CYBER SECURITY CONFERENCE

SECUR!TY DAY '25

Security for AI for Security

Behind the Data Breach: Leadership, Tech and Legal in Action

DOVILĖ KĖRIENĖ
SOC Manager
Santa Monica Networks

MIGLĖ PETKEVIČIENĖ
Partner
Sorainen

MANTAS DUBAUSKAS
Director
Repoint PR

JUSTAS GUDAVIČIUS
Managing Director
twoday Lithuania

Questions:

Dovilė Kėrienė

SOC Manager, Santa Monica Networks

Mantas Dubauskas

Director, Repoint PR

Justas Gudavičius

Managing Director, twoday Lithuania

Miglė Petkevičienė

Partner, Sorainen

Dovilė Kėrienė

SOC Manager, Santa Monica Networks

Mantas Dubauskas

Director, Repoint PR

Justas Gudavičius

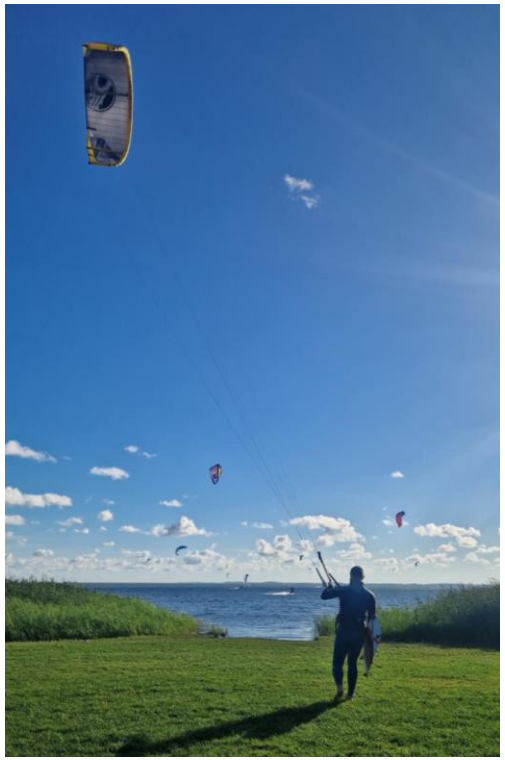
Managing Director, twoday Lithuania

Miglė Petkevičienė

Partner, Sorainen

Dovilė Kėrienė

SOC Manager, Santa Monica Networks



Mantas Dubauskas

Director, Repoint PR

Justas Gudavičius

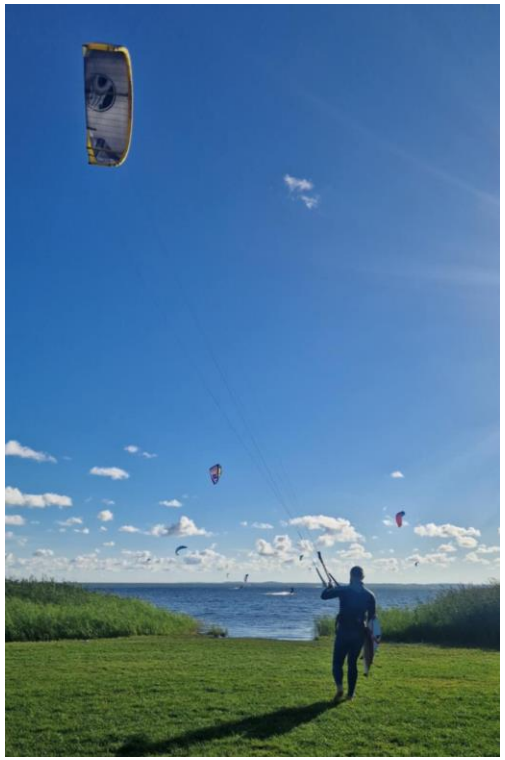
Managing Director, twoday Lithuania

Miglė Petkevičienė

Partner, Sorainen

Dovilė Kėrienė

SOC Manager, Santa Monica Networks



Mantas Dubauskas

Director, Repoint PR

Justas Gudavičius

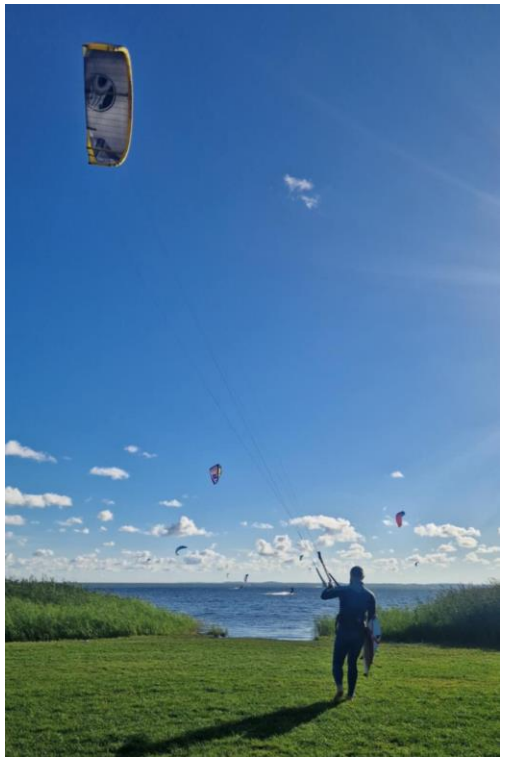
Managing Director, twoday Lithuania

Miglė Petkevičienė

Partner, Sorainen

Dovilė Kėrienė

SOC Manager, Santa Monica Networks



Mantas Dubauskas

Director, Repoint PR

Justas Gudavičius

Managing Director, twoday Lithuania

Miglė Petkevičienė

Partner, Sorainen

CYBER SECURITY CONFERENCE

SECUR!TY DAY '25

Security for AI for Security

Behind the Data Breach: Leadership, Tech and Legal in Action

DOVILĖ KĖRIENĖ
SOC Manager
Santa Monica Networks

MIGLĖ PETKEVIČIENĖ
Partner
Sorainen

MANTAS DUBAUSKAS
Director
Repoint PR

JUSTAS GUDAVIČIUS
Managing Director
twoday Lithuania

Questions:

Prieš pažeidimą

Ramybė prieš audrą

SORAINEN

Incidento metu

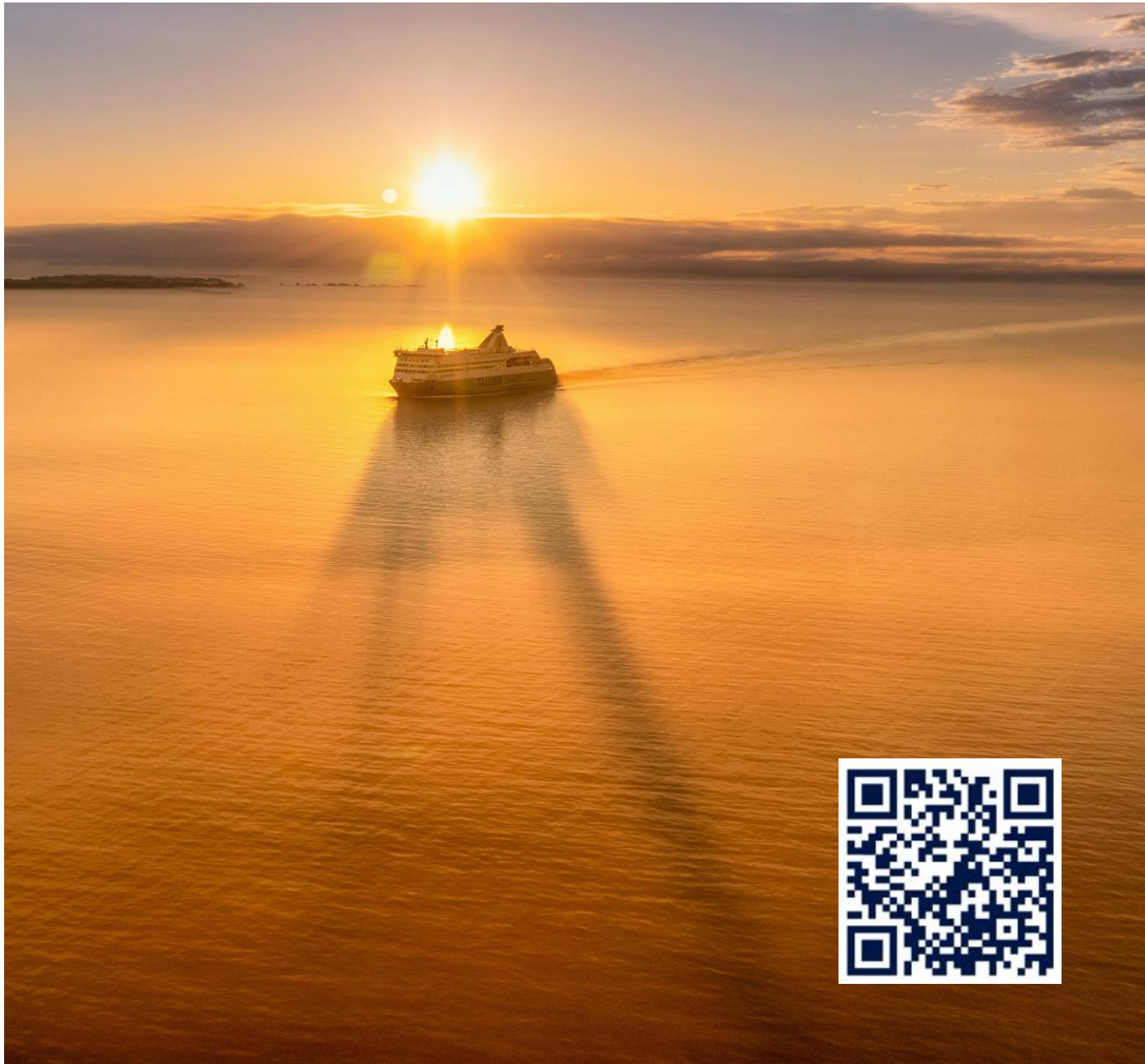
Kai viskas griūva

SORAINEN

Po pažeidimo

Nuo krizės prie kultūros

SORAINEN



KLAUSIMAI, KURIUOS KIEKVIENAS CISO TURĖTŲ UŽDUOTI SAVO ORGANIZACIJOJE

Prieš pažeidimą

Vadovybei:
- Ar kibernetinis saugumas yra įtrauktas į mūsų strateginius verslo tikslus, ar tai tik techninis aspektas?
- Kaip nustatome priimtiną rizikos lygį ir kiek esame pasirengę investuoti į prevenciją?
- Ar valdyba gauna reguliarias ataskaitas apie kibernetinio saugumo rizikas ir incidentų pasirengimo būklę?
- Ar yra aiškiai apibrėžtos atsakomybės grandinės, kas priima sprendimus kilus incidentui?
- Ar turime suderintą kibernetinio saugumo, IT, teisės ir komunikacijos veiksmų planą?

Teisės skyriui:
- Ar mūsų privatumo politika, duomenų tvarkymo ir atsakomybės sutartys atitinka BDAR, NIS2, DORA ir kitus reikalavimus?
- Ar turime atnaujintas sutartis su duomenų tvarkytojais ir tiekėjais dėl incidentų valdymo?
- Ar yra aiškūs vidaus procesai, kaip ir kada pranešti priežiūros institucijoms ar klientams?
- Ar mūsų incidentų reagavimo planas teisiškai suderintas su verslo tęstinumo planais?
- Kaip tvarkome įrodymų saugojimą ir vidinį tyrimą, kad vėliau galėtume juos panaudoti teisiniame kontekste?

Komunikacijos skyriui:
- Ar turime parengtus iš anksto suderintus krizių komunikacijos scenarijus (vidiniai ir išoriniai)?
- Kas krizės metu tvirtina pranešimus viešai – komunikacija, teisininkai, ar vadovybė?
- Ar yra parengti skirtingi komunikacijos kanalai – klientams, partneriams, žiniasklaidai, darbuotojams?
- Ar turime apmokytą atstovą spaudai ir aiškiai nustatytą toną tokio tipo pranešimams?
- Kaip treniruojame vadovus ir komunikacijos komandą kalbėti apie saugumo temas nepažeidžiant konfidencialumo?

Savo (IT/saugumo) komandai:
- Ar esame atlikę praktines pratybas (table-top ar simuliacijas) pagal realų pažeidimo scenarijų?
- Ar turime 24/7 reagavimo pajėgumą ir aiškią eskalacijos grandinę?
- Kaip stebime tiekėjų saugumą ir jų prieigą prie mūsų sistemų?
- Ar turime patikimą atsarginių kopijų politiką, testuojamą realiomis sąlygomis?
- Ar įvertinome, kaip dirbtinis intelektas gali padėti grėsmių aptikimui arba pats tapti nauja rizikos sritimi?

SORAINEN

KLAUSIMAI, KURIUOS KIEKVIENAS CISO TURĖTŲ UŽDUOTI SAVO ORGANIZACIJOJE

Incidento metu

Vadovybei:
- Kokią informaciją vadovybė turi gauti per pirmąsias valandas po pažeidimo?
- Kas priima sprendimą dėl sistemos atjungimo ar veiklos sustabdymo?
- Ar vadovybė pasirengusi komunikuoti krizei realiu laiku – tiek viduje, tiek išorėje?
- Ar turime aiškų procesą, kaip suderinti verslo tęstinumą su saugumo veiksmų prioritetais?
- Kaip užtikriname, kad sprendimai priimami remiantis faktais, o ne panika?

Teisės skyriui:
- Kada ir kam privalome pranešti apie incidentą pagal galiojančius teisės aktus?
- Kaip fiksuojame incidento eigą, kad vėliau galėtume pagrįsti savo veiksmus priežiūros institucijoms?
- Ar turime iš anksto suderintą veiksmų planą su išoriniais teisininkais ar konsultantais?
- Kaip valdome konfidencialią informaciją, kad neprarastume teisinės gynybos privilegijos?
- Ar turime pasirengę šablonus pranešimams institucijoms ir klientams?

Komunikacijos skyriui:
- Kaip užtikrinti, kad pirmieji vieši pranešimai būtų tikslūs, bet nekenktų tyrimui?
- Kaip išlaikyti komunikacijos nuoseklumą tarp vadovybės, IT ir teisės?
- Kaip reaguoti į klaidingą informaciją ar gandus socialiniuose tinkluose?
- Ar komunikacijos komanda turi aiškią patvirtinimo grandinę, prieš paskelbdama informaciją?
- Kaip komunikuoti viduje, kad darbuotojai patys netaptų nevalingais informacijos šaltiniais?

Savo (IT/saugumo) komandai:
- Ar aiškiai nustatyti techniniai prioritetai: sustabdyti ataką, apsaugoti duomenis, išsaugoti įrodymus?
- Kaip koordinuojamės su teisininkais ir komunikacija dėl informacijos, kurią galima viešinti?
- Kaip įsitikinti, kad reagavimo veiksmai nesukels papildomos žalos ar sistemų praradimo?
- Ar įtraukiame trečiųjų šalių ekspertus (forensinius tyrėjus, kibernetinius partnerius)?
- Ar mūsų DI įrankiai realiai padeda priimti sprendimus, ar kelia papildomų klaidingų signalų?

SORAINEN

KLAUSIMAI, KURIUOS KIEKVIENAS CISO TURĖTŲ UŽDUOTI SAVO ORGANIZACIJOJE

Po pažeidimo

Vadovybei:
- Kaip informuojame klientus, partnerius ir investuotojus po incidento?
- Ar įvykis tapo pamoka ir paskata keisti organizacijos kultūrą bei saugumo politiką?
- Kaip vertiname, ar priimti sprendimai incidento metu buvo veiksmingi?
- Ar skiriame biudžetą tolesniam brandos augimui ir sisteminiams pokyčiams?
- Kaip integruojame patirtį į rizikos valdymo strategiją?

Teisės skyriui:
- Ar buvo užbaigtos visos privalomos ataskaitos institucijoms ir klientams?
- Kaip tvarkome įrodymus, jei laukia teisiniai procesai ar derybos dėl kompensacijų?
- Ar atlikome visų sutarčių, politikų ir procedūrų peržiūrą po incidento?
- Kaip įvertiname, ar teisinės rizikos valdymo sistema buvo pakankamai stipri?
- Ar reikia papildomų mokymų teisiniam personalui dėl naujų technologijų ir DI naudojimo?

Komunikacijos skyriui:
- Kaip palaikyti pasitikėjimą ir parodyti skaidrumą po krizės?
- Ar komunikacijos strategija buvo veiksminga ir ką reikia keisti ateityje?
- Kaip stebime ilgalaikį reputacijos atsigavimą?
- Ar komunikacijos komanda turi įrankius analizuoti visuomenės reakcijas po krizės?
- Kaip DI įrankiai gali padėti suprasti, ar visuomenė vėl pasitiki mūsų organizacija?

Savo (IT/saugumo) komandai:
- Ar atlikome išsamų techninį post-incident analizės (post-mortem) procesą?
- Ar atnaujinome sistemų architektūrą ir prieigos politiką pagal gautas pamokas?
- Kaip įvertinome DI vaidmenį: ar jis padėjo, ar sukėlė klaidų?
- Ar komanda gavo aiškią grįžtamojo ryšio sesiją ir mokymosi planą?
- Ką darysime kitaip kitą kartą, kad toks incidentas nepasikartotų?

SORAINEN

CYBER SECURITY CONFERENCE

SECUR!TY DAY '25

Security for AI for Security

Behind the Data Breach: Leadership, Tech and Legal in Action

DOVILĖ KĖRIENĖ
SOC Manager
Santa Monica Networks

MIGLĖ PETKEVIČIENĖ
Partner
Sorainen

MANTAS DUBAUSKAS
Director
Repoint PR

JUSTAS GUDAVIČIUS
Managing Director
twoday Lithuania

Questions:

Apibendrinimas
Namų darbai
Klausimai

Ačiū!

SORAINEN