Anexă

Specificație tehnică și cerințe: Complex de sisteme de securitate, model ZTNA.

Acest document descrie specificațiile tehnice și cerințele pentru implementarea unui sistem integrat de securitate care include **Next Generation Firewall (NGFW)**, **Web Application Firewall (WAF)**, **Mail Security Gateway**, **Sandboxing**, și **Zero Trust Network Access (ZTNA)**, configurate în conformitate cu principiile ZTNA și aliniate la standardele **ISO 27000**, **ISO 27001:2022**, **NIS**, și **NIS 2**. Soluțiile trebuie să asigure protecție avansată, scalabilitate, reziliență cibernetică, și gestionare centralizată pentru rețele moderne, distribuite, cu accent pe securitate proactivă, conformitate, și adaptabilitate la amenințările cibernetice actuale.

1.1. Obiectiv

Furnizarea unei soluții integrate de securitate care să asigure:

- **Protecția perimetrului**: Securizarea limitelor rețelei împotriva amenințărilor externe și interne, conform cerințelor ISO 27001:2022 (Anexa A, controale 8.20, 8.21).
- **Lucru hibrid securizat pentru utilizatori**: Facilitarea accesului securizat al utilizatorilor la resurse, indiferent de locație (on-premises, remote), cu politici bazate pe principiul „least privilege” (ISO 27001:2022, control 5.15).
- **Acces securizat al utilizatorilor la resursele interne**: Control granular al accesului bazat pe principiul Zero Trust, cu verificarea continuă a identității și conformității dispozitivelor (NIS 2, Articolul 21).
- **Securitatea resurselor interne**: Protejarea datelor și aplicațiilor interne împotriva accesului neautorizat și atacurilor cibernetice, prin segmentare și monitorizare continuă (ISO 27001:2022, control 8.34).
- **Identity and Access Management (IAM)**: Gestionarea identității și accesului prin autentificare multifactorială (MFA) continuă, politici bazate pe roluri, și integrare cu sisteme IAM (ISO 27001:2022, control 5.16; NIS 2, Articolul 20).
- **Conformitate cu directivele NIS și NIS 2**: Asigurarea conformității cu cerințele Uniunii Europene pentru securitatea rețelelor și sistemelor informatice, inclusiv gestionarea riscurilor, raportarea incidentelor în 24/72 de ore (NIS 2, Articolele 23, 24).
- **Protecție proactivă, scalabilitate și conformitate** cu standardele de securitate (ex. GDPR, PCI DSS, ISO 27001:2022, NIS, NIS 2).

1.2. Cerințe generale

- **Compatibilitate ZTNA**: Toate componentele trebuie să suporte modelul Zero Trust, incluzând autentificare multifactorială (MFA), politici bazate pe identitate, segmentare granulară a rețelei, și verificarea continuă a conformității (ISO 27001:2022, control 5.15; NIS 2, Articolul 21).
- **Protecția perimetrului**: Capacitate de blocare a amenințărilor la nivelul perimetrului rețelei prin filtrare avansată, inspecție a traficului, și detectarea amenințărilor avansate persistente (APT) (ISO 27001:2022, control 8.20).
- **Lucru hibrid securizat**: Suport pentru acces securizat al utilizatorilor din medii diverse (birou, domiciliu) cu politici consistente de securitate și verificare a conformității dispozitivelor (ISO 27001:2022, control 8.9).
- **Acces securizat la resurse interne**: Implementarea controalelor stricte pentru accesul la aplicații și date interne, bazate pe principiul „never trust, always verify" (NIS 2, Articolul 21).
- **Securitatea resurselor interne**: Protecție avansată pentru servere, baze de date și alte resurse interne prin segmentare dinamică, criptare, și monitorizare continuă (ISO 27001:2022, control 8.34).
- **Identity and Access Management (IAM)**: Integrare cu soluții IAM pentru autentificare, autorizare și administrarea accesului bazat pe roluri, contexte și riscuri (ISO 27001:2022, control 5.16).
- **Scalabilitate**: Soluțiile trebuie să fie scalabile pentru medii on-premises, fără compromisuri de performanță (ISO 27001:2022, control 8.1).
- **Management centralizat**: Platformă unificată pentru configurare, monitorizare, și raportare, cu integrare SIEM (ex. QRadar, Splunk, ArcSight) și suport pentru rapoarte automate de conformitate (ISO 27001:2022, control 5.36).
- **Conformitate cu standardele generale**: Respectarea standardelor de securitate (ex. GDPR, PCI DSS, ISO 27001:2022).

Specificații tehnice

1.3. Soluție de tip Next Generation Firewall (NGFW)

1.3.1.	**Cluster of 2x Next Generation Firewall (NGFW)**	
1.3.2.	Cerințe generale	- Echipamentul furnizat în cadrul achiziției trebuie să fie nou, de înaltă calitate, fabricat de producători de renume, recunoscuți pe plan internațional în industria IT. Configurația acestuia trebuie să includă componente compatibile între ele, garantând funcționarea optimă și integrată a sistemului.
1.3.3.	Performanță	- Threat protection Throughput (Full Protection): min. 6 Gbps - Max concurrent sessions: min. 1 M - New sessions per second: min. 140 000
1.3.4.	Interfețe/Porturi	- min. 1 x Console Port - min. 1 x Port GE RJ45 MGMT dedicat - min. 1 x Port GE RJ45 HA dedicat - min. 8 x Porturi GE RJ45 - min. 8 x Porturi 10GE/GE SFP+/SFP
1.3.5.	Transceivers	- min. 4 x transceivere 10GBASE-SR SFP+, compatibile IEEE 802.3ae, distanță operare min. 100 m pe fibră multimode OM3/OM4, conector LC duplex; - min. 2 x AOC SFP+ active, lungime 1 m; - min. 2 x AOC SFP+ active, lungime 3 m; - Toate modulele și cablurile să fie noi, originale, testate din fabrică și certificate pentru compatibilitate cu echipamentele furnizate.
1.3.6.	High Availability Configurations	- Active-Active, Active-Passive, Clustering
1.3.7.	Routing protocols	- Static, OSPFv2/3, BGPv4
1.3.8.	VLAN Support (802.1Q)	- 4094 VLANs
1.3.9.	Funcționalități (incuzînd licențele necesare)	- Firewall de tip stateful - Filtrare URL, DNS - Antivirus, antispam, botnet detection - Virtual patching, security rating

		- Router cu suport protocoalelor de rutare dinamice (RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS) - SD-WAN Application aware routing - VRF support - Virtual firewall with license included – min 10 - Gruparea interfețelor în zone de securitate - Rutare între zonele de securitate - Policy-based routing - Funcționalități NAT, PAT si Transparent Bridge - Opțiune de a aplica NAT per politică - Suport VLAN Tagging 802.1Q - Suport VoIP SIP/H.323/SCCP Traversal NAT - Criptare de date: IPSec VPN, SSL VPN, ZTNA - Suport ZTNA, reguli de firewall in baza tag-rilor ZTNA, criptare canalului ZTNA prin DTLS cu autentificare mutuala client din poziția 1.8 și NGFW in baza certificatelor digitale - Suport pentru QoS si Traffic Shaping - Detecția și prevenirea intruziunilor – IDS/IPS - Protecție Anti-Malware prin folosirea tehnologiei AI - Blocarea și controlul traficului din rețea generat de aplicații - Identificarea și controlul aplicațiilor - Opțiune de Traffic-Shaping per aplicație - Clasificare granulară a aplicațiilor după criterii multiple precum: Categorii de aplicații, Popularitate, Tehnologie și Risc - Monitorizarea aplicațiilor pe bază de IP/Utilizator, consum de bandă - Posibilitatea de definire a semnăturilor de aplicație personalizate - Protecție pentru atacuri de tip brute force - Detectarea anomaliilor de protocol - Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de stație folosit – funcționalitate de tip BYOD - Integrare cu soluția de tip Sandbox (solicitată la poziția 1.8) - Actualizări automate de semnături de securitate AV de la sandox pentru protecția eficienta de la zero day attacks - Actualizări automate de semnături de securitate pentru îndeplinirea tuturor funcționalităților solicitate

1.3.10.	Funcționalități de administrare, logare, autentificare a utilizatorilor	- Administrare prin WEB UI, Secure Command Shell (SSH) si Command Line Interface (CLI) - Utilizatori/Administratori cu drepturi configurabile - Funcționalitate de export/import a configurației - Monitorizare grafică în timp real și istorică - Suport syslog - Suport SNMP v1/v2c/v3 - Notificare prin e-mail pentru alerte - Definire locală a utilizatorilor - Integrare cu Windows Active Directory (AD) - Suport pentru autentificarea grupurilor de utilizatori prin LDAP - Suport pentru autentificare prin doi factori - Centralized Security Data Lake: Collects and consolidates logs and telemetry data - Advanced Analytics and Event Correlation - Unified Logging and Analytics Platform - Real-Time Threat Intelligence Integration - Automated Reporting and Customizable Dashboards - Log Forwarding Capabilities - Attack Surface Security Scoring and Compliance Monitoring Service
1.3.11.	Chassis	- Rackmount, 1U, metal, all mounting accessories included
1.3.12.	Power	- min. 2 x Redundant Power Supplies, with 2 Power cables, PDU connection - 100–240V AC, 50/60Hz
1.3.13.	Licensing	- Minimum 3 Years, including all security subscriptions and updates

1.3.14.	Garanție și suport	- **Perioada minimă de garanție**: 36 luni, acordată de producător, care să includă:
		  - Înlocuirea echipamentului în caz de defect hardware;
		  - Diagnosticare și remediere defecțiuni;
		  - Furnizarea pieselor de schimb necesare;
		  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
		  - Actualizări de firmware/software, atât pentru versiuni minore, cât și majore;
		  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;

		- **Suport tehnic local** din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună;
		- Perioada de **End-of-Support** și **End-of-Life** a echipamentului nu trebuie să fie mai devreme de anul 2030;
		- Garanția și suportul se acordă indiferent de păstrarea ambalajului original.
		- **Cerințe privind instalarea și serviciile aferente:**
		  - Implementarea completă a soluției;
		  - Migrarea regulilor de securitate existente către noul echipament;
		  - Integrarea echipamentelor noi cu infrastructura existentă;
		  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
		  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.
		- **Cerințe privind acreditările furnizorului:**
		  - Minimum două persoane tehnice, deținând certificări emise de producător (vendor), pentru echipamentele și soluțiile propuse;
		  - Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.

1.4. Soluție de tip Web Application Firewall (WAF)

1.4.1.	**Web Application Firewall (WAF)**	
1.4.2.	Tip	- Modelul de licențiere trebuie să fie de tip perpetual. - Virtual Machine (On-premises)
1.4.3.	Deployment Platform	- Microsoft Hyper-V - High availability support - Min. 10 domene Web
1.4.4.	HTTP Throughput	- Min. 100 Mbps
1.4.5.	Web Security	- Protection against OWASP Top 10 vulnerabilities - Cross-Site Scripting (XSS) prevention - Session hijacking defense - Brute force attack mitigation

		- IP address reputation services - Geolocation-based IP blocking - WebSocket traffic security - HTTP protocol compliance and validation
1.4.6.	Application Attack Protection	- SQL Injection prevention - Integration with third-party scanners for virtual patching - Session hijacking protection
1.4.7.	Security Services	- Malware detection - Virtual patching capabilities - Denial-of-Service (DoS) attack prevention - Advanced threat detection through correlation - Brute force attack defense - Credential stuffing - Defense against known and zero-day attacks - Web services signature validation - Advanced threat intelligence and analytics
1.4.8.	Application Delivery	- HTTPS/SSL Offloading - Caching
1.4.9.	Authentication	- Support for LDAP, RADIUS, and SAML authentication protocols - SSL client certificate authentication - SAML authentication compatibility
1.4.10.	API Protection	- RESTful API support - Web services signature verification - API Gateway functionality - Schema validation
1.4.11.	Management and Reporting	- Centralized management and reporting system - Real-time data dashboards - Role-based access control (RBAC) implementation - OWASP Top 10 threat categorization - Geolocation-based blocking with embedded analytics
1.4.12.	Licensing	- Minimum 3 Years, including all security subscriptions and updates

1.4.13.	Garanție și suport	- **Perioada minimă de garanție**: 36 luni, acordată de producător, care să includă:
		  - Diagnosticare și remediere defecțiuni;
		  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
		  - Actualizări de software, atât pentru versiuni minore, cât și majore;

		- Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate; - **Suport tehnic local** din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună; - Perioada de **End-of-Support** și **End-of-Life** a echipamentului nu trebuie să fie mai devreme de anul 2030; - **Cerințe privind instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - **Cerințe privind acreditările furnizorului:** - Personal tehnic certificat pentru echipamentele și soluțiile propuse; - Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.

1.5. Soluție Mail Security Gateway

1.5.1.	**Mail Security Gateway**	
1.5.2.	Tip	- Modelul de licențiere trebuie să fie de tip perpetual. - Virtual Machine (On-premises) - Working mode: Gateway
1.5.3.	Supported Hypervisors	- Microsoft Hyper-V - KVM QEMU
1.5.4.	Mailbox Compatibility	- Microsoft Exchange Server 2019 - Supports up to 500 mailboxes - Inbound/Outbound messages inspection and routing
1.5.5.	Performance (with Threat Protection Enabled)	- performanța de prelucrare a mesajelor e-mail min. 50 000 pe ora - Antispam and antiphishing capture rate: min 99.9 %

1.5.6.	User Interface	- Robust webmail interface for server-mode deployments and quarantine management - Comprehensive mail queue management system

1.5.7.	Antispam	- Sender and domain reputation analysis
		- Spam and attachment signature detection
		- Adaptive heuristic rules for dynamic threat response
		- Outbreak protection mechanisms
		- Filtering for spam, malware, and phishing URLs
		- Detection of newly registered domains
		- Greylisting for IPv4, IPv6, and email accounts
		- Local sender reputation tracking (based on IPv4, IPv6, and Endpoint ID)
		- Behavioral analysis for advanced threat detection
		- Integration with third-party spam URI and real-time blacklists (SURBL/RBL)
		- Detection of newsletters (greymail) and suspicious newsletters
		- PDF scanning and image analysis
		- Global, domain, and user-level block/safe lists
		- Support for enterprise sender identity standards:
		  - Sender Policy Framework (SPF)
		  - DomainKeys Identified Mail (DKIM)
		  - Domain-Based Message Authentication, Reporting, and Conformance (DMARC)
		- Multi-system and per-user self-service quarantine options

1.5.8.	Targeted attack protection	- Content Disarm and Reconstruction (CDR) - Neutralization of Office and PDF documents (removal of macros, active content, and attachments) - Sanitization of email HTML content by removing hyperlinks or rewriting URLs - Protection against Business Email Compromise (BEC) - Multi-layered anti-spoofing measures - Manual and automated impersonation detection - Cousin domain detection - URL Click Protect for URL rewriting and real-time rescanning
1.5.9.	Content detection	- CPRL signature verification - Heuristic-based behavioral analysis - Greyware identification - Global threat intelligence and data analytics - Active content detection in PDF and Office documents - Threat rescanning upon quarantine release - Custom file hash verification

		- MIME and file type identification - Advanced data-loss prevention with file fingerprinting and sensitive data detection - Automated fingerprinting for Windows fileshares and manual uploads - Detection of healthcare, financial, personally identifiable information (PII), and profanity - Decryption of archives, PDFs, and Office documents using built-in and admin-defined password lists - Word detection within email bodies - Dynamic Image Analysis Service
1.5.10.	Encryption	- Comprehensive encryption support - Server-to-server TLS with granular ciphersuite control and optional enforcement - S/MIME support - Clientless encryption to recipient desktops using Identity-Based Encryption (IBE) - Optional Outlook plugin for triggering IBE
1.5.11.	Management, logging, and reporting	- Basic and advanced management modes - Role-based administration accounts per domain - Detailed logging for activities, configuration changes, and incidents - Built-in reporting module - Comprehensive message tracking - Centralized quarantine for large-scale deployments - Centralized logging and reporting system - SNMP support with standard and private MIBs, including threshold-based traps - Support for local or external storage servers, including iSCSI devices - External Syslog integration - Open REST API for configuration and management
1.5.12.	High availability support	- Active-Passive mode - Active-Active configuration synchronization - Synchronization of quarantine and mail queues - Device failure detection and notifications - Support for link status monitoring, failover, and redundant interfaces
1.5.13.	Licensing	- Minimum 3 Years, including all security subscriptions and updates
1.5.14.	Garanție și suport	- **Perioada minimă de garanție**: 36 luni, acordată de producător, care să includă:

		- Diagnosticare și remediere defecțiuni; - Suport tehnic non-stop (24x7x365) direct din partea producătorului; - Actualizări de software, atât pentru versiuni minore, cât și majore; - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate; - **Suport tehnic local** din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună; - Perioada de **End-of-Support** și **End-of-Life** a echipamentului nu trebuie să fie mai devreme de anul 2030; - **Cerințe privind instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - **Cerințe privind acreditările furnizorului:** - Personal tehnic certificat pentru echipamentele și soluțiile propuse; - Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.

1.6. Soluție Zero Trust Network Access (ZTNA)

1.6.1.	**Tip**	- Soluție pentru gestionarea securizată a accesului utilizatorilor la resursele interne, în conformitate cu conceptul ZTNA și cu implementarea protecției avansate la nivel de endpoint.
1.6.2.	**Cantitate**	- min. 200 stații de lucru
1.6.3.	**Cerințe generale:**	- Soluția trebuie să ofere un instrument centralizat de administrare;

		- Clientul endpoint trebuie să fie compatibil cu sistemele de operare: Windows 10 și mai sus, OS X 10.14 și mai sus, Linux Ubuntu 22 și mai sus.
1.6.4.	**Funcționalități**	- Remote Client deployment. - Endpoint onboarding, custom client installers, email invitations - Integration with Windows Active Directory - Real-time dashboard - Software inventory management - Vulnerability detection and remediation - Automatic group assignment - Remote triggers - Remote Logging and Reporting prin integrare cu soluția de gestiune, analiză și raportare pe baza jurnalelor de rețea (solicitată la poziția 1.3.10) - ZTNA Remote Access - IPSEC, SLL VPN Access - Split Tunnel on application basis - Removable media control - Application control, firewall - AI-driven antivirus - Automated quarantine - Ransomware protection - Patch Policy Enforcement: instalarea automata a patch-rilor pentru aplicațiile instalate in sistemul de operare a utilizatorului. Raportarea vulnerabilității aplicațiilor identificate cu oferirea CVE score-ului - Multifactor factor authentication, integrare cu soluția de gestiune a autorizării în rețeaua securizată (solicitată la poziția 1.7) - Integrarea cu soluția Sanbox (solicitată la poziția 1.8)
1.6.5.	Licensing	- Minimum 3 Years, including all security subscriptions and updates

1.6.6.	Garanție și suport	- **Perioada minimă de garanție**: 36 luni, acordată de producător, care să includă:
		  - Diagnosticare și remediere defecțiuni;
		  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
		  - Actualizări de software, atât pentru versiuni minore, cât și majore;
		  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;

		- **Suport tehnic local** din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună;
		- Perioada de **End-of-Support** și **End-of-Life** a echipamentului nu trebuie să fie mai devreme de anul 2030;
		- **Cerințe privind instalarea și serviciile aferente:**
		  - Implementarea completă a soluției;
		  - Migrarea regulilor de securitate existente către noul echipament;
		  - Integrarea echipamentelor noi cu infrastructura existentă;
		  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
		  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.
		- **Cerințe privind acreditările furnizorului:**
		  - Personal tehnic certificat pentru echipamentele și soluțiile propuse;
		  - Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.

1.7. Soluție de gestiune a autorizării în rețeaua securizată

1.7.1.	**Tip**	- Soluție pentru gestionarea autorizării în cadrul rețelei securizate, bazată pe identificarea utilizatorilor și pe permisiunile de acces furnizate de sisteme terțe (Identity-Based Policies).
1.7.2.	**Cantitate**	- 200 de utilizatori
1.7.3.	**Cerințe generale**	- Soluția trebuie să asigure integrarea cu echipamentele de tip firewall din poziția 1.3 în vederea permiterii accesului în rețeaua securizată. - Soluția trebuie să asigure integrarea cu soluția de gestiune, analiză și raportare pe baza jurnalelor de rețea (solicitată la poziția 1.3.10) - Soluția trebuie să ofere un instrument centralizat de administrare. - Soluția trebuie să fie oferită ca Appliance Virtual. - Compatibilitate cu platforma de virtualizare: Microsoft Hyper-V.

		- Soluția trebuie să conțină cel putin 200 licențe de software de tip One-time password application pentru iOS, Android
1.7.4.	**Funcționalități**	- Enables identity and role-based security policies in the secured enterprise network without the need for additional authentication through integration with Active Directory - Integration with LDAP and Active Directory for group membership - Enablement of identity and role-based security - Support of 802.1x, RADIUS, TACACS+, SAML IdP - Support of Single Sign-On (SSO) - Support wide range of multi-factor authentification metods: One Time Password (OTP) tokens, e-mail and SMS OTP, digital certificates. - Support of Facial/PIN/Fingerpring security in Mobile OTP application - Support of RFC6238, RFC4226 specifications in Mobile OTP application
1.7.5.	Licensing	Minimum 3 Years, including all security subscriptions and updates

1.7.6.	Garanție și suport	- **Perioada minimă de garanție**: 36 luni, acordată de producător, care să includă:
		  - Diagnosticare și remediere defecțiuni;
		  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
		  - Actualizări de software, atât pentru versiuni minore, cât și majore;
		  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;
		- **Suport tehnic local** din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună;
		- Perioada de **End-of-Support** și **End-of-Life** a echipamentului nu trebuie să fie mai devreme de anul 2030;
		- **Cerințe privind instalarea și serviciile aferente:**
		  - Implementarea completă a soluției;
		  - Migrarea regulilor de securitate existente către noul echipament;
		  - Integrarea echipamentelor noi cu infrastructura existentă;

		- Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - **Cerințe privind acreditările furnizorului:** - Personal tehnic certificat pentru echipamentele și soluțiile propuse; - Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.

1.8. Soluție de Sandboxing

1.8.1.	**Tip**	- Soluție de tip Sandbox
1.8.2.	**Integrare**	- Pentru analiza fișierelor și altor resurse, Soluția trebuie să fie capabila să se integreze și să accepte și analizeze informația cu echipamentele: - Next-Generation Firewall (NGFW) - Web Application Firewall (WAF) - Mail Security Gateway - Zero Trust Network Access (ZTNA) client - Third-party integrations via APIs
1.8.3.	**Cerințe generale:**	- Modelul de licențiere trebuie să fie de tip perpetual. - Soluția trebuie să fie oferită ca Appliance Virtual. - Soluția trebuie să suporte min 5 mașini virtuale locale (nested VM) pentru simulare, să conțină 5 licențe pentru MS Windows 11 si 1 x licența MS Office (cu capabilitatea pentru 5 VM) - Compatibilitate cu platforma de virtualizare: Microsoft Hyper-V. - Soluția trebuie să suporte generarea rapoartelor detailate a amenințărilor identificate, cu posibilitatea de export in format STIX/TAXII pentru import-ul in sisteme SIEM compatibile - Soluția trebuie să ofere câteva nivele de scanare: statică (in baza de metadate: IP adresa sursă, domain, email), asistata AI (simulare in modele de AI) și in cele din urmă scanare dinamică (in sistemele de operare virtualizate in sandbox)

		- Pentru optimizarea performanței Soluția trebuie să suporte scanare paralelă, cu distribuția sarcinii intre diferite mașini virtuale. - Pentru optimizarea performantei Soluția trebuie să fie capabilă sa creeze înregistrări cache pentru resursele scanate ulterior (fișiere, link-ri, etc) și să ofere instant verdictul scanării in cazul in care aceeași resursa este solicitată de către Clienți mai mult decât 1 data. - Soluția trebuie să fie capabilă sa creeze semnături AV, care vor fi populate de NGFW din poziția 1.3 și de soluția din poziția 1.6 - Soluția trebuie să suporte neutralizarea URL-rilor malițioase si impunerea executării URL-rilor din email in sandox (CDR - content disarm and reconstruction)
1.8.4.	**Funcționalități**	- Zero-day threat detection and antiphising blocking in real-time mode - AI/ML analyze and detection - Inline blocking - Modes of working: File submission from NGFW/ESG/WAF/Endpoint, URL submission, sniffer, network share scanning (SMB, NFS, FTP, sFTP, OneDrive) - Antivirus, IPS, Web filtering - Sandboxing virtual mashines OS types: Windows 10/11, MacOS, Linux, Android - Possibility to create custom VMs - OCR scanning - URL, QR-code scanning - Supported file types: exe, documents, web, emails, Linux/Andoid/MacOS files, user-defined types - Advanced monitoring and reporting functionality - CLI, WEB management - Integration with external systems via ICAP, API
1.8.5.	Licensing	- Minimum 3 Years, including all security subscriptions and updates

1.8.6.	Garanție și suport	- **Perioada minimă de garanție**: 36 luni, acordată de producător, care să includă:
		  - Diagnosticare și remediere defecțiuni;
		  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
		  - Actualizări de software, atât pentru versiuni minore, cât și majore;
		  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;

		- **Suport tehnic local** din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună;
		- Perioada de **End-of-Support** și **End-of-Life** a echipamentului nu trebuie să fie mai devreme de anul 2030;
		- **Cerințe privind instalarea și serviciile aferente:**
		  - Implementarea completă a soluției;
		  - Migrarea regulilor de securitate existente către noul echipament;
		  - Integrarea echipamentelor noi cu infrastructura existentă;
		  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
		  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.
		- **Cerințe privind acreditările furnizorului:**
		  - Personal tehnic certificat pentru echipamentele și soluțiile propuse;
		  - Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.

Minimum două persoane tehnice, deținând certificări emise de producător (vendor), pentru echipamentele și soluțiile propuse.

Ofertantul trebuie să facă dovada experienței prin prezentarea a cel puțin trei proiecte similare în ultimii 5 ani