Kyberturvallisuus yrityksen liiketoiminnan turvana

Veli-Matti Järveläinen
Senior Advisor , Atea Finland Oy

Veli-Matti Järveläinen

Atea Finland Oy

Senior Advisor

IT-maailman moniottelija, joka viihtyy parhaiten siellä, missä liiketoiminta ja teknologia kohtaavat.

Pidän siitä, että monimutkaisista kokonaisuuksista saadaan selkeitä ja ymmärrettäviä – eli mieluiten toimin ”tulkkina” eri maailmojen välillä.

Osaamisalueet:

- Kyberturva ja hallintamallit (riskienhallinta, ISACA CRISC, ISO 27001, IEC 62443, Zero Trust)
- Kokonaisarkkitehtuuri ja palvelunhallinta (TOGAF, ITILv4, PRINCE2 Agile)
- Ketterät toimintamallit, (DevOps, Scrum, SRE)
- IT/OT Verkko- ja pilviteknologiat (Cisco, Arista, ST 2110, AES67, PTP)

veli-matti.jarvelainen@atea.fi
linkedin.com/in/vmjarvelainen

Agenda

Miksi ?

1. Kyberturvallisuus tänä päivänä
2. Mitä tapahtuu, jos tätä ei hoideta?

Miten ?

3. Kyberturvallisuus käytännössä
4. Riskienhallinta yrityksessä
5. Mistä aloittaa?

5. Tyypilliset virheet
6. Yhteenveto & keskustelu

ATEA

Kyberturvallisuus tänä päivänä

Nykytila • Tärkeimmät uhat • Kyberturva liiketoimintaympäristönä

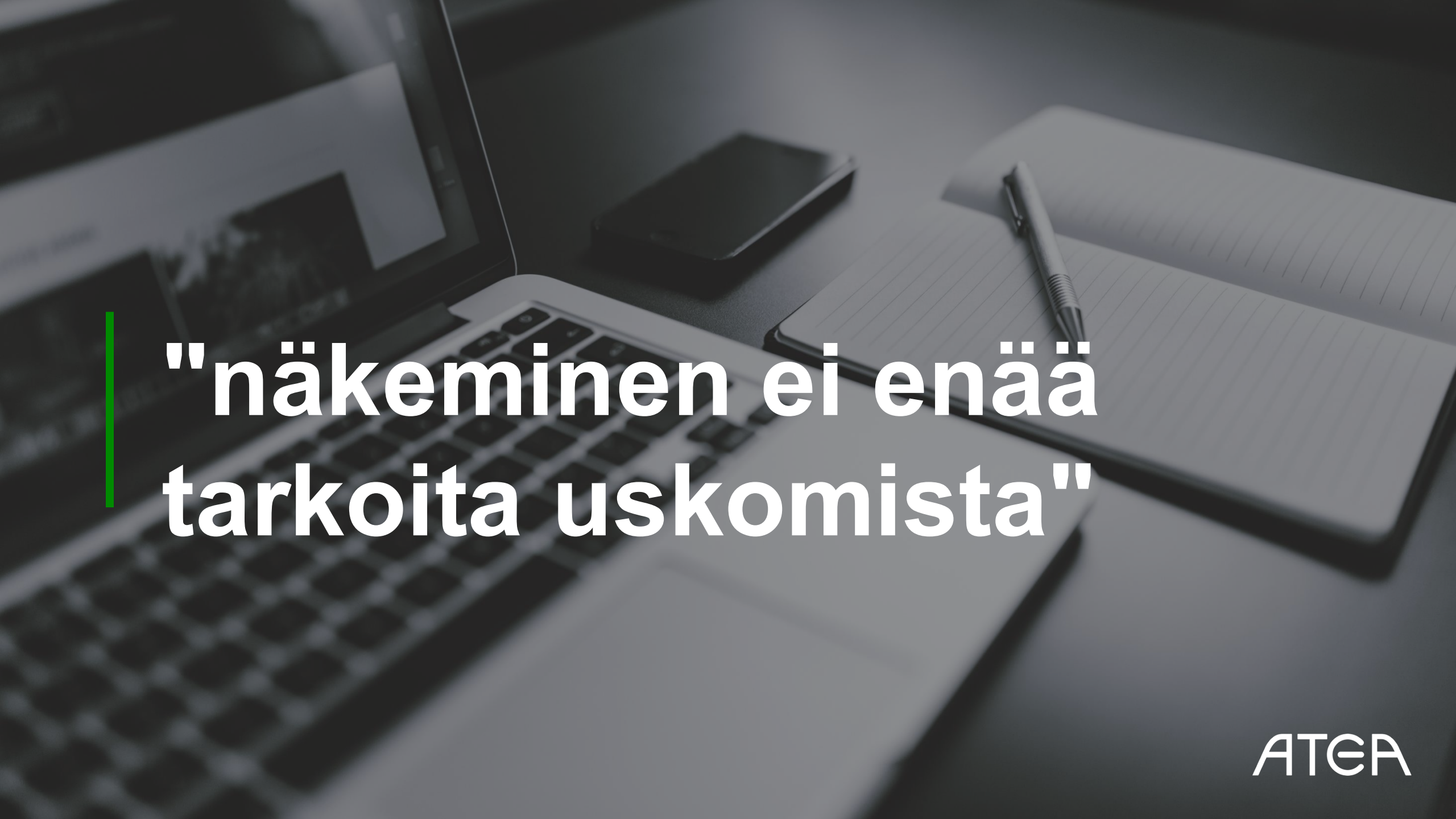
Uhkamaisema 2024 - 2025

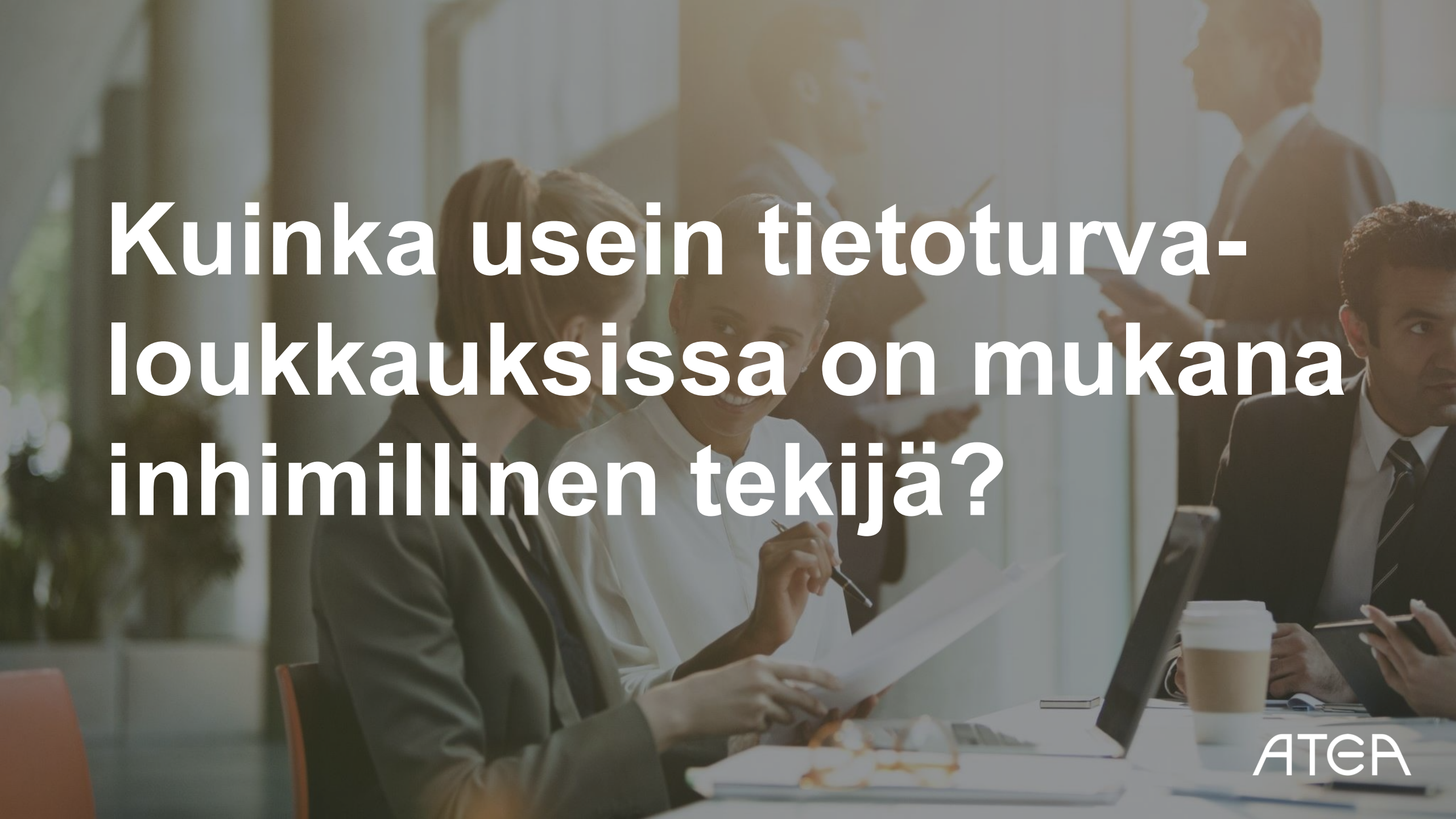
- → Ransomware & kiristyshaittaohjelmat
- ↗ Toimitusketjuhyökkäykset
- ↗ Tekoälyllä tehostettu tietojenkalastelu
- ↗ OT/ICS -ympäristöt kasvavassa riskissä
- → Sisäiset uhat ja inhimilliset virheet
- ↗ Geopoliittinen kybervaikuttaminen

ATEA

Esimerkki Deepfake

- Deepfake, Morgan Freeman, https://www.youtube.com/watch?v=F4G6GNFz0O8
- Real Fake News, https://youtu.be/Qn4SP5Z2wOY
- Show this to Uncle Fred before he shares another fake video, https://www.instagram.com/reel/DKW27I7I7RJ/?hl=en


"näkeminen ei enää
tarkoita uskomista"


Kuinka usein tietoturva-
loukkauksissa on mukana
inhimillinen tekijä?

OT / ICS

Russian Hackers Linked to 'Largest Ever Cyber Attack' on Danish Critical Infrastructure

Ravie Lakshmanan Nov 16, 2023

Russian threat actors have been possibly linked to what's been described as the "largest cyber attack against Danish critical infrastructure," in which 22 companies associated with the operation of the country's energy sector were targeted in May 2023.

"22 simultaneous, successful cyberattacks against Danish critical infrastructure are not commonplace," Denmark's SektorCERT said [PDF]. "The attackers knew in advance who they were going to target and got it right every time. Not once did a shot miss the target."

https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

Miksi toimitusketju on houkutteleva kohde?

- Pääsy valmiiksi luotettuun asemaan
- Vähemmän valvontaa kuin omassa ympäristössä
- Usein epäselvät vastuut ja rajapinnat
- Sama toimittaja → useita asiakkaita yhdellä iskulla

Kuka valvoo ja kuinka toimitusketjuja voisi valvoa?

Toimitusketjut

What is the Xz Utils Backdoor and what threat does it pose?

A week ago, on March 29th, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned that two versions of xz Utils, were found to have been compromised. The xz Utils code had been tampered with to include a malicious "backdoor" that would ultimately give attackers the same level of control over affected systems as authorized administrators. Xz Libs is a set of open source libraries widely-used as dependencies for Unix operating systems, including Linux—the operating system supporting most of the world's server infrastructure.

On the same day of the CISA warning, open source software provider Red Hat sent out an urgent security alert advising users that two of their Linux ecosystem products were affected by the xz Utils malware. *"Immediately stop using Fedora 40 or Fedora Rawhide until you can downgrade your xz version,"* the alert noted.

"The best executed supply chain attack we've seen… a nightmare scenario: malicious, competent, authorized upstream in a widely used library."

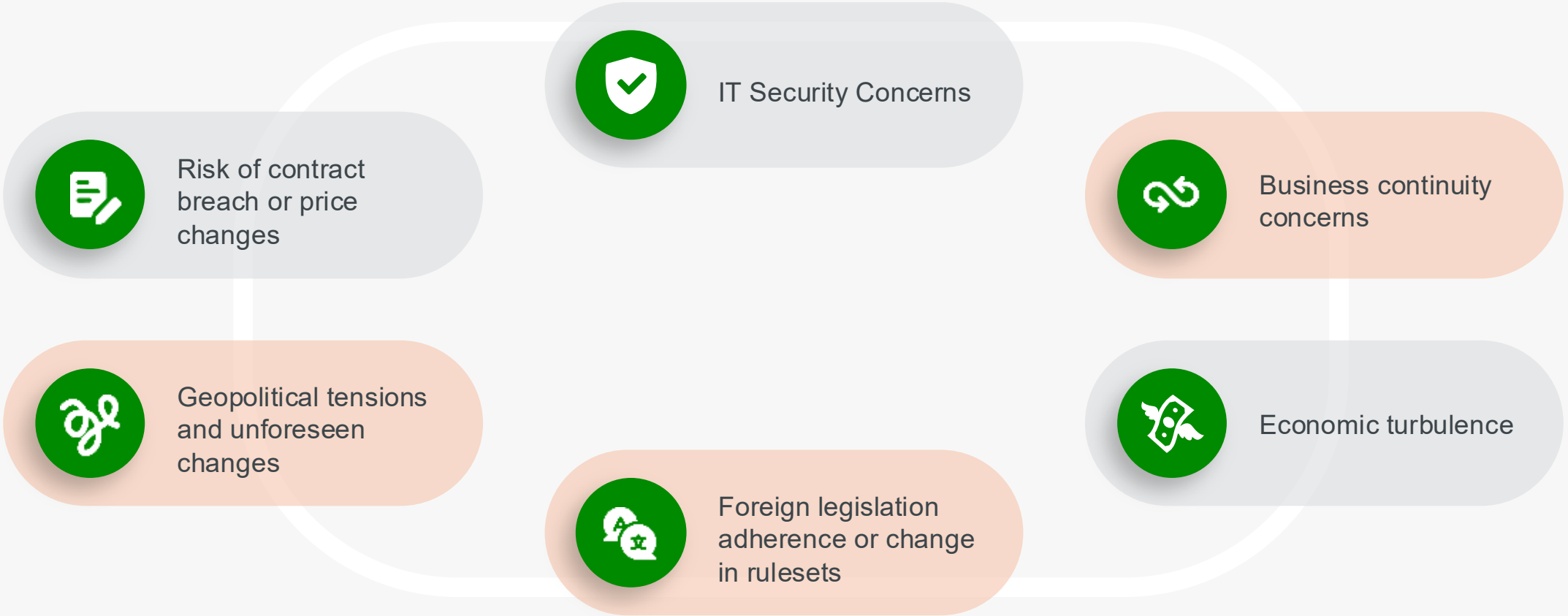
Astonishingly, the attack appears to have been as long as three years in the making. In 2021, a GitHub account was created by an unknown person or organization. The entity behind the account gradually became a co-maintainer of the xz Libs as the original maintainer, citing overwork and burnout, ceded primary oversight of updates.

In early 2024 malicious code linked to the new maintainer was inserted into the xz Libs project. *"This might be the best executed supply chain attack we've seen … it's a nightmare scenario: malicious, competent, authorized upstream in a widely used library,"* wrote another open source maintainer. Had the backdoor remained undetected, said computer scientist Alex Stamos, "*it would have given its creators a master key to any of hundreds of millions of computers around the world…*"

https://www.blackduck.com/blog/xz-utils-backdoor-supply-chain-attack.html

Main **Cloud Exit Drivers**

Geopolitiikka



Main Cloud Exit Drivers, Gartner

Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers

By 2030, More Than 75% of All Enterprises Outside of the U.S. Will Have a Digital Sovereignty Strategy

Toiminnan itsearviointi

- Onko organisaatiosi johdolla yhteinen, ajantasainen käsitys siitä, mitkä ovat teidän konkreettiset uhkanne?
- Tiedämmekö mikä on teille kriittistä, jos katsotaan liiketoimintaa eikä IT:tä?
- Oletteko arvioineet toimitusketjunne kyberkypsyyttä - tiedättekö, kuka alihankkijoistanne on suurin riskitekijä?
- Onko teillä tällä hetkellä selkeä omistajuus siitä, kuka vastaa geopoliittisista pilviriskiarvioinneista?

Mitä tapahtuu, jos tätä ei hoideta?

Business impact • Kustannuslaskenta • Kypsyysajattelu

Business Impact

- Operatiivinen toiminnan keskeytyminen
- Mainevahinko & asiakasluottamus
- Regulatoriset sanktiot & oikeudelliset seuraukset
- Kilpailukyvyn menetys
- Tietopääoman menetys

Mikä kustannus on hyväksyttävää?

- Välittömät kustannukset (näkyvä jäävuori)
- Välilliset kustannukset (piilossa oleva osa)

- Laskentaharjoitus – ROI - Mihin panostaa ensin?

- Investointi = Riskin todennäköisyys × Vaikutuksen arvo

Kuinka kauan organisaationne kestää ilman keskeisiä järjestelmiä?

‘This happens more frequently than people realize’
- Arup chief on the lessons learned from a $25m deepfake crime

https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/
https://coverlink.com/case-study/case-study-25-million-deepfake-scam/

‘Chemical manufacturing company Orion has revealed it has lost $60m in a business email compromise (BEC) scam.’

https://www.infosecurity-magazine.com/news/manufacturing-loses-60m-bec/

‘NIS2 ja kyberturvallisuus-laki muuttivat pelin - vastuu ei enää kuulu IT:lle. Se kuuluu johdolle, henkilökohtaisesti.’

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Suositus%20NIS-valvoville%20viranomaisille%20kyberturvallisuuden%20riskienhallinnan%20toimenpiteistä.pdf

Kyberturvallisuuden kypsyys – kehityspolku?

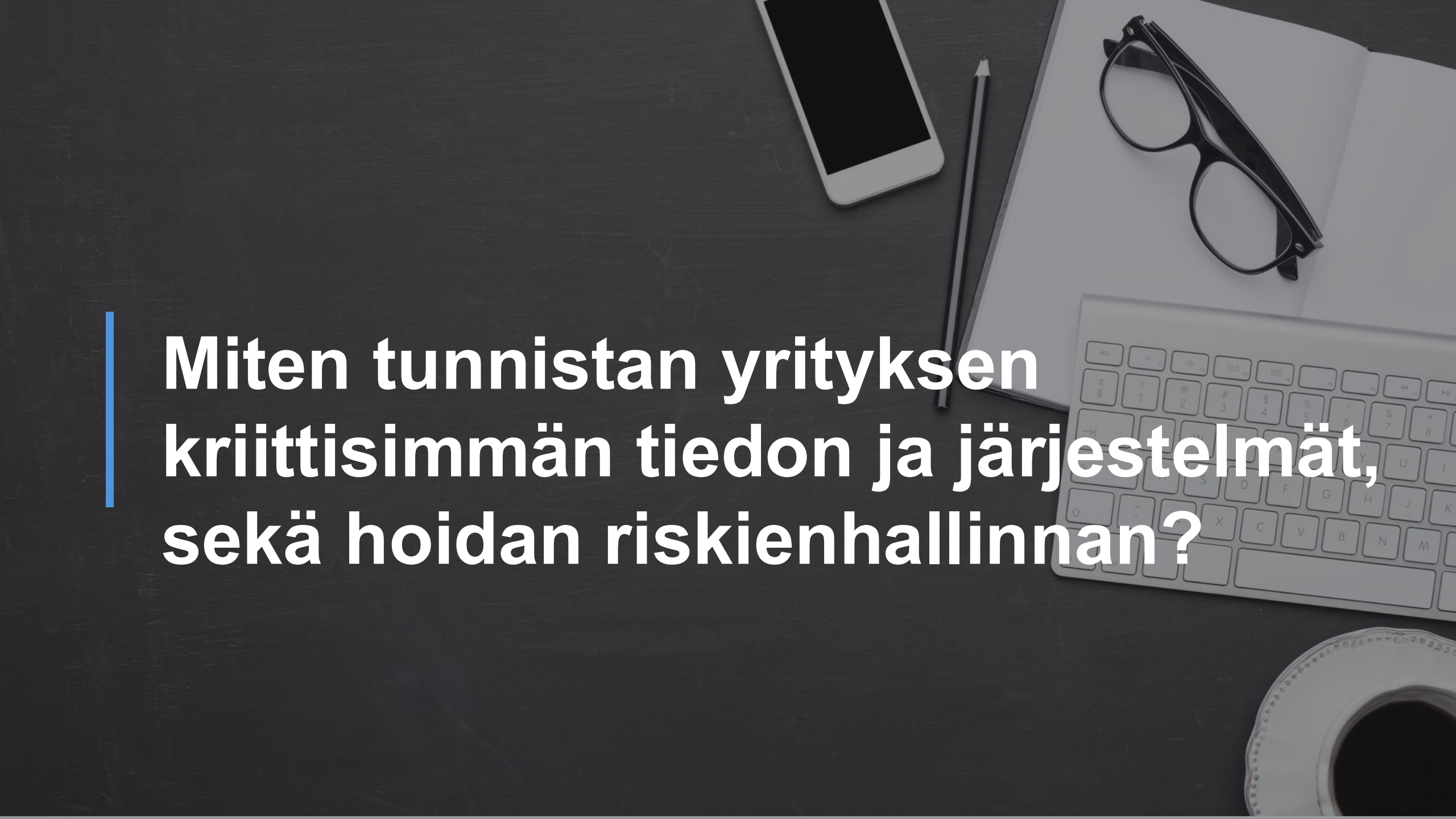
TAVOITE: Organisaatiosi nykytila → Realistinen kehityspolku → Mitattavissa oleva edistyminen

Toiminnan itsearviointi

- Paljonko edellä miettimänne kyberturvan ongelma / poikkeama maksaisi teille tunnissa – päivässä – viikossa?
- Missä kohtaa kypsyysasteikkoa (1–5) uskotte organisaationne tällä hetkellä olevan — ja oletteko johdon kanssa samaa mieltä siitä?
- Oletteko koskaan laskeneet, kuinka kauan liiketoimintanne kestää ilman keskeisimpiä järjestelmiä - ja onko luku tiedossa johdolla?
- Onko teillä jokin mittari, jonka perusteella voitte osoittaa kyberturvan edistymisen hallitukselle tai johtoryhmälle?

Kyberturvallisuus käytännössä

Riskienhallinta • Suojattava omaisuus • Liiketoiminnan toipuminen



Miten tunnistan yrityksen kriittisimmän tiedon ja järjestelmät, sekä hoidan riskienhallinnan?

Johdon tiivistelmä

Selvitys osoittaa, että kansallinen kyberkypsyyden taso on kehittynyt vuodesta 2022 vain maltillisesti. Samalla teknologian ja uhkakentän murros etenee merkittävästi nopeammin kuin organisaatioiden kyky uudistua ja investoida kyberturvallisuuteen.

Kehityksen hitaudesta kertoo se, että parannuskohteet ovat edelleen samoja, kuin kolme vuotta sitten tehdyssä selvityksessä. Samalla viidennes otannan yrityksistä jää matalalle kypsyystasolle.

Pienet ja keskisuuret yritykset sijoittuvat korostuneesti alemmille kypsyystasoille, eikä ilmiö selity yksinomaan resurssien rajallisuudella. Selkein puuttuva tekijä on ylimmän johdon tuki. Korkeamman tason yrityksissä johtoryhmä on tehnyt tietoisen päätöksen nostaa kyberturvallisuuden prioriteettia.

Verkostoituneessa yhteiskunnassa oma korkea kypsyystaso ei riitä suojaamaan uhkilta. Yhdistettynä toimitusketjujen riskienhallinnan heikkouksiin, altistuvat myös korkean kyberkypsyystason toimialat ja yritykset verkostojen kautta kyberuhkille. Riski korostuu entisestään, mikäli suomalaisten yritysten valmiustaso pääsee eriytymään liikaa.

Kyberuhkatietoisuus lisääntyy, mutta konkreettiset toimet jäävät jälkeen

Organisaatioiden kyberuhkatietoisuus on kasvanut ja johdon tietoisuus uhkista vahvistunut. Kuitenkin erityisesti matalamman kypsyystason yrityksissä kehitystä hidastavat resurssi- ja rakenteelliset puutteet sekä kyberturvallisuuden eriytyminen liiketoiminnasta.

Kyberriskienhallinnan kehitys on epätasaista, eikä sen tuottamaa tietoa kyetä hyödyntämään päätöksenteossa

Kyberriskienhallinnan taso vaihtelee merkittävästi eri toimialojen ja yritysten välillä. Korkeammalla tasolla se on liiketoimintalähtöistä ja aktiivista, kun taas erityisesti PK-sektorilla riskienhallinta on useammin satunnaista tai reaktiivista.

Häiriötilanteisiin varautuminen on ottanut harppauksen eteenpäin

Valtaosa yrityksistä on laatinut varautumissuunnitelman ainakin kriittisille palveluille ja monissa yrityksissä suunnitelmien laatiminen on myös johtanut konkreettisiin toimenpiteisiin. Kehitys on kuitenkin usein reaktiivista, ei ennakoivaa, ja harjoittelua tehdään edelleen vain vähän.

https://www.huoltovarmuuskeskus.fi/julkaisu/kyberkypsyys-toimialoilla-2025-kansallinen-koosteraportti

Kyberturvan haasteet

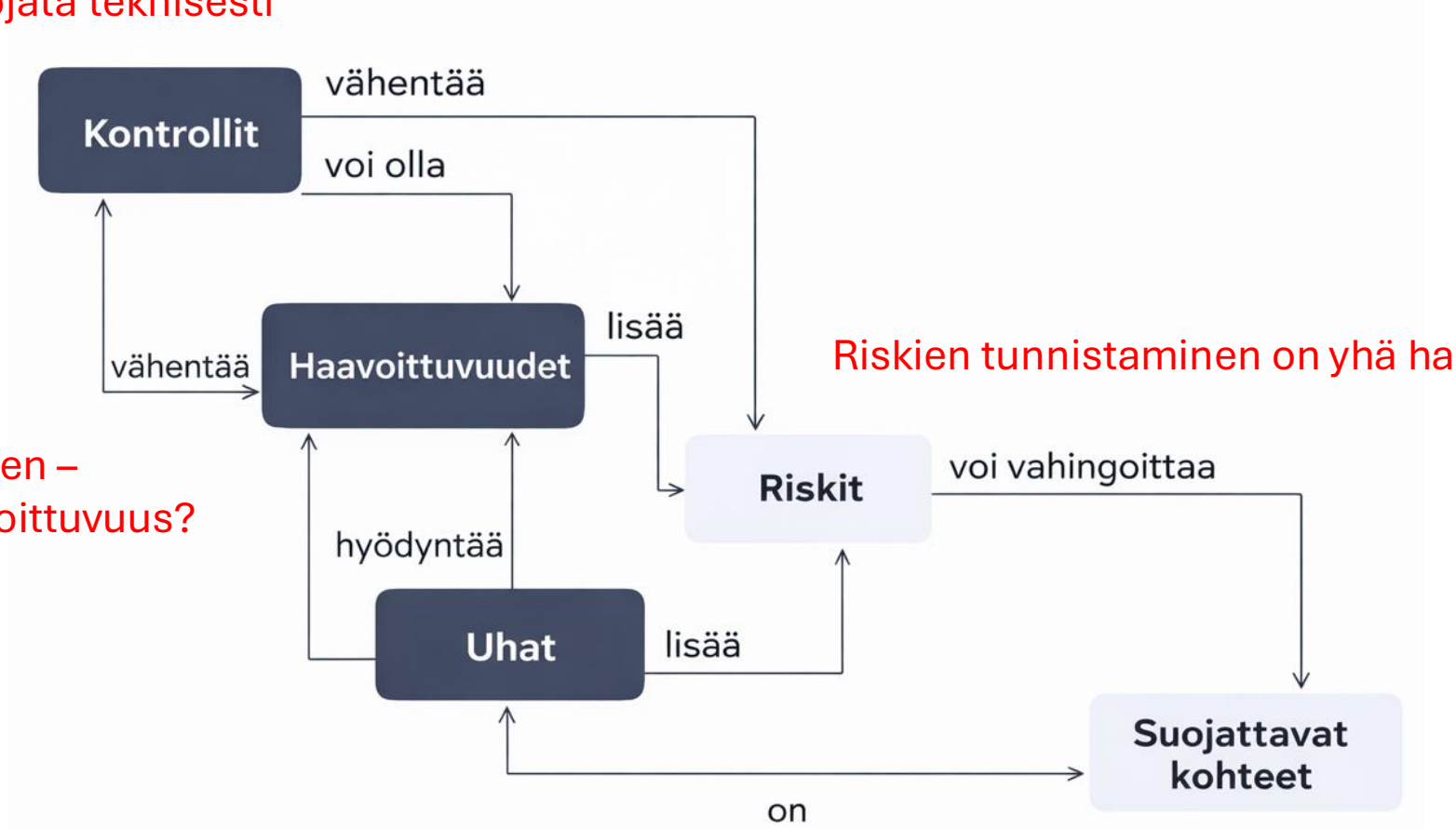
Viimeisimmät tutkimukset osoittavat, että teknologinen muutos ja kyberuhkien kehitys etenevät nopeammin kuin yritysten suojaustoimenpiteet.

Kyberturvallisuuspoikkeamat yrityksissä voivat johtaa vakaviin taloudellisiin riskeihin ja menetyksiin.

Kyberturvallisuus ei ole erillinen IT-teema, vaan keskeinen osa liiketoiminnan riskienhallintaa ja päätöksentekoa

Mitä tämä tarkoittaa – mikä ratkaisee?

Kaikkea ei voi suojata teknisesti



Riskien tunnistaminen on yhä hankalampaa

Ihminen –
suurin haavoittuvuus?

Uhat kasvavat jatkuvasti – AI?

Kriittinen omaisuus on eri paikoissa – cloud?

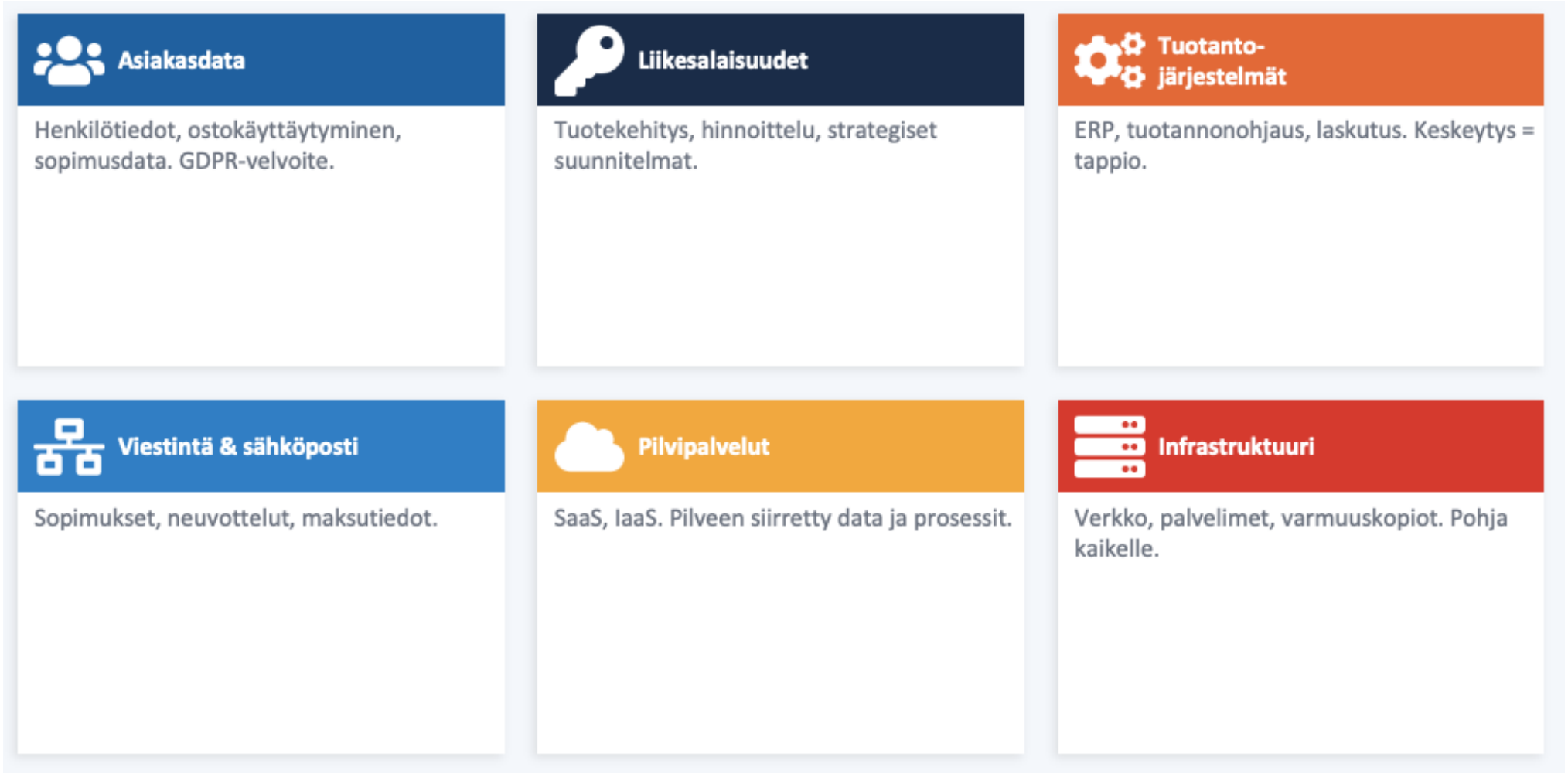
Riskien käsittely

0 - Määritä riskin sietokyky
1 - Selvitä mikä on tärkeätä
2 - Selvitä uhat ja haavoittuvuudet
3 - Arvio riskin vaikutus ja todennäköisyys
4 - Priorisoi ja keskity tärkeimpiin
5 - Vähennä riski sopivalle tasolle
6 - Seuraa ja tarkista

Riski = Todennäköisyys x Vaikutus
Todennäköisyys = Uhka x Haavoittuvuus

Riskin vähentäminen
Riskin poistaminen
Riskin siirtäminen
Riskin hyväksyminen
Riskin kasvattaminen

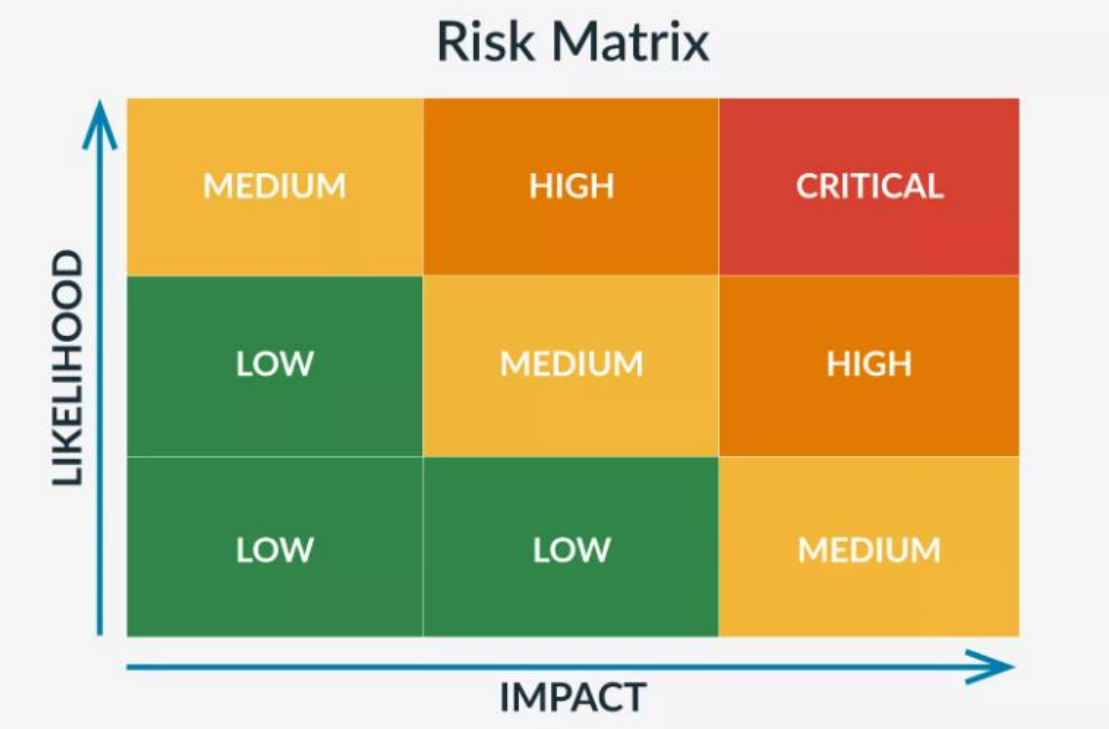
Suojattava omaisuus



Riskien vaikutus yrityksen toimintaan

Table 1. CSF 2.0 Core Function and Category names and identifiers

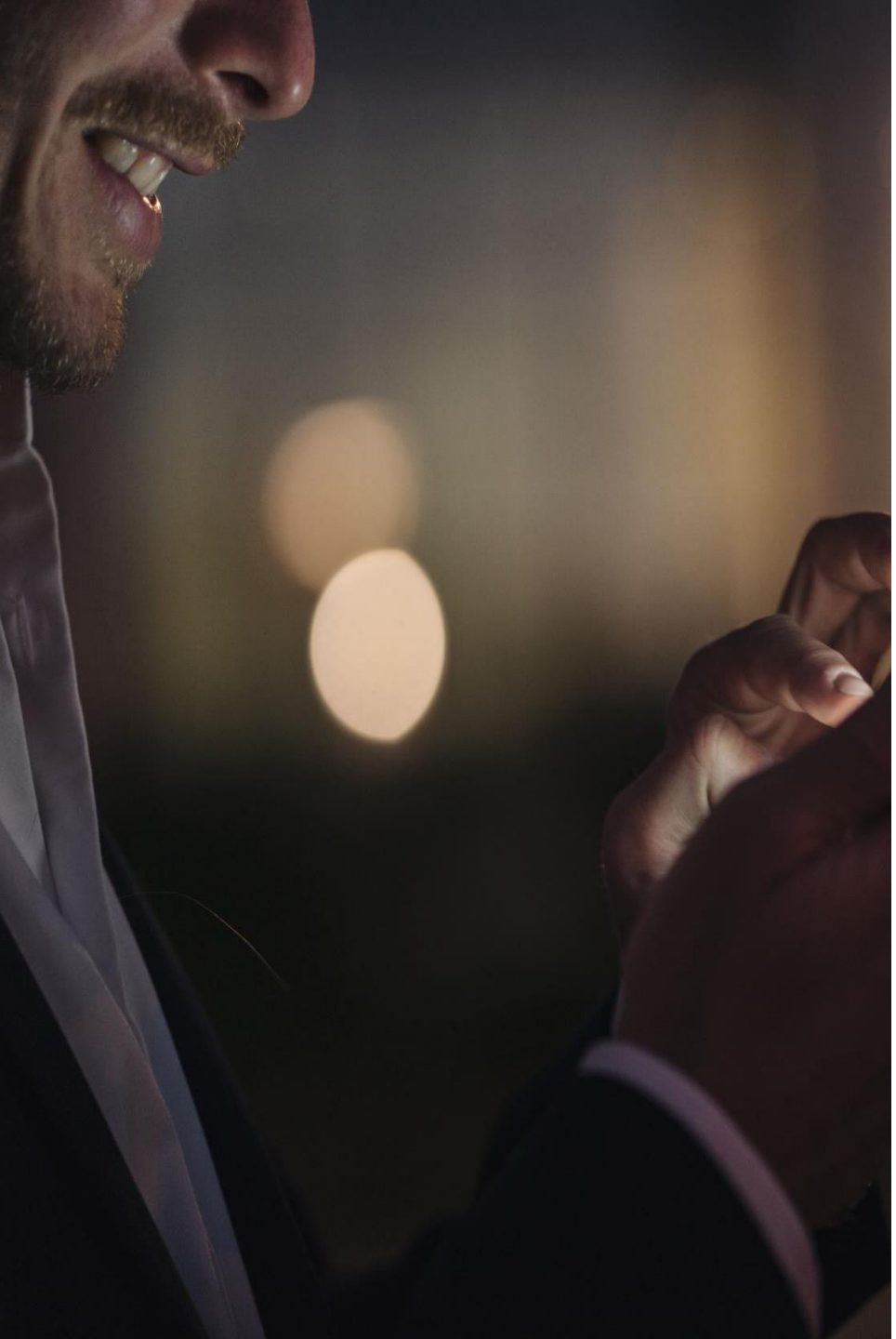
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



Riskien priorisointi

- Ennakkoon määritelty hyväksyttävä riskitaso
- Riskien luokittelu ja vertaaminen, samat mittarit
- Kriittisten riskien ja vaikutuksen arviointi
- Keskitä toimet kriittisiin riskeihin

Riskien arviointi on jatkuvaa toimintaa!



Kuinka jatkaa toimintaa häiriön jälkeen?

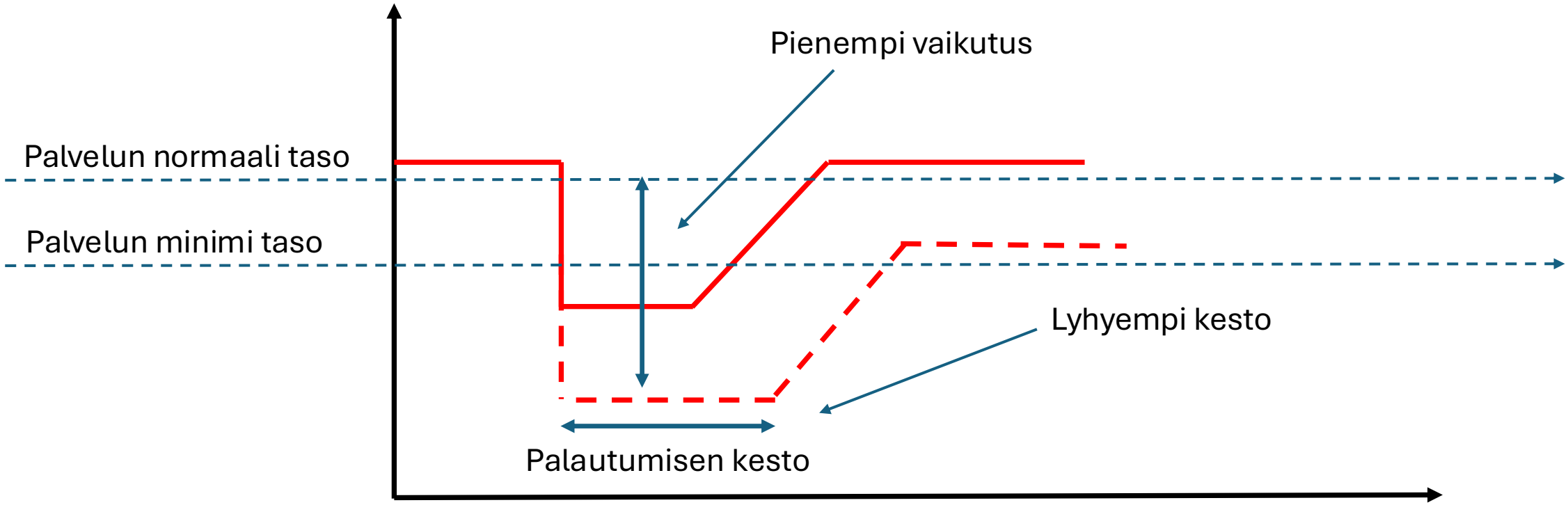
- Jatkuvuussuunnitelma (BCP)
- Toipumissuunnitelma (DRP)

- RTO — Recovery Time Objective → toipumisen aika
- RPO — Recovery Point Objective → menetetty tieto

- Harjoittelu
- Viestintä

Kuinka kauan organisaatio kestää ilman keskeisiä järjestelmiä?

Varautuminen ja jatkuvuuden hallinta



ISO 22313 - Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät

Riskienhallinta yrityksessä

Kyvykkyydet • Toteutus • Hankinta • Kokonaisuus

ATEA

Yhteiskunnan kybervarautumista edistävät suositukset:

Toimitusketjujen kyberturvallisuus huomioitava laajemmin
Kansallinen kyberkypsyyden hidas kehitys ja yritysten valmiustason eriytyminen voi uhata kaikkia kokonaisketjun yrityksiä kypsyystasosta riippumatta. Toimitusketjujen riskien- ja kyberturvallisuuden hallinta on keskeinen kehitettävä kyvykkyys yrityksen kyberkypsyystasosta riippumatta.

Yhteisharjoittelu yhteiskunnallisesti ja toimialoittain on tärkeää
Yhteisharjoitukset ovat monille pk-yrityksille ainoa tapa harjoitella jatkuvuuden hallintaa. Siksi ne ovat tärkeitä paitsi näille yrityksille, myös korkeamman kypsyystason organisaatioille, jotka voivat altistua toimitusketjun kyberturvapoikkeamille.

Kyberturvallisuuslain toimeenpano
NIS2-direktiivin kansallisen toimeenpanon valvonnassa tulee painottaa käytännön toteutusta. Yrityksiltä on vaadittava konkreettisia todisteita kyberturvatoimien jalkautumisesta, jotta laki nostaa todellista eikä näennäistä kypsyyttä.

Liiketoimintajohtajille suunnattu kyberturvallisuuskoulutus
Johdon kyberuhkatietoisuuden heijastuminen käytännön kyberkypsyyteen vaatii koulutusta, joka puhuttelee kohderyhmää ja kytkee kyberturvallisuuden suoraan liiketoiminnan jatkuvuuteen ja taloudelliseen menestykseen.

Liiketoiminnan jatkuvuutta edistävät suositukset:

Johdon osallistuminen avain kyberkypsyystason nostoon
Tukea voi edistää aktiivisella yhteistyöllä ja seurattavilla mittareilla sekä kehittämällä johdon kyberturvallisuusosaamista kohdennetuin koulutuksin.

Kyberturvallisuusosaamisen kehittäminen
Yritysten tulisi organisaation koosta ja toimialasta riippuen varmistaa riittävä kyberturvallisuusosaamisen taso palkkaamalla asiantuntijoita, hyödyntämällä kumppaneita sekä tukemalla työntekijöiden uudelleenkouluttautumista.

Kokonaisvaltainen turvallisuusjohtaminen
Monissa organisaatioissa kyberturvallisuus, teollisuus- ja tuotantojärjestelmien (OT) turvallisuus sekä fyysinen turvallisuus johdetaan erillisinä kokonaisuuksina. Yhtenäinen tilannekuva parantaa kyberriskien ja resurssien priorisointia sekä auttaa tunnistamaan laajempia vaikuttamisyrityksiä.

Operatiivisen kyberriskienhallinnan sisällyttäminen osaksi liiketoiminnan kokonaisvaltaista riskienhallintaa
Erityisesti pienissä ja keskisuurissa yrityksissä kyberriskienhallinta on vähäistä, reaktiivista ja irrallista muusta liiketoiminnan riskienhallinnasta.

Suositukset

- Toimitusketjut
- Harjoittelu
- Kyberturvallisuuslain toimeenpano
- Liiketoimintajohdon koulutus

- Johdon osallistuminen
- Kyberturvallisuusosaamisen kehittäminen
- Kokonaisvaltainen turvallisuusjohtaminen
- Operatiivinen + liiketoiminnan riskienhallinta

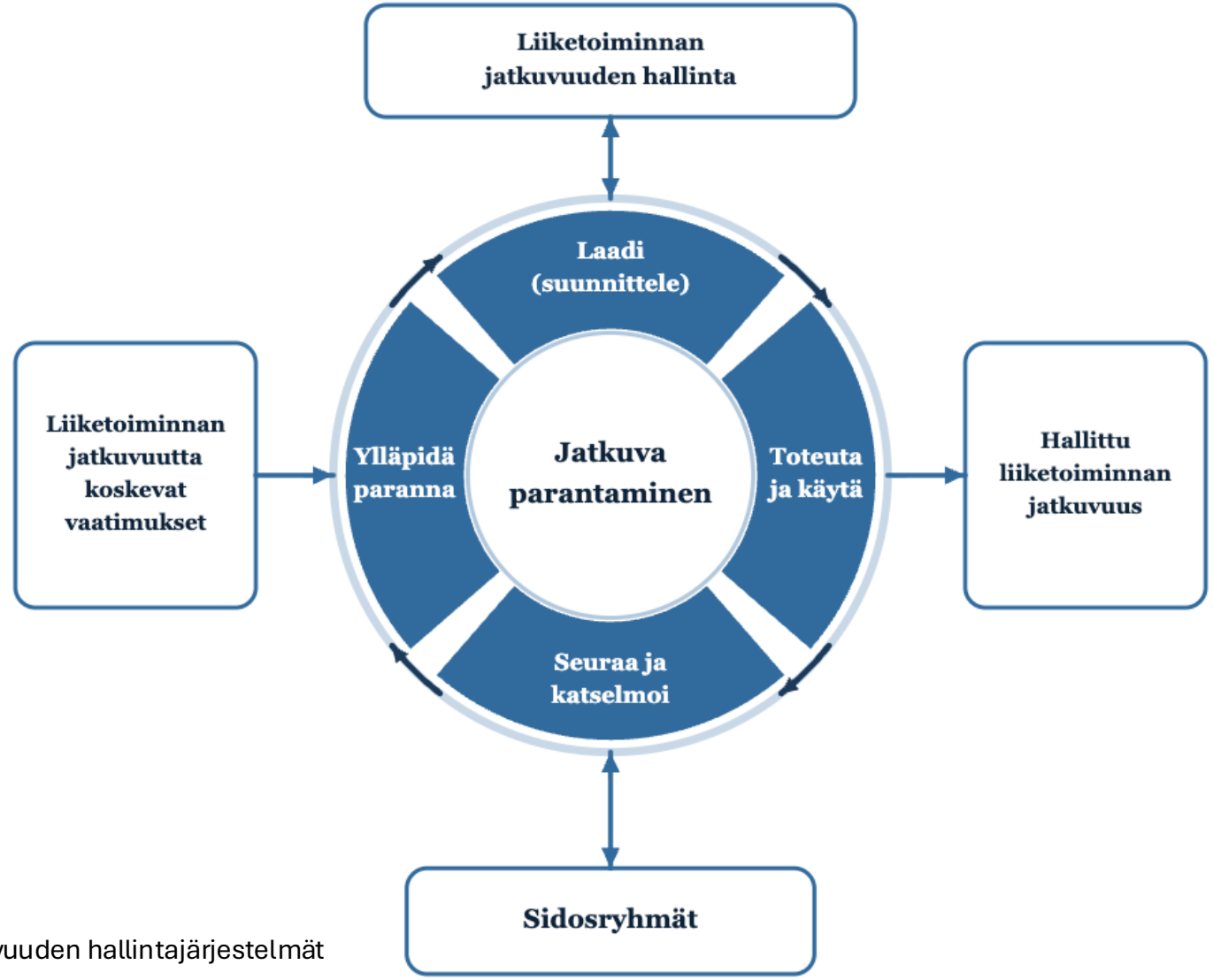
Tarvittavat kyvykkyydet — Mitä ymmärrystä tarvitaan?

STRATEGINEN	TAKTINEN	OPERATIIVINEN
✓ Riskienhallinta & priorisointi	✓ Tietoturvapolitiikat & prosessit	✓ Pääsynhallinta & identiteetti
✓ Liiketoiminnan jatkuvuus	✓ Toimittaja- & kumppaninhallinta	✓ Haavoittuvuuksien hallinta
✓ Regulatory compliance (NIS2, GDPR)	✓ Koulutus & tietoisuus	✓ Monitorointi & lokienhallinta
✓ Hallituksen & johdon vastuu	✓ Hankintaosaaminen	✓ Tapahtumanhallinta (IR)

Riskien arviointi ja hallinta

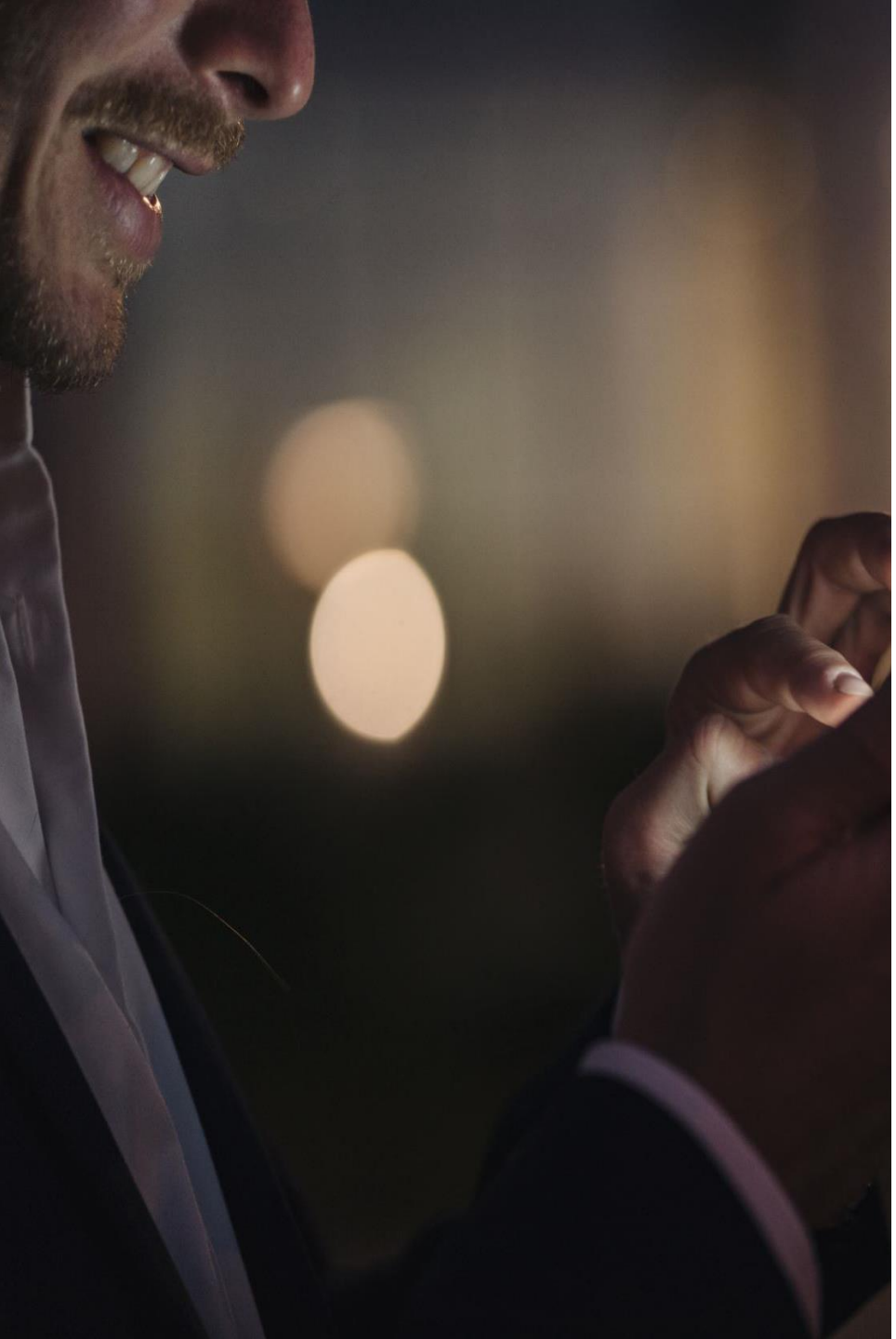
ISO 31000 – Riskienhallinta, ohjeet

Riskienarviointi, ja -hallinta, sekä jatkuvuudenhallinta



ISO 31000 – Riskienhallinta, ohjeet

ISO 22313 - Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät



Ihmiset, prosessit, teknologia

- Ihmiset — Tärkein tekijä
- Prosessit — Toistettavuus & hallinta
- Teknologia — Mahdollistaja, ei ratkaisu
- Johtaminen & kulttuuri — Pohja kaikelle
- Mittaaminen — Et voi johtaa mitä et mittaa

Staattinen kyberturva on vanhentunutta kyberturvaa

Miten toteutan tämän? - Itse vai osanko tämän ulkoa?

ITSE HOIDETTAVAA (sisäinen kyvykkyys)

- Kyberturvastrategia & riskienhallinta
- Politiikat & prosessit
- Johdon vastuut & raportointilinja
- Henkilöstön koulutus & tietoisuus
- Kriittisten omaisuuserien tunnistaminen
- Hankintapäätökset & toimittajahallinta
- Tapahtumavaste-prosessi (vastuut)

HANKITTAVAA (ulkoinen palvelu)

- SOC / SIEM-palvelut (monitorointi)
- Penetraatiotestaus & haavoittuvuusskannaus
- Forensiikka & tapahtumavaste (IR)
- Pilviturvallisuuden hallinta
- Uhkatiedustelu (Threat Intelligence)
- Compliance-auditoinnit (ISO 27001, NIS2)
- Spesialistiosaaminen (OT, Cloud, IAM)

AI vs. AI – Kyberturvallisuuden asevarustelua

HYÖKKÄÄJÄ käyttää AI:ta

- Massoiteltu, kohdennettu phishing — automaattisesti
- Haittaohjelmat, jotka kiertävät havaitsemisen
- Deepfake-ääni ja -video huijauksissa
- Haavoittuvuuksien etsintä ja exploitointi
- Salasanojen krakkaus (AI-avusteinen)
- Disinformaatio ja sosiaalinen manipulointi
- Nopeus: hyökkäykset käynnistyvät sekunneissa

VS

PUOLUSTAJA käyttää AI:ta

- Anomalioiden, poikkeamien havaitseminen suuresta datamäärästä
- Käyttäytymisanalyysi (UEBA) sisäpiiriuhkiin
- Automaattinen triage ja priorisointi
- Haavoittuvuuksien älykäs priorisointi (EPSS)
- Uhkatiedon rikastaminen reaaliajassa
- Generatiivinen raportointi ja dokumentaatio
- Nopeus: reaktioaika sekunneissa

Kilpailua ei voiteta teknologialla — prosessit, osaaminen ja reagointikyky ratkaisevat

AI hyödyt ovat selkeät – toiminta pitää ymmärtää

	HYÖTY	AI nopeuttaa havaitsemista, automatisoi rutiini selvityksen ja mahdollistaa suuremman volyymin käsittelyn
	HYÖTY	Automattinen käyttäjien ja järjestelmien analyysi tuovat laadullisesti uutta kykyä, jota perinteiset säännöt eivät korvaa
	UHKA	Hyökkääjät hyödyntävät AI:ta: deepfake, LLM-phishing ja adaptiiviset haittaohjelmat ovat jo arkipäivää
	UHKA	AI-järjestelmät ovat itse hyökkäyskohteita: data poisoning ja adversarial evasion uhkaavat puolustuskykyä
	GOVERNANCE	EU AI Act + NIS2 edellyttävät hallittua käyttöönottoa: läpinäkyvyys, ihmisvalvonta ja auditointikyky

AI vs. AI – Kyberturvallisuuden asevarustelua

🔍 Luottamus & läpinäkyvyys

- AI-päätösten selitettävyys (XAI)
- Bias-arviointi ennen käyttöönottoa
- Ihminen päätöksenteossa (Human-in-loop)
- Auditointiloki AI:n suosituksista
- Ei täydellistä automaatiota kriittisissä päätöksissä

⚖️ Tietosuoja & compliance

- GDPR: henkilödata AI-mallien koulutusdatassa
- EU AI Act: kyberratkaisut high-risk -kategoriassa
- NIS2: AI-järjestelmien riskienhallinta
- Datan minimointi ja säilytysajat
- Toimittajan AI:n sijaintimaa ja auditointimahdollisuus

🔄 Resilienssi & jatkuvuus

- Adversarial robustness -testaus
- Fallback ilman AI:ta (degraded mode)
- Model drift -seuranta ja uudelleenkoulutus
- Toimittajariippuvuuden hallinta
- Red team -harjoitukset AI-järjestelmille

EU AI Act (2025) luokittelee monet kyberturvallisuuden AI-sovellukset korkean riskin kategoriaan — vaatimustenmukaisuus on huomioitava hankinnassa.

Toiminnan itsearviointi

- Defence in Depth: palomuuri, endpoint, identiteetti, verkko, data — kaikilla kerroksilla oma roolinsa. Mitä teidän organisaatiossa tapahtuu, kun yksi niistä pettää?
- Tiedättekö, mitä AI-pohjaisia palveluja teillä on käytössä - joko suoraan hankittuina tai toimittajienne kautta - ja onko niiden riskejä arvioitu EU AI Actin näkökulmasta?
- Jos kyberturvakumppanilta tulisi tänä yönä vakava hälytysilmoitus, onko teillä selkeä toimintamalli: kuka vastaa, kuka päättää, kenen puhelimeen se menee?
- Mikä on sisäinen "ei ulkoistettava ydin" — onko johto tunnistettavissa vastuuhenkilö, joka omistaa kyberriskin liiketoimintapäätöksenä, ei IT-asiana?

Mistä aloittaa?

Tarvittavat kyvykkyydet • Palveluiden tuottaminen vs Hankinta

Mitä jää itselle ja mitä voi hankkia?

YDIN — Ei ulkoistettavissa	YHDISTELMÄ — Osittain ulkoistettavissa	OPERATIIVINEN — Ulkoistettavissa
• Riskienhallinnan omistajuus • Strategiset päätökset • Johdon vastuu & governance • Toimittajavalvonta • Kriisinhallinta johtotasolla	• Tietoturvapolitiikat (ulk. asiantuntija) • Riskiarvioinnit (yhdessä toimittajan kanssa) • Henkilöstökoulutus (ulk. sisältö) • Compliance-valmistautuminen • Arkkitehtuurisuunnittelu	• SOC & jatkuva monitorointi • Penetraatiotestaukset • Haavoittuvuusskannaus • Forensiikka & IR-tuki • Tekninen infrastruktuuri
Vastuu pysyy aina omistajalla	*Sisäinen osaaminen + ulkoinen asiantuntijuus*	*Tehokkuus & erikoisosaaminen*

Manuaalinen työ ei enää riitä

- Haavoittuvuuksia ilmestyy joka päivä
- Uhkatieto päivittyy reaaliajassa
- Säädökset ja standardit muuttuvat
- Lokeja ja hälytyksiä tulee jatkuvasti
- Manuaalinen käsittely ei skaalaudu
- Inhimilliset virheet lisääntyvät ylikuormittuessa

Kuinka tästä voi selvitä?

74 päivää

keskimääräinen aika havaita tietomurto

20 000+

uutta haavoittuvuutta vuodessa (CVE)

68 %

Tietoturvahenkilöistä kokee burnoutin

Skaalautuva perusta – tiedon hallinta ja automaatio

01

Tietojen hankinta

Automatisoitu selvitys

SIEM / Threat Intel Feed
Vulnerability Scanner (Tenable)

02

Dokumentointi

Sähköinen tallennus

GRC-alusta / Confluence
Netbox
SharePoint / CMDB

03

Tietojen hyödyntäminen

Automaatio & analytiikka

Konfiguraatiohallinta, IaC
SOAR / Playbook-automaatio
Dashboard & raportointi

04

Tapahtumien seuranta

Reaaliaikainen monitorointi

Tietojen yhdistäminen, EDR & NDR
SIEM-korrelaatio / XDR
Hälytys- ja tikettijärjestelmä

05

Muutosten hallinta

Hallittu muutosprosessi

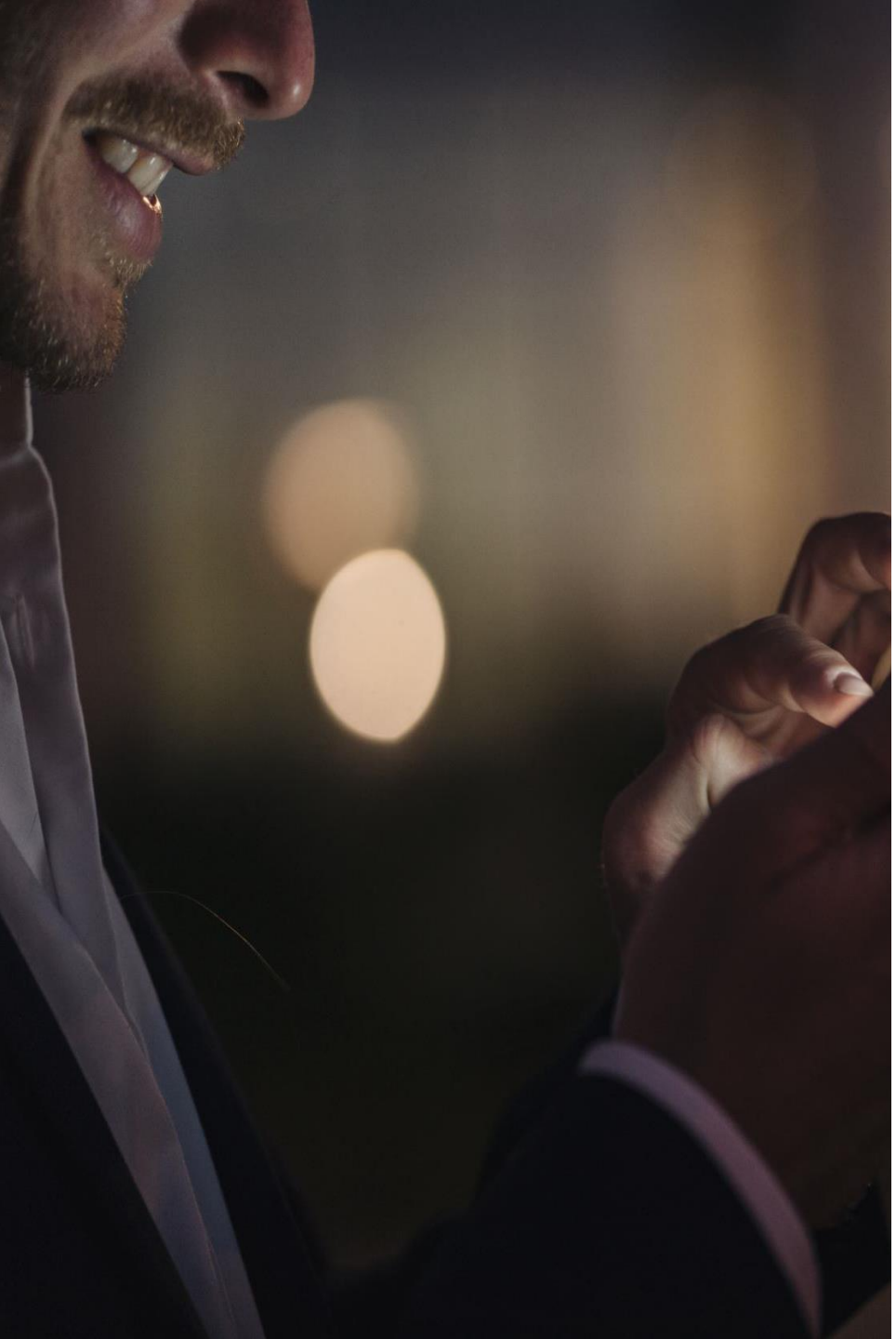
ITSM (ServiceNow/Jira)
CAB-prosessi / Change log

06

Kokonaisuuden arviointi

Jatkuva parantaminen

Maturity Assessment
KPI-mittarit / Gap-analyysi



Kyberturvan kumppani?

- Valinta
- Kumppanuus- ja kyvykkyyskriteerit
- Riskienhallinta
- Sopimus ja vastuut
- Operatiivinen ohjaus
- Irtautuminen (exit & resilienssi)

Kyberturvakumppani ei ole vain valvontapalvelu.
Se on osa organisaation toimintaa, hermostoa / sisältöä

Millä perusteella valinta voidaan tehdä?

Toimialakokemus

- Relevantti kokemus omalta toimialalta
- Vastaavien ympäristöjen (IT/OT) tuntemus
- Paikallistuntemus ja sääntelyosaaminen

Sertifikaatit

- ISO 27001, SOC 2 Type II
- IEC 62443 (OT-ympäristöt)
- Henkilösertifikaatit: CISSP, CISM, CRISC

Referenssit

- Vastaavan kokoluokan asiakkaat
- NIS2-toteutukset ja auditoinnit
- Tarkistettavat referenssiorganisaatiot

SLA-vasteajat

- Kriittinen häiriö: ≤1h / Normal ≤4h / Low ≤24h
- Ilmoitusvelvollisuusajat (NIS2: 24h/72h/30d)
- Eskalointipolku ja 24/7-päivystys

Hinnoittelumalli

- Kiinteä vs. aika+materiaali vs. subscription
- Hintakehityksen sidosmuuttujat ja revisiot
- Lisätyöhinnasto ja muutoshallinnan ehdot

Kommunikointi ja viestintä

- Ymmärrys liiketoiminnan riskeistä
- Kykeneekö toimija analysoimaan ja kommentoimaan tilanteen johdolle
- Miten tekniikka ja johtaminen yhdistyvät

Selkeä vastuunjako – RACI-matriisi

R – Responsible
Tekee työn

A – Accountable
Vastaa tuloksesta

C – Consulted
Konsultoidaan

I – Informed
Pidetään tietoisena

Tehtäväalue	Asiakas	Toimittaja	3. osapuoli
Riskianalyysi ja priorisointi	A	R	C
Turvakontrollien toteutus	A	R	I
SOC-valvonta (24/7)	I	R	C
Tietoturvapolitiikka	R/A	C	–
Poikkeamanhallinta (1. taso)	I	R	–
Poikkeamanhallinta (2. taso)	A	R	C
Auditointi ja vaatimustenmukaisuus	A	C	R
Käyttäjätunnushallinnan hyväksyntä	A/R	I	–

Toiminnan itsearviointi

- Tiedättekö tällä hetkellä, mitä tietoa ja pääsyä kyberturvakumppanillanne on organisaatioonne - ja onko se dokumentoitu?
- Jos nykyinen toimittajanne lopettaisi huomenna, kuinka kauan kestäisi ennen kuin toiminta on taas hallinnassa?
- Kuka organisaatiossanne omistaa toimittajasuhteen johtamisen — IT, hankinta, vai johto?
- Pystyykö toimittajanne selittämään tietoturvatilanteen johdolle ymmärrettävästi — vai tuleeko raportti pelkkinä teknisistä mittareina?

Tyypilliset virheet

Mitä ei kannata tehdä — Opittu kantapään kautta

Tyypillisiä hallinnollisia virheitä

01

Vastuu ulkoistetaan

Kyberturvallisuuden vastuuta ei voi ulkoistaa. Toimittaja tuottaa palvelua — johto vastaa aina.

→ Nimeä sisäinen omistaja. Johto raportoi hallitukselle.

02

Pelkkä tekninen ajattelu

Ostetaan kallis teknologia, unohdetaan ihmiset ja prosessit. Teknologia ilman koulutusta on turha.

→ Ihminen + Prosessi + Teknologia -malli.

03

'Ei koske meitä' -syndrooma

Pienetkin yritykset ovat houkuttelevia kohteita — usein juuri siksi, että niillä on heikompi suojaus.

→ Toimitusketjuriskit, automaattiset hyökkäykset. Kaikki ovat kohteita.

04

Ostetaan & luotetaan

Tietoturvatuote ostetaan, asennetaan ja unohdetaan. Ei testata, ei ylläpidetä, ei päivitetä.

→ Säännölliset testaukset, penetraatiotestit, päivitysohjelmat.

05

'Liian vaikea meille'

Oppiminen koetaan mahdottomana. Kyberturva jätetään IT:lle. Johto ei ota asiaa haltuun.

→ Alku on yksinkertainen. Riskimatriisi + 3 prioriteettia + mittari.

06

Liian vähän resursseja

Varataan liian vähän resursseja ja johto ei sitoudu toimintaan riittävästi

→ Arvioidaan resurssien ja tekemisen arvo suhteessa liiketoimintaan. Oikea BI arvio ja laskenta

Tyypillisiä teknisiä virheitä

01 **Varautuminen**

Varautumisen ja palautumisen unohtaminen

Testatut varmuuskopiot ja palautumissuunnitelmat

02 **Haavoittuvuudet ja päivitykset**

Päivitysten ja haavoittuvuuksien hallinnan laiminlyönti

Vastuut, prosessit

03 **Riskienhallinta**

Riskienhallinnan puute tai väärä priorisointi

Riskienhallintaprosessi

04 **Tapahtumien seuranta**

Puutteellinen lokien hallinta ja valvonta

Keskitetty lokien keräys, hälytykset poikkeavasta toiminnasta

05 **Identiteetinhallinta**

Heikko identiteetin ja pääsyn hallinta

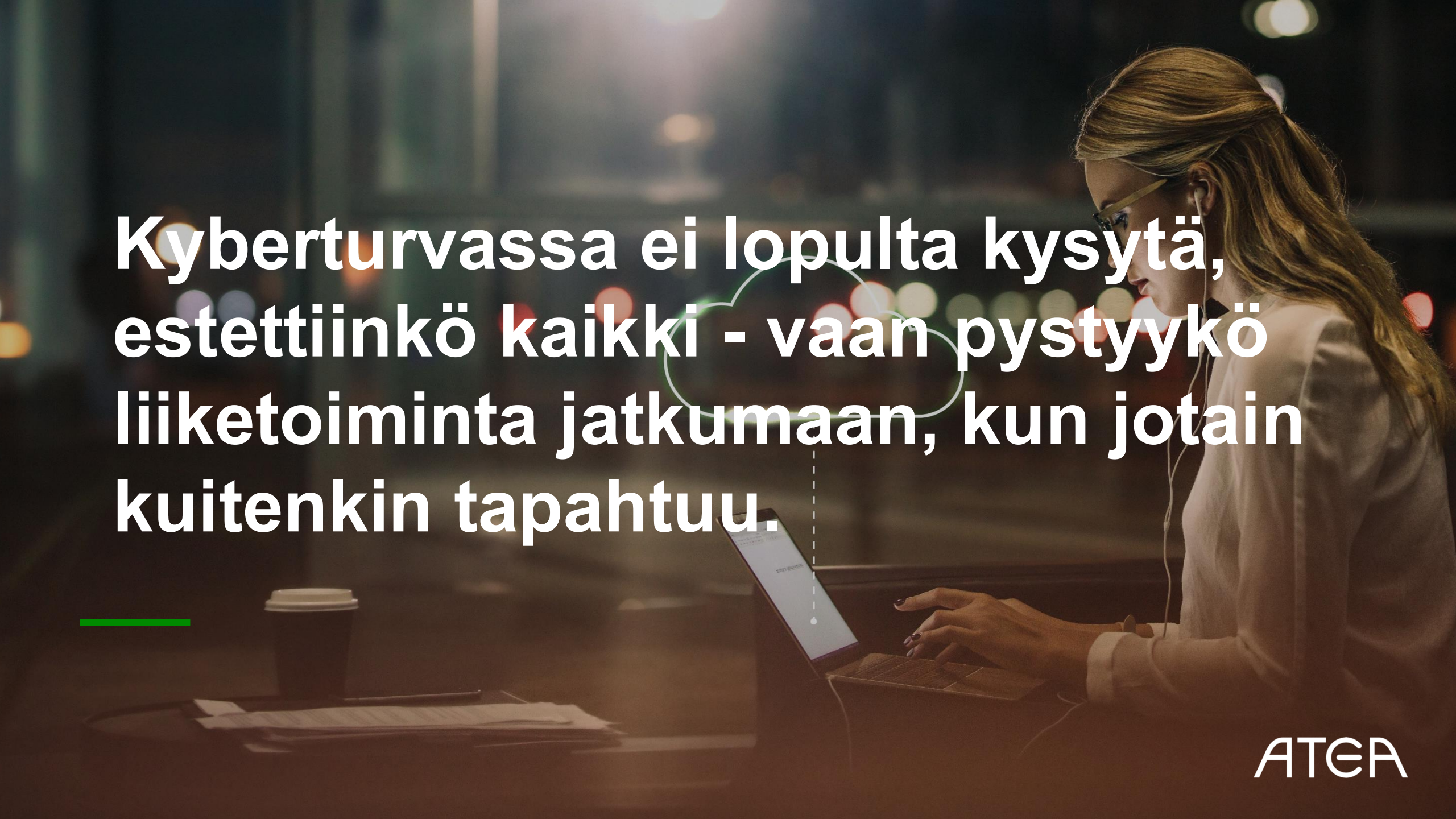
MFA, säännöllinen oikeuksien tarkistus, least priviledge

06 **Toimitusketjut**

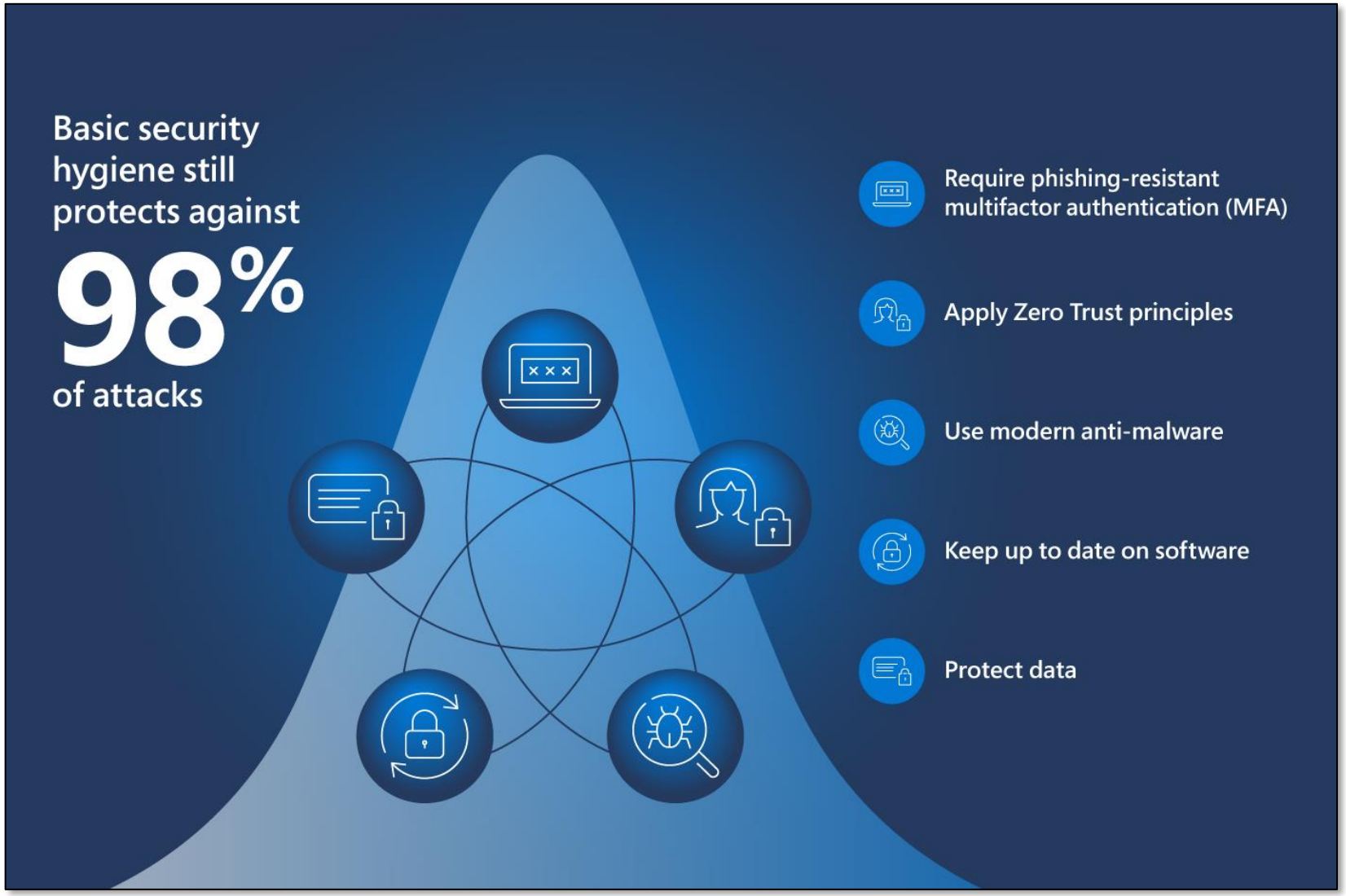
Kolmannen osapuolen riskit

Toimittajien tietoturvan vaatimukset, sopimusten tarkastelu

Yhteenveto


Kyberturvassa ei lopulta kysytä, estettiinkö kaikki - vaan pystyykö liiketoiminta jatkumaan, kun jotain kuitenkin tapahtuu.
ATEA

Kyberturva ei todellakaan ole vaikeata!



https://techcommunity.microsoft.com/blog/microsoft-security-blog/basic-cyber-hygiene-prevents-98-of-attacks/3926856?utm_source=chatgpt.com

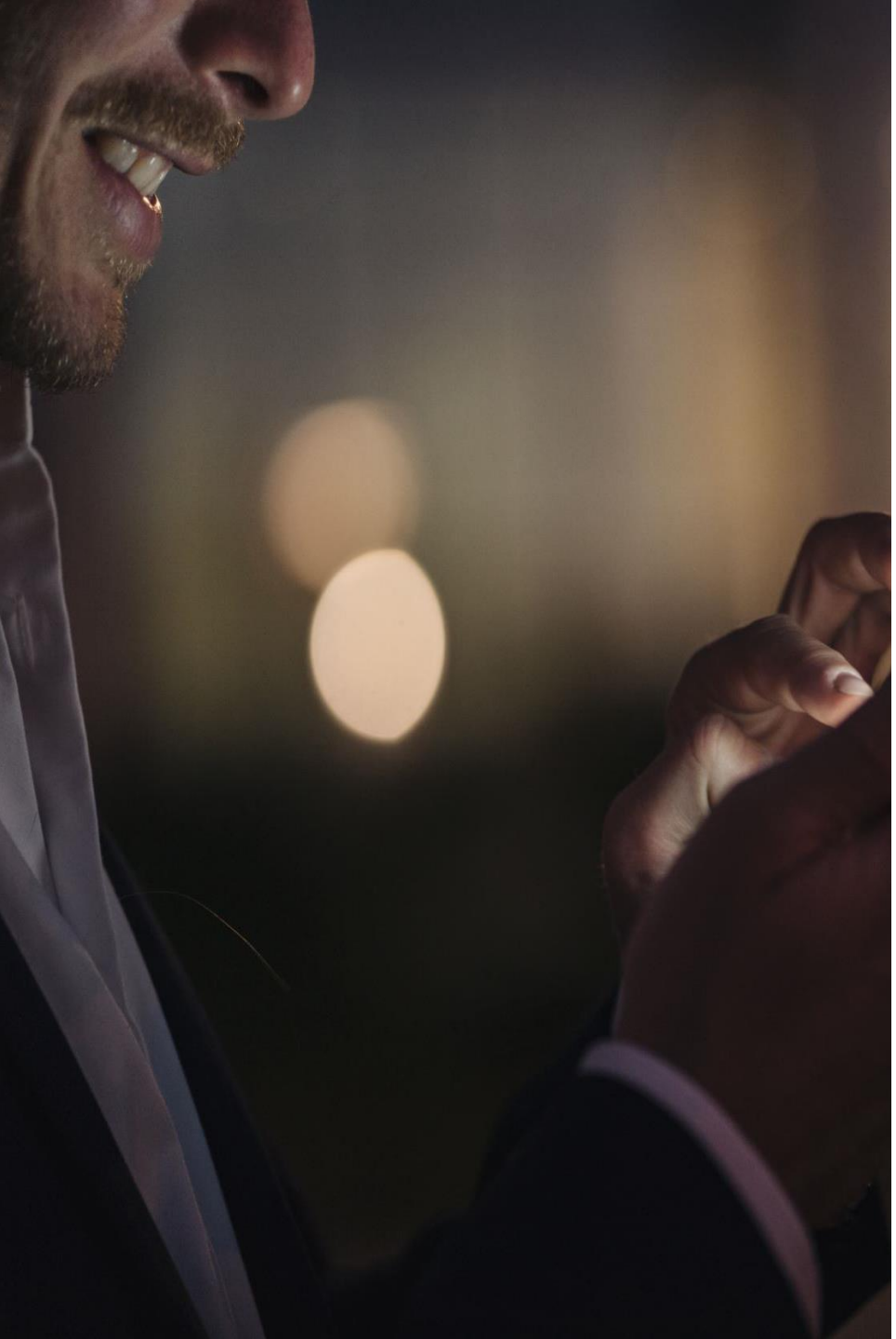
Kyberturva ei todellakaan ole vaikeata!

The majority (92%) of enterprises that fell victim to a security breach believe more robust cyber hygiene practices could've prevented disaster, according to new research.

In a new study from Swimlane, more than half (52%) of organizations said their "greatest weakness" lies in human mistakes, underlining the need for better employee training and awareness.

Yet despite this, efforts to improve cyber hygiene are still often overlooked by leadership, with just 32% of respondents noting that hygiene and resilience rank high on C-suite priority lists.

https://www.itpro.com/security/enterprises-need-to-acknowledge-the-importance-of-basic-cyber-hygiene?



Havaintoja kentältä…

- Yleisin haaste ei ole teknologia – vaan riskien tietämättömyys
- Johdon ja IT:n yhteinen kieli puuttuu – todelliset uhat jäävät korjaamatta
- Compliance toimii minimitasona, ei tavoite johon lopetetaan
- Suurimmat tulokset syntyvät pienistä, toistuvista parannuksista
- Ihmisten päätökset ratkaisevat enemmän kuin teknologia
- Parhaiten menestyvät organisaatiot ymmärtävät riskinsä ja tekevät niistä näkyviä

Yhteenveto - 6 avaintoimenpidettä

1. Tunnista suojattava omaisuus ja kriittiset prosessit
2. Arvioi riskit ja vaikutukset — yksinkertainen riittää
3. Nimeä omistaja ja tee riskistä päätös, ei dokumenttia
4. Laita ihmiset ja prosessit kuntoon — teknologia tukee
5. Selkeytä toimitusketju — vastuut, oikeudet ja kontrollit
6. Harjoittele toipumissuunnitelma — testaa varmuus-kopiot

Kiitos osallistumisesta!

Veli-Matti Järveläinen
Senior Advisor , Atea Finland Oy