TECHNICAL SPECIFICATIONS

1. DEFINITIONS AND ABBREVIATIONS

1.1. **Buyer** – UAB „Ignitis grupės paslaugų centras“

1.2. **Supplier –** entity – an individual, a private legal entity, a public legal entity, other organizations and their subdivisions or a group of such persons the Buyer enters into a Contract with.

1.3. **Contract -** a contract concluded between the Buyer and the Supplier regarding the Procurement object.

1.4. **Goods/Licenses** – Vulnerability Scanning Master Software Licences.

2. PROCUREMENT OBJECT

2.1. Vulnerability Scanning Master Software Licences.

3. SCOPE OF PROCUREMENT OBJECT

3.1. The quantities of Goods are specified in Table No.1 below:

Table No.1

No.	Object of procurement	Quantity, unit
1.	Vulnerability Scanning Master Software Licence with a three (3) year Subscription	1
2.	Vulnerability Scanning Slave Software Licence with a three (3) year Subscription	7

4. PLACE OF PERFORMANCE OF CONTRACTUAL OBLIGATIONS

4.1. The Goods must be delivered: remotely.

5. REQUIREMENTS FOR THE PROCUREMENT OBJECT

5.1. Technical requirements for the Vulnerability Scanning Master Software Licence are specified in table No. 1 below:

Table No. 1

No.	Technical parameters and requirements
1.	The Vulnerability Scanning Master Software shall be able to manage seven (7) Slave Software Units.
2.	The software must be able to scan at least 3000 unique IP addresses within 24 hours.
3.	The software shall support SSH, SMTP (email), SNMP, SysLog, LDAP, RADIUS, NTP, DHCP and IPv4/IPv6 protocols.
4.	The software shall be able to perform network vulnerability scanning using WMI, LDAP, RADIUS, HTTP, SMB, SSH, TCP, UDP protocols.
5.	The software must have a graphical control interface (GUI) via a web browser (*Web GUI*) to manage vulnerability scanning tasks.
6.	The management of software users shall be carried out through a graphical management interface.
7.	It must generate vulnerability scanning reports that: a) allow filtering and grouping of the vulnerabilities detected, and risk assessment of the vulnerabilities identified; b) can be exported in PDF, HTML, TXT and XML formats; c) has a classification of CVE and CPE vulnerabilities.

8.	There must be a vulnerability criticality assessment using CVSS.
9.	Load reports must be generated for the load at the time of the scan.
10.	The software must: a) perform automated vulnerability scanning according to a schedule set by the Buyer; b) notify the Buyer of the end of the vulnerability scanning.
11.	The software must support centralised management.
12.	The software must be compatible with and work seamlessly with Microsoft Edge 11, Google Chrome 110, Mozilla Firefox 110 or above.
13.	All actions performed by the software user in the graphical control interface via a web browser must be performed in parallel in the application programming interface (API).
14.	It shall be possible to control the Software by means of locally permitted commands (CLI).
15.	The software must use the TCP/IP protocol.
16.	If the DHCP protocol is not working on the Buyer's network, it must be possible to assign a specific IP address in the Software.
17.	Software backup and software recovery from backup must be supported.
18.	The software shall be compatible with the Buyer's existing virtualisation platforms: a) Microsoft Hyper-V server 2019 or later; b) VMware vSphere Hypervisor ESXi version 6.7 or higher.

5.2. Technical requirements for Vulnerability Scanning Slave Software Licence are specified in table No. 2 below:

Table No. 2

No.	Technical parameters and requirements
1.	The vulnerability scanning slave software shall be capable of scanning a minimum of 200 unique IP addresses within 24 hours. Vulnerability scanning of a minimum of 200 (two hundred) unique IP addresses.
2.	The software shall support SSH, SMTP (email), SNMP, SysLog, LDAP, RADIUS, NTP, DHCP and IPv4/IPv6 protocols.
3.	The software shall be able to perform network vulnerability scanning using WMI, LDAP, RADIUS, HTTP, SMB, SSH, TCP, UDP protocols.
4.	The software must have a graphical control interface (GUI) via a web browser (*Web GUI*) to manage vulnerability scanning tasks.
5.	The management of software users shall be carried out through a graphical management interface.
6.	Must generate vulnerability check reports that: a) allow filtering and grouping of the vulnerabilities detected, and risk assessment of the vulnerabilities identified; b) can be exported in PDF, HTML, TXT and XML formats; c) has a classification of CVE and CPE vulnerabilities.
7.	There must be a vulnerability criticality assessment using CVSS.
8.	Load reports must be generated for the load at the time of the scan.
9.	The software must: a) perform automated vulnerability scanning according to a schedule set by theBuyer;

	b) notify the Buyer of the end of the vulnerability scanning.
10.	The software must support centralised management.
11.	The software must be compatible with and work seamlessly with Microsoft Edge 11, Google Chrome 110, Mozilla Firefox 110 or above.
12.	All actions performed by the software user in the graphical control interface via a web browser must be performed in parallel in the application programming interface (API).
13.	It shall be possible to control the Software by means of locally permitted commands (CLI).
14.	The software must use the TCP/IP protocol.
15.	If the DHCP protocol is not working on the Buyer's network, it must be possible to assign a specific IP address in the Software.
16.	Software backup and software recovery from backup must be supported.
17.	The software shall be compatible with the Buyer's existing virtualisation platforms: a) Microsoft Hyper-V server 2019 or later; b) VMware vSphere Hypervisor ESXi version 6.7 or higher.

6. TERMS OF PROVISION OF GOODS

6.1. The goods must be activated no later than within 5 (five) working days from the date of signing Contract.

7. QUALITY ANT ELIMINATION OF DEFICIENCIES

7.1. The goods shall be subject to 3 (three) years warranty period starting from the date of activation of the Goods signing of the transfer-acceptance certificate.

7.2. During the warranty period, the Supplier must:

7.2.1. warranty support shall be carried out in accordance with the terms and conditions and procedures established by the licensor, which shall apply to the extent that they do not conflict with the Procurement Terms and Conditions and the provisions of the Republic of Lithuania Law on Public Procurement and the related legal acts.

7.2.2. ensuring access to bug fixes and newer versions of software;

7.2.3. provide access to the technical resources available on the manufacturer's website, including the software library;

7.2.4. enable the Buyer to independently submit a request (up to a maximum number of requests) to the software manufacturer's technical support website, monitor the status of the resolution of the request, and access other resources provided by the website.

7.3. The time limit for rectification of defects (e.g. wrong or non-functioning activation keys/codes issued, wrong licenses provided, etc.) identified in the Supplier's Tender and in the Contract shall be set by the time limit set out in the Contract, which shall commence from the date of the notification of the Buyer of the defective Goods.

7.4. The Supplier certifies that the Goods sold are fit for their intended use and that there are no latent defects in the Goods which would prevent the Goods from being used for their intended purpose or which would impair the utility of the Goods.

8. PAYMENT CONDITIONS

8.1. The Buyer shall pay the Supplier in advance for the delivered Goods of good quality within 30 (thirty) calendar days from the date of receipt of the Invoice.