OIXIO Cyber

Detalizacija	Auditas			Paslaugos				
	Kibernetinio saugumo brandos įvertinimas	IT Rizikų vertinimas	IT auditas	Soc Inžinerija	vCISO	Pažeidžiamumų šalinimas	SOC	Nuolatinė organizacijos išorės stebėsena ir pažeidžiamumų valdymas
Pateikiamas paprastas klausimynas, susijęs su IT valdymu, gerosiomis praktikomis ir kt., padedantis Jums įsivertinti savo kibernetinio saugumo brandą.	✓							
Pateikiamas klausimynas parengtas pagal CIS. Į klausimus atsakoma kartu susitikimo su klientu metu. Tai pradinis vertinimas (angl. *assessment*).		✓	✓					
Skaitmeninis pėdsakas – tai visa informacija, kurią asmuo ar organizacija palieka internete ir kuri gali būti panaudota identifikuojant, analizuojant ar net išnaudojant saugumo spragas. Tikriname ir „dark web“.		✓	✓					
Išorinis pažeidžiamumų skenavimas – tai kibernetinio saugumo procesas, kurio metu tikrinama, ar organizacijos viešai prieinamos IT sistemos, tokios kaip interneto svetainės, serveriai ar tinklo įrenginiai, neturi saugumo spragų. Tai atliekama išorinėje organizacijos tinklo aplinkoje – t. y. taip, kaip tai darytų potencialus įsilaužėlis. Skenavimas padeda identifikuoti atvirus portus, nesaugias konfigūracijas, pasenusią programinę įrangą ir kitus pažeidžiamumus, kurie galėtų būti išnaudoti kenkėjiškai veiklai. Reguliariai atliekant tokį skenavimą, galima sumažinti organizacijos riziką patirti kibernetinius išpuolius ir sustiprinti sistemų saugumą.		✓	✓					✓
Vidinis pažeidžiamumų skenavimas – tai kibernetinio saugumo procesas, kurio metu tikrinamos organizacijos vidinės IT sistemos: darbuotojų kompiuteriai, vidiniai serveriai, duomenų bazės ir tinklo infrastruktūra. Skirtingai nei išorinis skenavimas, kuris analizuoja viešai prieinamus resursus, vidinis skenavimas atliekamas organizacijos viduje. Jis padeda identifikuoti pažeidžiamumus, kylančius dėl netinkamų konfigūracijų, pasenusios programinės įrangos ar net darbuotojų klaidų. Tai svarbus procesas, padedantis užkirsti kelią vidinėms grėsmėms ir užtikrinti aukštą organizacijos kibernetinio saugumo lygį.		✓	✓					✓

OIXIO Cyber

Entra ID/AD auditas – tai organizacijos „Microsoft Entra ID“ (anksčiau žinomo kaip „Azure Active Directory“) ar „Active Directory“ (AD) saugumo ir efektyvumo vertinimas. Audito metu analizuojamos autentifikacijos, prieigos valdymo ir identitetų apsaugos praktikos, siekiant užtikrinti tinkamą infrastruktūros veikimą ir sumažinti kibernetines grėsmes. **Pagrindiniai audito aspektai:** *Prieigos kontrolė* – tikrinama, ar vartotojų teisės ir leidimai yra tinkamai sukonfigūruoti, ar nėra per didelių privilegijų. *Autentifikacijos mechanizmai* – įvertinama, ar naudojamas daugiafaktorinis autentifikavimas (MFA), ar slaptažodžių politika yra saugi. *Grėsmių aptikimas ir reagavimas* – peržiūrimi žurnalo įrašai (audit logs), ieškoma neįprastų prisijungimų ar įtartinos veiklos. *Identitetų valdymas* – tikrinama, ar neaktyvios paskyros yra pašalintos, ar vartotojai turi prieigą tik pagal „mažiausių privilegijų“ principą. *Saugumo politikos ir atitiktis* – vertinama, ar grupių ir politikų valdymas atitinka gerąsias praktikas ir reglamentus (pvz., ISO 27001, NIST). *Tiekėjų ir trečiųjų šalių prieiga* – analizuojama, ar išoriniai vartotojai ir tiekėjai turi saugiai ribotą prieigą. *Avarinis atkūrimas ir atsarginės kopijos* – peržiūrima, ar yra planai ir priemonės AD duomenų atkūrimui pažeidimo atveju. Šis auditas padeda nustatyti silpnąsias vietas, optimizuoti autentifikacijos procesus ir sustiprinti organizacijos tapatybės valdymo saugumą.		✓	✓					✓
IT Fizinio saugumo vertinimas – tai organizacijos IT infrastruktūros fizinės apsaugos priemonių analizė, siekiant užtikrinti saugų IT sistemų, duomenų centrų ir įrenginių veikimą. Tikslas – įvertinti, ar infrastruktūra tinkamai apsaugota nuo fizinių grėsmių, kylančių dėl vagysčių, vandalizmo, gamtinių nelaimių ar neautorizuotos prieigos. **Pagrindiniai IT fizinio saugumo vertinimo elementai:** *Įrenginių saugumas* – tikrinama, ar serveriai, maršrutizatoriai ir kiti įrenginiai yra fiziškai apsaugoti (pvz., spintos su užraktais). *Avarinių situacijų valdymas* – įvertinami evakuacijos planai, atsarginiai elektros šaltiniai (UPS) ir įrangos perkėlimo galimybės ekstremaliomis situacijomis. *Prieigos kontrolė* – tikrinama, kas turi fizinę prieigą prie IT įrangos ir ar tai tinkamai ribojama. Toks vertinimas padeda užtikrinti patikimą infrastruktūros veikimą net ir iškilus fizinėms grėsmėms. Reguliarus vertinimas padeda išvengti pavojų ir kurti saugią darbo aplinką.			✓					

OIXIO Cyber

Politikų ir procedūrų peržiūra			✔		✔			
Duomenų atsarginių kopijų politikos vertinimas – peržiūrint Jūsų atsarginių kopijų politiką ir procedūras, užtikrinamas verslo tęstinumas ir greitas duomenų atkūrimas.			✔		✔			
Veiklos tęstinumo dokumentacijos vertinimas (angl. *disaster recovery*)			✔		✔			
Trečiųjų šalių saugumo vertinimas – tai procesas, kurio metu organizacija analizuoja partnerių, tiekėjų ar paslaugų teikėjų taikomas kibernetinio saugumo priemones. Kadangi daugelis organizacijų priklauso nuo išorinių paslaugų, svarbu įsitikinti, kad šios šalys nekelia papildomos saugumo rizikos. **Pagrindiniai vertinimo aspektai:** *Prieigos kontrolė* – ar tiekėjai turi tinkamai ribotą prieigą prie organizacijos sistemų? *Duomenų apsauga* – ar naudojami šifravimo ir duomenų privatumo užtikrinimo mechanizmai? *Pažeidžiamumų valdymas* – ar tiekėjai reguliariai tikrina savo IT infrastruktūrą? *Incidentų valdymas* – kaip tiekėjai reaguoja į kibernetinius incidentus? *Atitiktis standartams* – ar laikomasi tokių reglamentų kaip GDPR, ISO 27001 ar NIS2? Reguliarus trečiųjų šalių saugumo vertinimas padeda sumažinti rizikas ir užtikrinti verslo tęstinumą.			✔		✔			
Incidentų reagavimo planų vertinimas – padėsime įvertinti turimus planus: ar jie atitinka realybę ir Jūsų organizacijos RTO/RPO reikalavimus.			✔					
Vidutinis valandų skaičius, reikalingas paslaugai suteikti		**X val. – priklausomai nuo infrastruktūros elementų apimties (nuo–iki).**						