MANAGED SECURITY SERVICES PROVIDER (MSSP)

REQUEST FOR PROPOSAL

CGIAR SYSTEM ORGANIZATION

Request for Proposals: Managed Security Services Provider (MSSP)

1. Objective:

CGIAR seeks to identify a qualified Managed Security Service Provider (MSSP) that can deliver Network Security Monitoring and Incident Response Services, ensuring security for our main offices and public cloud providers. The Provider should be able to support, at minimum, the following services: Security Event Monitoring 24/7/365, Incident Response to promptly react to any malicious/unexpected activity in any center/OSU (Operations Support Unit), Forensic Analysis to respond to critical incidents, periodic Vulnerability Assessment (VA) to evaluate and report on external surface the vulnerabilities across centers/OSU and provision of Threat Intelligence services to proactively safeguard the information assets of centers/OSU.

This request for proposal does not guarantee that CGIAR will contract with any of the responding vendors for the services and/or products described herein; CGIAR also reserves the right to defer the awarding of a contract and/or to reject all proposals, if deemed to be in CGIAR' best interests.

2. Background/Context:

CGIAR is a global research partnership whose mission is to create a world with sustainable and resilient food, land, and water systems that deliver diverse, healthy, safe, sufficient, and affordable diets and ensure improved livelihoods and greater social equality within planetary and regional environmental boundaries. Our research is carried out in close collaboration with hundreds of partners, including national and regional research institutes, civil society organizations, academia, development organizations, and the private sector.

Therefore, it is imperative that our chosen MSSP has a proven track record in delivering high-quality, consistent support to complex international entities, particularly within the non-profit sector. Please refer to Appendix 2 for important details on CGIAR's unique structural model, as its understanding is essential for our valued suppliers to engage in the procurement process effectively. Our procurement model's flexibility is designed not only to benefit CGIAR but also to offer suppliers the opportunity to present the most advantageous proposals.

The cornerstone of a successful partnership will be the supplier's ability to present a value-added proposal that not only meets our extensive requirements but also serves as an attractive proposition for group purchasing. This proposal should be compelling enough to give the 13-member Centers the confidence to adopt the MSSP's proposition, driven by a proposal that offers advantageous incentives and the promise of a successful pilot implementation that will act as a proof of concept.

We seek an MSSP that understands the unique challenges and opportunities of working with a partnership of our scale, diversity, and impact. The ideal provider will exhibit innovation, expertise, and a strong commitment to delivering services that safeguard the security of our data and research operations.

3. Scope of Services

CGIAR, the world's largest publicly-funded agricultural research network, operating as thirteen independent legal entities (Centers), and collectively home to more than 9,000 scientists, researchers, technicians, and staff working in over 80 countries, seeks a MSSP that can deliver the following essential services to CGIAR:

- Network Security Monitoring and Incident Response Services, ensuring security for our main offices and public cloud providers. The goal is to have at least:
    - Security Event Monitoring and detection 24/7/365.
    - Incident Response to promptly react to any malicious/unexpected activity in any center/entity according to the severity and complexity of the incident.
    - Forensic analysis during the eradication phase for critical incidents.
- Periodic Vulnerability Assessment (VA) to evaluate and report on external surface the vulnerabilities across centers/OSU.
- Provision of Threat Intelligence services to proactively safeguard the information assets of centers/OSU.

The aim of this effort is to set up a system where all CGIAR's cyber security layers are monitored for attacks or malicious activity, and all cyber security events are addressed quickly and effectively by trained, responsible, and accountable professionals.

The initial term of any contract awarded as a result of this RFP is anticipated to be two-years (2) with the option to renew subject to supplier performance review and market analysis.

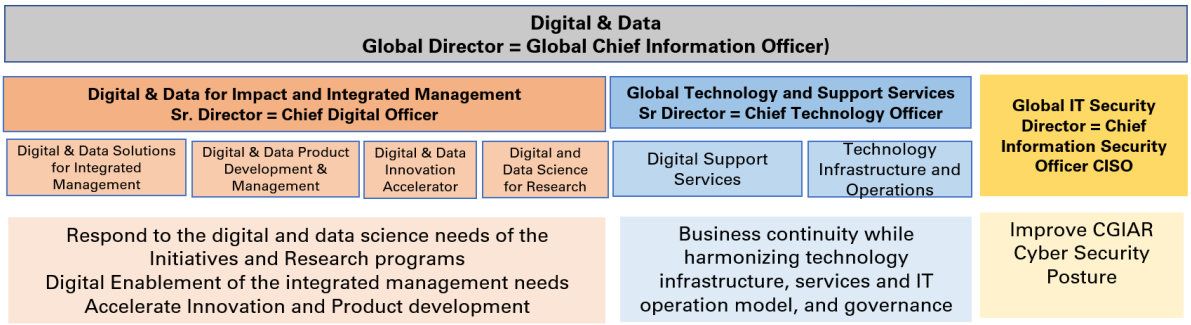
Information Technology (IT) Organization Model

CGIAR currently associates with 12 research centers and a secretariat office (SMO) distributed globally, each of which operates its own dedicated IT department. In addition to these decentralized IT units, the consortium has established a central global department known as Digital & Data (D&D).

Digital & Data (D&D) focuses on building a digital and data empowered CGIAR that adapts to change and harnesses the power of technology and data science to operate in an efficient, effective, and timely manner. It is responsible for building and harmonizing CGIAR's IT infrastructure, establishing governance structures to support the development of cross-cutting digital research and data capabilities, and creating an enabling environment for digital and data innovation in food security research and development.

Within our organization, there is a dedicated team of technical security personnel (1CGSec) tasked with monitoring, implementing security controls, vulnerability management, and working closely with the Managed Security Services Provider (MSSP). Each team member is a representative of a specific Center and holds the responsibility for incident response, vulnerability remediation, and threat advisory remediation within their respective infrastructure.

3.1 D&D Structure



D&D serves as a strategic partner to the individual research centers, facilitating the seamless integration of technology solutions and best practices. The value proposition includes:

- Building digital and data capabilities of CGIAR to operate in a secure, efficient, effective, and agile manner.
- Strengthening & harmonizing CGIAR's digital and data infrastructure and services
- Establishing digital and data governance structure, management, and operational models based on global standards and best practices (centers of excellence).
- Empowering the development of cross-cutting digital and data science capabilities for research.
- Creating a digitally enabled environment for operational excellence and innovation in food security research and development.

For the purpose of this document, the general functions of the Global IT Security Unit are described:

- The Global IT Security Unit provides globally integrated cyber security and cyber risks management services, systems, and processes to optimize the security posture of the organization including effective incident response, IT security governance, and risk monitoring and mitigation.
- The unit maintains and enhances standards and practices to manage the confidentiality, integrity, and availability of digital systems, information, and data assets.

CGIAR works in six regions: Central and West Asia and North Africa, Latin America and the Caribbean, West and Central Africa, East and Southern Africa, South Asia, Southeast Asia, and the Pacific.

3.2 Current Systems

CGIAR comprises 13 research centers and one operation support unit distributed worldwide, each with its distinct portfolio of platforms and services.

#	Name	Type
1	AfricaRice	Research Center
2	Alliance	Research Center
3	CIMMYT	Research Center
4	CIP	Research Center
5	ICARDA	Research Center
6	ICRISAT	Research Center
7	IFPRI	Research Center
8	IITA	Research Center
9	ILRI	Research Center
10	IRRI	Research Center
11	IWMI	Research Center
12	OSU	Support Unit
13	SMO	Research Center
14	WorldFish	Research Center

At present, CGIAR maintains a shared Microsoft 365 tenant, expertly managed by CGNET. This tenant adopts a hybrid configuration, with individual centers hosting on-premises Windows Active Directory (AD) servers and managing staff licenses tailored to their specific needs. License types range from the fundamental E2 to the comprehensive E5, with the latter being less frequently utilized. A subset of centers has transitioned to an Azure AD-bound approach. Also, many centers

are utilizing a number of Microsoft Enterprise Mobility + Security (EMS) licenses, with different levels of adoption of Intune and other end point management tools.

While some centers/OSU exclusively rely on cloud-based solutions for production workloads, server infrastructure, and platforms (employing various cloud vendors, including managed private clouds), the majority operate with hybrid workloads.

Currently, we maintain external surface monitoring for the centers/OSU at central level, actively tracking the locations where on-premises AD operations are in progress. In Annex *3*, we will furnish the actual resource list for your reference.

Regarding user endpoints, most of our users employ Windows devices, given our organization's reliance on a Microsoft tenant (with one Center operating as a Google Workspace tenant). Nevertheless, specialized teams of developers, scientists, and bioinformaticians comprise a smaller subset of users who operate Linux and, Mac devices.

Furthermore, CGIAR maintains a limited allocation of mobile phone devices for select users, currently not being centrally managed by the centers. We allow access to our Microsoft O365 and other AD/AzureAD authenticated services from privately managed devices.

In summary, CGIAR represents a vast and intricate organization with a diverse array of IT platforms and services. This tender statement offers a broad overview of our IT landscape, encompassing our shared Microsoft 365 tenant, production workloads, user endpoint diversity, and mobile device provisioning.

3.3 Deliverables

In this section, we outline the expected deliverables from the Managed Security Services Provider (MSSP), including both core services and any additional services offered.

3.3.1 Core Services

The core services are integral to ensuring the ongoing security and resilience of CGIAR operations, and these are the minimums required for the operation of the MSSP in our environment:

i. Network Security Monitoring and Incident Response Services:

The service should be Original Equipment Manufacturer (OEM) agnostic. These services must cover CGIAR's current productivity and collaboration suites, the monitored internal networks, and the external surface that is integrated with the AD. More details are in Annex 3: section a)-b)-c)-d).

- Comprehensive monitoring of security events 24/7/365.
- Describe how security technologies will be used throughout the extended network to obtain visibility into network behavior and to apply control over questionable network behavior.

- Manual network hunting where an expert analyst will thoroughly examine network traffic and flow data to identify signs of anomalous or suspicious activity. This hunting will be conducted manually through in-depth analysis and is intended to detect threats that may not be identified through automated tools alone.
- Incident response coordination with the center/entity: Shared responsibility model.

Step	CIO and ICT Leaders for each Center	CISO	DPO	Help Desk	Incident Coordinator per Center and Global	IT	MSSP	Data Owner	Legal	AFRC
Register Incident				AR	CI	I	R			
Conduct Initial triage		I			AR	C	R	I	I	
Assign Classification		I	I		AR		R	C	C	
Assign Severity		I	I		AR		R	C	C	
Determine next steps based on severity	I	CI	CI		AR	C	R			
Resolve using business as usual (BAU) process				I	I	AR	I	CI		
Mobilize CSIRT	I	I		I	AR	CI	CI			
Collect Incident Data					A	R	R	C		
Determine Scope		I	CI	CI	AR	R	R	CI	CI	
Identify whether personal data is potentially Impacted	I	CI	R		A	C	CI	CI		

Step	CIO and ICT Leaders for each Center	CISO	DPO	Help Desk	Incident Coordinator per Center and Global	IT	MSSP	Data Owner	Legal	AFRC
Reassess Incident			R		R		R	CI	A	
Notify Relevant Parties	A	R	CI		CI			C	A	R
Develop Containment Plan			C	I	AR	R	C	C		
Execute Containment Plan			C	I	A	R	I			
Determine if the Incident is Contained	I	I	C		AR		CI	I		
Update Ticket					AR		I	I		
Communicate to Stakeholders	I	AR	C	I	R		C	I	I	
Develop Eradication Plan			C	I	AR	R	C	C	I	
Execute Eradication Plan				I	A	R	I			
Determine if the Threat Is Eradicated	I	I	C		AR		I	I		
Update Ticket					AR		I	I		
Communicate to Stakeholders	I	AR	C	I	AR		I	I	I	

Step	CIO and ICT Leaders for each Center	CISO	DPO	Help Desk	Incident Coordinator per Center and Global	IT	MSSP	Data Owner	Legal	AFRC
Develop Recovery Plan			C	I	AR		I	C		
Execute Recovery Plan			C	I	AR	R	I			
Determine if the Systems Are Recovered	I	I			A	R	I	I		
Update Ticket			C		AR		I	I		
Communicate to Stakeholders	I	AR	C	I	AR		I	I	I	
Conduct Root Cause Analysis		I	C		A	R	R	C	C	
Document Findings	I	I	C		AR		CI	C		
Assign Action Owners		AR	I		R		I	I	C	
Update Controls and Policies	AC	R		I	IR	I	I	I		
Demobilize CSIRT	I	CR	I		AR		I	I		
Close Ticket	I	I	I		AR		R	I		I

- Responsible: People or stakeholders who do the work. They must complete the task or objective or make the decision.
- Accountable: Person or stakeholder who is the “owner” of the work. He or she must sign off or approve when the task, objective or decision is complete.

- Consulted: People or stakeholders who need to give input before the work can be done and signed-off on.
- Informed: People or stakeholders who need to be kept "in the picture." They need updates on progress or decisions, but they do not need to be formally consulted, nor do they contribute directly to the task or decision.

ii. Digital Forensics and Incident Response (DFIR)

- Forensic analysis for incidents categorized as critical. Pay as you go.

Note: Any incident that affects a server that is exposed to the Internet and that is connected to the active directory is considered critical.

iii. Vulnerability Assessment:

- Conduct vulnerability assessments for the external surface reported by the centers. More details in Annex 3, section *e)*.
- Generate detailed reports of findings (Responsibility for remediation actions is managed directly by each center/entity).

iv. Threat Intelligence Analysis:

- Provide threat intelligence analysis.
- Priority notification in cases of identification of threats that directly affect the services/applications reported by each center/entity.

v. Portal, reports, and dashboards

- A centralized portal designed for visualizing, tracking, and interacting with centers for event management via web and with Multifactor authentication.
- The service delivery should be closely observed and evaluated throughout the lifetime of the contract.

3.3.2 Additional services

The service provider may propose additional security services to complement Core Services, and these must be presented separately from the Core Services offering. It should be possible to contract these additional services individually for each center, as needed.

4. Performance Measurement and Review:

In this vital section of the Request for Proposal (RFP), we delineate the framework for performance measurement and review. The structured approach and predetermined Key Performance

Indicators (KPIs) provided are designed to ensure seamless evaluation and continuous improvement of the services.

4.1 Performance Indicators

The Managed Security Service Provider (MSSP) will be required to provide specific performance indicators as part of their proposed service level agreement. Below are the minimum requirements and SLA benchmarks. The MSSP may expand indicators and commitments based on their expertise. The MSSP is invited to note any discrepancy in their capacity to meet a benchmark only with a detailed technical explanation to support it.

Indicator Category	Indicator	SLA benchmark
Incident Response Time	Incidents detected, assessed, and reported to the Centers/Entity within 24 hours of occurrence	95% measured monthly
	Critical incidents assessment and notified to the security focal point of each Center/Entity within 4 hours of occurrence. *Note: Any incident that affects a server that is exposed to the Internet and that is connected to the active directory is considered critical.*	95% measured monthly
	False Positive Rate: Percentage of reported incidents that turn out to be false alarms.	10% measured monthly
Availability and Uptime for the Detection Platform	System availability and uptime percentage.	99.5% measured monthly
Availability of SOC monitoring services	SOC platform availability and uptime.	99.999% measured monthly
Vulnerability Advisories Effectiveness	Percentage of identified and reported vulnerabilities within 24 hours of manufacturers' reports. For systems that the CGIAR has installed.	95% measured monthly
	Threat Intelligence Effectiveness: Percentage of identified threats on the platforms reported by the Centers/OSU	90% measured monthly
Reporting Accuracy	Accuracy of security reports and alerts provided to the client.	95% measured monthly

Indicator Category	Indicator	SLA benchmark
	Inaccurate or incomplete data will require remediation or re-delivery of reports.	
Forensic Analysis	Reports for critical incidents should be available within 7 days after the collection/investigation is completed (with the support of the affected Center).	90% measured monthly
Client Satisfaction	Evaluation average of service satisfaction measured by the CGIAR security group (Client feedback through a satisfaction survey Annex 4).	≥4measured quarterly

4.2 Performance Evaluation and Review

Performance reviews will be conducted every 4 months, managed by the security group, and will be reported to the D&D director and the ICT Leaders for each Center. All feedback and assessments provided during the review meetings will be formally documented. This documentation will serve as a record for performance assessment and will be referenced in future evaluations and reviews.

The MSSP will have the opportunity to respond to the feedback, offering insights into their performance, challenges faced, and the strategies employed for issue resolution and project advancement. A collaborative approach will be adopted to identify areas of improvement and the necessary steps to enhance performance in subsequent periods.

Criterion	Definition	Weight
SLA Compliance	For agreed indicators and targets.	90%
Fit for purpose	Other aspects of the service (quality, completeness, scalability).	5%
Client-centric approach	Understands the business and demonstrates a client-centric approach. Identification of new innovations that could provide more value to the MSSP service.	5%

5. Legal Considerations

5.1. RFP Participation non-disclosure agreement

By submitting a proposal, the MSSP commits to the following non-disclosure agreement:

Confidentiality Obligation: The MSSP acknowledges that during the RFP process, it will receive confidential information pertaining to CGIAR and CGIAR Centers. The MSSP agrees to keep this information confidential and not to disclose it to any third party without the prior written consent of CGIAR.

GDPR Compliance: Recognizing that some CGIAR Centers operate under the General Data Protection Regulation (GDPR), the MSSP agrees to comply with GDPR requirements in relation to any personal data processed in the course of providing services. The MSSP will ensure that all such data is protected and processed in alignment with the legal framework established by GDPR and will take all necessary measures to safeguard the privacy and security of this data.

Use of Information: The MSSP agrees to use the confidential information solely for the purpose of preparing and submitting a proposal in response to the RFP and not for any other purpose.

Duration of Confidentiality: The obligation of confidentiality shall remain in effect until such time as the confidential information becomes publicly known through no fault of the MSSP, or until the CGIAR entity releases the MSSP from this Agreement in writing through an authorized party.

Return or Destruction of Information: Upon request of the CGIAR entity or upon conclusion of the RFP process, the MSSP shall return or destroy all confidential information received, including any copies made.

Access to Confidential Information: Access to Confidential Information will be limited to those of its employees or contractors who have a legitimate need to know such information for the project and who have agreed in writing to be bound by the terms of this NDA.

All reasonable precautions will be taken to prevent the unauthorized disclosure or use of Confidential Information, including but not limited to implementing and maintaining adequate security measures. Access to CGIAR systems shall only be made from trusted machines with current protection standards. Access to CGIAR systems shall not be made from any sanctioned country by US laws applicable to MS products.

Acknowledgment of Terms: By participating in the RFP process, the MSSP acknowledges its acceptance of the terms of this Agreement and its commitment to abide by them.

Additionally, CGIAR commits to protecting any confidential information received from the MSSP during the RFP process and will use such information solely for the purposes of the RFP process.

This Agreement is effective as of the date of the MSSP's Intent to Submit Proposal letter submission.

5.2 Data Management, Security, and Confidentiality Standards

By submitting a proposal, the Firm acknowledges that CGIAR expects adherence to data management, security, and confidentiality standards, as detailed in this RFP, which will be reflected in the final agreement.

Data Ownership

- The Client retains full ownership of any data uploaded to or generated by the MSSP systems as part of the managed security services.
- The MSSP shall not claim any rights or ownership over CGIAR's data. The Client may request return or deletion of data upon termination of services.
- The MSSP is granted a limited license to access and process CGIAR'S data solely for delivering the contracted services. No other uses are permitted without the Client's explicit written consent.

Data Security

- The MSSP shall protect the confidentiality, integrity and availability of CGIAR's data with appropriate technical and organizational measures.
- The CGIAR's data shall be logically or physically separated from other client data and protected against unauthorized access or leakage.
- The MSSP shall encrypt the CGIAR's data both at rest and in transit using industry standard methods.
- Access controls shall restrict data access only to authorized personnel. Controls shall be regularly reviewed and updated.
- Controls implemented shall be reported to CGIAR every time a modification/update is made.

Data Privacy

- Any transfer or sharing to third parties of the CGIAR's data shall only occur after CGIAR's explicit written consent.
- The geographic location of data storage and processing shall be disclosed to CGIAR and comply with applicable regulations.
- The MSSP shall cooperate fully with any data protection authority inquiries and data subject access requests.
- The MSSP shall promptly notify the Client of any unauthorized access or breach of personal data.

Data Protection and Privacy

- The MSSP shall implement appropriate technical and organizational measures to protect any personal data processed or accessed in the course of providing the managed security services, in accordance with applicable data protection laws and regulations.
- The MSSP shall not process any personal data beyond what is necessary to perform the services or as authorized by CGIAR.
- The MSSP shall assist CGIAR in conducting data protection impact assessments and consultations with any relevant authorities, if required by law.

Access Control

- The MSSP shall restrict access to the CGIAR's data and systems only to those personnel who require such access to perform the services. Access shall be authorized by the Client before provisioning.
- User access provisioning and de-provisioning procedures shall be implemented to ensure access privileges are adjusted appropriately as personnel change, provider will provide evidence when a new member is added/retired.
- The MSSP shall maintain audit logs of all personnel accessing the Client's data and systems.. And the MSSP shall provide on demand an access control report when a request is generated by the client.

Breach Notification

- The MSSP shall promptly notify the CGIAR within 24 hours of becoming aware of any actual or suspected breach of the CGIAR's data or systems.
- Breach notification shall include details of the data affected, source, recommendation to mitigate impact, as well as any information reasonably requested by the CGIAR.
- The MSSP shall fully cooperate with the CGIAR to investigate, remediate, and fulfil any legal obligations arising from a data breach.

Data Portability

- The Client retains full ownership of its data. The MSSP shall allow the Client to extract or export its full data set in a standard portable format upon request or contract termination, besides the MSSP will provide a feasible way to make use of the exported data, if not possible, the MSSP also can provide an extended access to its own portal for a 6-months period upon contract termination.
- Deletion of the Client's data shall be executed after confirmation from the Client and completion of any migration activities.

Service Changes and Updates

- The MSSP should provide reasonable notice (15 days) before making changes or updates to services that impact the client.

- For major changes the MSSP should provide the capability to do the testing updates in staging environments.
- For major changes, the contract should specify the MSSP's rollback capabilities to previous stable versions in case issues arise.

Compliance with Regulations

- The MSSP should represent and warrant that its services will comply with relevant regulations such as GDPR.
- Include indemnification for the CGIAR in case the MSSP's failure to comply with regulations causes penalties, fines or other losses.
- Emphasize the importance of maintaining the confidentiality and security of sensitive information.

Termination

- Allow the client to terminate the contract for any material breach by the MSSP (See Annex 1-CGIAR General Terms & Conditions of contract).
- Ensure MSSP's assistance with data migration continues for a transition period of 30 days after termination.
- The MSSP must retain the client's data after completing data migration before deletion for 60 days.

5.3. Contracting

The MSSP's should accept the CGIAR System Organization standard terms and conditions of contract in Annex 1.

If the MSSP requires amendment of specific clauses, the MSSP must submit those contract clauses or the MSSP's template for our review and consideration in a Word format as a separate document, along with the letter of confirmation of intent to submit a proposal.

CGIAR reserves the right to request additional information or clarification regarding the suggested contract clauses or templates during the evaluation process. Submitting suggested clauses or templates does not guarantee that the MSSP will be awarded the contract. Final contract negotiations will be conducted with the selected firm based on the evaluation results.

5.4. Payment Terms

Standard payment terms will be Net 30 days from the date of invoice receipt. The invoicing schedule may vary based on the approach outlined in the Firm's commercial proposal. This flexibility allows for alignment with MSSP's preferred billing structure while ensuring that payments are made in a timely manner following the standard Net 30-day policy. The monthly invoices shall be directed to each respective Center/Entity. CGIAR's policy does not support advanced payments for services not yet delivered. We encourage suppliers to clearly outline in

their commercial proposal a payment schedule that aligns payments with the delivery of services. If your proposal includes significant discounts for any type of advance payment, please ensure this is reflected in your pricing structure.

6. Required Proposal Content

This RFP document is not intended to limit the Firm's submission content but rather to provide a framework for CGIAR to evaluate each proposal and determine which submission most closely addresses the needs. Firms are encouraged to provide any additional information or innovative approaches not specifically outlined in this RFP. Firms will provide any reasonable additional information upon request by the CGIAR.

a) General Information:

Name: Clearly state the legal entity name and address.

Primary Contact: Provide the name and title of the contact person including the full mailing address, e-mail address, and telephone number for direct communication.

b) Business Profile:

Overview: A brief summary of the Firm's business operations.

History: State the date and place of incorporation or establishment and the duration for which all core services and products have been provided.

Clientele and Sector Experience: Describe the types of clients and sectors the Firm has previously served, including the number of clients and geographic or sectoral spread, to demonstrate the breadth and diversity of experience.

Sustainability and Corporate Social Responsibility: Provide any information on the company's sustainability practices and corporate social responsibility initiatives.

The technical and commercial proposals should be submitted in separate documents.

6.1. Technical Proposal

The technical proposal must be a clear, detailed, rational, and concise description of how the Firm will address the CGIAR Security Operation challenge.

As the MSS industry is marked by innovation and complexity, your responses will help us navigate through the multitude of services offered and identify the solutions that best align with our collective requirements. To this end, we request that you adhere to the following guidelines in completing your proposal:

- **Required sections:** The proposal must contain a section corresponding to each of the areas identified below in the same order. Submission of the completed Technical Requirements

document is mandatory, and it must be maintained in the format and the xlsx extension of the file.

- **Structured Responses:** Please ensure that your answers are provided in the format specified in this document. This structured approach is vital for enabling an efficient and fair comparison and evaluation process by CGIAR Centers.
- **Clarity and Conciseness:** We ask that you provide clear, concise, and essential information in response to each question. It is important that your answers directly address the queries to facilitate our understanding of your offerings.
- **Reference to Appendices:** Should you wish to provide additional, detailed information beyond the scope of a direct answer, please feel free to include this in an appendix. Reference to these appendices in your responses will allow us to delve deeper into your value-added offerings as needed.

6.1.1. Corporate Capabilities

a) Where is your company headquartered? Indicate how many security operation centers (SOCs) you have, and where each one is located.

b) Provide a brief overview of your managed security services and any supporting products. Describe how a defense in-depth security approach will be used in the design, implementation and support of the SOC

c) Describe the architecture of your MSS delivery capability, including elements in your SOC, data center (on your premise, colocations, and private and public cloud services), network and our premises, as well as the centrally delivered log management, analytics and portal tiers, and capabilities for collecting event logs and data from other locations (e.g., software as a service [SaaS] and infrastructure as a service [IaaS]). Provide example architectural diagrams and descriptions. Indicate where there are any regional differences in architectures or technologies used. Finally, include and identify any elements that are delivered by third-party partners.

d) How many years have you been providing managed security services (MSSs)?

e) Describe all documented policies, procedures, and audit requirements that will ensure maintaining the privacy and confidentiality of CGIAR's data from the data of your other customers. Disclose all applicable national and international industry standards with which this service will comply.

f) Describe alliances with other companies you have that are related to your MSSs, such as using third-party software as part of your MSS portfolio.

g) Does your company subcontract MSS work to other third parties? If so, please list them based on the services in scope and describe your business relationship with each one.

h) Please provide an overview of your plans for continuity of service to CGIAR.

6.1.2. Qualifications and Staffing

a) Indicate how many MSS customers you have.

b) Please provide three or more references from companies using your service that are of a similar size to CGIAR with global operation (Preferably if the references are within the same sector as CGIAR). Firms should be prepared for checks with those references. CGIAR reserves the right to check references other than those provided by any Firm, and to verify with any Firm or with any third party any information set out in a Firm's Proposal. CGIAR may contact the references and others to confirm the details of the implementation of products and services like the Deliverables contemplated by this RFP.

c) Indicate the total number of employees in your company, and the number of employees responsible for MSS delivery.

d) Please describe the relative distributions of employees in your MSS company providing delivery, project management, and customer service and how these employees are geographically distributed.

e) What percentage of your staff has security certifications (list the certifications), and what is the average number of years of experience they have in performing security monitoring or security consulting? Are there any differences based on geographic location and/or SOC in terms of your staff's certifications and experience?

f) Provide a matrix of the staffing resources that will be involved with the design, implementation, administration, and support of the managed security solution. This must include their training, certifications, experience, qualifications, and responsibilities.

g) What is the ratio of monitored security devices to personnel? What is the ratio of managed security devices to personnel?

h) What is the average employment time of an MSS analyst within your company?

i) Describe your customer support tiers, including the capabilities and location of staff at each tier.

j) Indicate any industry certifications/attestations your security operation centers hold, such as the International Organization for Standardization (ISO) 27001. If so, please provide evidence.

6.1.3. Service Management

a) Indicate device/agent management and real-time event management notification service levels. Explain how they are measured and how they will be communicated to CGIAR. What outbound communication channels do you offer, and include any licensing price if CGIAR needs to cover it?

b) What access to internal auditing documentation will you provide if our auditors, customers, or business partners require this documentation in support of legal, regulatory, or contractual requirements? What is your process for requesting documentation? What are the time frames to which you will commit to producing documentation?

c) Describe the process should CGIAR have a complaint.

d) Indicate your process for notifying us of your non-compliance with the SLA and vice versa.

e) Describe the remedies available to CGIAR should you fail to meet any SLAs. Explain any regional variations to remedies.

f) Outline early termination penalties and charges. Describe how the costs are calculated to extract all captured data to be moved to another MSSP, if applicable.

g) Describe how CGIAR's data (including data generated by your company about security events and incidents affecting CGIAR) will be governed and protected in transit. Consider this from a technological perspective, as well as via processes and procedures. How will the treatment of CGIAR's confidential data assist with better job performance (e.g., creating internal architecture and topology maps)?

h) Provide examples of how your company has met specific regulatory or statutory requirements for the data within specific geographic or political boundaries. Provide answers only for regions or specific countries where there is concern.

6.2. Commercial Proposal

Proposed costs should be presented in US$ in a separate document from the technical proposal. The Firm should provide the cost structure, including (but not limited to) the cost breakdown for professional services, subscription and maintenance costs, one-off charges, recurrent costs, hourly rates, etc.

6.2.1. One-Time Costs:

MSSP should clarify the services that are paid for under this modality (e.g., implementation fees, shipping costs, training, etc.). Please be specific if these costs are per center/entity, per contract, or any other cost drivers for the one-time costs.

6.2.2. Maximum Cost:

A maximum total contract cost for the entire assignment. This "not to exceed" price will be based upon the Firm's analysis of the tasks, time, and talents required to perform the scope of services effectively.

6.2.3. Forensic Analysis Hours Package:

- Package Description: A package of forensic analysis hours will be available on demand for all CGIAR. The costs associated with forensic analysis of infrastructure that only affects

one center must be assumed by it. If the damage affects the shared infrastructure by all the centers, the cost will be divided among all the centers. Specify the number of hours included in the forensic analysis package for each billing cycle. Monthly reports detailing the usage of forensic analysis hours must be provided to CGIAR.

- Hourly Rate: Specify hourly rates for forensic analysis services required outside the package.
- Additional charges: Clearly outline any additional charges for forensic analysis hours beyond the package allocation.

6.2.4. Payment Terms for recurrent costs:

Please be specific on the cost per center/entity as well as the cost drivers used to determine the price allocated to each center/entity.

- The monthly invoice must be directed to each Center/Entity.
- Payment Due Date: Define the payment due date after the issuance of the invoice (e.g., Net 30).
- Late Payment Charges: Specify any late payment charges or penalties for overdue invoices if applicable.
- Early Payment Discounts: Specify any discounts offered for early payment of invoices.

6.2.5. Cost modeling for the engagement

- Core Services: Indicate and describe the licensing model(s) for your MSS offering for the Core Services (Scope of Services, Section D).
- Additional Services: Managed security service packages beyond the Core Services (e.g., Response support), which can be added at the discretion of individual Centers/OSU, should be presented separately. These additional services are being requested for informational purposes only so that CGIAR can evaluate the options. The inclusion of these additional managed security services does not imply an obligation to purchase them.
- How are costs negotiated for upgrading or expanding services? Please provide volume discounts if applicable.
- Can we add devices or data sources without affecting pricing or services?
- How would the purchase of the new security platform affect cost? Will the platforms (e.g., Sentinel, ADAudit) be included or available at a reduced price if recommended for the performance of the MSS offering?
- Will upgrading our current devices affect pricing?
- Provide any licensing and warranty information for third-party products you may require CGIAR to purchase to support this service.
- Indicate the discounts available based on the volume of services and contract length.
- Indicate any consulting support hours built into your standard MSS services.
- Indicate hourly or daily pricing for additional consulting hours we can purchase during the MSS engagement.

7. Proposal Evaluation

The purpose of this section is to outline the evaluation criteria and process that will be used to assess and select the most qualified firm.

7.1. Evaluation Criteria:

In the selection of the ideal service provider, a comprehensive evaluation will be conducted based on the subsequent criteria.

The evaluation and selection of a Firm will happen as a four-stage process, as follows:

a) Phase 1 – Mandatory Compliance
b) Phase 2 – Technical Proposal
c) Phase 3 – Presentations and Demonstrations
d) Phase 4 – Commercial Proposal

The overall scoring will be as follows:

Phase	Points
Phase 1 – Mandatory Compliance	No points – Pass/Fail only
Phase 2 – Technical Proposal	45 points
Phase 3 – Presentations and Demonstrations	30 points
Phase 4 – Commercial Proposal	25 points
Total	**100 points**

In our evaluation process, we may utilize the services of external agencies such as Dun & Bradstreet to assess the financial stability and business credibility of potential vendors. This assessment may include a review of creditworthiness, financial strength, and other relevant factors to ensure that we engage with reliable and reputable partners.

7.1.1. Compliant and Innovative Solutions

In addition to submitting a fully conforming Proposal that complies with all mandatory requirements, Firms are encouraged to demonstrate innovation through unique abilities, features, functions, or services.

7.1.2. Phase 1 – Mandatory Compliance

All Proposals will be reviewed for completeness and compliance with the RFP; this means the proposal needs to include all the answers to the technical requirements and the financial model for the services.
Subject to the terms of this RFP, any Proposals that do not meet the mandatory requirements, either through failure to meet or omission in any material respect, will be deemed noncompliant and will not be evaluated further. Proposals deemed to meet the mandatory response requirements will proceed to Phase 2 evaluation.

7.1.3. Phase 2 – Technical Proposal

In Phase 2 of the bid evaluation process, each Firm's Technical Proposal will be reviewed by the Evaluation Panel based on a set of technical evaluation criteria and scored accordingly. The weighting of the scoring of each section will be as follows:

Section	Max Score
Understanding of the Challenge	2
Proposed Solution	5
Project Management, Plan, and Timeline	3
Value Added Services	1
Qualifications and Staffing	4
Corporate Capabilities	5
Service Management	5
Technical Requirements	15
SLA	5
Total	**45**

7.1.4. Phase 3 – Presentations and Demonstrations

Phase 3 of the evaluation process will involve inviting Firms to present and demonstrate their solutions to a panel of subject matter experts, stakeholders, and decision makers at CGIAR to gain additional understanding regarding their proposals. This will include:

- Presentations from the Firm highlighting the key advantages of its proposal.
- A reference check and interview with former clients of the Firm.
- Interactive demonstrations to be conducted by representatives of the Firm, who will work with CGIAR's expert users to show how the Deliverables proposed to be provided by the Firm work.

Once the interactive demonstrations are complete, points will be awarded to each Proposal to which this Phase 3 applies. The score breakdown for Phase 3 will be as follows:

Section	Max Score
Bidder Presentation	10
Reference Checks	10
Scenarios and Demonstrations	10
Total	**30**

a) Bidder Presentation

Firms selected, based on the scores awarded in Phase 2, to move on to Phase 3 of the evaluation

process will be invited to present their Proposal. The Proposal will be presented virtually through "Microsoft Teams" in a 90-minute session, considering:

- The agenda and content for these meetings will be at the discretion of the Firm but are expected to include details of the Firm's proposed deliverables as relevant to the requirements of CGIAR, the way the Firm would perform the services, and specifics about the implementation team. Duration 60 minutes.
- A Question-and-Answer session should be scheduled at the end of the Firm's presentation. The Firm should use its discretion as to which of its representatives attend the presentation. Duration 30 minutes.

b) Scenarios and Demonstrations

In order to demonstrate both the functionality and usability of their proposed Deliverables, the Firms will be asked to run through specific usage scenarios see Annex 5. These scenarios will cover a variety of typical tasks that CGIAR staff do during normal operations. The demonstration will include an interactive session of two hours where the client can ask questions, seek clarifications, and provide feedback. The scenario run-throughs will:

- Be executed by key members of the Firm's implementation team.
- Be attended by CGIAR's operational and management employees.
- Cover a broad range of functional and cross-functional tasks.
- Provide CGIAR with a hands-on understanding of the Firm's system.

CGIAR will not, in any way, be responsible for any costs incurred by the Firm.

7.1.5. Phase 4 – Commercial Proposal

Following the completion of Phase 3, Phase 4 of the evaluation process will involve reviewing and comparing the cost of the Deliverables proposed by the Firm based on the pricing and terms information set out in the Firm's Commercial Proposal.

7.1.6. Final Scoring

Final scoring of the Firm submissions will be based on the combined scores achieved in Phases 2, 3, and 4.

NOTE: The Firms with the best scores will be called for the implementation of a proof of concept of the service. See Annex 6.

7.1.7. Other Evaluation Considerations

- Proposal Alignment:
  Expectation: The Firm's proposal should be clear, concise, and directly aligned with our specific requirements, demonstrating a thorough understanding and thoughtful approach to the project's objectives and deliverables.

- Experience:
  Expectation: The submission of relevant case studies that highlight the Firm's experience and success in similar projects. The showcased experience should resonate significantly with the needs and requirements of CGIAR.

- Reputation and References:
  Expectation: Provision of contact information for at least two previous clients or references who can attest to the Firm's competence, professionalism, and reliability in delivering high-quality service.

- Project Management and Communication:
  Expectation: Evidence of the Firm's proven strategies and tools for effective project management and communication, ensuring smooth collaboration, timely updates, and the efficient resolution of any issues or concerns.

- Contractual and Legal Compliance:
  Expectation: Assurance that the Firm comprehensively complies with all legal requirements and offers a transparent, fair contract that safeguards our interests.

- Data Security and Privacy:
  Expectation: Confirmation that the Firm adheres to industry best practices for data security and privacy, ensuring the utmost protection of sensitive information.

- Cost and Budget:
  Expectation: A clear, detailed breakdown of the Firm's pricing model, including upfront costs, ongoing maintenance fees, and any additional or hidden charges. The structure should offer value and offer reasonable fees while minimizing overall security-related expenses.

- Project Timeline
  Expectation: Presentation of a realistic yet flexible project timeline, ensuring the timely completion of deliverables without compromising quality.

- Deliverables:
  Expectation: Explicit definition of the scope of work and anticipated deliverables, ensuring they robustly align with the requirements.

- Scalability:

Expectation: To select an MSSP that can scale its services in line with our organization's growth and evolving security needs, ensuring long-term partnership viability.

- Flexibility and Customization:
  Expectation: To evaluate the MSSP's ability to customize security solutions and services to align with our specific business requirements, IT infrastructure, and risk profile.
- Reporting and Analytics:
  Expectation: To receive comprehensive and actionable security reports and analytics that provide insights into our organization's security posture and help inform strategic security decisions.
- Transition and Onboarding:
  Expectation: The MSSP will facilitate a smooth transition and onboarding process, ensuring minimal disruption to our existing security operations during the integration of MSSP services.
- Legal and Regulatory Compliance:
  Expectation: Assurance of the MSSP's stringent adherence to all relevant local, national, and international laws and regulations, including data protection standards like GDPR.

7.1.8. Basis for Contract Award

A contract will be awarded pursuant to this RFP to the Firm whose proposal is determined to be the most advantageous to CGIAR, taking into consideration the price, commercial terms and such other factors or criteria that are set forth in this RFP. The contract award will be subject to the timely completion of contract negotiations between CGIAR and the selected Firm.

CGIAR reserves the right to evaluate and/or reject all proposals, in whole or in part, and to waive or modify technicalities, irregularities, and omissions, or solicit new proposals if, in CGIAR's judgment, the best interests of CGIAR will be served. Following selection and prior to signing a contract, CGIAR reserves the right to further negotiate costs or other specifics.

CGIAR will conduct contract negotiations with the successful proposer(s). Should negotiations fail to result in an agreement within a reasonable period of time, CGIAR shall have the right to terminate negotiations. CGIAR may then select the next highest-rated Firm or take other actions consistent with the best interests of CGIAR.

7.2. Evaluation Process

The evaluation will be conducted based on the criteria outlined in this RFP. The RFP timeline may be modified if needed to benefit the RFP results while keeping interested parties well informed.

Evaluation Panel: An evaluation panel will be established to review and evaluate all proposals received. The panel will consist of representatives from CGIAR's relevant departments. The panel members will be selected based on their expertise and experience relevant to the RFP.

Evaluation Criteria: The panel will evaluate each firm's technical capabilities, including team composition, proposed approach and methodology, references, and cost.

Evaluation Process: The evaluation process will consist of the following steps:

- **Proposal review:** All proposals accepted by CGIAR will be reviewed to determine whether they are responsive or non-responsive to the requisites of this RFP. The panel will review all qualified proposals, assessing them against the evaluation criteria outlined in this RFP.
- **Evaluation and Scoring:** The evaluation panel will evaluate each shortlisted firm's proposal and presentation based on evaluation criteria. The scoring system listed below will be used to ensure consistency and objectivity in the evaluation process.
- **Proof of Concept (PoC):** After completing the presentations and demonstrations, the panel will recommend the selection of the firm(s) that best meet the RFP requirements and evaluation criteria to implement the proof of concept for a period of 30days with objective to evaluate the ability of MSSP to effectively monitor, detect, and respond to security incidents across on-premise and cloud infrastructure.
- **Firm(s) Selection:** After completion of the proof of concept duration, the panel will recommend the selection of the firm that best meet the RFP requirements and has successfully demonstrated the ability to provide the security services based on the outcome of the PoC.
- **Confidentiality and Conflict of Interest:** All evaluation panel members will be required to sign a Conflict-of-Interest statement and treat all information submitted by participating firms as confidential and used solely for the purpose of firm selection.

8. Bid Schedule and Dates:

The following schedule includes key milestones and their associated completion dates and is provided primarily for planning purposes. CGIAR System Organization may modify the project timeline at its discretion.

Event	Date
RFP Issue Date	March 1, 2024
Submission of letter of intent	March 10, 2024
Mandatory Bidder's Conference	March 15, 2024, at 2 pm CET
Deadline for Bidder's Questions	March 21, 2024, at 5pm CET

Event	Date
Responses to bidders Questions released	April 02, 2024,
Proposal Submission Deadline	Apr 22, 2024, at 2pm CET
Bidders Presentations	May 23 & 24, 2024
Bidder's Reference Checks	May 21-24, 2024
Interactive Demonstrations	May 27-31, 2024
Shortlisted Bidders Notified	Jun 10, 2024
PoC Implementation and development	June 17, to 1 Aug,2024
Notification to Selected Bidder	August 9, 2024
Timeframe for Contract Negotiations	30 days

9. How to submit a proposal:

Please submit via email a technical proposal and a commercial proposal as two separate documents to smo-bidding@cgiar.org. Both documents can be attached to the same email with the subject line "Managed Security Services Provider RFP."

The Proposal must be written in English and submitted in an electronic version in a Microsoft Word, Microsoft PowerPoint, Microsoft Project and/or Microsoft Excel, or searchable PDF format of the entire Proposal comprising the "Original" of the Firm's Proposal. Plus, the Excel file Technical Requirements.

a) Technical proposal document:

The Technical Proposal must answer the questions in section 6.1 of this document and include the answers to the RFP in the Excel file Technical Requirements.

It shall not contain pricing or financial data. The inclusion of any pricing or financial data within the Technical Proposal may render the Firm's proposal invalid.

b) Commercial proposal document:

This document will contain the detailed pricing as described in section 6.2. Indicate and describe the licensing model(s) for your MSS offering. We are interested in exploring several package options encompassing a range of services, starting from basic offerings and progressing to complete managed services. These package options should enable individual centers/OSU to choose the most suitable level of service while adhering to CGIAR's global policies.

All proposals must be received by April 22, 2024. Only electronically submitted proposals will be considered. Late proposals will not be accepted.

Annexes

Annex 1: CGIAR Standard terms and conditions (Attachment)

Annex 2: CGIAR Structural Model (Attachment)

Annex 3: Resources lists and distribution.

We have collected some global information that can help the MSSP to seize the required resources to cover the CGIAR environment.

a) **Productivity and Collaboration Suites:** The connection with these three tenants must be guaranteed so that they can be monitored.

Center/Entity	Productivity and collaboration suites
AfricaRice	M365 CGIAR tenant
Alliance	M365 CGIAR tenant
CIMMYT	M365 CGIAR tenant
CIP	M365 CGIAR tenant
ICARDA	M365 CGIAR tenant
ICRISAT	*M365 ICRISAT tenant*
IFPRI	M365 CGIAR tenant
IITA	M365 CGIAR tenant
ILRI	M365 CGIAR tenant
IRRI	*Google Workspace*
IWMI	M365 CGIAR tenant
OSU	M365 CGIAR tenant
SMO	M365 CGIAR tenant
WorldFish	M365 CGIAR tenant

b) **Monitored internal networks:** For the internal monitoring requirement we have requested to monitor the local networks from the centers, mainly from their headquarters locations, but also some centers are monitoring regional offices that have AD on-premises servers. The current distribution for devices is listed below:

#	Center/Entity	MDR Device (Throughput)	Number of Users	Bandwidth	Location
1	AfricaRice	1 x 1Gb			Abidjan
2	Alliance	1 x 1Gb 1 x 10Gb	800 70	1420 Mbps 1 Gbps	Palmira, Colombia Montpellier, France

#	Center/Entity	MDR Device (Throughput)	Number of Users	Bandwidth	Location
		1 x 10Gb	80	1 Gbps	Rome, Italy
3	CIMMYT	1 x 1Gb			Texcoco, Mexico
4	CIP	1 x 1Gb	400	1 Gbps	Lima, Peru
5	ICARDA	1 x 1Gb	100	2x20 Mbps	Cairo, Egypt
6	ICRISAT	1 x 1Gb	600	550 Mbps	Hyderabad, India
7	IFPRI	1 x 1Gb	300 (LAN and backup for the Wi-Fi) 300 (Wi-Fi and backup for the LAN)	1Gbps 1 Gbps	Washington, United States
8	IITA	1 x 10Gb	1400	2 Gbps	Ibadan, Nigeria
9	ILRI	1 x 1Gb 1 x 1Gb	375 692	150 Mbps 500 Mbps	Adis Adaba, Ethiopia Nairobi, Kenya
10	IRRI	1 x 1Gb	706	1 Gbps	Los Banos, Philippines
11	IWMI	1 x 1Gb	210	500 Mbps 50 Mbps	Colombo, Sri Lanka
12	OSU	NA			AWS Cloud
12	SMO	1 x 1Gb	60	1 Gbps	Montpellier, France
14	WorldFish	1 x 1Gb	120	200 Mbps	Penang, Malaysia

c) External surface that is integrated with the AD:

- For monitoring cloud-based entities, we are deploying EDR agents of SentinelOne, due to the characteristics of this environment.

Center	EDR count	Location
CGNET	10	Azure EU and CA
OSU	17	AWS

- For the servers (on-premises of the Centers) that are integrated with the AD, is also protected by the EDR platform of SentinelOne, the current agent distribution per center is listed below:

#	Center	Agents
1	AfricaRice	3
2	Alliance	24
3	CGNET	56
4	CIMMYT	5
5	CIP	2
6	ICARDA	13
7	ICRISAT	500 (for all computers)
8	IFPRI	141

#	Center	Agents
9	IITA	17
10	ILRI	18
11	IRRI	6
12	IWMI	1
13	OSU	17
14	WorldFish	2

d) **Active directory AD Audit Plus:** We currently have ADAudit Plus, integrated with the domain CGIAR.ORG and the M365 CGIAR Tenant.

Center/Entity	Integration with ADAuditPlus
AfricaRice	Yes
Alliance	Yes
CIMMYT	Yes
CIP	Yes
ICARDA	Yes
ICRISAT	No
IFPRI	Yes
IITA	Yes
ILRI	Yes
IRRI	No
IWMI	Yes
OSU	Yes
SMO	Yes
WorldFish	Yes

e) **External Surface reported by the centers:** This referred to the external surface that we have been monitoring. It comprises the centers IP ranges that belong to the shared AD hybrid platform, but also, it contains IP for cloud providers and regional offices.

Center/Entity	Ips	Locations
AfricaRice	5	2
Alliance	1341	5
CGNET	4	1
CIMMYT	21	2
CIP	33	2
ICARDA	31	12
ICRISAT	28	1
IFPRI	15	1
IITA	8	3

Center/Entity	Ips	Locations
ILRI	7	2
IRRI	30	1
IWMI	11	7
OSU	39	2
SMO	31	2
WorldFish	6	4

Annex 4: Satisfaction Survey

On a scale of 1 to 5, How satisfied are you with the delivered service in terms of the following aspects? where:

1. = Extremely dissatisfied.
2. = Somewhat dissatisfied.
3. = Neither satisfied nor dissatisfied.
4. = Somewhat satisfied.
5. = Extremely satisfied.

N/A. = Not Applicable *

	1	2	3	4	5	N/A
How would you rate the overall quality of the MSSP's security services?	○	○	○	○	○	○
How effective is the MSSP at detecting threats and reducing risk to your organization?	○	○	○	○	○	○
Relevance and usefulness of the recommendations provided by the MSSP	○	○	○	○	○	○
Completeness and accuracy of the incidents and the reports.	○	○	○	○	○	○

Annex 5: Scenarios and Demonstration

The demonstration will focus on showcasing the key features and capabilities of the MSSP services. Considering the infrastructure currently managed around the CG Centers, the proposed minimal components to be included in the demo are presented. The demo needs to run for three days to capture data and show historical dashboard for this period.

1. Infrastructure:

- 3 Windows Server VMs
- 2 Linux Server VMs
- AWS VPC with a public-facing web server
- Network with 2 windows client machines.
- Integration with Microsoft 365 Tenant

2. Monitoring Configuration:

2.1. MSSP Platform:

- Deploy MSSP platform in all the infrastructure for comprehensive security event collection.
- Configure the MSSP platform to ensure seamless data aggregation.

2.2. Detection Signatures and Analytics Rules:

- Enable relevant detection signatures and analytics rules tailored to the environment's specific needs.

2.3. Access for Client Security Team:

- Provide the client security team with access to the MSSP platform for real-time monitoring.

3. Simulated Attacks:

3.1. Web Application Attacks:

- Execute simulated OWASP Top 10 web application attacks on the public web server within the AWS VPC.

3.2. Malware Execution:

- Run malware executables on endpoint VMs to assess the effectiveness of endpoint protection.

3.3. Vulnerability Scans:

- Conduct vulnerability scans using nmap from a separate VM to identify potential weaknesses.

3.4. SSH Brute Force:

- Attempt brute force SSH attacks on Linux servers to evaluate intrusion detection and prevention.

3.5. Endpoint client attack:

- Attempt to connect (browsing) to a suspicious website from the windows client machine.

4. Demonstration Session:

4.1. Platform Capabilities:
- MSSP conducts a comprehensive walkthrough of core platform capabilities over a 2-hour session.

4.2. Dashboard Views:
- Showcase dashboard views illustrating real-time security events and alerts.

4.3. Incident Reports:
- Provide detailed incident reports for each injected threat, outlining impacted assets, severity ratings, and mitigation advice.

4.4. Threat Hunting and Forensics:
- Discuss the MSSP's process and capabilities for threat hunting and forensic data collection.

5. Success Criteria:

5.1. Timely Incident Detection:
- Detection of injected incidents with alerts within 1 hour to demonstrate real-time responsiveness.

5.2. Comprehensive Incident Reports:
- Incident reports include details on impacted assets, severity ratings, and actionable mitigation advice.

5.3. User Interface Expectations:
- Platform UI and reports meet expectations around usability, clarity, and customization.

Annex 6: Proof of Concept

1. Objective:

The objective of this PoC is to evaluate the ability of MSSP to effectively monitor, detect, and respond to security incidents across on-premise and cloud infrastructure.

2. Scope:

The PoC will cover monitoring and detection of security events for:

- 2 Centers located in different Time Zone (If agent installation is required, it will cover at least 10 servers on Windows and 5 on Linux, and 20 end-user computers).
- At least 3 virtual machines in AWS
- At least 2 virtual machines in Azure
- CGIAR Microsoft 365 Tenant

For the vulnerability and threat intelligence:

- Vulnerability assessment of at least 10 public IP addresses (one per month)
- Threat intelligence for 5 platforms/services (once per week)

3. Duration:

The PoC will run for 30 days.

4. Monitoring and Detection Approach

- MSSP will deploy their monitoring platform on all in-scope assets to collect security event data.
- Signatures and analytics will be configured to detect potential incidents like malware execution, unusual network activity, privilege escalation attempts etc.
- Alerts will be generated in the MSSP SIEM platform when thresholds are crossed.
- Daily, weekly, and monthly reporting will provide visibility into security events.

5. Response Approach

- MSSP will provide 24x7 monitoring and alert triage capabilities.
- Incidents will be documented with comprehensive details on symptoms, impacted assets, severity, recommendations etc.
- For critical incidents, MSSP will notify client contacts within 2 hours via email and phone.

6. Vulnerability and threat management Approach

- MSSP will run a vulnerability assessment for the Public IP addresses.
- MSSP will provide the report on the findings.
- MSSP will report per week the threat intelligence associated with the reported platforms/services.

7. Success Metrics

- Mean time to detect (MTTD) threats across the environment should be less than 1 hour.
- At least 200 valid security events detected each day.

- A false positive rate < 10% monthly.
- Incident reports should document root cause, specific assets impacted and include response recommendations.
- Client contacts are notified by MSSP of critical incidents within 2 hours at least 95% of the time.
- Vulnerability assessment report.
- Threat intelligences reports.

Annex 7: Technical References (Attachment)