (TPM), Hypervisor & Host OS security to secure data and resources.		
9.2	The proposed solution shall support integration with Etisalat/Leading Container Security Solution, where applicable, to scan the container images and ensure malware protection of CI/CD pipeline.		
9.3	Suppliers must inform EA Cybersecurity of any non-conformity with defined EA policies and processes that are agreed upon in advance to acquire a written approval from EA Cybersecurity Department or senior management as required otherwise Supplier will be responsible for all the potential losses		

RFP General Terms Compliance to be filled by Bidder:

S/N	Clause No. and General Terms	Comply (Yes/No)	Remarks
1	**4. VALIDITY OF OFFERS:**		
2	**6. ACCEPTANCE OF OFFERS:**		
3	**7. REGISTRATION/LEGAL DOCUMENTS OF THE BIDDER**		
4	**8. PAYMENTS**		
5	**10. CONSTRUCTION OF CONTRACT:**		
6	**11. TERMINATION OF THE CONTRACT BY THE PURCHASER**		
7	**12. LOCAL TAXES, DUES AND LEVIES:**		

The following Information must be submitted with offer.

Bidder Contact Details	
Bidder Name	
Bidder Address	
Bidder Email Address	
Bidder Phone Number	
Bidder Contact Person Name	
Bidder Contact Person Phone No	
Bidder Contact Person Email Address	
Bidder Registration License Number	
License Validity	
TIN Number /Tax Number	

**********End of Doc**********