Project KSV/023
Sustainable and Inclusive Growth in Kosovo

Addendum N°2- To the tender dossier KSV/023•25 7989

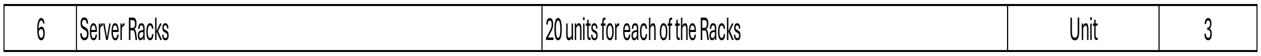
Title: Cybersecurity lab equipment supply, installation and training within the cybersecurity agency (goods)

The following part of the Tender dossier is replaced /modified as follows:

Part I:

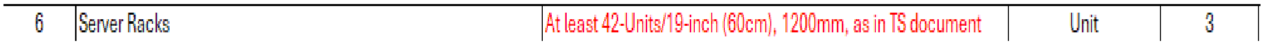
- **8 KSV/023 • 25 7989 Price Schedule**

Previous version:



6	Server Racks	20 units for each of the Racks	Unit	3

Replaced by:
The description of Item 6 of the Price schedule is replaced with the updated text as follows



6	Server Racks	At least 42-Units/19-inch (60cm), 1200mm, as in TS document	Unit	3

Part II:

- **7 KSV/023 • 25 7989 Technical specifications**

Previous version:

7 KSV/023 • 25 7989 Technical specifications

Replaced by:

The previous version of the Technical Specifications is replaced by the attached updated document. All modifications have been highlighted using track changes for ease of reference.

TECHNICAL SPECIFICATIONS

TENDER N°KSV/023•25 7989

1. BACKGROUND INFORMATION AND CONTEXT

The mission will take place in the context of the project “Sustainable and inclusive growth” in Kosovo. This area is relatively new and follows SDG 8 of the United Nations, defined as “Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all”. Both governments see the area as an opportunity to open a way to diversify their partnership on topics of high interest, such as the green transition, digital transformation, strengthening the innovation ecosystem and the capacities in cybersecurity.

The KSV/023 “Sustainable and inclusive growth in Kosovo” project aims to contribute to sustainable economic growth by supporting innovation, inclusiveness, and social development in a greener Kosovo. The project aims to encourage innovation and local and foreign investments in an e-secured and transparent environment. The assumption is that through fostering innovation and foreign investments, more jobs are created, resulting in an improvement of the government finances and people wellbeing.

The project’s first component is establishing the Sovereign fund of the Republic of Kosovo (SFRK). The fund promises to improve government finances and attract foreign investments, which would lead to economic growth. The counterpart is the Office of the Prime Minister (OPM).

The second component will improve cybersecurity, as Kosovo has a growing Information and Communication Technologies (ICT) sector undergoing a digital transformation, which needs protection against hybrid cybersecurity threats. The partner is the Ministry for Internal Affairs (MIA).

The third component refers to entrepreneurs' stimulation of innovation in the private sector to increase the value added to products and services and overcome barriers to export, leading to economic growth. It will be implemented by the Ministry of Industry, Entrepreneurship and Trade (MIET).

The fourth component relates to the support for digitalization at Parliament in replacing its non-functional electronic voting system as it will improve not only transparency and accountability of voting but also is expected to enhance information services to the public and remove a specific hurdle on the path to integration into the European Union (EU). The counterpart is the Parliament of Kosovo.

Therefore, the project is structured around four results, which are:

- Result 1: the SFRK is ready for implementation;
- Result 2: civil servants’ cyber security capabilities are improved;
- Result 3: the innovation fund for the development of private companies is up and running;
- Result 4: an e-voting system for Parliament is operational.

The current mission will focus on the result 2 – civil servant’s cybersecurity capabilities are improved. Main partner for this result is the Ministry of Internal Affairs (MIA).

In October 2023, the Government of Kosovo approved the National Cybersecurity Strategy 2023-2027 and Action Plan 2023-2025. The strategy has six key objectives, two of which pinpoint the importance of creating institutional cybersecurity capacities at the national level and developing a sustainable cybersecurity capacity for the government and the private sector.

As one of the highest-potential industries in the country, ICT holds a very important role in Kosovo. About 99.7% of households have access to the internet through different devices, and optic fiber connectivity. In an ever-growing environment of cybersecurity threats, Kosovo finds a great need to establish mechanisms such as the Cybersecurity Agency – in the quest for reaching Cybersecurity Strategy Objectives. Deriving from the strategy and action plan, Law no. 08/L-173 on Cybersecurity has given a legal foundation to the Cybersecurity Agency, while defining its scope of activities and responsibilities in implementing the Cybersecurity Law in Kosovo.

The main cybersecurity stakeholders include but are not limited to the Cybersecurity Agency (CSA), Agency for Information Security (AIS), Ministry of Internal Affairs (MIA), the Office of the Prime Minister (OPM), and Kosovo Institute for Public Administration (KIPA). Cyber defense actors exist yet are governed by the Ministry of Defense and belong to a different security domain. Respective to cybersecurity the CSA, MIA, AIS, and OPM remain imperative actors toward providing important suggestions and ensure the content is always informed by national security policies and objectives.

During 2024, the project assessed the cybersecurity lab needs to determine the scope for the cybersecurity lab to be placed within the Cybersecurity Agency (CSA). Supporting advice was provided by the Luxembourg House of Cybersecurity (LHC), online and through site visits in Kosovo. In such a perspective, the contractor may be required to interact with different stakeholders and consider the baseline studies as documents made available by the project.

With the rapid rise of cyber threats globally, malware continues to be one of the most disruptive and sophisticated attack vectors. From ransomware targeting public institutions to nation-state actors developing advanced persistent threats (APTs), there is a growing need for specialized resources dedicated to understanding and mitigating these risks. The Kosovo Cyber Security Agency (CSA) is tasked to maintain the cybersecurity posture of public institutions, private critical infrastructure, and private sector.

In this respect, the document outlines the proposal for establishing an **Integrated Malware and Threat Analysis Lab** within the Cyber Security Agency (CSA). The lab aims to enhance the national capability to detect, analyse, and respond to malware and cyber threats affecting public institutions, private sector, and critical infrastructure. The proposal integrates advanced technologies and methods for malware analysis, reverse engineering, and threat mitigation, supporting CSA's mission to safeguard national cybersecurity.

1. OBJECTIVES AND EXPECTED OUTCOMES

As the Cyber Security Agency (CSA) is about to be established, there is currently no dedicated lab or tools in place to support their cybersecurity efforts. This lack of infrastructure means that the agency is unable to effectively address the growing complexity of malware threats. Without advanced and scalable tools, the agency will struggle to conduct reverse engineering, analyse emerging and evasive malware, or respond promptly to advanced threats. Therefore, equipping the agency with the necessary capabilities to establishing a Malware and Threat Analysis Lab will be vital for enabling the agency to protect the country's critical assets effectively.

The **Integrated Malware and Threat Analysis Lab (here forth: Lab)** aligns with the CSA's mission to enhance national cybersecurity capabilities by providing:

- **Advanced malware analysis:**
  Conduct malware analysis, dissect malware, and understand tactics used by attackers.
- **Threat intelligence and collaboration:**
  Work with global bodies to ensure integration with international threat intelligence platforms.

The key objectives of the **Integrated Malware and Threat Analysis Lab** are:

- Perform in-depth **static and dynamic malware analysis** using advanced sandboxing and reverse engineering tools.
- **Reverse engineer malware samples** to gain insight into their functionalities, uncover attack vectors, and understand threat actors' TTPs (Tactics, Techniques, and Procedures).
- Use **AI/ML-driven tools** for **behavioural analysis and anomaly detection**, improving identification of new and unknown malware.
- Support **incident response** through actionable intelligence, identification of Indicators of Compromise (IOCs), and creating detection signatures.
- Foster **cybersecurity research**, developing tools and techniques to pre-emptively counter emerging threats.

The expected outcomes of the Lab include the establishment of a comprehensive sample repository, complete with detailed analyses of their behaviors and functionalities. This shall enhance the understanding of threats and improve mitigation strategies.

Additionally, the lab shall strengthen detection and mitigation capabilities for both known and emerging malware through refined analytical processes and specialized toolkits.

In-depth reverse engineering reports shall outline the **tactics, techniques, and procedures (TTPs)** of threat actors, aiding in the formulation of effective defense strategies. Furthermore, the development of case studies will provide valuable training resources for cybersecurity professionals and incident response teams, enhancing their skills and knowledge.

The lab shall also improve the identification and classification of previously unrecognized malware variants by **employing AI-driven behavioral analysis techniques**. **Automated malware** detection systems shall be implemented to enhance real-time threat identification capabilities. Moreover, the lab shall ensure the timely production of actionable threat intelligence reports containing **Indicators of Compromise (IOCs),** to support organizations in proactively preventing and responding to cyber threats. Precise detection signatures shall be created and integrated into cybersecurity solutions to bolster network defenses.

2. TASKS AND DELIVERABLES

2.1. Scope of Work

The **Scope of Work** description aims to ensure that the **Integrated Malware and Threat Analysis Lab** aligns with the strategic needs of the Cybersecurity Agency and positions the lab to be at the forefront of malware research, threat intelligence, and incident response.

Establishing a Malware Analysis Environment:

- Setting up isolated virtual environments (VMs) for safe malware analysis and reverse engineering;
- Deploying automated sandbox environments (e.g., Cuckoo Sandbox) to study malware behaviour in a controlled setting;
- Implementing tools for both static analysis (e.g., Ghidra, IDA Pro) and dynamic analysis (e.g., process monitoring, memory dumps).

Conducting Research on Advanced Threats:

- Setting up dedicated systems for conducting research on advanced malware, APT campaigns, and global threat trends;
- Collaborating with international cybersecurity forums, CERTs, and other research institutions for knowledge exchange;
- Developing long-term research projects aimed at addressing specific threat landscapes, such as ransomware or nation-state-sponsored attacks.

Integrating and Managing Threat Intelligence Feeds:

- Configuring and maintaining threat intelligence platforms such as MISP and integration of both open-source and commercial threat feeds;
- Building correlation engines to compare the lab's findings with global trends to detect new patterns;
- Creating threat-sharing protocols with partners to maintain a continuous feedback loop.

Developing Incident Response Playbooks:

- Creating step-by-step guides and playbooks to handle different attack scenarios (e.g., ransomware, DDoS, phishing campaigns);
- Training personnel to improve response time during active incidents;
- Documenting lessons learned from each incident and updating the response strategies accordingly.

2.1.1. Malware Analysis

The lab shall establish specialized environments for conducting comprehensive malware analysis, encompassing both static and dynamic analysis techniques. This dual approach will enable researchers to gain deeper insights into malware behaviour and functionalities.

Static Analysis: In this phase, the lab will utilize advanced tools such as PEStudio and Binary Ninja to perform an in-depth examination of malware samples without executing the code. Static analysis involves extracting valuable metadata and characteristics from the binaries, including file properties, entropy levels, and embedded resources. By analysing these elements, researchers shall be able to identify indicators of compromise (IOCs), such as file hashes, and discern potential malicious functionalities. Static analysis also aids in understanding the structure of the malware, helping to reveal coding patterns, potential vulnerabilities, and the methodologies employed by malware authors.

Dynamic Analysis: Complementing the static analysis, the lab will employ robust sandboxing environments, such as Cuckoo Sandbox or like execute malware samples in isolated, controlled settings. This dynamic analysis will allow researchers to observe malware behaviour in real time as it interacts with the operating system and network resources. By monitoring various activities, such as file creation, registry modifications, and network communications, the lab will gain critical insights into the malware's operational tactics, techniques, and procedures (TTPs). Dynamic analysis is essential for identifying the impact of malware on a system, as well as for detecting any attempts at evasion or obfuscation.

2.1.2. Reverse Engineering

This industry-standard disassembler and debugger will be utilized for detailed analysis of executable files. IDA Pro allows researchers to disassemble binaries and examine their structures, enabling a deeper understanding of malware functionalities and logic.

To dissect and understand the internal mechanisms of malware, the lab may use:

- **IDA Pro** for disassembly and debugging;
- **Ghidra** and **x64dbg** for decompiling malware code and studying its logic.

This will allow the lab to break down obfuscated malware, identify embedded code, and analyse malicious scripts.

2.1.3. Memory and Network Analysis

For memory forensics, the lab may utilize tools such as Volatility and Rekall, Memorize, Security Onion to analyse memory dumps, enabling the identification of hidden malware artifacts that may not be visible through standard analysis methods. This process is crucial for uncovering advanced persistent threats (APTs) and other sophisticated malware that operates within system memory.

In addition to memory analysis, the lab may implement network traffic analysis using tools like Wireshark and Zeek. These tools will monitor network behaviours associated with malware infections, allowing the lab to detect and analyse command-and-control (C2) traffic. By scrutinizing network traffic patterns, the lab can identify malicious communications between compromised systems and external entities, providing vital insights into ongoing attacks.

2.1.4. AI/ML-Driven Detection

The integration of machine learning into the Integrated Malware and Threat Analysis Lab will significantly enhance its capabilities in malware detection and classification. By employing advanced frameworks such as TensorFlow, Scikit-learn, PyTorch, and Keras, the lab can efficiently classify various types of malwares and gain a deeper understanding of the threat landscape.

This approach will enable the detection of anomalies within datasets, helping identify unusual patterns indicative of malicious activity. Additionally, algorithms like Random Forest, Support Vector Machines (SVM), and Neural Networks will improve the accuracy of analyses and facilitate the discovery of previously unknown malware variants.

The ability to rapidly analyse large volumes of data will empower the lab to respond to evolving threats in real time, thereby strengthening its overall cybersecurity posture. Furthermore, the incorporation of deep learning techniques will enhance the detection of sophisticated malware that may evade traditional methods. Ultimately, this diverse array of machine learning tools will foster continuous innovation in threat detection and response strategies.

2.1.5. Threat Intelligence Integration

The lab shall connect with threat intelligence platforms like MISP or similar and create custom YARA rules for identifying specific malware strains based on emerging threat intelligence feeds.

TECHNICAL SPECIFICATIONS TABLE

	HARDWARE EQUIPMENT		
#	Description	Unit	QTY
1	**High-Performance Servers** Purpose: The servers will run dynamic malware analysis, manage virtual environments, and host data-intensive AI/ML models. **Technical Specifications:** - **Processor:** Number of processors: 2 5th Gen Intel® Gold Xeon® Scalable Processors, 16 cores, minimum 37 MB Cache, at least 2.8Ghz - **Memory**: 32DIMM slots. Must be offered with 512 GB RAM Memory using DDR5-5600 - **BOOT optimized storage** 2 x 480 GB M.2 NVMe SSD - **HDD Bays** Up to 8 SFF - **Storage** Server must be supplied with 5 x 1.92TB SSD Drives, Server must be supplied with RAID Controller with 4GB Cache. - **Networking features** Server must be supplied with: 2 x 10GB 2-port BASE-T adapter - **Power Supply** Server must be supplied with minimum 2 x 1000W Titanium Hot Plug Power Supply - **Fans** Redundant hot-plug system fans - **Operating Systems and Virtualization Software Support:** Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Vmware ESXi, Canonical Ubuntu, Oracle Linux and Oracle VM, Citrix - **Chassis** 1U Rack Mountable **Example Hardware:** Dell PowerEdge R750 or HP ProLiant DL380 Gen10 servers with the above specifications. The hardware must also include effective precision cooling system with the set.	SET	2
2	**Advanced Workstations** **Purpose:** Perform reverse engineering, memory analysis, and malware monitoring. Should be optimized for heavy workloads, including running disassemblers, debuggers, and analyzing network traffic. **Technical Specifications:** - **Type** Business Class Workstation Desktop - **Form factor** Tower - **Processor** At least Intel i9, Intel Xeon W5-2545 vPro, Ryzen 9 or latest - **RAM Memory** Installed 64GB DDR5 4800, with support up to 512GB - **Graphics** Discrete NVIDIA RTX 4000 Ada 20GB 4DP GFX - **Storage**1x 2TB PCIe 2280 TLC M.2 SSD, 1x 4TB 7200 SATA Enterprise 3.5-inch Hard Disk Drive - **Network** Integrated Gigabit Ethernet RJ-45 - **Ports** 2x USB-C 3.2 Gen 2x2 with 20Gbps speed and Power Delivery, 8x USB-A 3.2 Gen 1x1 with 5Gbps speed, 1x Headphone/Microphone Combo - **Security** Integrated TPM 2.0 convertible to FIPS 140-2 - **Power Supply** At least 750W, 220-230V - **Input/output** Same brand QWERTY Keyboard and Mouse, included - **Operating System** Genuine Windows 11 Pro, factory preinstalled **Example Hardware:** Dell Precision 5820 or HP Z4 G5 workstations with the above specifications.	SET	4

3	**Secure Storage Solutions** The lab will deploy NAS (Network Attached Storage) or SAN (Storage Area Network) systems with built-in encryption and daily backups to securely store malware samples and analysis reports. All storage will be configured with AES-256 encryption to protect sensitive data from unauthorized access. **Technical Specifications:** - **Operating System & Clustering Support:** The storage array must support Windows (2016, 2019, 2022), VMware, and Linux, with clustering for all. - **Capacity & Scalability:** Must have 86TB RAW capacity with 12G Enterprise 10K SFF SAS drives, support SFF and LFF drives, and scale up to 90 SAS SFF drives. - **Front-end & Back-end Ports:** Must include 10GBaseT iSCSI controllers (2 ports each) and support 12G SAS back-end connectivity. Servers and storage must be from the same vendor. - **Architecture:** Must have dual, redundant, hot-pluggable, active-active array controllers for high performance and reliability. - **No Single Point of Failure:** Must ensure redundancy in controllers, cache, fans, and power supply. - **Disk Drive Support:** Must support enterprise SAS, SSDs, near-line SAS 7.2K RPM, and FIPS 140-2 self-encrypting drives. - **Cache:** Each controller must have at least 12GB cache with backup. Must support a minimum of 8TB flash cache. - **RAID Support:** Must support RAID 1, 10, 5, and 6 with thin provisioning, and include all required licenses. - **Virtualization & Thin Provisioning:** Must allow volume striping across spindles in a disk pool with RAID 1, 10, 5, and 6, and support thin provisioning. - **Warranty:** Vendor must provide a three-year warranty with 8x5 next business day basic support. **Example Hardware: Synology NAS RS4021xs+** or **QNAP TS-883XU-RP** for NAS, or **Dell EMC PowerVault ME4024** for SAN.	SET	1
4	**Network Infrastructure** A secure and fast network infrastructure is crucial for seamless communication between servers, workstations, and external threat intelligence platforms. This infrastructure will also help isolate the malware analysis environments from the rest of the organization's network. - **Networking:** 10GbE switches will be used for high-speed communication between servers and workstations, ensuring low latency and high throughput during analysis. - **Security:** Firewall solutions will be configured, with segmentation to isolate the malware lab from other networks, ensuring secure operation. **Technical Specifications:** - **4.3: Two (2) Core Switches:** Managed Layer-3 switches with 10GbE support (e.g., **Cisco Catalyst 9300**). - **4.1: One (1) Firewall:** Enterprise-grade firewalls with next-generation features like **Deep Packet Inspection (DPI)**, **Intrusion Detection Systems (IDS)**, and **Intrusion Prevention Systems (IPS)**. - **4.4: 25 VPN Access:** Secure VPN for remote analysts to access the lab in a controlled manner, with two-factor authentication and encryption, for min. 38 users. - **4.5: One (1) IPS/IDS:** Tools-like **Snort** or **Suricata** for real-time intrusion detection and prevention.		

	Segmentation: VLAN and subnet configurations to isolate malware research networks from internal systems. **Technical Specifications for Switches (4.3):** - **Interfaces** Ethernet Ports: 24 ports gigabit Ethernet. SFP ports: 4 SFP+ slots 10Gigabit with transceiver 10G SR included for each port, 1 console port, 1 USB port, Rack mounted - AC 100- 240V (60 Hz), - **Performance** Switch capacity at least 120 Gbps, VLAN supported at least 3900 VLAN - RAM Memory - 1 GB, Flash - 512 MB, Layer Supported – Layer 2, 3, Should support Stacking functionality - **Functions** IPv4 dhe IPv6, ARP, STP BPDU port protection, DHCP, QoS, Static Routing, RIPv2, PBR, Dynamic Segmentation, IEEE 802.1q – VLAN, IEEE 802.1p, - **Security** SSH, SSL, 802.1X, port security, DHCP snooping, IP source guard, STP Root Guard - Storm control, ACLs - **Management** Device management - via Web GUI, SSH, console - **Warranty and Licensing** Warranty and support for a minimum period of 3 years **Technical Specifications for Routers (4.2):** - **Interfaces:** Minimum 9 ports gigabit Ethernet, Minimum 1 port gigabit SFP, 1 console Port. 1 Usb Port, 8 GB Memory, External Power supply, AC 100- 240V (60 Hz) - **Capacity:** Forwarding throughput at least 1.6 Gbps, IPsec Throughput at least 0.45 Gbps - Number of IPsec tunnels at least 95, Number of routes at least 700K - **Features:** IPv4, IPv6, static routes, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Classification, prioritization, remarking, shaping, scheduling, policing, mirroring, Multicast IPv4 Support, SNMP, NTP, DNS client, Dynamic Host Configuration Protocol (DHCP), DHCP client, DHCP server, NAT, SSH, ACL - **Security:** Security Zone Network Firewall, IPsec site to site VPNs, PKI Encryption: AES-256, Internet Key Exchange (IKE), PKI Authentication: AAA, RSA (2048 bit), ESP-256-CBC, HMAC-SHA1, Integrity: SHA-1, SHA-2 - **Management:** Device management - via Web GUI, SSH, console. - **Warranty and Licensing:** The device must include all necessary licenses for the described services along with vendor support for a minimum period of three years. **Technical Specifications for Firewall (4.1):** - **Interfaces:** Minimum 8 ports gigabit Ethernet, 1 port gigabit Ethernet management port, 1 console port, 1 USB port, external power supply (AC 100-240V, 60 Hz). Onboard storage must be at least 480GB, and the device must be rack-mountable. - **Performance:** Firewall throughput must be at least 6.4 Gbps, IPsec VPN throughput at least 5 Gbps, IPS throughput at least 5.7 Gbps, and the system must support at least 200,000 concurrent sessions. - **Security Features:** Encrypted traffic analysis, VPN and remote user access support, intrusion prevention system, advanced malware protection, and URL filtering services. The solution should include 25 secure VPNs for remote analysts to access the lab with two-factor authentication and encryption. - **Management:** Device management via Web GUI, SSH, and console. - **Warranty and Licensing:** All necessary licenses for described security services and vendor support for a minimum period of three years.	SET	1

	IPS/IDS (e.g., Snort & Suricata) (4.5) : (as separate software solutions) General Requirements - The solution must be Network Intrusion Detection and Prevention System (NIDS/NIPS) based on open source that monitors network traffic in real-time to detect and block threats. The solution must have the following features - Packet sniffing and logging - Extensive Rule Set, rule-based language that combines anomaly, protocol and signature inspection methods, additionally it uses free community rules and commercial rules. - The solution must have the possibility to for custom rule creation, - To have the possibility to integrate with SIEM and security tools, - Every type of IDS/IPS, with every mode of detection - packets based on rules; - Can block potential attack vectors (IPS part). - Real-time traffic monitor on IP level. - Flexible rulemaking. - Debug logged traffic (needs to be logged with the use of rules). - Can generate alerts based on rules, with precise conditions. The solution has to be High-Performance Network Threat Detection & Prevention Engine and Network Security Monitoring (NSM) tool and to provide multi-threaded, high-speed packet processing with advanced detection capabilities. The solution must have: - Multi-threaded Architecture - Protocol Awareness - Extensive Rule Sets - File Extraction and Inspection - Logging and Output Flexibility - Resource heavy - Incident Response - Hybrid detection capabilities - Active Response (IPS)		
5	**Monitors for High-Performance Servers and Workstations - 29-inch monitors** - **Type** Professional 29-inch 4K Thunderbolt 4 Monitor - **Size** 29-inch - **Resolution** 4K UHD (3840 x 2160 @ 60 Hz) - **Display Panel** IPS Black; LCD - **Aspect Ratio** 16:9 - **Contrast Ratio** At least 2,000:1, and 10000000:1 dynamic - **Mechanical** Tilt, Swivel, Pivot +- 90, Height Adjustment - **Response time** At least 5ms - **Connectivity** 1 RJ-45 (10/100/1000 Mbps). 1x DP 1.4, 1x HDMI 2.0. 1 SuperSpeed USB Type-C with at least 5Gbps signalling rate (Up to 15W USB Power Delivery) - **Features** Flicker Free, Low Blue Light Certified - **Security** Security Lock ready - **Warranty** 3 Years manufacturer's warranty must be offered. *Four (4) monitors for the high-performance servers. Eight (8) monitors for the workstations.	Unit	12
6	**Server Racks** **Technical specifications:** - **Type** Floor-standing Rack Cabinet - **Height/Width** At least 42-Units/19-inch (60cm) - **Depth** 1200mm	Unit	3

	- **Locks/Doors** Front and rear doors with lock/Front door can be made from glass. - **Protection** IP20 minimum. - **Construction material** Metallic, Steel. - **Load** At least 1000kg - **Plug type: Kosovo and EU Standards**		
7	**Power cooling system as and where relevant (thermostat-controlled air cooled fans)**	Unit	3
INSTALLATION (on premise), AND MAINTENANCE FOR ALL EQUIPMENT SHALL BE INTEGRATED IN THE PRICE. Warranty of 3-years must be offered from the vendor inclusive of 8 x 5 x next business day service warranty must be included. The installation and setup must be conducted, completed, and functionalized to work seamlessly, including relevant maintenance matching the patching requirement from the tools section below.			
8[1]	**Reinstallation of the equipment (See note regarding conditional pricing and Cyber Agency readiness)**	**Set**	**1**
TOOLS AND TECHNOLOGIES			
#	**Description**	Unit	QTY
9	**Sandboxing and Malware Analysis Tools** - e.g. Cuckoo Sandbox for real-time malware behavior analysis in isolated environments. - e.g. VirusTotal for cross-referencing malware samples with global threat databases. **General Requirements:** The vendor must provide, implement, and support a scalable malware analysis sandbox, assisting with setup, optimization, and maintenance. It must support on-premises deployment with optional cloud execution, allow customization, and update detection automatically. The vendor must also provide support documentation, and the manual of installation. A volume of minimum 700 sample analysis per day, burst rate 30 per hour. **Malware Analysis Capabilities:** The solution must support analyzing executables (.exe, .dll, .bat, .scr, .msi), office documents (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .rtf), PDFs, archives (.zip, .rar, .7z, .tar, .gz), scripts (.vbs, .ps1, .js, .py, .sh), URLs, web content (HTTP, HTTPS, JavaScript, Flash), and Android APKs. It must generate comprehensive reports detailing API calls, process execution, registry modifications, file system changes, network activity (DNS, HTTP/HTTPS, C2 detection), memory analysis, execution screenshots, and YARA rule results. The system must support static and dynamic analysis, leveraging machine learning and heuristic detection for advanced threat identification. **Virtualization and Execution Environment:** The solution must support a multi-VM architecture for analyzing malware across Windows (10, 11, Server), Linux (Ubuntu, Debian, CentOS), and Android (emulated). It should allow custom VM images, kernel and user-mode monitoring, snapshot rollback for VM resets, and bare-metal analysis on physical machines. **Integration & API Support:** The solution must offer a RESTful API for automated submissions and result retrieval. It should integrate with SIEM, SOAR, and threat	Licenses	3

[1] Reinstallation of the equipment and tools Items 8 and 25 are conditional upon the readiness of the Cyber Agency. If the Cyber Agency is not ready and the reinstallation does not take place, these items shall not be invoiced, but the contractor guarantees the price up to 31.10.2026.

	intelligence platforms like ELK, Splunk, Security Onion, TheHive, and MISP. It must support STIX/TAXII for threat sharing and allow custom plugin and module development. **Security & Isolation:** The sandbox must be fully isolated from the internal network and support network simulation with TOR, VPN, proxy, and fake traffic. It must prevent detection and evasion techniques and include anti-VM detection bypass mechanisms. **Performance & Scalability:** The system must support parallel sample execution and distributed deployment with separate nodes for submission, analysis, and reporting. It must optimize resource usage for fast processing. **Reporting & Logging:** The solution must generate detailed, customizable reports in HTML, JSON, and PDF. It should support real-time logging, monitoring, and automatic alerts for IOC matches, with automated report forwarding to threat intelligence platforms. **User Interface & Management:** The solution should include a web-based dashboard for submitting files for analysis, monitoring running jobs, viewing detailed reports, and managing system settings. It must support multi-user access with role-based permissions. **Compliance & Data Handling:** The solution must comply with GDPR and ISO 27001 security requirements. It should support secure storage of analyzed samples and must allow log retention policies for compliance needs. **Vendor Support & Maintenance:** The vendor must provide installation and configuration assistance, training for analysts and administrators, periodic performance tuning, best practices guidance, and security patches and updates for system stability.		
10	**Reverse Engineering Tools** e.g. IDA Pro & Ghidra (Pro/Premium/Ultimate) / used for advanced binary analysis and reverse engineering to study malware internals. The provided solution must have ability to analyze binary code, decompile executables, identify vulnerabilities, and integrate with existing or future SOC infrastructure and threat intelligence platforms. - The platform must support both static and dynamic malware analysis. - It must provide a GUI and a file upload feature. - It should be cross-platform compatible (Windows, Linux, macOS). - Must include both GUI-based and command-line (CLI) interfaces. - Should support multi-user collaboration for team-based analysis. - Must offer automation and scripting with Python (Jython) and Java support. - Should have a modular architecture for custom scripts and plugins. - Must support batch mode processing for automated binary analysis. - Must provide up to twenty (20) parallel analysis concurrence, average daily volume of four (4), and average peak volume thirty (30). **Supported Architectures & File Formats** - Must support x86, x86-64, ARM, MIPS, PowerPC, SPARC, RISC-V, and other architectures. - Ability to analyze PE (Portable Executable), ELF (Linux Executables), Mach-O (macOS), raw binary, and firmware files. - Support for firmware and embedded system binary analysis. - Should allow importing custom processor architectures via plugin-based extensions. **Scripting & Automation** - Must provide a full scripting API supporting Python (Jython) and Java. - Should allow users to develop custom plugins to enhance or modify analysis capabilities. - Support for batch processing of multiple binaries to enable large-scale automated analysis.	Licenses	3

	- Ability to integrate with third-party forensic and security tools for extended functionality. **Malware Behavior Analysis** - Function signature matching against known malware behaviors. - Dynamic linking and symbol resolution for striped binaries. - Cross-referencing functions, system calls, and API imports. - Detection of obfuscated and packed binaries, including the ability to detect anti-analysis techniques. - Automated decryption and string extraction to uncover hidden indicators of compromise (IoCs). - Must support self-learning behavioral analysis to identify novel malware techniques.		
11	**Malware Analysis Software and Mobile App Security Tools** e.g. (PEStudio, Mobile Threat Defense) Pro / Premium / Ultimate - **General Requirements:** The vendor must provide, implement, and support a Software Reverse Engineering (SRE) framework, assisting with setup, configuration, optimization, and maintenance for effective reverse engineering, vulnerability research, and malware analysis. Necessary to have capability to scan ten's of thousands of samples per day, with a burst rate of 200/hour. - The solution must support on-premises and cloud deployment with scalable nodes. It must provide automatic detection updates and analyze multiple architectures, including x86 (32/64-bit), ARM, MIPS, PowerPC, RISC-V, Java, Android (DEX), and other compiled binaries. - **Analysis and Reverse Engineering Features:** The solution must offer interactive disassembly and decompilation with cross-referencing of functions, data, and instructions. It should support custom scripting in Python and Java and enable collaborative reverse engineering with multi-user capabilities. - **Integration and Automation:** The solution must integrate with VMs for safe malware execution and support external debugging tools like GDB, WinDbg, and IDA Pro. It should enable automated code analysis, function annotation, and provide a RESTful API for automation. Integration with SIEM, SOAR, and threat intelligence platforms is required, along with STIX/TAXII support and custom plugin development. - **Security and Isolation:** The solution must ensure full isolation from internal networks, provide secure execution of potentially malicious binaries, and include secure storage and controlled access to analyzed samples. - **Performance and Scalability:** The solution must support large-scale binary analysis, distribute tasks across multiple nodes, and optimize resources for fast processing times. - **Reporting and Monitoring:** The system should generate reports in HTML, JSON, and PDF formats, support real-time monitoring, and provide automated alerts for suspicious code patterns. - **User Interface and Access Control:** The solution must include a web-based dashboard for submission, monitoring, and reporting, as well as role-based access control (RBAC) to manage user permissions. - **Compliance:** The solution must comply with GDPR and ISO 27001 standards.	Licenses	3

12	**AI/ML frameworks and AI/ML software for automating malware detection and classification.** **e.g. Darktrace, Cylance or Vectra AI** – AI cybersecurity solutions that specialize in different aspects of detecting and mitigating cyber threats. **Technical requirements** - The NDR hardware platform provided must include at least a 3-year maintenance contract. - The capacity (memory, persistent storage) must be upgradable. - The appliances must provide full out-of-band management ports. - The vendor must provide hardware TAPs and network aggregators. - The appliance must have 4 network ports capable of supporting both copper and fiber optic media and must be expandable to 8 ports. **Architecture** - The solution must operate fully on-premises, including metadata and data analysis. - It must support air-gap mode with no Internet access. - The NDR sensor and management console must be deliverable as virtual machines. - The sensor and management console must run on separate physical or virtual machines. - It must allow separate network interfaces for management (UI) and sensor communication. - Sensor-to-management communication must support AES256 encryption and use IPSec. - It must not create tunnels to vendor infrastructure for detection efficiency. - Must include shellcode analysis, malware analysis, ransomware detection, and Advanced C2 Detection (Beaconing Detection). **Threat Intelligence** - The vendor must provide a threat intelligence source. - The NDR must integrate a source of threat intelligence (CTI) as part of real-time detection. - The NDR must integrate a source of threat intelligence (CTI) as part of a retrospective analysis. - The CTI source must be used to perform detection. - The CTI must be combined and correlated with other forms of detection. - The CTI must share the information in STIX format. - The CTI must share the information via the TAXII protocol. **Integration and Services** - The NDR solution must support integration with SIEM solutions - The NDR solution must integrate with the MISP platform. - The offeror must provide in-person or online training courses and certifications for the product to the staff Additional information: The cybersecurity lab is required to function in an offline environment. The solution must be capable of collecting traffic from all VLANs. IP Addressing: Private address ranges (RFC 1918 / ULA IPv6). DNS: Only internal resolvers (or static host files). NTP: Internal time server(s) or hardware clock source. Minimum IPSec with AES-256 encryption, with termination occurring on each host. Up to 4Gb throughput with traffic splitting defined on the firewall. Retention targets for metadata are required for up to 10 days. The Solution must support investigation must support (beaconing/C2, ransomware, lateral movement, data exfiltration, DNS/HTTP(S) tunneling and beyond. It must also include sandbox and payload emulation capabilities, encompass MITRE ATT&CK framework and detect threats like Cobalt Strike, Silver, and Brute Ratel. Up to 300 Ips scanned must be considered, and excpected traffic to be monitored shall be up to 4GB.	Licenses	2

13	**AI/ML frameworks and AI/ML software for automating malware detection and classification.** - **(e.g.) TensorFlow** or **PyTorch** can be used for developing AI models that automatically classify malware based on behavior and characteristics.	Licenses	2
14	**Malware Analysis Software and Mobile App Security Tools** **e.g. VirusTotal, Verimatrix Platform Pro** / Premium / Ultimate The solution must provide comprehensive mobile device protection against threats from applications, files, networks, and operating systems while safeguarding corporate data from unauthorized access, malware, and phishing attacks. It must operate without impacting device performance or user experience and support rapid deployment across a large number of devices. Additionally, the solution should be highly scalable to accommodate an increasing number of users and devices seamlessly. **Technical specifications** The solution must provide comprehensive mobile security across all attack vectors, including: - **Application Protection:** Real-time detection and blocking of malicious apps. - **File Security:** Blocking and detecting malicious files via threat analysis and sandboxing. - **Network Security:** Protection against phishing, MITM attacks, bot infections, and unsafe URLs, with DNS and Wi-Fi security. - **OS Protection:** Detects vulnerabilities, jailbreaking/rooting, and misconfigurations; supports iOS and Android. - **Scalability:** Suitable for organizations of all sizes. - **Centralized Management:** Cloud-based console for real-time threat visibility. - **Automation & Analytics:** Automated reporting, policy enforcement, and mobile threat intelligence.	Licenses	2
15	**Reverse Engineering Tools** e.g. Disassembler/Decompiler such as Binary Ninja, Radare2 - reverse engineering tools for low-level code analysis. The disassembler/decompiler tools must support binary analysis, reverse engineering, debugging, and low-level security research. The solution must provide multi-architecture support, enabling analysis across x86, ARM, MIPS, RISC-V, and PowerPC. It should also handle multiple file formats, including ELF, PE, Mach-O, and raw binaries. Number of uses/workstations is 2. **Technical requirements** The solution has to have possibility for dynamic and static analysis with following features: - Disassembly and reassembly functionalities for inspecting executable code. - Hexadecimal and assembly-level views for fine-grained binary inspection. - Cross-referencing capabilities for function, symbol, and string analysis The solution must have possibility for Debugging and Emulation with following features. - **Live Debugging:** Supports breakpoints, register inspection, and memory manipulation. - **Process Attachment:** Allows attaching to running processes to inspect execution flow. - **Emulation:** Integrated lightweight emulation for simulating execution paths.	Licenses	2

	- **Binary Modification:** Enables dynamic code changes, custom instruction insertion, and patching. - **Function Hooking:** Supports replacing functions and redirecting execution flow. - **Extensibility:** Integrates with external tools and frameworks. - **Code Analysis:** Supports structured function flow and variable recovery. The solution must decompile assembly instructions into high-level representations for easier analysis and identify Return-Oriented Programming (ROP) gadgets while supporting structured function flow and variable recovery. It should provide both a graphical and command-line interface, enabling intuitive scripting and visual representation of control flow graphs and function maps. The solution must be cross-platform, running on Linux, Windows, and macOS with minimal dependencies, and support deployment in containerized environments like Docker.		
16	**Threat Intelligence Platforms - (e.g., MISP, YARA)** Open Source - cost for deploy. **General Requirements** The solution must offer advanced threat intelligence, robust automation, seamless API integration, and a scalable architecture for on-premises, cloud, and hybrid deployments. It should support collaboration among internal teams, partners, and external cybersecurity communities while ensuring compliance with regulations like GDPR and ISO 27001. The selected solution must meet all functional, security, and operational requirements. **Threat Intelligence Collection and Management** The platform must support structured storage, correlation, and management of cyber threat intelligence, including: - **Threat Intelligence Storage:** Stores IoCs like IPs, domains, file hashes, emails, and malicious URLs. - **Correlation:** Automatically links intelligence data to detect relationships, attack campaigns, and adversary behaviors. - **Threat Classification:** Maps threats to MITRE ATT&CK, aligning with adversarial TTPs. - **Tagging & Filtering:** Enables granular classification using custom/predefined tags like TLP and adversary groups. Malware Sample Handling: Secure storage and analysis of malware samples with integration options for sandboxing environments (e.g., Cuckoo Sandbox, Hybrid Analysis). **Technical requirements** - **Federated Sharing:** Enables secure threat intelligence exchange with trusted entities through customizable sharing policies. - **Standards Interoperability:** Supports STIX 2.x and TAXII 2.x for seamless integration with other threat intelligence platforms. - **Access Control:** Implements granular RBAC to manage user permissions at event, attribute, and organizational levels. - **Notifications & Alerts:** Provides real-time alerts via email, webhook API, and SIEM integration. - **Audit & Compliance:** Maintains detailed logs of user activities and system interactions to meet regulatory requirements. **Ability to query external threat intelligence services such as:** - VirusTotal – Malware and URL reputation checks. - AbuseIPDB – IP address abuse reporting. - Passive DNS & WHOIS Services – Historical domain analysis.	Licenses	3

	- OSINT Threat Feeds – Automated ingestion from AlienVault OTX, URLHaus, Abuse.ch, Emerging Threats, etc. **Advanced API & Automation Capabilities** - **REST API:** Fully documented API for seamless integration with SIEM, SOAR, EDR, and other security platforms. - **Security Tool Integration:** Prebuilt connectors or API support for Splunk, QRadar, TheHive, OpenCTI, Elastic Security, and IDS/IPS solutions like Suricata, Snort, and Zeek. - **Python SDK:** Supports PyMISP or equivalent Python libraries for scripting and automation. **Scalability & Deployment Models** The proposed platform should be scalable and support multiple deployment models: - **On-Premise Deployment:** Installable on dedicated servers or virtualized environments for full control. - **Cloud Deployment:** Compatible with AWS, Azure, GCP, and private cloud solutions for flexible hosting. - **Containerized Deployment:** Supports Docker and Kubernetes for rapid deployment and scalability. - **High Availability & Load Balancing:** Multi-node clustering, replication, and failover mechanisms ensure reliability. - **Plugin & Module Support:** Extendable with custom modules and third-party integrations for enhanced functionality. - **Custom Data Export:** Supports exporting intelligence in JSON, CSV, STIX, OpenIOC, Suricata rules, and other formats.		
17	**Web Vulnerability Analysis** **e.g. Acunetix Web Vulnerability Scanner** - Web Application Vulnerability Analysis and Report Generation **General Requirements** - **End-to-End Web Security:** Provides comprehensive protection for the organization's web infrastructure. - **SDLC Integration:** Detects vulnerabilities early by integrating with the Software Development Life Cycle. - **WAF Compatibility:** Supports integration with Web Application Firewalls to block threats before reaching production. - **SmartScan Technology:** Enables efficient scanning and early vulnerability detection. **Vulnerability Detection** The solution must detect web vulnerabilities including: - SQL Injection (SQLi) - Cross-Site Scripting (XSS) - Remote Code Execution (RCE) - Cross-Site Request Forgery (CSRF) - Server-Side Request Forgery (SSRF) - Broken Authentication and Access Control Issues The scanner must identify network vulnerabilities affecting web applications. It should provide malware detection capabilities to alert if malicious scripts are found.	Licenses	1

	Scanning Capabilities - **Incremental Scanning:** Analyzes only changes since the last scan to reduce scanning time. - **Template-Based Scanning:** Prioritizes unique templates to minimize redundant scans. - **Comprehensive Coverage:** Supports scanning of web applications, databases, and APIs. - **Detailed Reporting:** Provides actionable insights for developers and security teams. - **Vulnerability Tracking:** Monitors resolution progress internally and externally. **Reporting and Compliance** The system should generate detailed security reports with: - Vulnerability severity levels - Recommendations for fixes It must provide exportable reports that can be shared with security teams and developers. Added clarification: To meet the end-to-end web security requirements, the web application scanner must be capable of identifying and reporting all potential vulnerabilities across the entire web application stack, including but not limited to OWASP Top 10, business logic flaws, and authentication/authorization weaknesses. Requirement: *at least 20 targets, unlimited scans*. Foreseen number of users is one (1).		
18	**Network Vulnerability Analysis** - **Nessus Vulnerability Scanner**: scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources. **Technical requirements** The solution must provide comprehensive vulnerability scanning for both internet and intranet environments, supporting on-premises assets, including various hardware network devices. It should enable modern attack surface management, ensuring security for both internal and internet-facing assets. The system must allow unlimited scans, including external attack surface analysis, to identify vulnerabilities continuously. Additionally, it should detect unknown security issues as part of the Software Development Lifecycle assessment. The solution must support both authenticated and non-authenticated scans for vulnerability detection and system hardening. Furthermore, it must comply with PCI DSS requirements for internal vulnerability scans. **The solution must cover the following** - Network devices: firewall/router/switches (Fortinet, Juniper, Check Point, Cisco, Palo Alto) - Peripheral devices: printers, storage - Infrastructure: Windows, OS X, IBM, Cisco iOS, Solaris, VMWare, Hyper-V, Citrix - Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB - Web Applications: Web servers, web services, OWASP vulnerabilities - Compliance: assists in meeting government, regulatory, and corporate requirements Requirement: Unlimited number of IP scans.	Licenses	2

19	**Network Traffic Analysis Tools** - (e.g., Wireshark, Zeek) - Installation, Configuration and Training for Staff. General Requirements - The solution must provide monitoring for servers, network devices, applications, and cloud infrastructure. - It should support both agent-based and agentless monitoring methods. - The system should offer an intuitive web-based user interface for configuration and monitoring. - The tool should allow customization and extendibility via plugins and third-party integrations. - The solution must be capable of generating real-time alerts and notifications. - It should be able to perform automated remediation actions upon issue detection. - The monitoring solution must support reporting and dashboard features. Core Monitoring Features - Must monitor hosts (servers, virtual machines, cloud instances) for availability and performance. - Service monitoring must include HTTP, SMTP, POP3, ICMP, SNMP, FTP, SSH, and custom-defined services. - Ability to monitor CPU usage, memory utilization, disk usage, and network traffic. - Capability to check log files and system events for anomalies. - Configurable alerts based on predefined thresholds. - Multi-channel notification system (email, SMS, Slack, webhooks, etc.). - Integration with incident management platforms like PagerDuty or ServiceNow - Trend analysis for capacity planning. - Predictive failure analysis. - Must provide audit logs for security tracking. - Role-based access control (RBAC) for managing permissions. - Secure authentication mechanisms (LDAP, Active Directory, OAuth support). - Must support installation on Linux-based systems (e.g., Ubuntu, CentOS, RHEL). - Automated installation and configuration scripts should be available. - Regular software updates and security patches must be provided. - Documentation and community support should be readily accessible.	Licenses	2
20	**Memory Analysis Tools** - (e.g., Volatility) The solution needs to be a digital forensics tool that focuses on memory analysis of RAM memory. It is designed to help investigators in cybersecurity, digital forensics, and incident response situations by providing detailed insights from volatile memory (RAM). The solution needs to enable forensic investigators to analyze RAM memory dumps from systems and gain insights into the state of a machine. Key capabilities should include: - Memory image analysis. - Extraction of artifacts like process information, DLLs, and network sockets. - Platform support for Windows, Linux, macOS, and Android memory formats. - Extensible architecture for plugin/module development. - Raw memory dumps (DD format). - Windows hibernation files (hiberfil.sys). - Linux crash dumps (vmcore).		

	- macOS memory dumps (via vmem format). Features the solution should provide - Process Analysis: - Be able to list active processes. - Be able to extract process details such as PIDs, executable paths, and parent-child relationships. - Be able to Identify hidden processes and rootkits. Memory and Kernel Module and Network Connection Analysis: - Be able to identify loaded kernel modules/drivers. - Be able to extract module names and addresses. - Have support for both userland and kernel memory analysis. - Be able to list active network connections (TCP, UDP). - Be able to capture IP addresses, ports, and protocols. - Identifying anomalous network activity. Artifact Extraction: - Be able to detect and extract artifacts such as command-line arguments, registry hives, and DLL injections. - Be able to do research for potential indicators of compromise (IOCs). - Dynamic Analysis: - Support volatile state analysis (active processes, open files, registry keys). - Investigate ongoing or recently terminated system activity. - Support for analysis profiles (a profile with a configuration of the current UI layout or memory import config). - Extraction of handles, threads, and other low-level system structures. - Detection of malicious code execution, including in-memory shellcode	Licenses	2
21	**Hardware Check** **AIDA64 Extreme** - detailed information about both hardware and installed software, but also helps users diagnose issues and offers benchmarks to measure the performance of your computer. The system shall feature an advanced hardware detection engine, providing detailed information about installed software and offering diagnostic functions with support for overclocking. It shall monitor sensors in real time to collect accurate voltage, temperature, and fan speed readings. The system's diagnostic capabilities shall assist in detecting and preventing hardware issues. Additionally, it shall include benchmarking tools to assess the performance of individual hardware components or the entire system. Compatibility shall extend to all 32-bit and 64-bit Windows editions, including Windows 11 and Windows Server 2022.	Licenses	1
22	**Hardware Check** **AIDA64 Engineer** - diagnose issues and offers benchmarks to measure the performance of Windows PCs. The system shall provide advanced hardware detection capabilities, delivering detailed information about installed software and offering diagnostic functions with support for overclocking. It shall monitor sensors in real time to gather accurate voltage, temperature, and fan speed readings. The system's diagnostic functions shall assist in detecting and preventing hardware issues. Additionally, it shall include benchmarking tools to measure the performance of individual hardware components or the entire system. Compatibility shall extend to all 32-bit and 64-bit Windows editions, including Windows 11 and Windows Server 2022.	Licenses	1

23	**Hardware Check** **AIDA64 Network Audit** - detailed hardware and software inventory of the company PC fleet, supports IT decision-making with essential statistics, and helps companies reduce their IT costs. The system shall collect detailed hardware and software inventory data from Windows client computers within the corporate network. It shall support command-line execution to enable full automation of the inventory process. The collected reports shall be exportable in open formats for further processing and shall support storage in an SQL database. The system shall provide change monitoring by comparing network audit snapshots taken at different times. Compatibility shall extend to all 32-bit and 64-bit Windows editions, including Windows 11 and Windows Server 2022.	Licenses	1
24	**Hardware Check** - **AIDA64 Business** - detailed hardware and software inventory from Windows client computers connected to the corporate network. The system shall collect detailed hardware and software inventory data from Windows client computers within the corporate network. It shall support command-line execution to enable full automation of the inventory process. The collected reports shall be exportable in open formats for further processing and shall support storage in an SQL database. The system shall provide change monitoring by comparing network audit snapshots taken at different times and shall notify administrators in real time of any critical events. Additionally, it shall support PC fleet management through remote monitoring and remote control. Compatibility shall extend to all 32-bit and 64-bit Windows editions, including Windows 11 and Windows Server 2022.	Licenses	1
SETUP, INSTALLATION, MAINTENANCE AND TRAINING FOR ALL TOOLS ABOVE SHALL BE INCLUDED IN THE PRICE. Warranty of 3-years must be offered from the vendor inclusive of 8 x 5 x next business day service warranty must be included. Routine system updates, patching of two (2) times per year for three (3) years must also be included.			
25	Reinstallation of the tools (See note regarding conditional pricing and Cyber Agency readiness)		**1**

TRAINING AND CAPACITY BUILDING COSTS

#	**Description**	**Unit**	**QTY**
26	Integration of threat intelligence platforms from KosCERT, to be absorbed by the Cybersecurity Agency **may be necessary, and as such must also be considered in the price**.	**Systems**	**3**
27	Setup of forensic and incident response systems Playbooks.	**Docs**	**2**
28	Training for Ethical Hacking - Certified Ethical Hacker (CEH) for 3 CSA Staff. Examination vouchers must be provided by the company for the CSA staff to use for accredited exam purposes.	**Persons**	**3**
29	Training for malware analysis, incident response - SANS FOR610, GIAC Reverse Engineering Malware (GREM) (or similar), for the CSA staff.	**Persons**	**3**

**Specific training measures have been further foreseen in the sections below also in more detail*.

Technical Documentation

On completion of the project, the supplier shall ensure at least:

- A detailed technical scheme of installed equipment. The scheme shall include all markings on installed cables. The scheme is delivered in any of ACAD or MS Visio format and 3 hard copies.
- A user manual for delegates and a user manual for technical staff. Manuals shall be delivered in digital format and 3 hard copies.
- All manufacturer's documents on the installed equipment.
- A detailed presentation of all installed equipment based on the technical specifications. It shall be delivered in the form of an Excel table and in 3 hard copies.

All documents shall be written in both English and Albanian as well as approved in writing.

Rules of Origin

The equipment, tools, and other services are being purchased for the Ministry of Internal Affairs and, therefore, due to national restrictions, equipment manufactured from the prohibited companies list or countries in the sanctions list are not acceptable. Kosovo Public Procurement Regulatory Commission, has notified contracting authorities that it is prohibited to purchase equipment manufactured by the following companies, including telecommunications, video surveillance or services provided by such entity or that use and produce such equipment, including; a) Dahua Technology Company; b) Hikvision Digital Technology Company; c) Huawei Technologies Company; d) ZTE Corporation; e) Hytera Communications Corporation; f) AO Kaspersky Lab and, g) other companies as the list of sanctioned parties' updates by the Republic of Kosovo.

Kosovo Public Procurement Regulatory Commission published a Notice to Contracting Parties, notifying state institutions that the Regulation No. 01/2022 on Public Procurement, which entered into force on November 01, 2022, has made important updates to complete and clarify the provisions of the Law on Public Procurement and to follow the latest developments in the public procurement sector.

When describing technical specifications for work, supplies, or services in the field of information technology and telecommunications, contracting authorities are forbidden to draft technical specifications that: a) specify suspicious equipment, services and manufacturers of information and telecommunication technology; b) pose a cybersecurity risk and threaten the country's critical infrastructure; and c) pose a national security risk threat for the country.

Contracting Authorities must ensure the equipment, the specified services, and manufacturers do not belong to the countries (states) or companies for which the Government of Kosovo has imposed sanctions on import/export, or countries, products, services, and whose supplies are considered unreliable by any of organizations/countries, such as: the European Union, the United States of America, NATO, OECD or European Free Trade Association.

Kosovo Public Procurement Regulatory Commission, has instructed the Contracting Authorities that, based on the reference and practices of the listed countries and organizations specified in Article 19.8, that it is forbidden to establish technical specifications, and therefore procurements from suppliers, goods and services included according to the list of equipment and services covered by Article 2 of the United States Secure Network Act.

NOTE: The above-mentioned Notice to Contracting Parties has a reference on three important documents/decisions, as following:

- REGULATION No.001/2022 ON PUBLIC PROCUREMENT
- MINISTRY OF FOREIGN AFFAIRS – SANCTIONS
- List of Equipment and Services Covered By Section 2 of The Secure Networks Act | Federal Communications Commission

Warranties

The supplier guarantees all installed tools equipment are new, unused, include everything necessary to meet the technical requirements and undertakes that the spare parts will be available in the market for a period of at least 5 years after the expiration of the warranty period. The warranty period begins as of the signing of the takeover minutes and lasts for at least 3 years, for both the tools and equipment.

During the warranty period, the tenderer will provide any assistance necessary based on the technical specifications and provide replacement options. All provided software or/and feature licenses shall be with the perpetual license and the bug updates during the whole warranty period. The proposal from the offeror should include provisions for robust SLAs, comprehensive after-sales services for **Hardware**

Infrastructure, and warranties with a minimum duration of 3 years to ensure sustained product reliability and customer satisfaction.

Min. SLA requirement

- Emergencies (an Operational Issue -- Obstacle) – response time of maximum 2 hours
- Non-urgent cases (a Non-Operational Issue) – response time of maximum 24 hours

Each bidder is required to provide a formal **Letter of Confirmation** from the vendor or partner organization. This letter must explicitly confirm the following:

1. **Support for the Tendering Process**:

   The vendor acknowledges and supports the bidder's participation in this tendering process.

2. **Commitment to Future Support:**

   The vendor commits to providing all necessary support for maintenance, technical assistance, and other requirements as outlined in the tender agreement, for the full duration specified in the agreement.

The confirmation letter must be signed and, on the vendor's, official letterhead, clearly stating their commitment to the above conditions. Failure to submit this document can result in disqualification from the tendering process.

Delivery, Installation, Testing

*All equipment shall be delivered and installed in the Cybersecurity Agency designated space for the cybersecurity lab. Provided that the designated facilities of the Cybersecurity Agency are not ready for the instalment, the contractor must consider their instalment in an alternative location (In Pristina, Kosovo) as determined in due time within the areas of the Ministry of Internal Affairs. Re-installation of equipment from the alternative location to the Cybersecurity Agency shall be considered, on a period of up to 31/10/2026.On completion of the works and before the takeover minutes are signed, the entire system shall be inspected and tested. All equipment must meet the EU standards concerning electrical equipment and comply with "rules of origin". In this respect, the tenderer shall ensure:

- Complete system installation of excellent quality, including testing;
- The tenderer shall provide all equipment and materials necessary for regular functioning of the system. The system takeover will be on the turnkey basis;
- The tenderer shall provide the required manpower and ensure good quality, safe installation without any additional costs.

Training and Capacity Building

The establishing of the lab will include also providing hands-on training and certification for a group of employees related to the tools and technologies that will be used.

Training should be focused but not limited to:

- **Hands-on training workshops:** Reverse engineering, malware detection, memory forensics, and AI-based threat detection, and the tools specified in the technical specifications table.
- Training of staff for operating the new system shall be conducted in the Cybersecurity Agency building for at least 4 employees.

The tenderer should make the training plan and present it, additionally it could be adjusted based on the needs of the Cybersecurity Agency. Mainly the training should include the presentation of each function of the system according to functional blocks, including the procedures, security protocol, troubleshooting, data management, accessibility, compliance, and other relevant parts.

Each participant in the training must try all these functions (scenarios) themselves - daily operations with maintenance intervals and basic diagnostics, enough to accurately describe it to the maintenance team to remotely try to eliminate the problem as well as be better prepared when the maintenance team comes over.

Training sessions can also be recorded by the beneficiary for the training needs of new staff, or to refresh the knowledge of the existing staff. Timing depends on the implementing company which will be required to provide the training plan according to the need and then according to their proposed technology and solution.

The tenderer is obligated to provide system use and maintenance instructions. Further, the tenderer shall also provide final technical documents, where schemes and drawings are delivered in the any of ACAD or MS Visio format, where possible and necessary.

3. PROFILE OF EXPERTS AND MISSION DURATION

The place of performance for the services will be in Pristina, Kosovo. Expected start period 2025 after the contract is awarded. All experts are expected and required to get engaged on a diligent and priority principle in this project. The team of experts shall consist of be overseen by a **Project Manager**, reporting to the CSA representative and other counterparts.

The team of people implementing the project should cover but not be limited to:

LEAD EXPERT: CYBERSECURITY EXPERT FOR PROJECT MANAGEMENT

(i) Qualifications and Skills:

- **Education:** Bachelor's degree in Cybersecurity, Computer Science, Information Technology, or a related field. Master's degree is preferred.
- **Professional Certifications:** Proficient in project management methodologies (e.g., PMP, PRINCE2). Certifications such as CISSP, CISM, or OSCP are highly desirable.

(ii) General Professional Experience:

- **Experience:** At least 15 years of experience in cybersecurity with 5 years in project management or leadership roles.

(iii) Specific Professional Experience:

- Demonstrated experience in setting up and managing security labs or similar technical environments.

(iv) General Description Responsibilities

- Oversee the entire lab setup, ensuring timelines, budget, and deliverables are met. Coordinate with various teams and stakeholders to achieve project goals.

EXPERT POOL 1: IT SUPPORT TEAM

(i) Qualifications and Skills per team member:

- **Education:** Bachelor's degree in computer science, Information Technology, Networking, or a related discipline.
- **Professional Certifications:** Proficient in virtualization platforms (e.g., VMware, Hyper-V). Certifications such as CCNA, CompTIA Network+, or CEH.
- **Skills:** Strong troubleshooting skills and knowledge of cybersecurity best practices.

(ii) General Professional Experience per team member:

- **Experience:** At least 4 years of experience in IT infrastructure setup, including servers, networks, and virtualization.

(iii) Specific Professional Experience per team member:

- Proven experience in implementing secure IT environments and configuring security appliances (e.g., firewalls, IDS/IPS).

(iv) General Description Responsibilities per team member:

- Responsible for deploying the infrastructure and ensuring smooth operation. Set up and configure lab infrastructure, including servers, storage, and network equipment. Ensure systems and tools are operational and secure.

EXPERT POOL 3: Certified Instructor(s)

(i) Qualifications and Skills per team member:

- Education: Bachelor's degree in Cybersecurity, Computer Science, or related field. Master's degree is an advantage.
- Certifications in relevant areas, such as CEH, CHFI, GREM/GIAC, or OSCP .
- Skills: Proficient in the use of malware analysis, sandboxing, and reverse engineering tools. Strong communication and teaching skills.

(ii) General Professional Experience per team member:

- Experience: Minimum of 6 years of experience in cybersecurity with at least 3 years as an instructor or trainer.

(iii) Specific Professional Experience per team member:

- Experience in delivering hands-on labs and workshops for technical tools and methodologies.

(iv) General Description Responsibilities per team member:

- Delivering a fast-track hands-on lab for the above-mentioned tools and technologies.
- Design and deliver hands-on training sessions tailored to the lab tools and technologies. Provide technical guidance to ensure teams are proficient in using lab resources.

EXPERT POOL 2: MALWARE ANALYSIS TEAM (at least 3 people)

(i) Qualifications and skills per team member:

- **Education:** Bachelor's degree in Cybersecurity, Computer Science, or related field.
- **Professional Certifications:** Certifications such as GIAC Reverse Engineering Malware (GREM) or Offensive Security Certified Expert (OSCE).
- **Skills:** Familiarity with scripting languages (e.g., Python, PowerShell) for automation in malware analysis.

(ii) General professional experience per team member:

- **Experience:** Minimum 5 years of hands-on experience in malware analysis, reverse engineering, and threat intelligence (each expert).

(iii) Specific professional experience:

- Proven expertise in using tools such as IDA Pro, Ghidra, Wireshark, and sandbox environments like Cuckoo Sandbox or VirusTotal.

(iv) General Description Responsibilities

- **Responsibilities:** Conduct static and dynamic analysis of malware. Develop comprehensive reports on malware behaviour and attack vectors. Collaborate to create detection signatures and IOCs for incident response.

Team Composition Qualifications

Team Synergy:

- Proven ability to work collaboratively within multidisciplinary teams.
- Strong problem-solving, analytical, and documentation skills.

Project-Specific Requirements:

- Experience with cyber labs, malware analysis, and incident response projects.

- Demonstrated success in similar cybersecurity projects involving lab setup or operational training.

Deliverables:

- Fully functional cyber lab with documented processes, tools, and team knowledge transfer plans.

Note : Equivalence the certification required shall be considered.