Terms of Reference

Security Operations Center (SOC) and Security Information and Event Management (SIEM) implementation in the Private and Technological Network of the State of Cabo Verde (RTPE)

1. Background

The Republic of Cabo Verde has requested to the World Bank a $20 million loan to finance the Cabo Verde Digital Project (P171099). The project is designed to support the Government of Cabo Verde (GovCV) to implement the main priority initiatives of the national ICT and e-Governance policy implementation strategies, as well as to further support the strengthening of the national telecommunications sector, and is expected to apply part of the funds to contract Technical Assistance for project implementation, whose objective is to effectively contribute to transforming the country into a regional digital hub to accelerate its digital economy through an upgraded digital infrastructure and strengthened demand for digital services and skills.

To ensure the applicability of the principles defined in the RTPE (State Private and Technological Network) Law, the project under component 3, Digital Public Services and Marketplaces, sub-component E-ID, will support NOSi in its efforts to implement measures that allow the operationalization and improvement of RTPE cybersecurity, ensuring adequate, integrated, and systematic protection mechanisms of the electronic Governance system and its components that stem from the State-Citizen, State-Economic Operators, and State-Public Servers relationships, thereby boosting the Digital Economy and National Cybersecurity.

1.1 RTPE – State Private Technology Network

A communication platform that interconnects and integrates all Central and Local Government institutions, making communication and decision making easier, faster and more efficient.

It comprises an integrated set of physical and logical resources related to information and communication technologies, namely data centers, communication networks, platforms and electronic governance systems used by the institutions of the Central and Local Government of the State and by Public Institutes:

- 3 Data Centers: greater Security and access availability;
- +20Km Optical Fiber: greater speed in data sharing and transmission speed;
- +700 interconnected institutions: creation of the state private network (RTPE);
- +17k users: more speed and efficiency in communication and decision making;
- 100Gb Email box: more storage capacity;
- +100 eGov solutions: for digital transformation;
- +150 konekta spots: free access to Information and knowledge;

The information security management of RTPE, object of the Decree-Law nº19/2010 of June 14, is ruled by the following attributes and principles:

(i) *Integrity - the document or electronic system in the RTPE must not suffer unauthorized alteration*;

(ii) *Authenticity - identification and authentication of all parties involved in the use of RTPE*;

(iii) *Confidentiality - access to information, transactions or electronic communications in the RTPE should be confined exclusively to the authorized user*;

(iv) *Privacy - information or content of electronic transactions must be made available only to those who are authorized to do so*;

(v) *Availability - information in the RTPE must always be available to authorized users and systems*;

(vi) *Legality - in compliance with the laws, policies and standards established for RTPE*;

(vii) *Auditability - operations in RTPE are auditable*;

NOSi, as the managing entity of the RTPE, currently has several security management platforms operating, which support the RTPE's incident detection and response structure, namely:

Data Center, a modern, high standard and high availability infrastructure, with 7 levels of security. It is prepared with data processing and storage equipment to provide services with stability, security and quality in RTPE;

Identity and access management platform that allows you to identify, authenticate and authorize users, devices and systems in the RTPE.

Complete content analysis and filtering platform (antivirus), which ensures the security of the endpoints, with very advanced monitoring capabilities at the endpoint universe level (servers and workstations);

Perimeter protection platform, with state-of-the-art technologies that block unwanted external traffic from crossing the network edge and accessing RTPE's systems and equipment, with a plenty of capacity to generate valuable information about security events;

Electronic mail protection platform that allows protection of the information linked by e-mail, protection against unauthorized access, usurpation or compromise of these same contents, in the most diverse forms such as Anti-Spam, Anti-Phishing, Anti-Malware;

Data protection platform against loss and damage, through backup, version control, and replacement mechanisms;

Monitoring platform for greater control of the devices by checking the status and resources of the equipment/services.

Because there are several data structures for security events, NOSi security team has to monitor several dashboards (and associated alarms) which makes the operation much more complex, time-consuming and inefficient. Therefore, the main objective of this

project is to provide a single security data/event infrastructure, duly enriched with advanced intelligence, with a single operational dashboard and a single alarmist.

In short, the platform would centralize the responsibility for raising and standardizing security events from the multiple security platforms available on the RTPE

2. Objective(s) of the Assignment

The objective of the assignment is to recruit a consulting firm to implement the Security Operations Center (SOC) solution available 24/7 at RTPE, to ensure the continuous monitoring and detection of vulnerabilities and mitigation of the respective effects.
Includes:

- implementation of a single security data/event infrastructure, duly enhanced with automation, advanced intelligence, operational dashboard and alarming capabilities;
- SOP (Standard Operating Procedures) implementation to support 1st, 2nd and 3rd line team operations;
- Forensic laboratory implementation;
- SOC team training (1st Line, 2nd Line, 3rd Line);

The success of SOC implementation should allow the following:

- Increase data collection rate: increase the percentage of events and logs that are collected and processed by the SIEM solution.
- Reduce false positive rate: reduce the percentage of alerts generated by the SIEM solution that are not actual security incidents.
- Reduce Mean Time to Detection (MTTD): reduce the average time it takes for the SIEM solution to detect a security incident.
- Reduce Mean Time to Response (MTTR): reduce the average time it takes for the organization to respond to a security incident.
- Increase Incident resolution rate: increase the percentage of security incidents that are successfully resolved.

- Increase Threat detection rate: increase the percentage of potential security threats that are detected by the SIEM solution.
- Increase Compliance rate: increase percentage of systems and devices that are in compliance with organizational security policies.
- Increase User satisfaction: feedback from users regarding the ease of use and effectiveness of the SIEM solution.

3. Scope of Services, Tasks (Components) and Expected Deliverables

It describes the main requirements that the solution to be implemented must cover, as well as the technical and technological restrictions that the bids must observe. The requirements outlined should guide the drafting of the proposals by the bidders, but should not limit the bidders' proposal.

The consultant firm will be responsible for the conceptual project, the definition of the use cases, the implementation of SIEM, the elaboration of procedures and operations, and training of the 1st, 2nd and 3rd SOC line teams, among other deliverables mentioned in this term of reference, in strict coordination with NOSi.

3.1 Solution Description

The main objective of the SOC is to continuously monitor the RTPE network (24/7/365 days a week), acting in a reactive and preventive manner, in response and prevention of cyber incidents respectively, in order to ensure the confidentiality, integrity and availability of data and communications.

The SOC must provide the following services for RTPE (not limited):

- Security Monitoring: Continuous monitoring of systems, applications, and networks for malicious activity.
- Incident detection and response: identifying, triaging, analyzing, and responding to cyber security incidents.

- Security information and event management: real-time security data collection, correlation, and analysis, as well as detailed reporting.
- Threat analysis: real-time monitoring, analysis, and assessment of security threats.
- Vulnerability assessment: identifying and fixing vulnerabilities in systems and applications.
- Penetration testing: evaluation of system and network security, with cyberattack simulations.
- Security Incident Management: coordination and management of security incidents, including response, recovery, and damage assessment.

The following scheme illustrates the main components that must be observed in the bidders' proposed solution. Bidders must not limit themselves to the requirements described here, but must demonstrate their expertise in the matter when presenting their proposals.

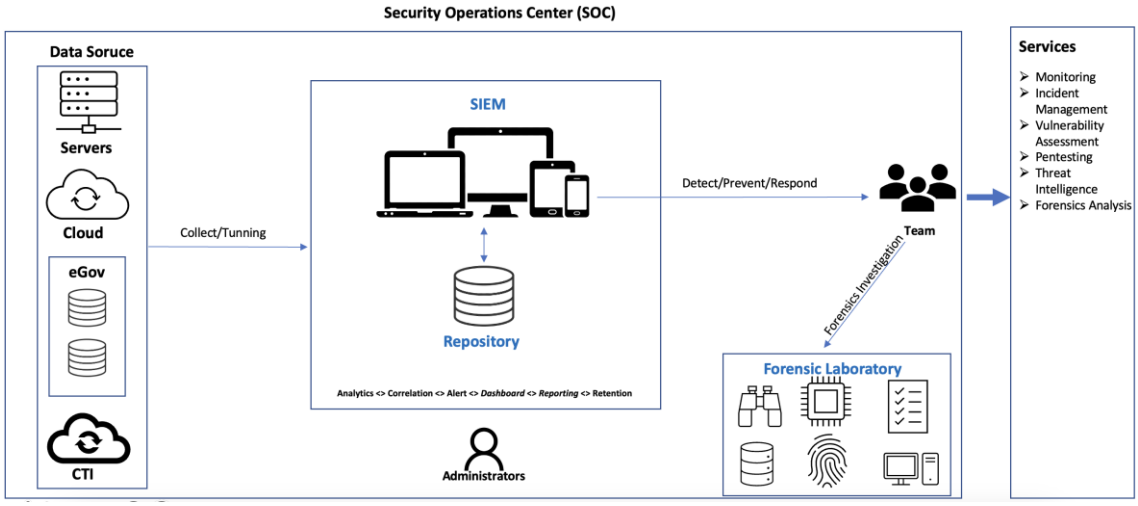

Fig. 1 – Solution Architecture

To design and implement the appropriate SOC to ensure the confidentiality, integrity, availability and auditability of RTPE assets and the consequent promotion of e-governance, the implementation of the following activities will be required:

3.1.1 Database Source

Given the diversity of the critical assets that support RTPE's core services, the SIEM platform must be capable of ingesting and standardizing a wide range of technologies, namely:

- **Servers** (Windows Server, GNU/Linux, MAC, Unix, among others);
- **Applications** (database, Web servers, ERP, CRM, among others);
- **Network** (Firewalls, VPN, Switching, Routing, among others);
- **Cloud** - involve the seamless integration of log and event data from various cloud platforms, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and other Software-as-a-Service (SaaS) applications. This integration allows the SIEM to collect and analyze logs from cloud-native services, virtual machines, containers, and other cloud-based resources.
- ***Backup*** (VEEAM, Commvault, Windows Backup, among others).
- ***CTI*** (*cybersecurity feeds on indicators of compromise (IoC) and indicators of attack (IoA)*)
- **Any future technologies** adopted by RTPE;

Hence, it should provide an architecture that allows:

- Existence of multiple data sources;
- Multiple source security event calibration and tuning;
- Integration with third party platforms (agents, SYSLOG, SNMP, API's, files, ...) and easily integrate with new technology assets that might be introduced in the future;

3.1.2 Implementation of the SIEM infrastructure – Security Information and Event Management

The SIEM platform is a vital component for SOC, it must allow to centralize, manage and analyze security events generated by multiple devices and systems, using a combination of rules and learning algorithms to correlate, enhance and identify possible threats, in the shortest possible time, and prompt timely response. The platform must be both scalable and flexible in order to ensure future expansion, without any limitation on events per

second, devices monitored, or amount of data retained. It must allow the inclusion of all intelligent RTPE systems, and in accordance with the future growth of the technological infrastructure, the possibility of inserting new assets that may be incorporated internally in the organization without any additional financial cost. The platform should have the following core functionalities (not limited to):

- Log collection and analysis - collect large amounts of data from various sources, including network devices, servers, applications, and security appliances;
- Event correlation - gather and correlate events to detect possible malicious events;
- Threat Intelligence - leveraging valuable insights on known and emerging threats, by enriching log data with contextual information from threat feeds, allowing correlate events with indicators of compromise, prioritize alerts based on threat severity, and facilitate proactive threat hunting from various CTI sources and information sharing with third party organization;
- Network intrusion detection - must be able to receive and analyze information that is circulating on the network and identify potentially malicious behavior;
- User and Entity Behavior Analytics (UEBA): ability to create a baseline of normal activity and alert on deviations from this baseline can be valuable in identifying potential threats, by employing machine learning and behavioral analytics to identify anomalous user and entity behavior, thereby enabling the detection of sophisticated attacks and insider threats beside reliance on signature-based or rule-based approaches;
- Real-Time Alerts and Response – promptly detect security incidents, analyze events and scale alerts in real-time and initiate immediate response to potential threats;
- View and dashboard customization - must allow you to create views for reviewing data and events, identifying patterns and activities that do not comply with processes and event flows;
- Report generation - understanding and reporting incidents in a customized view;
- Log retention - long-term storage capacity to enable analysis, tracking, and reporting;
- Failover and Redundancy – deployed in high-availability to ensure continuity in event of system failure;

- Compliance and regulatory requirements: ensure data privacy and security, by implementing access controls, encryption, and data retention policies according to national Personal Data Protection Law: 121.IX.2021;

3.1.3 SOP Implementation (Standard Operating Procedures)

Given the operationalization of the SIEM platform and the services provided by the SOC team to detect, protect and respond to cyber incidents, a set of processes and procedures must be developed and documented, including (but not limited to):

- Incident Escalation: specify escalation criteria and procedures to ensure that critical incidents are handled with priority, as well as ensure that SOC team members have a clear understanding of the escalation steps.
- Incident Identification and Classification: describe the procedures to identify and classify incidents, including the definition of severity and impact levels, as well as the criteria to classify incidents as "false positives".
- Incident Analysis: specify the procedures for incident analysis, including identifying the source of the incident, determining its root cause, assessing damage, and defining corrective action.
- Response Procedures: describe incident response procedures, including steps for notifying stakeholders, coordinating with other security teams, containing the incident, gathering evidence, and recovering affected systems.
- Communication: specify guidelines for internal and external communication during incident detection and response, including coordination with other security teams, stakeholder notification, and crisis management.
- Monitoring: describe the procedures for continuous monitoring of systems and data, including the monitoring tools used, identifying anomalies, and evaluating the effectiveness of security controls.
- Identity and Access Management: specify procedures for identity and access management of SOC team members, including defining roles and responsibilities, assessing the need for access to confidential information, and managing access credentials.

- Incident Management: describe incident management procedures to ensure that incidents are handled consistently and efficiently, including documenting incidents, evaluating the effectiveness of response procedures, and implementing improvements.
- Testing and Review: specify the procedures for periodic testing and review of the SOP, including evaluating the effectiveness of the procedures, identifying opportunities for improvement, and updating the SOP in accordance with changing SOC needs.
- Training and Qualification: describe the policies and procedures for training and qualification of the SOC team, including assessing training needs, defining training programs, and periodically assessing the competence of team members.

3.1.4 Forensic Laboratory Implementation

The consultant firm shall propose and arrange for the purchase of forensic equipment necessary to operate a forensic laboratory that will be used by the SOC team in the forensic investigation to produce the correct forensic results. The equipment can be as hardware, software, free software, or commercial tools with the capability to produce the correct results.

The software acquisition process must consider the initial price, annual license values, maintenance value, training value and the following forensics analysis capabilities:

- First responders
- Network forensic
- Image Acquisition (memory, disk, …)
- Computer forensic
- Memory forensic
- Mobile forensic
- Malware analysis (Static, Dynamic)

Below is a suggested list of basic equipment for a forensic laboratory. It should be noted that the list is not exhaustive and further equipment may be needed depending on the nature of the cases received:

- *Laptop with high processing power (GPU)*
- Computer analysis software
- Network analysis software
- Data recovery software
- Mobile device analysis software
- Internet artifact analysis software
- *Imaging Hardware*
- *Docking system*
- *Write blocker*
- Storage media (Pen drive, External hard drive, Hard drive, ...)
- PC Forensic Toolkit

Tools and accessories such as cables, screwdrivers, and power extensions are just as important as the software and hardware. Here is a list of possible items you may need to perform everyday tasks:

- Power extension
- Cables and adapters
- Screwdrivers
- Tool kit
- Camera, video recorder
- Magnetic tapes
- Communication devices
- Storage box or container to carry equipment
- Magnifying glass
- Evidence sealing or evidence bags
- Tamper-evident stickers
- Permanent markers
- Faraday bag

3.1.5 SOC team training (1st Line, 2nd Line, 3rd Line)

Provide a plan to empower the team of security specialists and analysts with skills and experience needed to effectively monitor and manage security-related activities and incidents in accordance with the following competencies and responsibilities:

Competencies	Responsibilities
1st Line Team	• Initial Event Screening • Initial classification of events • Vulnerability scans • Call Center
2nd Line Team	• Advanced Malicious Behavior Detection • Incident response • Gathering and utilization of Cyber Threat Intelligence (CTI) • Vulnerability Management
3rd Line Team	• Malware Analysis • Forensic Investigation • Large-scale Incident Response • Incident Response Coordination • Building Cyber Threat Intelligence (CTI) • Threat Hunting
System Administrators	

3.2 Technical Restrictions

Below are some technical restrictions that must be observed by bidders when submitting their bids:

- The SOC should be operationalized in accordance with the best practices established by:
  - *SOC2 (Service Organization Control 2), is focused on operations and compliance. Its objective is to have and demonstrate internal controls*

aligned with the latest Trusted Service Criteria - security, availability, integrity, confidentiality, and privacy. SOC2 Controls:

- ✓ Logical and physical access controls;
- ✓ System and Operations Controls;
- ✓ Change Management Controls;
- ✓ Risk Management Controls;

- *SIM3* (*Security Incident Management Maturity Model*), a model for self-assessing the maturity of all types of CSIRTs;
- *SOC-CMM* (M*easuring Capability Maturity in Security Operations Centers*), model for self-assessing the maturity of a Security Operations Center (SOC);

- The SOC incident management service shall be provided in accordance with the standards defined by *NIST SP 800-63*;
- The collection, analysis and preservation of evidence must be provided in accordance with the Electronic Evidence Guide and the Cybercrime Law,
- The SIEM platform shall have enough functionality to enable log management and real-time detection of security incidents, incorporating the SIEM and security analytics capabilities and artifacts stipulated in *SOC CMM 2.1 advanced*.
- The SIEM platform must be configured to support data enrichment with context-sensitive information such as geographic data, malicious IPs, domains, URLs, threat indicators, and custom tags and annotations. Enrichment fields should be indexed along with the real-time event at an individual event level and should not be done as a separate search process;

4. Team Composition & Qualification Requirements

4.1 Experience Requirements and References

The assignment will require a consulting firm with at least 10 years of experience in the areas of cybersecurity to ensure a security and data governance strategy, monitoring and alarming systems, security operations center, incident response teams, and emerging technologies in island countries.

a) The consultant must have at least ten (10) years of experience in SIEM, SOC or CSIRT implementation;
b) The consulting company must have at least 3 (three) experiences in the elaboration of architecture and operational procedures for SIEM and SOC;
c) The consultant should have experience in designing and implementing cybersecurity awareness campaigns.
d) The consultant must have experience in SIEM implementation;
e) The consultant must have experience in SOC or CSIRT implementation;
f) They must have experience in working on similar projects and countries.
g)) The experience and knowledge of Cabo Verde's technological environment will also be relevant

4.2 The project team should be composed by the following key experts

1) Team Leader

- Degree or post-graduate in Computer Science or related field;
- Minimum of 7 years in the management of large cybersecurity jobs;
- Solid background in information security and IT security assessment processes with proven experience (plus certification to this effect: CISSP, CISM, ISO 27001 Lead Auditor, PMBok, ITIL, COBIT 5, SIM3, SOC);
- Minimum of 5 project assignments related to information security and SOC/CSIRT implementation;
- Fluency in Portuguese and English; and
- Experience in these areas in Africa will be an added advantage.

2) Cybersecurity Expert

- Degree or post-graduate in Computer Science or related field;
- Over five (5) years of experience as a senior cybersecurity technician;
- Hold a Cloud Security, SOC Analyst, Pentest, Network Defender, CyberOps, GIAC Intrusion Analyst, GIAC Incident Handler or related certification;

- Have implemented at least three (3) SIEM, SOC or CSIRT projects;
- Have experience in security traffic tuning of various network devices (firewall, ids, ips, antivirus, desktop, server, ...)
- Experience in incident management according to ISO/IEC 27035 or NIST SP 800-63
- Fluency in Portuguese and English; and
- Experience in training as referred to in this ToR;

3) *Forensic Expert*

- Degree or post-graduate in Computer Science or related field;
- More than 5 (five) years of experience as a forensic analyst;
- Hold a Cloud Security, CHFI, Pentest, GIAC Forensic Analyst, GIAC Malware Analyst or related certification;
- Have experience in forensic analysis of network, mobile devices, cloud, windows and Linux operating systems, ...
- Experience in computer forensics according to NIST SP 800-61
- Fluency in Portuguese and English; and
- Experience in training as referred to in this ToR;

5. Deliverables, Reporting Requirements and Time Schedule

Component	***Deliverable***	***Description***	***Type***	***Payment after Approval by the Client***	***Schedule***
Strategy Approach	***D0. Inception Report***	*Overview document of the work to be done within the scope of the work prepared*	Report	*10%*	Signing of the Contract (SoC) + 15 days
SIEM + Forensic Laboratory	***D1. SIEM Requirements Specification*** +	*Technical Specification Document for SIEM elaborated;*	Report	*15%*	SoC + 3 months

	BoQ for Forensic Laboratory	*Operational and functional SIEM;* *List of materials and services for the implementation of the Forensic Laboratory and the respective procurement process elaborated*			
SOP (Standard Operating Procedures) + SOC team training	***D2.*** ***Operational Documents*** + ***SOC 1st Line Team Training***	*Incident Identification and Classification, and Incident Escalation Procedures documents, elaborated* *Program Document and Training Content elaborated;;* *Training Report elaborated and approved;*	Manual + Report	*15%*	SoC + 4 months
SOP (Standard Operating Procedures) + Forensic Laboratory + SOC team training	***D3. Operational Documents*** + ***Forensic Laboratory*** + ***SOC 2st Line Team Training***	*Incident Analysis Documents; Response Procedures; Communication; Monitoring; Incident Management; Access Management; Testing and Reviewing; and* *Elaborate training and qualifications* *Operational and functional Forensic Laboratory;* *Technical Manual and Operational Manuals elaborated* *Program Document and Training Content elaborated;* *Training Report elaborated and approved;*		*25%*	SoC + 5 months

SOC team training	**D4.** ***SOC 3st Line Team Training***	*Program Document and Training Content elaborated;* *Training Report elaborated and approved;*		*15%*	SoC + 6 months
Project Conclusion	**D5.** ***Final Report***	*SOC Policy and Security Solution Documents prepared;* *Solution Acceptance Agreement approved and signed;*		*20%*	SoC + 7 months

If otherwise specified in this ToR, all results and reports will be provided in Portuguese and English language in Word, Excel and PowerPoint or equivalent format. Draft versions of the final results will be submitted electronically and successive versions of the reports will be marked to show changes from the previous draft. Submissions should be sent to NOSi EPE with copy to Special Projects Management Unit (UGPE).

6. Client's Input and Counterpart Personnel

a) *The following information should be made available to the project:*
   (i) Core Network Architecture, Distribution and RTPE Access
   (ii) Inventory of RTPE's critical assets
   (iii) RTPE Information Security Policy
   (iv) Any additional information will be made available according to the requests of the project team.

b) Professional and support counterpart personnel to be assigned by the Client to the Consultant's team:
   (i) Technician of the NOSi's Cybersecurity Department

7. Duration of the Assignment

The mission will be carried out over a maximum period **of seven (7) months from the date of signature of the contract.**

8. Organization of the Assignment

The selected firm shall undertake the assignments in close consultation with the NOSI shall follow and support the assignment. The Consultant will report to Special Projects Management Unit (UGPE) for contract administration.

9. Contract

A Lump-Sum form of Contract shall be signed, payments to the consulting firm are linked to approval of deliverables, and the payment of reimbursable expenses are made upon presentation of the receipt of the expenses occurred at the real cost.