

Paslaugų kokybės susitarimas (toliau – Susitarimas)

Saugumo operacijų centro (SOC) paslaugą BITĖ teikia pasitelkdama partnerį Mediafon Technology, UAB. Technologies

SĄVOKOS

1. Paslaugos pasiekiamumas – laikotarpis per mėnesį, kuomet užtikrinamas SOC įrankio veikimas. Techninės profilaktikos laikas neįskaičiuojamas. Skaičiuojama formule: $(A - B) / A \times 100\%$, kur A – mėnesio valandos, B – paslaugos neveikimo valandos.
2. Techninė profilaktika – iš anksto suplanuoti darbai, apie kuriuos Jūsų įmonė informuojama prieš 48 val., nurodant trukmę. Maksimali trukmė – 2 val. per mėnesį
3. Incidentas – įvykęs sutrikimas ar pažeidimas, keliantis arba galintis sukelti padarinius Jūsų įmonės IT infrastruktūrai ar saugumui.
4. Įspėjimas – SOC įrankių sugeneruotas įspėjimas apie įtartiną veiklą ir/ar veiklą neatitinkančią pritaikytų saugumo kriterijų (angl. alert).

1. PASLAUGŲ KOKYBĖ IR PASLAUGOS APIMTIS

1. Paslaugos tiekėjas užtikrina, kad Paslauga Klientams veiktų 24 valandas per parą 7 dienas per savaitę.
2. Sutrikimo metu, sutrikus Paslaugai ar atskiram jos moduliui, laikoma, kad įvyko vienas sutrikimas, nepriklausomai nuo to, kiek galutinių naudotojų ar operacijų jis įtakojo, o sutrikimo laikas pradedamas skaičiuoti nuo pirmo registruoto sutrikimo ir skaičiuojamas iki pilno sutrikimo pašalinimo.

2. PASLAUGŲ TEIKIMO LYGIS

Automatinių Įspėjimų siuntimas	24/7 - Visą parą, ne vėliau nei per 30 min. nuo įvykio.
Reagavimas į automatinį Įspėjimą ir pirminė analizė	Darbo dienomis nuo 08:00 iki 18:00: Įspėjimo analizė ir atitinkamo Incidento lygio nustatymas ne vėliau nei per 30 min nuo automatinio Įspėjimo.
Reagavimo laikas į Incidentus pagal nustatytą lygį	Darbo dienomis nuo 08:00 iki 18:00: Aukščiausias lygis (Kritinis): Reaguojama į kritinius Incidentus per 15 minučių nuo pirminės analizės ir lygio nustatymo. Aukštas lygis (Aukštas): Reaguojama į aukšto prioriteto Incidentus per 1 valandą. Vidutinis lygis (Vidutinis): Reaguojama į vidutinio prioriteto Incidentus per 4 valandas. Žemas lygis (Žemas): Reaguojama į žemo prioriteto Incidentus per 24 valandas. Incidentų kritiškumo lygis nustatomas pagal poveikį Jūsų įmonės informacinėms sistemoms, duomenims, paslaugoms ir veiklos tęstinumui, taip pat pagal su Jūsų įmone normalizacijos etape suderintą incidentų klasifikavimo scenarijų. Incidentų lygiai yra derinami individualiai ir priklauso nuo su Jūsų įmone suderintų incidentų prioritetų. Incidentai skirstomi į šiuos lygius: Kritinis – incidentas, dėl kurio atsiranda visiškas paslaugų sustabdymas, duomenų praradimas ar nutekėjimas, arba kyla tiesioginė grėsmė informacijos konfidencialumui, vientisumui ar prieinamumui; Aukštas – incidentas, kuris gali sukelti reikšmingą paslaugų trikdymą ar duomenų pažeidimą, tačiau nėra visiško veiklos sustabdymo; Vidutinis – incidentas, sukeltiantis ribotą poveikį, kurio pasekmės gali būti suvaldytos taikant įprastas priemones; Žemas – incidentas, turintis minimalų poveikį, nesukeliantis tiesioginės grėsmės. Pažeidžiamumų valdymas: Pažeidžiamumai vertinami remiantis CVSS (Common Vulnerability Scoring System) metodika. Incidentų ir pažeidžiamumų registravimas Incidentai ir nustatyti pažeidžiamumai registruojami SOC Portalo savitarnos sistemoje, nurodant jų aptikimo laiką, kritiškumo lygį, atliktus veiksmus ir sprendimo būseną.
Paslaugų pasiekiamumas	99%
Kliento užklauso sprendžiamos:	Darbo dienomis nuo 08:00 iki 18:00, reakcijos laikas iki 2 val.

Standartinis ataskaitų teikimo laikotarpis	Kas mėnesį
Įvykių saugojimo laikotarpis:	90 dienų.
Įvykių saugojimo laikotarpis > 90 dienų	Pagal atskirą susitarimą bei norimą saugoti laikotarpį, bet ne daugiau nei 12 mėnesių.

3. PASLAUGŲ KOKYBĖ IR PASLAUGOS APIMTIS

Incidentų prioritetai nustatomi individualiai kiekvienam klientui, atsižvelgiant į jų IT infrastruktūros specifiką ir suderintus kriterijus.

4. ESKALAVIMO PROCEDŪRA

Jei per 2 val. nuo užklauso Jūsų įmonė negauna atsakymo, jūs turite teisę inicijuoti eskalaciją el. paštu ar telefonu, nurodytu sutartyje.

5. DARBO LAIKAS IR PASLAUGŲ PASIEKIAMUMAS

1. Klientas apie SOC paslaugos sutrikimus turi pranešti atsakingiems asmenims nuordytai kontaktais sutartyje.
2. Klientas apie sutrikimus taip pat gali pranešti BITĖS išsiaištinę parą dirbančiam Bitės Techninio aptarnavimo telefonu Nr.: +370 685 80000, techaptarnavimas@bite.lt arba užregistruodami gedimą <https://ict.bite.lt>
3. Pranešime Klientas privalo nurodyti: sutrikimo aprašymą, kontaktinį asmenį, sutrikimo lygį, veiksmus, atliktus iki sutrikimo, sutrikimo metu gautus rezultatus ir reikalaujamus rezultatus, kitą Kliento vertinimu svarbią informaciją.
4. BITĖ, gavusi pranešimą apie sutrikimą, nedelsiant patvirtina Klientui apie pranešimo gavimą. Po to, BITĖ išsamiai vertina situaciją ir konsultuodamasi su Klientu, nustato galutinį sutrikimo lygį. Sutarus galutinį sutrikimo lygį, BITĖ pradeda sutrikimo šalinimo veiksmus.
5. Šalys susitaria, kad asmuo, pateikęs pranešimą apie sutrikimą bus laikomas atsakingas už tinkamą bendradarbiavimą su BITE šalinant sutrikimą, už visos reikalingos informacijos apie sutrikimą teikimą BITEI. Klientas gali nurodyti ir kitą asmenį, kuris bus atsakingas už tinkamą bendradarbiavimą su BITE šalinant sutrikimą bei visos reikalingos informacijos apie sutrikimą teikimą BITEI.

6. PRIEŽIŪRA IR PLANINIAI DARBAI

1. **Planinė priežiūra:** informuojama ne vėliau kaip prieš 48 valandas
2. **Profilaktikos langas:** savaitgaliais arba po 22:00 val.
3. **Skubi priežiūra:** klientas informuojamas kuo greičiau
4. **Profilaktikos laikas:** negali būti didesnis nei 4val. per mėnesį

7. PASLAUGŲ KOKYBĖS NESILAIKYMAS

Nesilaikant terminų, nustatytų šio Susitarimo 2 punkte „Paslaugų teikimo lygis (SLA)“, Jūsų įmonė turi teisę reikalauti gauti baudą. Taikoma bauda – 25,00 (dvidešimt penkių) Eur už kiekvieną pradelstą valandą pagal nustatytą SLA (valanda laikoma pradelsta pilna valanda darbo dienomis nuo 08:00 iki 18:00).

Pavyzdžiai:

Jei vėluojama sureaguoti 15, 30 arba 45 minutes – 25,00 (dvidešimt penkių) Eur bauda už šį laiką taikoma nebus;

Jei vėluojama sureaguoti 2 valandas 15 minučių – bus taikoma 50,00 (penkiasdešimt) Eur bauda už pavėluotas 2 valandas;

Jei incidentas įvyko ne darbo valandomis numatytais šiame susitarime, reagavimo laikas pradedamas skaičiuoti nuo sekančios darbo dienos bei numatytų darbo valandų 8:00-18:00.

Kadangi BITĖS teikiamos paslaugos neapima techninių priemonių ar mechanizmų, tiesiogiai įgalinančių kibernetinių atakų ar incidentų automatinį užkardymą (pvz., M365 paskyrų, serverių, VM, ugniasienių ar XDR/EDR sistemų valdymo), BITĖ įsipareigoja nedelsdama informuoti Jūsų įmonę apie visus nustatytus ir potencialius saugumo incidentus ir deda maksimalias pastangas komunikacijai, teikia rekomendacijas pateikimui ir koordinavimui, siekiant kuo greičiau sustabdyti arba suvaldyti incidentą.

Tačiau BITĖ neprisiima tiesioginės atsakomybės už incidentų padarytą žalą, jei incidentas įvyko arba tęsėsi dėl to, kad Jūsų įmonė laiku neįgyvendino rekomenduojamų veiksmų, neturėjo atitinkamų techninių priemonių, ar jei SOC paslaugos pobūdis objektyviai neleido užkardyti incidento tiesiogiai.