



## HONEY POT SPRENDIMAS SU DIEGIMU

### TECHNINĖ SPECIFIKACIJA

#### 1. SĄVOKOS IR SUTRUMPINIMAI

**Pirkėjas** – Atsakinga vandentvarkos asociacija „VANDENS JĖGA“, asociacijos narys.

Pirkimą Pirkimo vykdytojo vardu atlieka AB „Klaipėdos vanduo“, juridinio asmens kodas 140089260, adresas Ryšininkų g. 11, Klaipėda, atstovaujanti atsakingą vandentvarkos asociaciją „Vandens jėga“.

**Tiekėjas** – ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė, su kuriuo Pirkėjas sudaro Sutartį.

**Sutartis** - sutartis, sudaroma tarp Tiekėjo ir Pirkėjo dėl Pirkimo objekto.

**Techninė specifikacija arba TS** – dokumentas, kuriame apibūdintas pirkimo objektas.

**Prekės** – TS nurodytas pirkimo objektas.

#### 2. REIKALAVIMAI PIRKIMO OBJEKTUI

##### 2.1. Esamos situacijos aprašymas.

Šiuo metu Asociacijos narių įmonės be specialių įrankių ir procesų neturi galimybių prevenciškai užkardyti, nustatyti ir reaguoti į kibernetinius incidentus. Siekiama įsigyti asociacijos nariams Masalų (Honeypot) sprendimą automatikos (OT) ir administraciniais (IT) tinklams. Ši sistema būtų vienas iš įrankių Kibernetinio saugumo operacijų centrui (SOC) Asociacijoje Vandens jėga.

Kibernetinės apgaulės („honeypot“) programinės įrangos tipas ir paskirtis – naujos kartos įsilaužimų aptikimo programinės įrangos sistema ir platforma (toliau – sistema), kuri kuria tinklo spąstus ir aptinka kenkėjišką elgesį galiniuose įrenginiuose

##### 2.2. Bendrieji reikalavimai tiekėjui:

2.2.1. Tiekėjas prieš diegdamas sprendimą turės susiderinti diegimo grafikus su kiekvienu asociacijos narės paskirtu bendrovės atsakingu asmeniu.

2.2.2. Tiekėjas tiekdamas Prekes, teikdamas paslaugas ir atlikdamas darbus privalo vadovautis Lietuvos Respublikos kibernetinio saugumo įstatymu ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams valdantiems ypatingos svarbos informacinę infrastruktūrą, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. Nr. 945“ (galiojančiomis aktualiomis redakcijomis).

#### 3. PIRKIMO OBJEKTAS

<i>Pirkimo objekto pavadinimas<sup>I</sup></i>	<i>Honeypot sprendimas su įdiegimu</i>
<i>Perkamas Kiekis<sup>II</sup></i>	<i>1 kompl.</i>



<b>Prekių pristatymo terminas (įskaitant diegimą ir kt. TS nurodytas paslaugas)</b>		<b>3 mėn.</b>
<b>Eil. Nr.</b>	<b>Savybė</b>	<b>Reikalaujami techniniai parametrai ar kita informacija</b>
<b>1.</b>	<b>Perkamas objektas</b>	
<b>1.1.</b>	Sistemos architektūriniai reikalavimai	<ol style="list-style-type: none"> <li>1. Sistema turi būti diegiama nereikalaujant pertvarkyti esamos galutinio vartotojo tinklo topologijos.</li> <li>2. Siūloma fizinė įranga negali būti naudota (refurbished) visa siūloma įranga turi būti nauja;</li> <li>3. Sistema turi apimti šiuos modulius - Centrinis valdymo mazgas (valdymo konsolė), Spąstų mazgas (kuriame veikia masalai) arba kai spąstų mazgai veikia centriniam valdymo mazge ir jie yra sujungti naudojant to paties gamintojo įrangą, norint užtikrinti galinių taškų pasiekiamumą. Centrinis taškas/valdymo mazgas (HoneyPOT) sistema turi būti pasiekiamas iš nutolusių taškų.</li> <li>4. Sistema turi turėti galimybę talpinti pasyvius klaidingus duomenis (pėdsakus) tikrose tinklo sistemose, veikiančiuose Linux OS ir Microsoft Windows sistemose.</li> <li>5. Sistema turi galėti būti išplečiama be poreikio iš naujo įdiegti sistemos komponentus.</li> <li>6. Sistema turi būti sukurta ir palaikyti architektūrą su keliais spąstų mazgais (masalais), turint vieną specializuotą funkcionalų mazgą valdymo operacijoms palaikyti.</li> <li>7. Sistema turi turėti galimybę talpinti simuliacijos spąstus (masalus) skirtinguose tinklo segmentuose.</li> <li>8. Sistema turi veikti be poreikio naudoti bet kokio tipo IP srautą kaip įvestį (t. y. NetFlow, sFlow, jFlow ir pan.).</li> <li>9. Gamintojas pateikia aparatinį (on prem) sprendimą, kurio visos sudedamosios dalys (prievalai, procesoriai, atmintis, ir t.t.) yra sukomplektuoti viename fiziniame įrenginyje to paties gamintojo kaip ir programinė įranga. Sprendimas/gamintojas taipogi turi turėti galimybę teikti ir programinę įrangą pagrįstą virtualizavimo pagrindu. Gamintojas taip pat privalo turėti spąstų fizinę įrangą pritaiktą industrinėms sąlygoms (rugged) variantą jei ateityje atsirastų poreikis diegti tokioje aplinkoje.</li> <li>10. Sprendimas centriniuose taškuose turi būti realizuotas virtualioje aplinkoje pateikiant įrangą ir programinę įrangą.</li> <li>11. Sprendimas nutolusiuose taškuose turi būti realizuotas gamintojo aparatinio įrenginiu arba virtualia sistema.</li> <li>12. Virtualios aplinkos palaikymas</li> </ol> <p>Sistema turi būti suderinama su virtualizacija ir leisti diegimą naudojant šias platformas:</p>



		<p>a. Centrinio valdymo serveriams:</p> <ul style="list-style-type: none"> <li>• VMware vSphere (6.0, 6.5 arba 7.0 versijos),</li> <li>• Microsoft Hyper-V (2022 metų arba naujesnės versijos),</li> <li>• Microsoft Azure Cloud,</li> <li>• KVM pagrindu veikiančios sistemos (tokios kaip Proxmox, OpenStack ir kt.).</li> </ul> <p>b. Spąstų (apgaulės) mazgams:</p> <ul style="list-style-type: none"> <li>• VMware vSphere (6.0, 6.5 arba 7.0 versijos),</li> <li>• Microsoft Hyper-V Server (2022 metų arba naujesnės versijos),</li> <li>• Microsoft Azure Cloud.</li> </ul> <p>13. Minimalūs reikalavimai pateikiamai techninei įrangai jei sprendimo fizinė įranga yra gamintojo aparatinis įrenginys: Centriniam valdymo mazgam - Aukštis: 1U; Talpa: ne mažiau 1 TB RAID1; Interneto prievadai: ne mažiau 2 vnt. SFP ir 2 vnt. 1 Gb RJ45; Apgaulės mašinų palaikymas: ne mažiau 20 vnt. Maitinimas: dubliuotas.</p> <p>Nutolę padalinių taškai: Interneto prievadai: ne mažiau 8 vnt. 1 GE RJ45</p> <p>14. Jeigu siūlomas sprendimas virtualizavimo pagrindu turi būti pateikti ne mažesni serverio resursai: Centriniam valdymo mazgam - Aukštis: 1U; RAM: ne mažiau 192GB DDR5; Talpa: ne mažiau 900 GB SSD RAID1, ne mažiau 2 TB HDD RAID1; CPU: ne mažiau 32 Core, 2.0 Ghz, 60 MB Cache, išleidimo data ne senesnė nei 2023 metai; Interneto prievadai: ne mažiau 2 vnt. SFP/SFP+ Maitinimas: dubliuotas.</p> <p>Nutolę padalinių taškai – Aukštis: 1U; RAM: ne mažiau 32GB DDR5; Talpa: ne mažiau 256 GB SSD RAID1; CPU: ne mažiau 8 Core, 2.0 Ghz, 10 MB Cache, išleidimo data ne senesnė nei 2023 metai; Interneto prievadai: ne mažiau 2 vnt. RJ45 arba SFP/SFP+</p>
--	--	---



1.2.	Apimtis	<p>Sistema turi būti pritaikyta veikti tokioje IT infrastruktūroje:</p> <ul style="list-style-type: none"> <li>- Centrinį valdymo mazgų (konsolių) skaičius - 5</li> <li>- Kiekvienoje asociacijos bendrovėje turi veikti atskiras centrinis valdymo mazgas.</li> </ul> <p>Nutolusių asociacijos padalinių kiekis ir bendras esančių skirtingų VLAN/tinklų kiekis per asociaciją įskaitant centrinį tašką:</p> <ol style="list-style-type: none"> <li>1. Nėra nutolusių taškų, 6 VLAN;</li> <li>2. 2 nutolę taškai, 12 VLAN;</li> <li>3. 3 nutolę taškai, 16 VLAN;</li> <li>4. 3 nutolę taškai, 20 VLAN;</li> <li>5. 4 nutolę taškai, 20 VLAN.</li> </ol> <ul style="list-style-type: none"> <li>- Kiekviename nutolusiame taške (mazge) ir centriname taške turi veikti ne mažiau 4 apgaulės mašinų (spąstų), įskaitant po vieną Windows 10 ir vieną Windows Server 2022 apgaulės mašiną.</li> <li>- Turi būti pateikta techninė ir programinė įranga reikalinga nurodytam mazgų kiekiui paleisti.</li> </ul>
1.3.	<b>Sistemos valdymo reikalavimai</b>	<ol style="list-style-type: none"> <li>1. Sistema turi turėti intuityvią sąsają ir nereikalauti didelių išlaidų jos priežiūrai ir palaikymui.</li> <li>2. Sistema turi valdymo konsolę – web sąsają su minimaliu palaikymu iš naršyklių: Mozilla Firefox, Safari, Google Chrome, naujausioje programinės įrangos versijoje.</li> <li>3. Sistema turi palaikyti RBAC (vaidmenimis pagrįstą prieigos kontrolę) teisių suteikimui sistemos administratoriams.</li> <li>4. Sistema turi registruoti ir kaupti audito įrašus apie visas veiklas valdymo modulyje. Kai keičiami nustatymai, audito žurnaliniuose įrašuose aiškiai turi būti nurodytos pradinės ir galutinės keičiamų nustatymų vertės.</li> <li>5. Sistema turi palaikyti kelių faktorių autentifikaciją (MFA) prie valdymo sistemos.</li> <li>6. Sistema turi turėti galimybę kurti žurnalinių įrašų archyvą techninių problemų sprendimui offline režime, kurį teikia gamintojo palaikymas.</li> </ol>
1.4.	<b>Sistemos funkcionalumo reikalavimai</b>	<ol style="list-style-type: none"> <li>1. Kiekvienas masalas (spąstas) turi būti unikalūs, turintis savo savybių rinkinį (MAC adresą, IP adresą, hosto vardą, imituojamas paslaugas/servisus ir nustatymus).</li> <li>2. Sistema turi suteikti galimybę kurti ir platinti klaidingus duomenis (pėdsakus) tikruose, gamybiniuose tinklo galiniuose įrenginiuose.</li> <li>3. Pėdsakų tipai turi apimti bent: <ul style="list-style-type: none"> <li>• išsaugotus automatinio prisijungimo duomenis;</li> <li>• prisijungimų profilius su imituojamais duomenų šaltiniais;</li> <li>• tinklo išteklius;</li> </ul> </li> <li>4. Sistema turi aptikti tinklo įsilaužimus (t. y., „brute-force“ atakas, bandymą prisijungti prie imituojamų sistemų), klasifikuoti jų kritiškumo lygį ir pobūdį, nepriklausomai nuo grėsmės tipo ir įgyvendinimo principo.</li> <li>5. Sistema turi rodyti spąstų prisijungimų istoriją ir įsilaužėlio manipuliacijos „spąstais“ istoriją: <ul style="list-style-type: none"> <li>• nurodant pažeidžiamos sistemos IP adresą;</li> </ul> </li> </ol>

		<ul style="list-style-type: none"> <li>• pažeistas paskyras;</li> <li>• protokolus/interakcijos portus/prievadus.</li> </ul> <p>6. Sistema turi turėti integruotas grafinės sąsajos skydelius, rodančius statistiką apie sistemos veikimą, įvykius ir kt.</p> <p>7. Sistema turi turėti galimybę kurti spąstus visiškai automatiškai.</p> <p>8. Sistema turi apimti bent šiuos spąstų tipus (masalus):</p> <ul style="list-style-type: none"> <li>• Microsoft RDP serveris,</li> <li>• Microsoft SMB failų serveris,</li> <li>• Serveriai, veikiantys Linux OS,</li> <li>• SCADA/HMI/PLC,</li> <li>• DNS serveris,</li> <li>• MySQL serveris,</li> <li>• FTP failų serveris,</li> <li>• Samba failų serveris,</li> <li>• Modbus TCP serveris,</li> <li>• MQTT brokeris.</li> </ul> <p>9. OT masalai turi imituoti žiniatinklio sąsajas bent jau SIEMENS ir Allen-Bradley (Rockwell Automation) PLC.</p> <p>10. OT masalai turi palaikyti bent S7comm ir Modbus TCP protokolus.</p> <p>11. Sistema turi tiksliai klasifikuoti ir sujungti įvykius, susijusius su aptikta ataka, į vieną įspėjimą, kad nesukeltų sistemos operatoriams poreikio peržiūrėti ir apdoroti daugybę įvykių.</p> <p>12. Sistema turi suteikti galimybę kurti savo tinklo masalų tipus, pagrįstus sistemoje esančiais pagrindiniais tipais. Sukūrus naują masalų tipą, vartotojas turi galėti automatiškai sukurti daugiau nei vieną tokio tipo masalą vienu metu, nesikreipiant dėl papildomų manipuliacijų.</p> <p>13. Sistema turi naudoti metodą, nepagrįstą parašų (signatūrų) aptikimu, kibernetinių grėsmių aptikimui.</p> <p>14. Sistema turi turėti galimybę kurti ir vizualizuoti tinklo išteklių tarpusavio sąveiką.</p> <p>15. Sistema taip pat turi mokėti generuoti ribotą netikrą tinklo srautą, kad atrodytų kaip tikri pasyviuose tinklo skenavimuose, kuriuos atlieka užpuolėjas</p> <p>16. Sistema turi generuoti žymas (netikrus talpykloje saugomus prisijungimo duomenis, duomenis ir konfigūracijos failus, tinklo dalinimus), kurie yra patalpinti tikruose ištekliuose.</p> <p>17. Sistema turi leisti kurti teisėtus IP adresus (Safelist/white list) sąrašas skirtas pridėti IP adresus, kurie laikomi teisėtais, kad jie nesukeltų įvykio ar incidento, kai prieinami masalai. Pavyzdžiui, tai gali būti stebėjimo sistemos IP adresas, kuris apklausia tinklą ir t.t);</p> <p>18. Sistema/agentas turi pasyviai skenuoti IT tinklą (IT įrenginius, tokius kaip serveriai, nešiojami kompiuteriai ir maršrutizatoriai), surinktą informaciją turi atvaizduoti ir rūšiuoti pagal IP, MAC, gamintoją, tinklą Hostą, OS, Firmware, įrenginio tipą;</p>
--	--	--



		<p>19. Sistema/agentas turi pasyviai skenuoti ICS tinklą šiais protokolais MODBUS, DNP3, ENIP, S7comm/S7comm plus, BACNET, Profinet, FINS, ATG, Kamstrup, Moxa, IEC104, FL-net, GE-EGD, GE-SRTP, Triconex ir PCOM.</p> <p>20. Sprendimas turi turėti iš anksto paruoštą karantinavimo konfigūraciją su tokiomis sistemomis kaip: Fortinet, CheckPoint, Palo Alto ugniasienėmis, Aruba Clearpass ir FortiNAC sprendimais, SentinelOne, CrowdStrike sprendimu.</p> <p>21. Sistema turi turėti integraciją su to paties gamintojo Sandbox sprendimu kaip ir Virus Total.</p> <p>22. Sistema turi veikti izoliuotoje aplinkoje (on prem);</p> <p>23. Sistema turi atvaizduoti atakuotojus interaktyviame žemėlapyje ir juos suskirstyti pagal šalis arba regionus;</p> <p>24. Galimybė perkrauti arba išjungti sistemą viena komanda;</p> <p>25. Turi būti galimybė eksportuoti incidentų sąrašą į CSV, PDF failą</p>
1.5.	<b>Valdymo konsolė (GUI)</b>	<p><b>Sistemos išteklių valdiklis turi atvaizduoti pagrindinę informaciją</b></p> <ul style="list-style-type: none"> <li>- Serijinius numerius;</li> <li>- Sistemos veikimo laiką;</li> <li>- Licencijų statusą;</li> <li>- Priskirtų vCPU kiekį,</li> <li>- Turi atvaizduoti CPU apkrovas procentaliai;</li> <li>- Priskirtų RAM kiekį;</li> <li>- Turi atvaizduoti RAM apkrovas procentaliai;</li> <li>- Turi atvaizduoti masalų kiekį;</li> <li>- Turi atvaizduoti masalų naudojamus servisus procentaliai vizualiai viename lange su galimybe filtruoti per pasirinktą servisą tokius kaip SSH, SAMBA, SMB, TCPLISTENER, ir kit;</li> <li>- Masalai turi būti atvaizduojami vienetais ir procentinę dalį, pagal operacinę sistemą, pateiktą vizualiai diagramoje;</li> <li>- Sistemos valdymas per GUI arba per CLI;</li> <li>- Valdymo konsolė turi atvaizduoti diskų būklę, diskų užimtumą procentaliai, diskų kiekį, diskų dydį, statusą, RAID lygį;</li> </ul> <p><b>Incidentų ir įvykių pasiskirstymas</b></p> <ul style="list-style-type: none"> <li>- Incidentas arba įvykis, kurio rizikos lygis nežinomas</li> <li>- Incidentas arba įvykis, kurio rizikos lygis yra žemas</li> <li>- Incidentas arba įvykis, kurio rizikos lygis yra vidutinis</li> <li>- Incidentas arba įvykis, kurio rizikos lygis yra aukštas</li> <li>- Incidentas arba įvykis, kurio rizikos lygis yra kritinis</li> <li>- Incidentai ar įvykiai turi būti atvaizduojami grafike, įvykiai turi būti suskirstyti pagal datą bent 4 savaitių laikotarpyje</li> <li>- Turi būti galimybė filtruoti incidentus pagal servisus tokius kaip SSH, SAMBA, SMB, RDP, ir kiti;</li> <li>- Turi būti galimybė filtruoti pagrindinius (TOP) atakuotojus pagal IP arba incidentus;</li> <li>- Turi būti galimybė filtruoti atakuotojus pagal įvykius;</li> </ul>



1.6.	<b>IT masalai</b>	<ol style="list-style-type: none"> <li>1. CentOS 7.9 - SSH, SAMBA, SMTP, TCP, HTTP, HTTPS, GIT, FTP, RADIUS;</li> <li>2. Custom Redhat 7.9/8.8/8.10/9.4 - SSH, SAMBA, SMTP, TCP, HTTP, HTTPS, GIT, FTP, RADIUS;</li> <li>3. Custom Win 10 / 11 - RDP, SMB, IIS, IISL, SMTP, TCP, NBNS, ICMP, FTP, SWIFT;</li> <li>4. Custom Win Server 2016/2019/2022 - RDP, SMB, IIS, IISL, SMTP, TCP, NBNS, ICMP, FTP, SWIFT;</li> <li>5. VMware ESXI - HTTP, HTTPS, SSH;</li> <li>6. FortiGate - SSLVPN, HTTPS;</li> <li>7. SSL-VPN - SSLVPN, HTTPS;</li> <li>8. Ubuntu 16.04 / 18.04 - SSH, SAMBA, SMTP, TCP, HTTP, HTTPS, GIT, FTP, RADIUS;</li> <li>9. Windows 7 / 10 / 11 - RDP, SMB, SMTP, TCP, NBNS, ICMP, FTP, SWIFT;</li> </ol>
1.7.	<b>IoT masalai</b>	<ol style="list-style-type: none"> <li>2. Printers: <ul style="list-style-type: none"> <li>- Brother MFC Printer (SNMP, HTTP, Jetdirect)</li> <li>- HP Printer Decoy (SNMP, HTTP, Jetdirect)</li> </ul> </li> <li>3. IP Camera: <ul style="list-style-type: none"> <li>- IP camera (SNMP, HTTP, RTSP, UPnP)</li> </ul> </li> <li>4. Network devices <ul style="list-style-type: none"> <li>- Cisco Router - Cisco images (models) 2691, 3660, 3725 ir 3745 (TELNET, HTTP, SNMP, CDP)</li> <li>- MikroTik Router (SNMP, TELNET, CDP, HTTP)</li> <li>- NetGear MR60 Router (HTTP, SNMP, UPnP)</li> </ul> </li> <li>5. Switch</li> <li>6. Kiti <ul style="list-style-type: none"> <li>- INFUSOMAT (HTTP, HTTPS, CanBus, B.BRAUN)</li> <li>- PACS (TELNET, FTP, PACS, PACS-WEB, DICOM Server)</li> <li>- SPACECOM (HTTP, HTTPS, FTP, CANBus, SSH)</li> <li>- SWIFT VPN Gateway (TELNET, HTTPS)</li> </ul> </li> </ol>
1.8.	<b>OT masalai</b>	<ol style="list-style-type: none"> <li>1. Masalai turi palaikyti SCADA v3 OS. Ir aukštesnę versiją</li> <li>2. Ascent Compass MNG (HTTP, FTP, SNMP, BACNET);</li> <li>3. C-More HMI (SNMP, HTTP, HTTPS, FTP)</li> <li>4. Emerson iPro by Dixell (SNMP, MODBUS, HTTP)</li> <li>5. GE PLC 90 (SNMP, HTTP, SRTP)</li> <li>6. Guardian AST (Guardian-AST/no-port)</li> <li>7. IPMI Device (HTTP, FTP, SNMP, IPMI)</li> <li>8. Kamstrup 382 (KAMSTRUP)</li> <li>9. Lantronix XPORT V1.8 (SNMP, HTTP, Lantronix/no-port)</li> <li>10. Lantronix XPORT V2.0 (SNMP, HTTP, Lantronix/no-port)</li> <li>11. Liebert Spruce UPS (TFTP, SNMP, HTTP)</li> <li>12. MOXA NPORT 5110 (SNMP, TELNET, HTTP, MOXA)</li> <li>13. Modicon M241 (TFTP, SNMP, MODBUS, ENIP, HTTP)</li> </ol>



		<ul style="list-style-type: none"> <li>14. Modicon M580 (TFTP, SNMP, MODBUS, ENIP, HTTP)</li> <li>15. Niagara4 Station (SNMP, HTTP, BACNET)</li> <li>16. NiagaraAX Station (SNMP, HTTP, BACNET)</li> <li>17. Phoenix contact AXC 1050 (HTTP, SNMP, PROFINET, FTP)</li> <li>18. PowerLogic ION7650 (SNMP, MODBUS, DNP3, HTTP)</li> <li>19. Rockwell 1769-L16ER/B LOGIX5316ER (SNMP, ENIP, HTTP)</li> <li>20. Rockwell 1769-L35E Ethernet Port (SNMP, ENIP, HTTP)</li> <li>21. Rockwell PLC (HTTP, TFTP, SNMP, ENIP)</li> <li>22. SIEMENS S7-1500 PLC (HTTP, TFTP, SNMP, S7COMM, IEC104, PROFINET)</li> <li>23. Schneider EcoStruxure BMS server (SNMP, BACNET, HTTP, TRICONEX)</li> <li>24. Schneider Power Meter - PM5560 (SNMP, BACNET, ENIP, HTTP, DNP3)</li> <li>25. Schneider SCADAPack 333E (SNMP, DNP3, TELNET)</li> <li>26. Siemens S7-200 PLC (HTTP, TFTP, SNMP, MODBUS, S7COMM)</li> <li>27. Siemens S7-300 PLC (TFTP, SNMP, IEC104)</li> <li>28. VAV-DD BACnet controller (SNMP, BACNET)</li> </ul>
1.9.	<b>Aplikaciju (APP) masalai</b>	<ul style="list-style-type: none"> <li>1. ERP Decoy (ERP-WEB/HTTP)</li> <li>2. POS Decoy (POS-WEB / HTTP);</li> <li>3. SAP Decoy (SAP Router, SAP Dispatcher, HTTP)</li> <li>4. Elastic Search ((Elastic Search) ScadaBR Decoy (ScadaBR-HTTP))</li> <li>5. Tomcat (HTTP, HTTPS, SSH)</li> <li>6. MySql MariaDB (SSH, MariaDB)</li> <li>7. VOIP: SIP (SIP/TCP, UDP)</li> <li>8. XMPP Decoy (XMPP/ HTTP)</li> <li>9. MQTT (MQTT/HTTP, CoAP)</li> <li>10. 4G/5G 3GPP (NextEPC/HTTP, SCTP&amp;GTP-C, GTP-U)</li> <li>11. SMTP</li> <li>12. RADIUS</li> <li>13. Mac (SSH, VNC)</li> <li>14. Webmin (HTTP, HTTPS)</li> <li>15. Citrix ADC (HTTP, HTTPS)</li> <li>16. Citrix Application Delivery Management (HTTP, HTTPS)</li> <li>17. Citrix Receiver (HTTP, HTTPS)</li> <li>18. Citrix Endpoint Management (HTTP, HTTPS)</li> <li>19. Nginx (HTTP, HTTPS)</li> <li>20. EV-CPO (HTTP, HTTPS)</li> <li>21. TrueNAS (SSH, HTTP, HTTPS, SAMBA, SNMP)</li> </ul>
1.10.	<b>Agentas (Token)</b>	<ul style="list-style-type: none"> <li>1. Windows - Cached Credential, HoneyDocs, Network Connection (static MAC address), ODBC, RDP, SMB</li> <li>2. Linux – HoneyDocs, RDP (xfreerdp), SMB (SAMBA), SSH</li> <li>3. MAC - RDP (xfreerdp), SMB (SAMBA), SSH</li> <li>4. SAP – SAP</li> <li>5. AWS Key - AWS Key</li> <li>6. Azure Key - Azure Key</li> </ul>





1.11.	<b>Sistemos integracijos reikalavimai</b>	<ol style="list-style-type: none"> <li>1. Sistema turi suteikti galimybę siųsti saugumo įspėjimus/įspėjimus el. paštu.</li> <li>2. Sistema turi suteikti galimybę perduoti sistemos ir saugumo žurnalus bet kuriam SIEM per syslog.</li> <li>3. Sistema turi turėti galimybę siųsti saugumo įspėjimus/įspėjimus per Webhook.</li> <li>4. Sistema turi turėti viešą API, kuris turi šias galimybes: <ol style="list-style-type: none"> <li>a. gauti informaciją apie sistemą, įskaitant licenciją, izoliuotas aplinkas (nuomininkus), masalus ir saugumo įspėjimus,</li> <li>b. valdyti masalų ir saugumo incidentų būseną.</li> </ol> </li> </ol>
1.12.	<b>Sistemos licencijų reikalavimai</b>	<ol style="list-style-type: none"> <li>1. Sistema neturi reikalauti jokių papildomų programinės įrangos licencijų pirkimo (išskyrus virtualizacijos programinę įrangą), įskaitant Microsoft Windows programinę įrangą, sisteminę programinę įrangą ir specializuotą programinę įrangą, užtikrinančią pateiktos platformos veikimą.</li> <li>2. Sistema turi sugebėti imituoti bent 20 aktyvių spąstų (operacinių sistemų, tinklo įrangos, tinklo paslaugų emuliacijų/atkartojimų) tinklo segmentuose be papildomos licencijos poreikio.</li> <li>3. Sistema turi turėti gamintojo techninę pagalbą, kuri apima: <ul style="list-style-type: none"> <li>• nemokamus dabartinės programinės įrangos komponentų, duomenų bazių ir kitos programinės įrangos, reikalingos pilnam ir teisingam Sistemos veikimui, atnaujinimus,</li> <li>• programinės įrangos atnaujinimus ir esamų klaidų taisymą gamintojo po programinės įrangos įdiegimo į eksploataciją, be poreikio iš naujo paleisti sistemos valdymo komponentus,</li> <li>• galimybę susisiekti su rangovu arba gamintoju dėl problemų sprendimo <b>365x24x7</b> režimu.</li> </ul> </li> <li>4. Turi būti pateiktos reikalingos virtualizacijos platformos licencijos ir visos kitos reikalingos licencijos sistemos veikimui.</li> <li>5. Licencijos turi būti pateikiamos su ne mažesniu nei <b>36</b> mėn. palaikymo laikotarpiu.</li> <li>6. Įrangos gedimo atveju diskai tiekėjui ar gamintojui negražinama, tiekėjas ar gamintojas įrangą keičia nemokamai visą palaikymo laikotarpį savomis lėšomis.</li> <li>7. Tiekėjas turi pateikti reikalingas licencijas Virtualizavimui sistemos</li> </ol>
1.13.	Dokumentacija	<p><u>Su prekėmis turi būti pateikta:</u></p> <ol style="list-style-type: none"> <li>1. Prekių važtaraštis su nurodytu Prekių pavadinimu ir kiekiu;</li> <li>2. Prekių perdavimo - priėmimo aktas;</li> <li>3. Įrangos techninį pasą lietuvių arba anglų kalba;</li> <li>4. Gamintojo ar jo oficialaus atstovo išduotos Prekių atitikties deklaracijos (sertifikatai) lietuvių arba anglų kalba.</li> <li>5. Prekių montavimo ir naudojimo instrukcijos lietuvių arba anglų kalba;</li> <li>6. Prieš montuojant Prekes, pateikti įrangos struktūrinės ir principinės schemas suderinimui.</li> </ol>



1.14.	Trūkumų šalinimas	<i>Prekių perdavimo - priėmimo ar Garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 10 (dešimt) darbo dienų terminas nuo Pirkėjo pranešimo apie sugedusias, nekokybiškas ar turinčias trūkumų Prekes. Tiekėjas netinkamas/sugedusias Prekes privalo pasiimti iš Pirkėjo nurodytų adresų ir suremontuotas Prekes savo lėšomis grąžinti Pirkėjo nurodytais adresais, iš kurių jos buvo paimtos.</i>
1.15.	Prekių pristatymo vieta	<p>UAB „Vilniaus Vandenys“: Spaudos g. 8-1, Vilnius, 05132.</p> <p>UAB „Kauno vandenys“: Aukštaičių g. 43, Kaunas, 44158 Kauno m. sav.</p> <p>UAB „Dzūkijos vandenys“: Pulko g. 75, Alytus, 62135 Alytaus m. sav.</p> <p>UAB „Utenos vandenys“: Vandenų gatvė 1, Naujasodžio kaimas, 28113 Utena; Palijoniškio gatvė 22, 28180 Utena;</p> <p>AB „Klaipėdos vanduo“: Ryšininkų 11, Klaipėda; Liepų g. 49A, Klaipėda; Šilutės pl. 49, Klaipėda; Uosių g. 8, Dumpių k., Klaipėdos r.; Laugalių g. 2B, Gargždai.</p>
1.16.	Kokybė	<i>Tiekėjas, teikdamas pasiūlymą patvirtina, kad parduodamos Prekės yra tinkamos naudoti pagal jų tikslinę paskirtį, kad nėra paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.</i>
2.	<b>Tiekėjo kartu su prekėmis atliekamos (-i) paslaugos/darbai:</b>	
2.1.	Tiekėjas turės	<ol style="list-style-type: none"> <li>1. Tiekėjas turės pateikti diegimo grafiką ir suderinti su Pirkėjo atstovais.</li> <li>2. Tiekėjas turi pateikti techninę dokumentaciją apie sistemos diegimą, administravimą ir naudojimą anglų kalba.</li> <li>3. Tiekėjas turi diegti ir sukonfigūruoti programinę įrangą serveriuose bei pateikti klientui techninę ir eksploatacinę platformos dokumentaciją.</li> <li>4. Tiekėjas turi suteikti konsultavimo ir mokymo paslaugas kliento techniniams specialistams (bent 8 asmenims) dėl Sistemos administravimo ir eksploatavimo (ne mažiau kaip 40 valandų) anglų, lietuvių, rusų kalbomis pasirinktinai.</li> <li>5. Tiekėjas turės pristatyti įrangą į nurodytas vietas, ją sumontuoti ir sukonfigūruoti.</li> <li>6. Tiekėjas turi pateikti ir sudiegti visą reikalingą programinę įrangą (OS, virtualizavimo platforma ir kitą programinę įrangą reikalingą sprendimui) reikalinga, kad sistema (sprendimas) tinkamai veiktų. Pirkėjas neapteikia jokių licencijų, visas reikalingas licencijas sprendimo veikimui pateikia Tiekėjas.</li> <li>7. Tiekėjas turės fiziškai pajungti techninę įrangą Pirkėjo objektuose.</li> </ol>



2.2.	Garantija suteiktoms Paslaugoms/Darbams	Ne trumpesnė kaip 36 mėn. nuo priėmimo-perdavimo dokumento pasirašymo
3.	<b>Žalieji reikalavimai prekėms</b>	
3.1.	Nustatomi žalieji reikalavimai prekėms	<p>Atliekamas žaliasis pirkimas. Pirkimas vykdomas vadovaujantis Lietuvos Respublikos aplinkos ministro 2022 m. gruodžio 13 d. įsakymo Nr. D1-401 „Dėl Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymo Nr. D1-508 „Dėl Produktų, kurių viešiesiems pirkimams ir pirkimams taikytini Aplinkos apsaugos kriterijai, sąrašo, Aplinkos apsaugos kriterijų ir aplinkos apsaugos kriterijų, kuriuos perkančiosios organizacijos ir perkantieji subjektai turi taikyti pirkdami prekes, paslaugas ar darbus, taikymo tvarkos aprašo patvirtinimo“ pakeitimo“ 4.4.3. punktu (nematerialiai daliai). Taip pat, nustatomi papildomi Aplinkos apsaugos kriterijai:</p> <p>1. Pirkimo objektas turi atitikti <b>2011/65/ES</b> RoHS direktyvą.</p> <p>Tiekėjas, Pirkėjui paprašius, pateiks atitiktą įrodančius dokumentus, jei informacijos nebus galima patikrinti viešai prieinamais duomenimis.</p>
4.	<b>Kiti reikalavimai</b>	
4.1.	Tiekėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).	
4.2.	Visa pateikiama įranga privalo būti ne prastesnių parametrų nei nurodyta šioje specifikacijoje arba geresnių parametrų.	
4.3.	Tiekėjas turi atitikti ISO 27001 arba lygiavertį standartą.	

<sup>i</sup> Jeigu techninėje specifikacijoje yra nurodytas konkretus perkamos prekės tipas, modelis, ženklas, taikomas standartas ar kita konkreti apibūdinanti informacija, Pirkėjui yra priimtina lygiavertė prekė, atitinkanti techninėje specifikacijoje nurodytos prekės parametrus ar taikomus standartus.

Šiame dokumente vartojami terminai „turi būti“, „turi turėti“, „turi leisti“, „turi būti galimybė“, „turi būti sukurtas (-a)“ yra lygiaverčiai ir reiškia, kad Tiekėjas pirkimo apimtyje privalo sukurti ir įdiegti (ar pateikti ir įdiegti) atitinkamą funkcionalumą ar suteikti atitinkamas paslaugas. Funkcionalumas, kuris yra nurodytas būsimuoju laiku (bus, leis, apims ir t.t.) nurodo siekiamą įgyvendinti būseną ir reiškia, kad Tiekėjas pirkimo apimtyje privalo sukurti ir įdiegti (ar pateikti ir įdiegti) atitinkamą funkcionalumą.

<sup>ii</sup> Kai nurodytas tikslus Prekių kiekis, Pirkėjas įsipareigoja išpirkti visą nurodytą prekių kiekį.