

TECHNINĖ SPECIFIKACIJA

PIRKIMO OBJEKTO APRAŠYMAS

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.

PIRKIMO OBJEKTAS

Programinė įranga ir licencijos (Saugumo įvykių stebėjimo ir valdymo informacinė sistema), (toliau – **Pirkimo objektas**).

Pirkėjas, atsižvelgdamas į tai, kad:

- 1) 2022 m. gruodžio 14 d. priimta Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 Dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (toliau – TIS 2 direktyva);
- 2) kibernetiniai incidentai gali:
 - a) trukdyti vykdyti ekonominę veiklą ES vidaus rinkoje;
 - b) sukelti didelių finansinių nuostolių;
 - c) pakirsti naudotojų pasitikėjimą;
 - d) padaryti didelę žalą ne tik Pirkėjui bet ir ES ekonomikai bei visuomenei;

taip pat siekdamas:

- 1) pasiruošti TIS 2 direktyvos įgyvendinimui;
- 2) užtikrinti tinkamą TIS 2 direktyvos įgyvendinimą – didinti kibernetinio saugumo lygį bei užtikrinti operatyvų reagavimą ir informavimą apie kibernetinius incidentus;

vykdo šį pirkimą ir siekia atsirinkti kompetentingą bei patikimą Tiekėją .

REIKALAVIMAI PIRKIMO OBJEKTUI

Eil. Nr.	Prekės, įrenginio, įrangos savybės, parametrų arba funkcijų išpildymas	Reikalaujamo parametro arba vykdomos funkcijos reikšmės išpildymas
<i>Programinė įranga ir licencijos (Saugumo įvykių stebėjimo ir valdymo informacinė sistema)</i>		
	Paskirtis	Užtikrinti Pirkėjo eksploatuojamų informacinių išteklių infrastruktūros kibernetinių grėsmių nustatymą bei kibernetinės saugos incidentų aptikimą 24/7/365 nenutrūkstamai, taip įgalinant Pirkėją efektyviai ir greitai šalinti atsiradusius trūkumus siekiant minimizuoti arba užkirsti kelią galimam žalos atsiradimui.

	Licencija gali būti teikiama tik programinė, kuri turi užtikrinti:	Nuolatinį žurnalų įrašų (anglų k. logs) surinkimą / koreliavimą, turi būti pritaikyta surinkti ir apdoroti ne mažiau kaip 5 000 įvykių / įrašų per sekundę (angl. EPS – Events Per Second) su galimybe padidinti surenkamų ir apdorojamų įvykių skaičių iki 10 000 įvykių / įrašų skaičių per sekundę. Integruojamos tinklo įrangos vienetų skaičius ir įvykių surinkimo agentų skaičius neturi būti ribojamas.
Licencijos teikimui reikalingos programinė įrangos charakteristikos:		
	Tiekėjo suteikiama programinė įranga privalo būti nenaudota, pateikiama originalioje gamintojo pakuotėje; gamykliškai atnaujinti (angl. Refurbished) – neleistini	Atitinka reikalavimus
	Tiekėjas turi užtikrinti, kad įrangos gamintojas nėra paskelbęs apie siūlomos įrangos gamybos arba tobulinimo nutraukimą (pvz. angl. „End of life time“ ar „Discontinued“)	Atitinka reikalavimus
	Tiekėjas turi būti oficialus siūlomų produktų gamintojų atstovas (jeigu Tiekėjas pats nėra siūlomų prekių gamintojas) ir turi turėti teisę parduoti siūlomą įrangą	Atitinka reikalavimus
	Tiekėjo suteikiama programinė įranga turi gebėti surinkti įrašus tiek užklaudama sistemas, tiek iš sistemų, kurios pačios siunčia žurnalinius įrašus	Atitinka reikalavimus
	Tiekėjo suteikiama programinė įranga turi leisti kurti specializuotus įvykių surinkimo komponentus oficialiai nepalaikomiems įvykių šaltiniams	Atitinka reikalavimus

	Tiekėjo suteikiamas sprendimas turi gebėti lanksčiai prisitaikyti ir paimti įvykius iš Pirkėjo taikomųjų programų sistemų	Atitinka reikalavimus
	Tiekėjo suteikiamas sprendimas turi turėti naudotojų elgesio analizės (angl. User Behavior Analytics) komponentą, galintį:	<ol style="list-style-type: none"> 1. Analizuoti standartinę naudotojų veiklą ir aplikti joje anomalijas; 2. Aptikti pavogtas, kompromituotas naudotojų paskyras; 3. Integruotis ir perduoti informaciją į kitus sistemos saugumo komponentus, pavyzdžiui, koreliacijos variklį; 4. Identifikuoti pasikeitimus naudotojų elgsenoje; 5. Stebėti privilegijuotų naudotojų veiksmus; 6. Gebėti naudoti grėsmių informaciją naudotojų stebėjime; 7. Naudotojai turi turėti grėsmės įverčius, kurie kinta laike ir gali būti naudojami incidentams generuoti.
	Tiekėjo suteikiama programinė įranga turi gebėti suglaudinti archyvinčius duomenis	Atitinka reikalavimus
	Visą Paslaugų teikimui reikalingą programinę įrangą turi būti įrengta Pirkėjo debesų aplinkoje.	Atitinka reikalavimus
	Prieiga prie programinės įrangos	Prie Paslaugų teikimui reikalingos programinės įrangos Tiekėjas jungiasi saugiu komunikacijos kanalu nuotoliniu būdu, patvirtintu Pirkėjo prieigos taisyklėse. Visa Paslaugų teikimui reikalinga kaupiama informacija (žurnaliniai įrašai, duomenų srauto įrašai ir kt.) yra laikoma Pirkėjo tinkle arba Tiekėjo infrastruktūroje. Paslaugų teikimui turi būti naudojama Tiekėjo debesijos infrastruktūra, esanti Europos sąjungos šalyse. Jei Tiekėjas Paslaugų teikimui naudos Pirkėjo debesijos paslaugas ar Pirkėjo debesijos paslaugų komponentus, tai visus papildomus kaštus (mokesčiai už resursus, duomenų perdavimą ir pan.) atsiirandančius dėl šių komponentų naudojimo prisiima Tiekėjas
Apimtis		

	<p>Nuolatinis žurnalų ir tinklo įrašų (anglų k. logs, netflows) surinkimas / koreliavimas bei pranešimų apie kibernetinės saugos grėsmes ir incidentus teikimas iš šių šaltinių (angl. log source):</p>	<p>Tinklo įrangos (ugniasienių, maršrutizatorių, komutatorių, VPN įrenginių, Load Balancer'ių ir kt.); Tinklo įrangos valdymo sistemų; Tarnybinių stočių su Microsoft ir Linux operacinėmis sistemomis; Virtualizacijos įrangos; AAD domeno kontrolierių; DNS, DHCP; Microsoft 365 Defender; Azure Log Analytics; Web aplikacijų ugniasienės (angl. Web Application Firewall); Duomenų nutekimo prevencijos (angl. Data Leakage Protection) sistemos; Web svetainių, esančių On-Prem ir Debesijos infrastruktūroje; OT saugumo sprendimo (naudojamas TAP tipo įrenginys, duomenų pateikimas)</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Žurnalinių įrašų koreliavimas ir analizė, kuri turi identifikuoti vidines ir išorines grėsmes susijusias su kenkėjiška veikla, technologiniais procesais ir žmogiškosiomis klaidomis:</p>	<p>technologines anomalijas ir saugumo spragas (Technologinės anomalijos ir saugumo spragos yra netinkamos sistemos veiklos ar silpnybės, kurios, analizuojant žurnalinius įrašus, gali atskleisti vidines ir išorines grėsmes susijusias su kenkėjiška veikla, technologiniais procesais ir žmogiškosiomis klaidomis); neteisėtos arba klaidingos autentifikacijos įvykius; nebūdingas naudotojų elgesys ar informacinių išteklių infrastruktūroje; kenkėjišką arba neteisėtai robotizuotą veiklą informacinių išteklių infrastruktūroje (Kenkėjiška arba neteisėtai automatiškai veikianči ir nuolat kartojama veikla informacinių išteklių infrastruktūroje yra nepageidaujamas ar neteisėtas sistemos naudojimas, kurio žurnalinių įrašų koreliavimas ir analizė padeda identifikuoti vidines ir išorines grėsmes, susijusias su šia veikla, technologiniais procesais ir žmogiškosiomis klaidomis); saugumo politikų nusižengimus; atakos susijusios su el. paštu (Atakos susijusios su el. paštu yra kenkėjiški veiksmai el. pašto sistemoje, kurių žurnalinių įrašų koreliavimas ir analizė padeda identifikuoti vidines ir išorines grėsmes, susijusias su šia veikla, technologiniais procesais ir žmogiškosiomis klaidomis); įsibrovimus į vidinį Pirkėjo tinklą; neteisėtą veiklą Pirkėjo tinkle (Neteisėta veikla Pirkėjo tinkle yra nepageidaujamas ar neteisėtas sistemos naudojimas, kuris gali atskleisti vidines ir išorines grėsmes susijusias su kenkėjiška veikla, technologiniais procesais ir žmogiškosiomis klaidomis); kenkėjiško programinio kodo veikimą; DDoS aptikimas; privilegijuotų naudotojų stebėjimas (Privilegijuotų naudotojų stebėjimas yra procesas, kai aukšto lygio prieigos teises turinčių naudotojų veikla yra fiksuojama ir analizuojama siekiant užkirsti kelią saugumo pažeidimams ir kitoms netinkamoms veikloms); aptinkamas nepatvirtintos naudoti programinės įrangos instaliavimas ir jos veikimas; paslaugų (service) rizikos stebėjimas (Paslaugų rizikos stebėjimas yra procesas, kuriame analizuojama ir stebima paslaugų veikla siekiant identifikuoti galimas grėsmes, nesėkmes ar kitus potencialius trūkumus); kompromituoti naudotojai; naudotojo veiksmai su failais (trynimai, kopijavimas daugiau nei > reikšmė derinama atskirai); debesų saugyklos taikomųjų programų kontrolė (Azure - Debesų saugyklos taikomųjų programų kontrolė yra procesas, kuriame stebima ir valdoma, kaip programinė įranga ir duomenys yra naudojami, saugomi ir valdomi debesyje); išpirkos reikalaujančios programinės įranga aktyvumas; duomenų praradimo indikacija; AV stebėjimas (išjungimo įspėjimas);</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		aptinkamas kompiuterinės įrangos komunikavimas / mėginimas komunikuoti su blogos reputacijos išoriniais šaltiniais; atliekami grupinės politikos pakeitimai; galimas šoninis judėjimas; kitus suderintus stebėjimo scenarijus.
	Garantiniai įsipareigojimai	Gamintojo garantuojamas visos programinės įrangos garantinis aptarnavimas nuo Paslaugos (antrojo etapo) priėmimo–perdavimo akto pasirašymo. Nemokamas programinės įrangos palaikymas (klaidų taisymas bei jų ataskaitų gavimas bei naujesnės programinės įrangos versijų diegimas), teisė kreiptis į gamintoją iškilus problemai Sutarties galiojimo laikotarpiu.
	Licencijos galiojimo laikotarpis	Licencija privalo galioti 24 mėnesius, o Licencijos pradeda galioti nuo pirmo etapo diegimo pabaigos
Reikalavimai diegimui ir konfigūravimui		
	Programinės įrangos diegimo ir konfigūravimo darbų (toliau – Diegimo darbai) etapai	Diegimo darbų etapai turi apimti: 1. Pasiruošimas tinklo srauto stebėsenai bei žurnalinių įrašų stebėsenos sprendimo diegimas 2. Likusių žurnalinių įrašų šaltinių integravimas į SIEM funkcionalumą atitinkantį sprendimą
	Pirmas etapas	Per Pasiūlyme Tiekėjo nurodytą terminą, kuris turi būti ne ilgesnis nei 21 darbo diena, po Sutarties įsigaliojimo, pagal Tiekėjo ir Pirkėjo suderintą planą, Tiekėjas sudiegia programinę įrangą, bei suderina žurnalinių įrašų stebėsenos sprendimui (angl. SIEM - Security information and event management) reikalingą konfigūraciją.
	Antras etapas	Ne ilgiau kaip per 2 mėnesius po Sutarties įsigaliojimo, pagal Tiekėjo ir Pirkėjo suderintą planą, Tiekėjas paruošia ją žurnalinių įrašų gavimui iš visų Pirkėjo šaltinių.

II DALIS. PRIEVOLIŲ VYKDYMAS

PRIEVOLIŲ VYKDYMO VIETA(-OS)

Ozo g. 12A-1, 08200 Vilnius

Techninių reikalavimų atitikties lentelė.

Reikalavimai platformos valdymo ir administravimo konsolės funkcionalumui	
Turi būti rolėmis su skirtingomis administravimo teisėmis paremtas administravimas (RBAC)	Privalomas
Turi būti galimybė kurti naudotojus su skirtingo lygio teisėmis	Privalomas

Turi būti galimybė deleguoti teises skirtingiems vartotojams	Privalomas
Turi turėti valdymo sistemos auditavimo funkcionalumą, leidžiantį atsekti koks sistemos vartotojas, kada ir kokius veiksmus atliko	Privalomas
Turi būti galimybė pačiai organizacijai kurti administravimo roles ir neturi būti ribojamas jų skaičius	Privalomas
Valdymo sąsaja turi veikti SSL pagrindu	Privalomas
Turi palaikyti vartotojų autentifikavimą SAML 2.0 SSO (Azure AD)	Privalomas
Turi integruotis su Active Directory ir veiksmai atliekami direktorijoje turi būti sinchronizuojami su platformos centralizuoto valdymo konsole	Privalomas
Valdymo serveriai privalo būti laikomi Europos Sąjungoje ir atitikti BDAR reikalavimus	Privalomas
Turi turėti galimybę iš valdymo konsolės automatiškai sugeneruoti agentų diegimo programinius kodus (ang. scripts) Windows (Powershell) ir Linux platformoms	Privalomas
Įdiegiami agentai turi būti automatiškai susieti su priskirta įrenginiui politika ir įdiegti su visais reikalingais moduliais	Privalomas
Įdiegiami agentai turi palaikyti komandinę eilutę (CLI) administravimo veiksams atlikti	Privalomas
Turi turėti integraciją (ang. native support) su VMware vCenter 6.0 ar aukštesnės versijos	Privalomas
Turi realiu laiku valdymo konsolėje sinchronizuoti pokyčius, atliekamus VMware vCenter platformoje	Privalomas
Turi turėti galimybę kurti įvairias galinių įrenginių grupes pagal individualiai pasirenkamus parametrus	Privalomas
Turi turėti galimybę atlikti automatinės užduotis pagal šiuos parametrus – naujo galinio įrenginio atsiradimas, įrenginio judėjimas, IP adreso pasikeitimas, ar įrenginys yra įjungtas ar išjungtas	Privalomas
Turi palaikyti tiesioginę integraciją su AWS, Azure ir Google debesijos platformomis, bei, gebėti atvaizduoti visus veikiančius ar sustabdytus resursus šiose platformose, nereikalaujant juose įdiegti atskiro agento	Privalomas
Turi turėti galimybę siųsti pranešimus apie incidentus į SIEM sistemas šiais formatais: raw syslog, CEF, LEEF	Privalomas
Turi palaikyti atvirą API integracijoms su kitomis sistemomis	Privalomas
Į darbo vietas ir tarnybines stotis diegiami agentai turi palaikyti šias operacines sistemas: Windows 10, 11 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Ubuntu 16, 18, 20 Debian 7, 8, 9, 10	Privalomas
Reikalavimai baziniam darbo vietų ir tarnybinių stočių antivirusinės apsaugos funkcionalumui, apimančiam visas Pirkėjo darbo vietas ir tarnybines stotis	

Turi turėti apsaugos modulį ir užtikrinti apsaugą nuo virusų, „spyware“, „adware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų	Privalomas
Turi realiu laiku skenuoti Windows bei Linux operacinių sistemų platformose	Privalomas
Turi turėti galimybę veikti „Air Gap“ tinkle (neturint interneto ryšio)	Privalomas
Turi turėti galimybę nuotoliniu būdu inicijuoti portų skenavimą	Privalomas
Turi turėti galimybę nustatyti skenavimo laiką ir dažnumą (Scheduled scan)	Privalomas
Turi turėti galimybę nuotoliniu būdu inicijuoti greitą arba pilną skenavimą nuo virusų ir žalingo kodo	Privalomas
Turi turėti galimybę nustatyti maksimalų procesoriaus apkrovimą rankinio ar reguliaraus pilno skenavimo metu	Privalomas
Turi turėti galimybę skenavimo metu taikyti išimtis atskiriems katalogams ar failams	Privalomas
Turi turėti galimybę skenuoti iterptus objektus Microsoft Office dokumentuose (OLE)	Privalomas
Turi turėti šiuos kenkėjiškos programinės įrangos aptikimo metodus: virusų aprašais pagrįstą (signature based), mašininio mokymosi (ML) ir elgsenos stebėjimo (Behaviour analysis)	Privalomas
Turi atlikti žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo turi būti analizuojamas jos elgesys (Behaviour analysis)	Privalomas
Turi automatiškai skenuoti failus prieš paleidimą naudojant mašininio mokymosi modelius	Privalomas
Turi gebėti dokumentuose atpažinti žinomus pažeidžiamumus pagal CVE	Privalomas
Turi turėti apsaugos nuo išpirkos reikalaujančios žalingos programinės įrangos („Ransomware“) funkcionalumą, veikiančią sistemos procesų stebėjimo principu ir stabdančią šifravimo procesą jam pradėjus veikti. Turi palaikyti atsarginių kopijų darymą dokumentams prieš užšifravimą, bei gebėti atstatyti užšifruotus failus	Privalomas
Turi gebėti skenuoti archyvuotas rinkmenas	Privalomas
Turi turėti integruotą karantino paskyrą	Privalomas
Turi turėti reputacija paremtą lankomų žalingų interneto adresų blokavimą. Turi būti galimybės nustatyti interneto adresų tikrinimo ir blokavimo laipsnį	Privalomas
Turi būti galimybė kurti interneto adresų leidžiamus ir blokuojamus sąrašus (angl. whitelists, blacklists) pagal domenų, URL arba raktažodžius	Privalomas
Turi būti galimybė kontroliuoti naudojamąs aplikacijas Windows ir Linux operacinių sistemų platformose	Privalomas
Turi būti galimybė leisti arba blokuoti individualiai pasirenkamas aplikacijas	Privalomas
Turi būti galimybė užfiksuoti galiniame įrenginyje veikiančių aplikacijų sąrašą ir versijas, leidžiant veikti tik joms ir blokuojant bet kokius bandymus įdiegti naują ar pakeisti esamas aplikacijas (Application lockdown režimas)	Privalomas
Papildomas funkcionalumas, skirtas kritinių tarnybinių stočių apsaugai	
Turi užtikrinti tarnybinių stočių žurnalinių įrašų stebėjimą, ir informavimą apie aptinkamą įtartina ar žalingą operacinės sistemos ar programinės įrangos veikimą:	Neprivalomas

<ul style="list-style-type: none"> • Turi būti stebimi ne mažiau kaip šie žurnalinių įrašų tipai – eventlog, snort, syslog, • Turi palaikyti atviro standarto sintaksę OSSEC, • Turi turėti galimybę kurti aptikimo taisykles pagal įvadą string ar regex formatais 	
<p>Turi užtikrinti nuolatinį įrenginių skenavimą ir automatinę apsaugą nuo pažeidžiamumų („vulnerabilities“) išnaudojimo:</p> <ul style="list-style-type: none"> • Turi būti atliekamas nuolatinis pažeidžiamumų skenavimas (ne rečiau kaip kartą per parą) ir atvaizduojami visi aptikti pažeidžiamumai pagal jų CVE numerius, • Turi būti automatiškai taikomos taisyklės blokuojančios aptiktų pažeidžiamumų (CVE) išnaudojimą. • Turi blokuoti pažeidžiamumų išnaudojimą, naudojantis periodiškai atnaujinamomis „host-based IPS“ taisyklėmis. • Turi būti dinamiškai pakeičiamas naudojamas IPS taisyklės, atnaujinus sistemą ar aplikaciją bei pašalinus pažeidžiamumą. • Turi nereikalauti jokios papildomos programinės įrangos ar agento įdiegimo. • Turi turėti galimybes atpažinti ir blokuoti XSS, SQL injection atakas. 	Neprivalomas
Reikalavimai Office 365 aplinkos (Exchange, One Drive, Sharepoint, Teams) skenavimo ir apsaugos funkcionalumui	
Funkcionalumas turi būti realizuotas API pagrindu, nekeičiant turimų el.pašto sprendimų konfigūracijos, bei MX įrašų	Privalomas
Turi realiu laiku skenuoti Exchange Online platformoje nuo virusų, žalingo kodo ir nepageidautinų laiškų, ir gebėti blokuoti ar karantinuoti pavojingus el.laiškus	Privalomas
Turi gebėti atpažinti ir informuoti arba blokuoti ransomware, phishing atakas, el.pašto kompromitavimo atvejus (ang. Business email compromise)	Privalomas
Turi realiu laiku skenuoti failus OneDrive, Sharepoint, Teams aplinkose, ir gebėti blokuoti ar karantinuoti žalingus failus pagal nustatomas politikas	Privalomas
Turi turėti integruotą smėliadėžę (Sandbox) įtartinų failų patikrinimui bei išsamios ataskaitos apie įtariamą žalingą kodą pateikimui	Privalomas
Turi turėti tiesioginę integraciją su siūloma saugumo operacijų platforma, ir gebėti siųsti el.pašto telemetrijos duomenis į bendrą „duomenų ežerą“ (Datalake) tolimesniam kibernetinių incidentų koreliavimui, atvaizdavimui ir reagavimui	Privalomas
Reikalavimai atakos perimetro valdymo bei organizacijos rizikų vertinimo (ASM) funkcionalumui	
Turi vykdyti organizacijos vidinių ir išorinių resursų stebėseną, atvaizdavimą bei rizikos vertinimą	Privalomas
Turi gebėti aptikti ir atvaizduoti visus žinomus (su įdiegtais agentais) ir nežinomus (be įdiegto agento) resursus tinklo viduje, skenuojant vidinę tinklo komunikaciją ir aptinkant IP adresus	Privalomas
<p>Turi turėti tiesioginę integraciją ir gebėti pasiimti duomenis iš ne mažiau kaip šių šaltinių:</p> <ul style="list-style-type: none"> • Galinių įrenginių (darbo vietų ir tarnybinių stočių), • Microsoft Azure AD ir on-premise AD, • Microsoft Office 365 aplinkos, 	Privalomas

<ul style="list-style-type: none"> • pažeidžiamųjų skenavimo įrankių Qualys, Tenable.io, Nessus Pro 	
<p>Turi turėti galimybes stebėti organizacijos išorinius resursus pagal pateiktus organizacijos išorinius domenus, ir gebėti aptikti bei atvaizduoti:</p> <ul style="list-style-type: none"> • pažeidžiamumus pagal CVE numeraciją, • atvirus prievadus (Ports), • silpnų sertifikatų ir protokolų naudojimą 	Privalomas
<p>Turi būti stebima ir atvaizduojama informacija apie pažeidžiamumus organizacijos vidiniuose įrenginiuose, bei turi būti pateikiamos rekomenduojamos apsaugos taisyklės jų užkardymui</p>	Privalomas
<p>Turi būti pateikiamas ir nuolatos atnaujinami organizacijos, vartotojų, galinių įrenginių, debesijos aplikacijų rizikos laipsniai, turi būti vertinami ne mažiau kaip šie parametrai:</p> <ul style="list-style-type: none"> • pažeidžiamųjų aptikimas, • galimą vartotojų paskyrų kompromitavimas, turi gebėti aptikti vartotojų paskyrų duomenų nutekėjimą tamsiajame internete (Darkweb). • anomalijų aptikimas, pagal neįprastą vartotojų elgseną, • incidentų aptikimas galiniuose įrenginiuose, • netinkamos saugumo konfigūracijos atvejai - dviejų faktorių autentifikacijos (MFA) nebuvimas, silpni slaptažodžiai ar silpna slaptažodžių politika. 	Privalomas
<p>Turi būti prioritetizuojami ir atvaizduojami rizikingiausių įrenginių bei aplikacijų sąrašai</p>	Privalomas
<p>Turi būti galimybė kurti automatizuotas politikas (Playbooks) rizikos laipsniui mažinti be administratoriaus įsikišimo</p>	Privalomas