Tero Ripattila

Organisaatioiden riskien hallinta ja toimintakyvyn varmistaminen: Liike-toimintakonsepti red teamingista

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tuotantotalouden tutkinto-ohjelma

Insinöörityö

28.4.2026

Tiivistelmä

Tekijä:	Tero Ripattila
Otsikko:	Organisaatioiden riskien hallinta ja toimintakyvyn varmistaminen: Liiketoimintakonsepti red teamingista
Sivumäärä:	43 sivua
Aika:	28.4.2026
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tuotantotalouden tutkinto-ohjelma
Ammatillinen pääaine:	Tuotantotalous
Ohjaaja:	Ohjaaja/vastuuarvioija Jarmo Toivanen

Tämän päivän nopeasti muuttuvissa toimintaympäristöissä organisaatioiden riskienhallinnan merkitys korostuu. Red teaming auttaa organisaatioita tunnistamaan haavoittuvuuksia ja testaamaan reagointikykyään simuloimalla todellisten uhkatoimijoiden menetelmiä.

Tämän insinöörityön tavoitteena oli muodostaa liiketoimintakonsepti kyberturvallisuus- ja riskiarviointipalveluita tarjoavalle case-yritykselle. Työ eteni nykytila-analyysistä kirjallisuuskatsauksen kautta liiketoimintakonseptiin, jonka toteuttamiskelpoisuutta arvioitiin markkinatilannetta, teoreettisia viitekehyksiä ja tekijän toimialakokemusta vasten.

Nykytila-analyysi osoitti, että EU:n sääntely-ympäristö, erityisesti DORA, NIS2 ja TIBER-EU, luo rakenteellista kysyntää kyberturvallisuuden testauspalveluille. Markkinalla tunnistettiin kaksi kilpailematonta aluetta: strateginen red teaming ja PK-sektori. Kirjallisuuskatsaus tarjosi teoreettiset viitekehykset liiketoimintakonseptin rakentamiseen.

Liiketoimintakonsepti muodostettiin Galbraithin (2002) tähtimallin mukaisesti, ja se kattaa strategian, palvelumallin, rakenteet, prosessit ja osaamisen. Case-yrityksen erottautumisstrategia perustuu Porterin (1985) erottautumismalliin kolmiportaisella palvelutarjonnalla.

Työn keskeisiä löydöksiä ovat auditointikelpoisuus kilpailuetuna ja palveluntarjoajan riippumattomuus palvelun arvona. Yritysryhmän sovelluskehitys- ja pilviosaaminen mahdollistaa korjauskapasiteetin, joka erottaa case-yrityksen pelkästä testauksesta. Tekoäly nähdään sekä uhkakenttää muuttavana voimana että palvelumallin mahdollistajana. Joidenkin liiketoimintasuunnitelman osien, kuten markkinointisuunnitelman ja kustannusarvion, todettiin soveltuvan toteutettaviksi vasta käynnistämispäätöksen jälkeen.

Avainsanat: Riskien hallinta, Tietoturva, Red teaming, Liiketoimintakonsepti

---

Abstract

Author:	Tero Ripattila
Title:	Managing organizational risks and ensuring operational capability: A business concept for red teaming
Number of Pages:	43 pages
Date:	28 April 2026
Degree:	Insinööri (AMK), Bachelor of Engineering
Degree Programme:	Degree Programme in Industrial Management
Professional Major:	Industrial Engineering and Management
Supervisor:	Jarmo Toivanen, Senior Lecturer

In today's rapidly evolving operating environments, organizational risk management is increasingly critical. Red teaming helps organizations identify vulnerabilities and test their response capabilities by simulating the methods of real threat actors.

The objective of this thesis was to develop a business concept for a case company offering cybersecurity and risk assessment services. The work progressed from an industry analysis through a literature review to a business concept, whose feasibility was assessed against market conditions, theoretical frameworks, and the author's industry experience.

The industry analysis demonstrated that the EU regulatory environment, particularly DORA, NIS2, and TIBER-EU, creates structural demand for cybersecurity testing services. Two uncontested market areas were identified: strategic red teaming and the SME sector. The literature review provided the theoretical frameworks for constructing the business concept.

The business concept was structured according to Galbraith's (2002) Star Model, covering strategy, service model, structures, processes, and competencies. The case company's differentiation strategy is based on Porter's (1985) differentiation model with a three-tier service offering.

Key findings include audit readiness as a competitive advantage and service provider independence as a core value. The business group's software development and cloud expertise enables remediation capacity that differentiates the case company from pure testing providers. Artificial intelligence is identified both as a force reshaping the threat landscape and as an enabler of scalable service models. Certain elements of the business plan, such as the marketing plan and cost estimate, were found to be more appropriately implemented after the decision to launch.

Keywords: Risk management, Cybersecurity, Red teaming, Business concept

Sisällys

Lyhenteet ja käsitteet

ATT&CK: Adversarial Tactics, Techniques and Common Knowledge. Hyökkäystekniikoiden ja -taktiikoiden tietokanta (MITRE).

Blue team: Puolustava tiimi, joka vastaa organisaation tietoturvan ylläpidosta.

BMC: Business Model Canvas. Liiketoimintamallin visuaalinen viitekehys.

CRA: Cyber Resilience Act. Kyberturvallisuusasetus. EU:n asetus digitaalisten tuotteiden turvallisuudesta.

CREST: Council of Registered Ethical Security Testers. Kansainvälinen tietoturvatestauksen sertifiointielin.

CSF: Cybersecurity Framework. Kyberturvallisuusviitekehys (NIST).

DORA: Digital Operational Resilience Act. Digitaalisen toimintavarmuuden asetus. EU:n asetus finanssialan kyberturvallisuudesta.

EBA: European Banking Authority. Euroopan pankkisektoria valvova viranomaistaho.

ECB: European Central Bank. Euroopan keskuspankki.

Elicitation: Social engineering -menetelmä, jossa tietoa hankitaan yksilön sitä itse huomaamatta.

GDPR: General Data Protection Regulation. Yleinen tietosuoja-asetus.

GRC: Governance, Risk and Compliance. Hallinto, riskienhallinta ja vaatimustenmukaisuus.

ISMS: Information Security Management System. Tietoturvallisuuden hallintajärjestelmä.

ISO/IEC 27001: Tietoturvallisuuden hallintajärjestelmän (ISMS) standardi.

ISO/IEC 27002: Tietoturvan hallintakeinojen standardi.

ISO 9001:2015: Laadunhallinnan standardi.

NIST: National Institute of Standards and Technology. Yhdysvaltain kansallinen standardi- ja teknologiainstituutti.

NIS2: The Directive on Security of Network and Information Systems. Euroopan Unionin uusi kyberturvallisuusdirektiivi.

OSCP: Offensive Security Certified Professional certification, PEN-200. Tunkeutumistestauksen kurssi ja sertifikaatti.

OSEP: OffSec Experienced Penetration Tester certification, PEN-300. Edistynyt tunkeutumistestauksen kurssi ja sertifikaatti.

OSINT: Open Source Intelligence. Avoimista lähteistä kerättävä tiedustelutieto.

PropTech Property Technology. Kiinteistöalan digitaalisia ratkaisuja ja palveluita.

Purple team: Yhteistoimintamalli, jossa red team ja blue team työskentelevät yhdessä puolustuksen kehittämiseksi.

Red teaming: Turvallisuustestauksen menetelmä, jossa pyritään löytämään organisaation heikkoudet ja reagointitavat simuloimalla oikean hyökkääjän toimintaa.

Red team: Hyökkäävä tiimi, joka simuloi todellisen uhkatoimijan menetelmiä.

ROE: Rules of Engagement. Toimintasäännöt. Testauksen rajat ja valtuudet määrittelevä sopimus.

Social engineering: Sosiaalinen manipulointi.

SWOT: Strengths, weaknesses, opportunities, threats. Vahvuudet, heikkoudet, mahdollisuudet ja uhat.

TIBER-EU: European framework for Threat Intelligence-Based Ethical Red teaming. EU:n uhkatietopohjaisen testauksen viitekehys.

TLPT: Threat-Led Penetration Testing. DORA:n mukainen uhkavetoinen tunkeutumistestaus.

White team: Toimii puolueettomana välittäjänä ja koordinaattorina punaisen ja sinisen joukkueen välillä harjoitusten aikana. Laatii toimintasäännöt, valvoo turvallisuutta, varmistaa, ettei simulointi häiritse toimintaa, ja järjestää harjoituksen jälkeisen arvioinnin.

1 Johdanto

1.1 Taustoitus

Tämän päivän nopeasti muuttuvissa toimintaympäristöissä organisaatioiden kyky tunnistaa ja hallita riskejä korostuu. Geopoliittiset jännitteet, toimitusketjujen häiriöt ja kasvavat kyberuhat edellyttävät yrityksiltä ennakoivaa varautumista. World Economic Forumin mukaan geopoliittiset tekijät ovat nousseet tärkeimmäksi kyberriskien hallintaan vaikuttavaksi tekijäksi: 64 prosenttia organisaatioista huomioi geopoliittisesti motivoituneet kyberhyökkäykset riskienhallintastrategioissaan. Toimitusketjujen haavoittuvuudet huolestuttavat 65 prosenttia suurista yrityksistä ja 87 prosenttia tunnistaa tekoälyyn liittyvät haavoittuvuudet nopeimmin kasvavaksi kyberriskiksi (World Economic Forum 2026). Euroopan unioni pyrkii samanaikaisesti vahvistamaan digitaalista strategista autonomiaansa vähentämällä riippuvuutta unionin ulkopuolisista teknologia- ja palveluntarjoajista, mikä luo kysyntää eurooppalaisille kyberturvallisuuspalveluille (European Commission 2026). Sääntelykehikot kuten rahoitussektorin toimintavarmuuslaki DORA, kyberturvallisuusdirektiivi NIS2 ja digitaalisten tuotteiden turvallisuutta koskeva Cyber Resilience Act asettavat organisaatioille aiempaa tiukempia vaatimuksia toimintakyvyn varmistamiseksi. DORA on ollut täysimääräisesti voimassa tammikuusta 2025, ja NIS2:n kansallinen toimeenpano etenee jäsenvaltioissa vuoden 2026 aikana. Yli 160 tuhatta EU-organisaatiota kuuluu uuden sääntelyn piiriin. Samaan aikaan tekoälyn nopea kehitys muuttaa sekä uhkakenttää että puolustuksen työkaluja, mikä asettaa palveluntarjoajille uudenlaisia kyvykkyysvaatimuksia.

Tämän insinöörityön tarkoituksena on laatia liiketoimintakonsepti red teaming -palvelun toteuttamiseksi case-yritykselle. Case-yritys on osa yritysryhmää, johon kuuluu useita alkuvaiheen yrityksiä. Yritysryhmän muu liiketoiminta kattaa sovelluskehityksen ja arkkitehtuurikonsultoinnin, hallitun pilvi-infrastruktuurin sekä avoimen lähdekoodin liiketoimintaohjelmistot eurooppalaisena vaihtoehtona suurten teknologiayritysten palveluille ja vuokra-asumiseen suunnatun

kiinteistöteknologian (PropTech) alustan. Yritysryhmän muiden yritysten liiketoiminta synnyttää sisäisen tarpeen kyberturvallisuuden testauspalveluille ja strategiselle sparraukselle.

Yritysryhmän rakenne on suunniteltu siten, että yritykset hyödyntävät toistensa palveluita osana perusliiketoimintaansa. Alustapalvelut tuottavat infrastruktuurin, sovelluskehitysosaaminen tukee digitaalista kehitystä ja kyberturvallisuuspalvelut varmistavat muiden yritysten tietoturvan tason. Tämä synergia tarjoaa case-yritykselle luonnollisen asiakaskunnan ja mahdollisuuden kehittää palvelukonseptia aidossa liiketoimintaympäristössä. Palveluita tarjotaan alusta lähtien myös yritysryhmän ulkopuolisille asiakkaille.

Case-yritystä ei ole tämän insinöörityön aloitushetkellä vielä perustettu, vaan työ toimii esiselvityksenä sen liiketoimintakonseptin muodostamiseksi. Konseptin muodostaminen ennen yrityksen perustamista mahdollistaa markkinapotentiaalin ja palvelumallin kriittisen tarkastelun ennen merkittävien resurssien sitomista.

Kyberturvallisuuden testauspalvelut kattavat laajan kirjon toimintamalleja: hyökkääjän roolissa toimivan red teamingin, puolustavan blue teamingin, näiden yhteistoimintaa edustavan purple teamingin sekä yksittäisten järjestelmien haavoittuvuuksiin keskittyvän penetraatiotestauksen. Red teaming ei kuitenkaan rajoitu pelkästään tekniseen tietoturvan testaukseen – sillä tarkoitetaan myös organisaation strategian, päätöksenteon ja toimintamallien haastamista ulkopuolisen näkökulmasta ilman sisäisiä ennakkoasenteita tai hierarkian asettamia rajoitteita. Tässä insinöörityössä keskitytään red teamingiin sen laajemmassa merkityksessä: sekä kyberturvallisuuden testauksena että strategisena työkaluna. Laajemman palveluvalikoiman kehittäminen tunnistetaan jatkotoimenpiteenä mutta rajataan tämän työn ulkopuolelle. Rajaus mahdollistaa syvällisemmän tarkastelun yhdestä palvelukonseptista ja sen liiketoimintaedellytyksistä.

1.2 Yleiskuva red teamingistä

Red teaming on menetelmä, jossa organisaation tietoturvaa, strategiaa tai toimintamalleja testataan simuloimalla todellisen vastustajan toimintaa. Zenkon (2015) mukaan red teaming on jäsennelty prosessi, jonka tavoitteena on ymmärtää paremmin organisaation tai sen kilpailijan kyvykkyyksiä, aikomuksia ja intressejä simulaatioiden, haavoittuvuustutkimusten ja vaihtoehtoisten analyysien avulla. Käsite on peräisin Yhdysvaltain asevoimista, jossa red team edusti harjoituksissa vastustajan roolia. Red team ei tee päätöksiä organisaation puolesta — se tuottaa tietoa ja suosituksia, joiden pohjalta päätöksentekijät voivat toimia.

Kyberturvallisuudessa red teaming eroaa penetraatiotestauksesta laajuudeltaan: siinä missä penetraatiotestaus keskittyy yksittäisten järjestelmien teknisiin haavoittuvuuksiin, red teaming arvioi organisaation kokonaisvaltaista kykyä havaita, reagoida ja toipua hyökkäyksistä. Luvussa 1.1 kuvatut sääntelykehikot — erityisesti DORA:n edellyttämä TLPT-testaus (Threat-Led Penetration Testing, uhkalähtöinen tunkeutumistestaus) ja TIBER-EU-viitekehys — velvoittavat valtaosaa EU-alueen organisaatioista tilaamaan red teaming -palveluita. Sääntelyvelvoitteiden lisäksi kasvava osa organisaatioista hakeutuu red teaming -palveluiden piiriin vapaaehtoisesti kehittääkseen valmiuksiaan ennakoivasti.

1.3 Tämän työn sisältö

Insinöörityö etenee empiirisestä nykytila-analyysistä teoreettisen kirjallisuuskatsauksen kautta liiketoimintakonseptin muodostamiseen ja sen toteuttamiskelpoisuuden arviointiin. Rakenne varmistaa, että liiketoimintakonsepti perustuu sekä markkinan tuntemiseen että tunnustettuihin teoreettisiin viitekehyksiin.

Luvussa 2 kuvataan työn vaiheet ja tiedonkeruun menetelmät. Luvussa 3 analysoidaan kyberturvallisuus- ja riskiarviointitoimialan nykytilaa: kilpailijoita, asiakastarpeita, kumppaneita ja kanavia sekä toimialan murrosta. Luku päättyy SWOT-analyysiin, joka tiivistää case-yrityksen aseman toimialalla. Luvussa 4

tarkastellaan kilpailullisia prioriteetteja, riskienhallintaa, red teaming -menetelmiä, laatujärjestelmiä sekä lakisääteisiä vaatimuksia hyödyntäen muun muassa McGahanin (2004), Hoffmanin (2017) ja Zenkon (2015) viitekehyksiä. Luvussa 5 muodostetaan liiketoimintakonsepti Galbraithin (2002) tähtimallin mukaisesti ja palvelumalli jäsennetään Osterwalderin ym. (2010) Business Model Canvasilla. Luvussa 6 arvioidaan konseptin toteuttamiskelpoisuutta, tekoälyn vaikutusta palvelumalliin sekä määritetään jatkotoimenpiteet. Luvussa 7 kootaan työn tulokset ja tarkastellaan niiden hyödynnettävyyttä.

2 Projektisuunnitelma

Tässä luvussa kuvataan insinöörityön eteneminen ja tiedonkeruun menetelmät. Projektisuunnitelma jäsentää työn vaiheet loogiseen järjestykseen ja auttaa lukijaa hahmottamaan, miten liiketoimintakonseptiin on päädytty.

2.1 Projektin vaiheet

Kuvassa 1 esitetään insinöörityön vaiheet ja niiden tuotokset.

Kuva 1 Projektin vaiheet

Insinöörityö etenee kolmessa päävaiheessa. Ensimmäisessä vaiheessa muodostetaan nykytila-analyysi toimintaympäristöstä. Tässä vaiheessa kartoitetaan kyberturvallisuusalan kilpailukenttä Suomessa ja Pohjoismaissa, tunnistetaan asiakastarpeet ja analysoidaan toimialan murrosta. Nykytila-analyysin aineistona käytetään julkisia lähteitä, kuten yritysten verkkosivuja, toimialaraportteja ja sääntelydokumentaatiota.

Toisessa vaiheessa muodostetaan kirjallisuuskatsaus, joka luo teoreettisen perustan liiketoimintakonseptille. Kirjallisuuskatsaus käsittelee toimitusketjujen riskienhallintaa, laatujärjestelmiä ja sertifiointeja sekä lakisääteisiä vaatimuksia, jotka määrittävät red teaming -palveluiden kysyntää ja sisältövaatimuksia.

Kolmannessa vaiheessa muodostetaan liiketoimintakonsepti nykytila-analyysin ja kirjallisuuskatsauksen pohjalta. Liiketoimintakonseptia arvioidaan case-yrityksen edustajien kanssa ja saadun palautteen perusteella ehdotusta tarkennetaan. Lopputuloksena syntyy arvio red teaming -palvelun liiketoimintaedellytyksistä ja ehdotus sen toteuttamiseksi.

2.2 Tiedonkeruusuunnitelma

Taulukko 1 kuvaa tiedonkeruusuunnitelman rakenteen.

Taulukko 1 Tiedonkeruusuunnitelma

	Sisältö	**Lähde**	**Avain-henkilö**	**Ajoi-tus**	**Tuotos**
Data 1	Nykytila-analyysi: toimintaympäristö, asiakkaat, kilpailijat, toimialan murros	Toimialaraportit, verkkosivut, sääntely-dokumentaatio	Toimitus-johtaja	Helmi-kuu	Yhteenveto kilpailukentästä, asiakastarpeista ja toimialan murroksesta
Data 2	Liiketoiminta-konseptin	Kirjallisuus-tutkimus,	Toimitus-johtaja	Maa-liskuu	Liiketoimin-takonsepti

	Sisältö	Lähde	Avain-henkilö	Ajoi-tus	Tuotos
	muodostami-neni	nykytila-ana-lyysi			
Data 3	Liiketoiminta-konseptin ar-viointi	Liiketoiminta-konseptin ar-viointi mark-kinadataa, teoriaa ja toi-mialakoke-musta vasten	Toimitus-johtaja	Huhti-kuu	Arvioitu lii-ketoiminta-konsepti ja jatkotoimen-piteet

Data 1 muodostaa pohjan toimintaympäristön ymmärtämiselle. Aineisto koostuu julkisista lähteistä: kilpailijoiden verkkosivuista, toimialaraporteista sekä EU-tason sääntelydokumentaatiosta, kuten DORA:sta, NIS2:sta ja TIBER-EU:sta. Lisäksi hyödynnetään case-yrityksen toimitusjohtajan toimialatuntemusta.

Data 2 rakentuu nykytila-analyysin ja kirjallisuuskatsauksen pohjalta. Liiketoimintakonsepti muodostetaan yhdistämällä toimialan kilpailutilanne, asiakastarpeet ja teoreettinen viitekehys liiketoimintakonseptiksi.

Data 3 kerätään case-yrityksen edustajien palautteella liiketoimintakonseptista. Palautteen pohjalta ehdotusta tarkennetaan ja muodostetaan lopulliset jatkotoimenpiteet.

3 Toimialan nykytilan analyysi

3.1 Kilpailijat

Kilpailija-analyysi rajataan toimijoihin, jotka tarjoavat red teaming-, penetraatiotestaus- tai TLPT-palveluita Suomessa tai Pohjoismaissa. Puhtaasti tuotemyyntiin keskittyvät yritykset sekä Pohjoismaiden ulkopuolella toimivat yritykset rajataan tarkastelun ulkopuolelle.

Suomen kyberturvallisuusmarkkinan arvo oli noin 348 miljoonaa dollaria vuonna 2025, ja sen ennustetaan kasvavan 488 miljoonaan dollariin vuoteen 2030

mennessä (Mordor Intelligence 2026). Kasvua vauhdittavat DORA- ja NIS2-sääntelykehikkojen voimaantulo, NATO-jäsenyyden tuomat investoinnit kriittisen infrastruktuurin suojaamiseen sekä yleinen kyberuhkien kasvu. Red teaming ja TLPT-testaus ovat markkinan nopeimmin kasvavia segmenttejä sääntelyvelvoitteiden myötä.

Taulukossa 2 esitetään tunnistetut suorat kilpailijat, jotka tarjoavat red teaming- tai TLPT-palveluita samalle kohderyhmälle kuin case-yritys.

Taulukko 2 Kilpailijat

Yritys	**Kotimaa**	**Erityisvahvuus**	**TIBER/TLPT**
2NS	Suomi	Red teaming, OSINT, TIBER-FI-kokemus	Kyllä
Fraktal	Suomi	50+ red teaming -toimeksiantoa, TIBER-FI	Kyllä
DNV Cyber (ent. Nixu)	Norja/Suomi	500+ asiantuntijaa, laaja palveluvalikoima	Kyllä
Truesec	Ruotsi/Suomi	300+ asiantuntijaa, Banshie-yrityskauppa 2025	Kyllä
Reversec (ent. WithSecure)	Ruotsi/Suomi	F-Secure/WithSecure-perintö, offensiivinen focus	Kyllä
Mint Security	Suomi	ISO 27001 -sertifioitu, laaja testausvalikoima	Ei
65Security	Suomi	Viranomais- ja oikeussektori	Ei
Advisense	Norja	TIBER/TLPT-erikoistuminen, finanssisektori	Kyllä

Suorien kilpailijoiden lisäksi markkinalla toimii epäsuoria kilpailijoita, joiden palveluvalikoima on osittain päällekkäinen mutta joiden painopiste on eri. Näihin kuuluvat suuret teleoperaattorit kuten Elisa, joka tarjoaa red teaming -palveluita osana laajempaa hallittujen tietoturvapalveluiden kokonaisuutta sekä Big Four -konsulttitalot kuten PwC ja Deloitte, joiden vahvuus on kokonaisvaltaisessa

GRC- ja vaatimustenmukaisuuskonsultoinnissa. IT-palveluyritykset kuten Digia ja NetNordic tunnistavat asiakkaidensa tietoturvatarpeita mutta eivät itse toteuta offensiivista testausta, mikä tekee niistä potentiaalisia kanavakumppaneita.

Markkinalla on käynnissä voimakas konsolidaatio: Nixu yhdistyi DNV Cyberiksi vuonna 2023, WithSecure Consultingin offensiivinen yksikkö irtautui Reverseciksi vuonna 2025, ja Truesec osti Banshie-nimisen red teaming -yrityksen vuonna 2025. Konsolidaatio kasvattaa suurten toimijoiden kapasiteettia mutta jättää tilaa erikoistuneille toimijoille, jotka pystyvät palvelemaan ketterämmin.

DORA:n TLPT-vaatimus astui voimaan heinäkuussa 2025, ja Suomen Pankin TIBER-FI 2.0 -ohjeistus päivitettiin maaliskuussa 2025. Todellisia TIBER-FI-kokemusta omaavia palveluntarjoajia on Suomessa tällä hetkellä alle kymmenen. Kysynnän ja tarjonnan epäsuhta luo markkinamahdollisuuden uusille toimijoille etenkin pienempien finanssialan organisaatioiden, kuten maksupalveluyritysten ja fintech-yhtiöiden, segmentissä.

3.2 Asiakastarve

Red teaming -palveluiden kysyntä jakautuu kahteen pääryhmään. Ensimmäisen ryhmän muodostavat organisaatiot, joita sääntely velvoittaa tilaamaan testausta. DORA edellyttää finanssialan merkittäviltä toimijoilta TLPT-testausta vähintään kolmen vuoden välein, ja NIS2-direktiivin piiriin kuuluvien organisaatioiden on osoitettava kyberresilienssi säännöllisillä arvioinneilla. Näille asiakkaille red teaming on vaatimustenmukaisuuden edellytys.

Toisen ryhmän muodostavat organisaatiot, jotka hakeutuvat palvelun piiriin vapaaehtoisesti kehittääkseen valmiuksiaan. Näiden asiakkaiden motivaationa on tyypillisesti liiketoiminnan jatkuvuuden varmistaminen, strategisen päätöksenteon haastaminen ulkopuolisella näkökulmalla tai henkilöstön reagointikyvyn testaaminen. Vapaaehtoisille asiakkaille red teaming on kilpailuetu ja riskienhallinnan työkalu.

Asiakastarpeet vaihtelevat organisaation koon mukaan. Suuryrityksillä ja finanssisektorin toimijoilla on tyypillisesti omat tietoturvatiimit ja selkeät vaatimukset TLPT-testaukselle. Keskisuuret yritykset tarvitsevat usein kokonaisvaltaisempaa neuvontaa, jossa testauksen lisäksi arvioidaan prosessit ja toimintamallit. Pk-yrityksissä kyberturvallisuustestaus on usein kokonaan ulkoistettu, ja palvelun pitää olla tuotteistettu ja kustannuksiltaan saavutettava.

3.3 Kumppanit ja kanavat

Case-yrityksen markkinoille pääsyn kannalta kanavakumppanit ovat tärkeässä roolissa, koska uuden toimijan on vaikea tavoittaa asiakkaita pelkällä omalla myynnillä. Tunnistetut kanavat jakautuvat kolmeen ryhmään.

Kyberturvallisuuden konsulttivälitysalustat, kuten CyberDo, yhdistävät asiantuntijat ja asiakasorganisaatiot. Välitysalustat tarjoavat case-yritykselle näkyvyyttä ja pääsyn asiakkuuksiin ilman suurta markkinointibudjettia. Rekisteröityminen TLPT- ja red teaming -osaajana on matalan kynnyksen toimenpide.

IT-palveluyritykset, kuten Digia, tunnistavat asiakkaidensa tietoturvatarpeita mutta eivät itse toteuta offensiivista testausta. Alihankintamalli, jossa IT-palveluyritys myy ja case-yritys toteuttaa, hyödyttää molempia osapuolia.

Kolmantena kanavana toimivat julkiset kilpailutukset, joiden kautta erityisesti julkishallinnon ja hyvinvointialueiden kyberturvallisuushankinnat toteutuvat.

Kanavien hyödyntäminen edellyttää case-yritykseltä tunnustettua osaamista, kuten toimialan sertifiointeja. Näitä käsitellään tarkemmin luvuissa 4.4 ja 5.4.

3.4 Toimialan murros

Luvuissa 1.1 ja 3 kuvatut kehityskulut muuttavat kyberturvallisuusalan kilpailudynamiikkaa. Sääntelyn laajeneminen, markkinan konsolidoituminen ja osaajapula luovat paineita vakiintuneille toimijoille, kun taas tekoälyn nopea kehitys

muuttaa sekä uhkakenttää että palvelutuotannon työkaluja. AI-avusteiset hyökkäystyökalut kasvattavat puolustavien palveluiden kysyntää, ja samalla tekoälyn hyödyntäminen omassa palvelutuotannossa mahdollistaa pienemmille toimijoille skaalautumisen, joka on aiemmin edellyttänyt suurta asiantuntijakapasiteettia.

Uusille toimijoille avautuu mahdollisuuksia erilaisissa segmenteissä, joissa suuret konsolidoituneet yritykset eivät pysty tai halua palvella kustannustehokkaasti: pienemmät finanssialan toimijat, NIS2-velvoitteiset keskisuuret yritykset ja organisaatiot, jotka tarvitsevat strategista red teamingia teknisen testauksen lisäksi. Muutos suosii toimijoita, jotka rakentavat palvelumallinsa tekoälyn varaan alusta alkaen.

Toimialan muutoksen luonnetta analysoidaan tarkemmin luvussa 4 McGahanin (2004) muutospolkujen kehyksellä. Tekoälyn vaikutusta case-yrityksen palvelumalliin tarkastellaan syvemmin luvussa 5.5.

3.5 Avainlöydökset toimialan nykytilan analyysissä

Taulukossa 3 esitetään SWOT-analyysi case-yrityksen asemasta toimialalla.

Taulukko 3 SWOT-analyysi

	Positiivinen	*Negatiivinen*
Sisäinen	**Vahvuudet** - Yritysryhmän sisäinen asiakaskunta - Tekninen osaaminen ja toimialatuntemus - Ketterä organisaatio ilman legacy-rasitteita - Yritysryhmän sovelluskehitys- ja pilviosaaminen → korjauskapasiteetti	**Heikkoudet** - Ei vielä red teaming -sertifiointeja - Pieni tiimi, rajallinen kapasiteetti - Tunnettuuden puute markkinalla
Ulkoinen	**Mahdollisuudet**	**Uhat**

	Positiivinen	*Negatiivinen*
	- DORA/NIS2 luovat pakollista kysyntää - PK-sektori alipalveltu segmentti - Strateginen red teaming tyhjä markkina Suomessa - Kanavakumppanit (CyberDo, Digia) madaltavat markkinoille pääsyä - Tekoäly tehostaa red teaming -palveluiden tuotantoa ja skaalautuvuutta	- Konsolidoituneet suuret kilpailijat (DNV Cyber, Truesec) - Hintakilpailu erityisesti perustason testauksessa - Osaajapula vaikeuttaa kasvua - Big Four -yritysten laajentuminen segmenttiin - Tekoälyavusteisten hyökkäystyökalujen yleistyminen madaltaa kynnystä ja kiristää kilpailua

Nykytila-analyysin keskeisin havainto on, että red teaming -markkinalla on samanaikaisesti sekä kova kilpailu vakiintuneissa segmenteissä että merkittäviä aukkoja. Suuret toimijat keskittyvät suuryrityksiin ja finanssisektoriin, minkä seurauksena PK-sektorin tuotteistetut palvelut ja strateginen red teaming ovat jääneet katveeseen. DORA- ja NIS2-sääntely laajentaa kohdemarkkinaa nopeasti, mutta todellisia TIBER-FI-kokemusta omaavia palveluntarjoajia on Suomessa alle kymmenen. Nämä havainnot ohjaavat liiketoimintakonseptin muodostamista luvussa 5.

4 Kirjallisuuskatsaus

Edellisessä luvussa kartoitettiin toimialan nykytila: kilpailijat, asiakastarpeet ja markkinan murros. Nykytila-analyysin pohjalta tässä luvussa muodostetaan teoreettinen perusta liiketoimintakonseptille tarkastelemalla kilpailun dynamiikkaa, riskienhallintaa, red teaming -menetelmiä, laatujärjestelmiä sekä lakisääteisiä vaatimuksia.

4.1 Kilpailulliset prioriteetit

Kaksi teoreettista kehystä auttaa hahmottamaan red teaming -palvelumarkkinan kilpailudynamiikkaa: toimialan muutospolkuja ja sinisen meren strategiaa.

Kumpikin kehys valottaa eri näkökulmasta, millaisia strategisia valintoja alalle tuleva yritys kohtaa.

4.1.1 Toimialan muutospolut

McGahan (2004) kehittää Porterin (1985) kilpailuanalyysiä eteenpäin tarkastelemalla, miten kokonaiset toimialat muuttuvat — ei vain yksittäisten yritysten asemaa toimialan sisällä. Hän esittää neljä toimialan muutospolkua sen perusteella, miten alan ydinresurssit ja ydinaktiviteetit muuttuvat. Progressive-muutoksessa (43 % tutkituista toimialoista) sekä resurssit että aktiviteetit kehittyvät asteittain. Creative-muutoksessa (6 %) molemmat korvautuvat uusilla. Radical-muutoksessa (19 %) sekä resurssit että aktiviteetit menettävät arvonsa samanaikaisesti. Intermediating-muutoksessa (32 %) ydinresurssit säilyttävät arvonsa, mutta ydinaktiviteetit — eli tapa, jolla arvo toimitetaan asiakkaalle — muuttuvat perusteellisesti.

Kyberturvallisuus- ja riskiarviointitoimiala noudattaa intermediating-muutospolkua. Ydinresurssit eli asiantuntijoiden osaaminen, sertifioinnit ja menetelmätieto säilyttävät arvonsa. Sen sijaan ydinaktiviteetit muuttuvat olennaisesti: DORA:n ja TIBER-EU:n kaltaiset sääntelykehikot ohjaavat palvelumallin siirtymistä kertaluonteisista toimeksiannoista jatkuvaksi, sääntelyohjatuksi kumppanuudeksi. McGahanin mukaan intermediating-muutoksessa paine kasvaa, kunnes asiakassuhteet muuttuvat äkillisesti. Menestyjiä ovat ne, jotka löytävät epätavanomaisia tapoja hyödyntää ydinresurssejaan uudessa toimintamallissa.

Luvussa 3.1 kuvattu markkinan konsolidoituminen tukee tätä tulkintaa: Nixun siirtyminen DNV:n omistukseen, WithSecuren offensiivisen liiketoiminnan eriytyminen Reverseciksi ja Truesecin laajentuminen Pohjoismaissa ovat kaikki esimerkkejä siitä, miten vakiintuneet toimijat järjestävät palvelumallejaan uudelleen vastauksena muuttuviin ydinaktiviteetteihin.

4.1.2 Sinisen meren strategia

Kim ja Mauborgne (2004) erottavat toisistaan punaiset ja siniset valtameret. Punaisella valtamerellä kilpaillaan vakiintuneilla markkinoilla tunnetuin säännöin, kun taas sinisellä valtamerellä luodaan kokonaan uusia markkinoita, joissa kilpailua ei vielä ole. Sinisen meren luominen ei edellytä täysin uutta innovaatiota — usein riittää, että olemassa olevia tekijöitä nostetaan, poistetaan, vähennetään tai luodaan uudelleen.

Red teaming -markkinalla tämä jaottelu näkyy selkeästi. Perinteinen kyberturvallisuuden penetraatiotestaus suuryrityksille on punainen valtameri: vakiintuneet toimijat kilpailevat samoista asiakkaista samanlaisilla palveluilla. Luvussa 3.1 tunnistettiin kahdeksan suoraa kilpailijaa, jotka kaikki tarjoavat teknistä tunkeutumis- ja red teaming -testausta pääasiassa suurille organisaatioille.

Sinisiä valtameriä sen sijaan avautuu kahdella alueella. Ensimmäinen on strateginen red teaming, jossa organisaation päätöksentekoa, liiketoimintastrategiaa ja toimintamalleja haastetaan ilman kyberturvallisuuskontekstia. Luvussa 3.2 todettiin, että organisaatiot tarvitsevat ulkopuolista haastamista strategisissa valinnoissaan, mutta yksikään luvussa 3.1 kuvatuista kilpailijoista ei tarjoa tätä palvelua. Toinen sininen valtameri on PK-sektorin kyberturvallisuustestaus. Luvussa 3.2 kuvattiin, miten NIS2-sääntely laajentaa velvoitteet yli 160 000 EU-organisaatioon, mutta nykyiset palveluntarjoajat ovat hinnoitelleet itsensä pois PK-markkinalta.

Kim ja Mauborgnen (2004) nelikenttää soveltaen case-yrityksen strategia voidaan jäsentää seuraavasti:

- Nosta: Strategisen tason palvelut, jotka yhdistävät kyberturvallisuuden liiketoimintariskien arviointiin.
- Poista: Raskaat konsultointirakenteet ja pitkät myyntisyklit, jotka tekevät palvelusta saavuttamattoman Pk-yrityksille.
- Vähennä: Riippuvuutta yksittäisten asiantuntijoiden henkilökohtaisesta myyntityöstä keskittymällä skaalautuviin palvelumalleihin ja kumppanuuskanaviin.

- Luo: Modulaarinen palvelukonsepti, joka skaalautuu asiakkaan kypsyystason ja budjetin mukaan.

Molemmat kehykset, McGahanin muutospolut ja sinisen meren strategia, osoittavat samaan suuntaan: red teaming -markkinalla on tilaa toimijalle, joka yhdistää olemassa olevan osaamisen uudenlaiseen palvelumalliin ja kohdistaa sen alueille, joita nykyiset toimijat eivät palvele.

4.2 Riskien hallinta

Riskienhallinta muodostaa teoreettisen perustan sille, miksi organisaatiot tarvitsevat red teaming -palveluita. Riskien tunnistamista ja arviointia tarkastellaan Manuj ja Mentzerin (2008) viitekehyksen kautta ja sovelletaan sitä red teaming -palvelun kontekstiin.

Manuj ja Mentzer (2008) esittävät viisivaiheisen riskienhallintamallin: riskien tunnistaminen, arviointi, strategioiden valinta, toteutus ja lieventäminen. Malli korostaa, että tehokas riskienhallinta edellyttää jatkuvaa arviointia ja yhteistyötä organisaation sidosryhmien välillä.

Riski määritellään ei-toivotun seurauksen, kuten vaaran, vahingon tai menetyksen, mahdollisuutena. (Harland; Brenchley; & Walker 2003.)

Mitchellin (1995) mukaan riski koostuu tappion todennäköisyyden ja sen vaikutuksen yhdistelmästä. Riskiarvioinnissa on siten vastattava kysymyksin, mitkä ovat mahdolliset tappiot, kuinka todennäköisiä ne ovat ja mikä on niiden seurausten merkitys.

Manuj ja Mentzer (2008) luokittelevat riskityypit kahdeksaan kategoriaan. Taulukossa 4 esitetään ne riskityypit, jotka ovat erityisen merkityksellisiä red teaming -palvelun kannalta.

Taulukko 4 Red teaming riskienhallinnan työkaluna (mukailtu, Manuj & Mentzer 2008)

Riskityyppi	**Kuvaus**	**Ennakointi**	**Reagoinnin testaus**	**Vaihtoehtoinen analyysi**
Toimintariskit	Ydintoimintojen häiriöt, prosessien epävakaus, teknologian vanhentuminen	Tunnistaa haavoittuvuudet ennen häiriötä	Testaa, havaitseeko organisaatio toiminnan poikkeaman ja kykeneekö se toipumaan	Haastaa oletukset siitä, mitkä prosessit ovat kriittisiä
Turvallisuusriskit	Tietojärjestelmien uhat, sisäpiiririskit, alihankkijoiden heikko tietoturva	Simuloi uhkia hallitusti ja paljastaa puutteet	Mittaa havaitsemiskykyä ja vasteaikaa todenmukaisessa hyökkäystilanteessa	Tuottaa näkemyksen siitä, mitä hyökkääjä todellisuudessa tekisi – ei sitä mitä puolustaja olettaa
Poliittiset riskit	Sääntelyn muutokset, geopoliittiset jännitteet	DORA ja NIS2 muuttavat poliittisen riskin konkreettiseksi velvoitteeksi	Sääntely edellyttää dokumentoitua näyttöä reagointikyvystä (esim. TLPT)	Auttaa arvioimaan, ovatko nykyiset compliance-toimenpiteet riittäviä vai näennäisiä

Red teaming asemoituu riskienhallinnan kentässä ennakoivaksi strategiaksi, mutta sen arvo ulottuu reagoinnin testaamiseen ja vaihtoehtoisten analyysien tuottamiseen. Zenkon (2015) mukaan red teamin tehtävä ei ole tehdä päätöksiä organisaation puolesta, vaan tuottaa tietoa ja vaihtoehtoisia näkemyksiä, joiden pohjalta päätöksentekijät voivat toimia. Tämä kolmiulotteinen rooli — ennakointi, reagoinnin testaus ja vaihtoehtoinen analyysi — tekee red teamingistä laaja-alaisen riskienhallinnan työkalun.

Yrityksen koko vaikuttaa siihen, millaiset riskityypit korostuvat ja miten niihin reagoidaan: suuret organisaatiot rakentavat ennakoivia hallintamalleja, kun taas pienemmillä toimijoilla riskienhallinta on usein reaktiivista ja aktivoituu vasta riskin eskaloituessa. Tämä ero selittää osaltaan, miksi PK-sektorilla red teaming -

palveluiden kysyntä on toistaiseksi ollut vähäistä. Siksi NIS2:n laajentuessa juuri tämä segmentti tarvitsee skaalautuvia palvelumalleja.

4.3 Red teaming -menetelmät

Red teaming -menetelmien tuntemus luo perustan liiketoimintakonseptille — palvelun sisältö, hinnoittelu ja osaamistarpeet rakentuvat käytettävien menetelmien varaan. Hoffmanin (2017) mukaan red teaming rakentuu kahdelle pilarille: devil's advocacylle eli suunnitelmien järjestelmälliselle haastamiselle ja vaihtoehtoiselle analyysille, jossa strukturoitujen menetelmien, kuten pre-mortem-analyysin ja oletusten tarkistuksen, avulla murretaan ryhmäajattelua ja tunnistetaan strategian sokeat pisteet. Hoffman korostaa, että organisaatiot epäonnistuvat harvoin tiedon puutteesta; useammin syynä ovat kognitiiviset vinoumat ja hierarkia, jotka tukahduttavat eriävät näkemykset. Red teaming on siis päätöksenteon tukityökalu — compliance-vaatimuksen täyttäminen on sivutuote, ei tavoite. Zenko (2015) vahvistaa näkemystä: red teamin tehtävä ei ole tehdä päätöksiä organisaation puolesta, vaan tuottaa tietoa ja vaihtoehtoisia näkemyksiä, joiden pohjalta päätöksentekijät voivat toimia.

Red teaming -harjoitus koostuu tyypillisesti kolmesta vaiheesta: tiedustelu ja suunnittelu (reconnaissance), toteutus (execution) sekä raportointi ja oppimisen tukeminen (reporting) (Vaadata 2025). Toteutusvaiheessa hyödynnetään sekä teknisiä menetelmiä — kuten verkkohyökkäyksiä ja järjestelmien tunkeutumistestausta — että ei-teknisiä menetelmiä, kuten social engineeringiä ja fyysistä tunkeutumista. Harjoitusta koordinoi white team, joka toimii puolueettomana välittäjänä, laatii toimintasäännöt ja varmistaa, ettei testaus häiritse organisaation toimintaa.

Seuraavissa alaluvuissa tarkastellaan red teamingin keskeisiä ulottuvuuksia: tiimidynamiikkaa, social engineeringiä ja agenttista red teamingia.

4.3.1 Red team – blue team -psykologia

Red teaming -harjoituksen onnistuminen riippuu teknisten menetelmien lisäksi tiimien välisestä dynamiikasta. Red team toimii hyökkääjän ja blue team puolustajan roolissa. Tiimien välistä yhteistyötä kutsutaan purple teamingiksi.

Red Team toimii ulkoa käsin, usein luovasti sääntöjä rikkoen simuloidakseen todellisia uhkia. Psykologisesti tämä vaatii ei-lineaarista ajattelua, kykyä olla epämukavuusalueella ja haastaa status quo. Hyvä red team -ammattilainen asettuu hyökkääjän asemaan – ei pelkästään teknisesti, vaan myös motivaation ja käyttäytymisen tasolla. Jos red team kokee olevansa älyllisesti ylempänä, se voi johtaa huonoon kommunikaatioon blue teamin kanssa tai ylimielisyyteen, mikä heikentää yhteistyötä ja luottamusta. (Zenko 2015.)

Blue team saattaa kokea red teamin testauksen uhkana omalle osaamiselleen, mikä voi johtaa puolustautumiseen ja vastakkainasetteluun. Onnistunut harjoitus edellyttää psykologista turvallisuutta: löydökset käsitellään oppimismahdollisuuksina, ei epäonnistumisina. Käytännössä tämä tarkoittaa huolellista aikataulutusta, selkeää viestintää ja johdon sitoutumista siihen, ettei tuloksia käytetä syyllistämiseen. (Zenko 2015)

Delizonna (2017) korostaa, että psykologista turvallisuutta voidaan edistää käytännössä: konfliktia lähestytään yhteistyön kautta, syyllistäminen korvataan uteliaisuudella ja palautetta kerätään aktiivisesti. Red teaming -harjoituksissa tämä tarkoittaa, että tulosten läpikäynti suunnitellaan yhtä huolellisesti kuin itse testaus.

4.3.2 Social engineering

Social engineering viittaa hyökkäystapaan, jossa pyritään manipuloimaan ihmisiä paljastamaan luottamuksellista tietoa tai mahdollistamaan pääsy organisaation järjestelmiin tai tiloihin. Social engineering -hyökkäykset kohdistuvat

erityisesti inhimillisiin tekijöihin, kuten työntekijöiden, asiakkaiden tai kumppanien päätöksentekoon ja käyttäytymiseen.

Social engineering on yksi yleisimmistä hyökkäysvektoreista red teaming -harjoituksissa. Sen tehokkuus perustuu siihen, että ihmisten manipulointi on usein helpompaa kuin teknisten järjestelmien murtaminen. Hyvin toteutettu harjoitus voi paljastaa vakavia puutteita organisaation turvallisuuskulttuurissa, käytännöissä ja henkilöstön tietoisuudessa uhista. Sekä Verizonin (2024) tietomurtotapauksia analysoiva DBIR-raportti (Data Breach Investigations Report) että ENISA:n (2024) uhkakatsaus osoittavat social engineeringin olevan yksi yleisimmistä tietomurtojen alkulähteistä.

Näissä hyökkäyksissä hyödynnetään psykologisia vaikuttamistekniikoita, kuten vastavuoroisuutta, auktoriteettiin vetoamista, niukkuutta, miellyttävyyttä, myönnytysten hakemista sekä velvollisuuden tunnetta. (Talamantes 2014)

Yleisimpiä social engineering -tekniikoita ovat:

- Phishing, eli huijausviestit, joiden tarkoitus on saada uhri klikkaamaan haitallisia linkkejä tai paljastamaan kirjautumistietoja.
- Vishing, puhelimen välityksellä tapahtuva huijaus.
- Tailgating, fyysinen pääsy esimerkiksi toimistotiloihin seuraamalla oikeutettua henkilöä sisään.
- Pretexting, eli keksittyjen henkilöllisyyksien tai tilanteiden käyttö tietojen saamiseksi, esimerkiksi esiintymällä IT-tukihenkilönä.
- Elicitation, huomaamaton tiedonhankinta keskustelun keinoin, esimerkiksi imartelun tai luottamuksen rakentamisen avulla.
- Malicious media dropping, kuten haitallisten USB-laitteiden jättäminen löydettäväksi organisaation tiloihin.

Social engineering -hyökkäyksen onnistuminen riippuu ensisijaisesti hyökkääjän valmistautumisesta ja kohdeorganisaation turvallisuuskulttuurista. Huolellinen taustatutkimus tekee hyökkäyksestä uskottavan, kun taas koulutettu ja tietoturvatietoinen henkilöstö tunnistaa manipulointiyritykset todennäköisemmin. Organisaation kyky havaita poikkeamia ja reagoida niihin nopeasti ratkaisee, jääkö hyökkäys yksittäiseksi yritykseksi vai eskaloituuko se tietomurroksi.

4.3.3 Agenttinen red teaming

Perinteisten menetelmien rinnalle on noussut agenttinen red teaming, jossa tekoälypohjaiset agentit suorittavat testaustoimenpiteitä itsenäisesti. Agentti voi kartoittaa hyökkäyspintaa, tunnistaa haavoittuvuuksia ja ketjuttaa niitä kokonaisvaltaisiksi hyökkäyspoluiksi ilman jatkuvaa ihmisohjausta.

Menetelmän metodologinen ero perinteiseen red teamingiin on siinä, että osa kognitiivisesta työstä, erityisesti toistettavat tekniset tehtävät, siirtyy koneen suoritettavaksi. Tämä ei kuitenkaan poista Hoffmanin (2017) kuvaamaa devil's advocacy -ajattelua, koska agentti ei haasta oletuksia samalla tavalla kuin kriittisesti ajatteleva asiantuntija. Agenttisessa lähestymistavassa asiantuntijan rooli muuttuu toteuttajasta ohjaajaksi: testauksen rajaaminen, löydösten tulkinta ja strategisten johtopäätösten muodostaminen säilyvät ihmisen vastuulla.

Agenttisen red teamingin soveltamista case-yrityksen palvelumalliin käsitellään luvussa 5.5.

4.4 Laatujärjestelmät ja sertifioinnit

Kyberturvallisuus- ja riskiarviointipalveluita tarjoavan yrityksen uskottavuus rakentuu tunnustettujen standardien ja viitekehysten hallintaan. Seuraavassa tarkastellaan laatu- ja tietoturvastandardeja sekä niiden suhdetta case-yrityksen palveluihin.

ISO/IEC 27001 on kansainvälinen standardi tietoturvallisuuden hallintajärjestelmälle (ISMS). Se edellyttää organisaatiolta dokumentoitua riskienhallintaa, tietoturvakontrolleja ja jatkuvan parantamisen prosessia. Palveluntarjoajalle ISO 27001 -sertifiointi on sekä laadun osoitus asiakkaalle, että sisäinen kypsyysmittari — palveluntarjoaja, joka testaa muiden turvallisuutta, osoittaa hallitsevansa myös omansa. (Cyberday Oy 2025c)

ISO 9001:2015 määrittää laadunhallintajärjestelmän vaatimukset ja painottaa jatkuvaa parantamista. Case-yritykselle standardi tarjoaa rungon palveluprosessien yhdenmukaistamiseen ja palvelun laadun todentamiseen.

NIST Cybersecurity Framework (CSF) on Yhdysvaltain NIST:n kehittämä viitekehys kyberturvallisuuden parantamiseksi. Vaikka NIST ei ole EU-sääntely, se toimii monissa organisaatioissa täydentävänä viitekehyksenä — erityisesti silloin, kun asiakas edellyttää NIST-yhteensopivaa raportointia.

MITRE ATT&CK on avoimesti saatavilla oleva kehikko, joka kuvaa kyberuhkatoimijoiden taktiikoita, tekniikoita ja menetelmiä (TTP) todellisten hyökkäysten pohjalta. Red teaming -harjoituksissa ATT&CK toimii suunnittelun ja raportoinnin viitekehyksenä: hyökkäysskenaariot rakennetaan tunnettujen TTP-profiilien pohjalta ja löydökset raportoidaan ATT&CK-taksonomiaa käyttäen. MITRE ATT&CK-kehikon suurin vahvuus on sen perustuminen dokumentoituihin hyökkäyksiin: jokainen tekniikka on yhdistetty todellisiin tapauksiin ja uhkatoimijoihin. Tämä tekee kehikosta red teaming -harjoitusten suunnittelun perustyökalun, jossa hyökkäysskenaariot rakentuvat realististen uhkaprofiilien pohjalta sen sijaan, että nojattaisiin teoreettisiin oletuksiin. Taulukossa 5 verrataan ATT&CK- ja TIBER-EU-viitekehyksiä.

Taulukko 5 MITRE ATT&CK- ja TIBER-EU-viitekehysten vertailu

	MITRE ATT&CK	**TIBER-EU**
Tarkoitus	Hyökkääjien TTP-kuvaukset	Uhkatietopohjainen red teaming -testaus
Kohderyhmä	Kaikki organisaatiot	Kriittinen infrastruktuuri ja finanssiala
Sovellusalue	Uhkien tunnistaminen ja puolustuksen kehittäminen	Kokonaisvaltaiset red teaming -harjoitukset
Tuotos	Matriisi puolustuksen suunnitteluun	Testausprosessi ja kypsyysraportti
Ylläpitäjä	MITRE (USA)	Euroopan keskuspankki (ECB)

4.5 Lakisääteiset vaatimukset

EU:n sääntely-ympäristö on muuttunut huomattavasti 2020-luvulla. Tässä alaluvussa tarkastellaan keskeisiä sääntelykehikkoja, jotka luovat kysyntää case-yrityksen palveluille.

DORA (Digital Operational Resilience Act) on EU-asetus, jota on sovellettu täysimääräisesti tammikuusta 2025. EU:ssa on suoritettu yli 100 TIBER-testiä, mikä osoittaa menetelmän vakiintuneen aseman finanssialan tietoturvassa (European Central Bank 2025). DORA yhdenmukaistaa finanssialan toimintavarmuutta koskevat säännöt ja koskee 20 erityyppistä rahoituslaitosta sekä niiden kolmannen osapuolen ICT-palveluntarjoajia. (European Insurance and Occupational Pensions Authority 2025)

NIS2 on kyberturvallisuusdirektiivi, jonka kansallinen toimeenpano etenee jäsenvaltioissa. Suomessa kyberturvallisuuslaki koskee erityisesti keskisuuria ja suurempia toimijoita liikenne-, energia-, terveydenhuolto- ja digitaalisen infrastruktuurin aloilla sekä elintarvike-, kemian- ja jätealoja. CER-direktiivin täytäntöönpano laajentaa soveltamisalaa myös kriittisiksi määriteltyihin pienempiin toimijoihin. (Cyberday Oy 2025d)

Cyber Resilience Act kohdistuu digitaalisiin tuotteisiin ja kytkettyihin laitteisiin edellyttäen turvallista kehitystä, haavoittuvuuksien hallintaa ja elinkaaripäivityksiä.

TLPT (Threat-Led Penetration Testing) on DORA:n myötä kehittyvä testausmenetelmä, jonka erityispiirteenä on uhkatiedon hyödyntäminen testauksen suunnittelussa. EU:n komissio on julkaissut delegoidun asetuksen TLPT:stä, ja käytännön toteutusta kehitetään viranomaisten kanssa. (Cyberday Oy 2025e)

Taulukossa 6 esitetään yhteenveto keskeisistä vaatimuskehikoista.

Taulukko 6 Pakolliset vaatimuskehikot

Vaatimus-kehikko	**Kohde**	**Vaatimukset**
DORA	Finanssiala	ICT-riskienhallinta, poikkeamien luokittelu, palautumisen testaus
TLPT	DORA-sääntelyn alaiset organisaatiot	Uhkatietopohjainen tunkeutumistestaus ja raportointi
NIS2	Kriittinen infrastruktuuri ja digitaaliset palvelut	Riskienhallinta, poikkeamailmoitukset, hallintovastuut
CRA	Digitaaliset tuotteet, kytketyt laitteet	Turvallinen kehitys, haavoittuvuuksien hallinta, elinkaaripäivitykset
GDPR	Kaikki toimialat (henkilötiedot)	Tietojen lainmukainen käsittely, tietosuojavastaava, tietoturvaloukkaukset

4.6 Avainlöydökset kirjallisuuskatsauksessa

Toimiala on intermediating-muutoksessa. McGahanin (2004) viitekehyksen mukaan kyberturvallisuus- ja riskiarviointitoimialan ydinresurssit, asiantuntijaosaaminen ja menetelmätieto säilyttävät arvonsa, mutta palvelumallit muuttuvat perusteellisesti. DORA:n ja TIBER-EU:n kaltaiset sääntelykehikot ohjaavat siirtymää kertaluonteisista toimeksiannoista jatkuvaksi kumppanuudeksi. Alalle tuleva yritys voi hyödyntää tätä murrosta, jos se rakentaa palvelumallinsa alusta asti uuden toimintalogiikan varaan.

Markkinalla on kaksi sinistä valtamerta. Strateginen red teaming — jossa haastetaan organisaation päätöksentekoa ja toimintamalleja ilman kyberturvallisuuskontekstia — on käytännössä kilpailuton markkina-alue. Toinen avautuu PK-sektorilla, jossa NIS2:n laajeneminen luo kysyntää mutta nykyiset palveluntarjoajat ovat hinnoitelleet itsensä pois.

Red teaming on riskienhallinnan työkalu, ei pelkästään tietoturvapalvelu. Manuj ja Mentzerin (2008) riskienhallintamalliin peilattuna red teaming kattaa kolme

ulottuvuutta: ennakoinnin, reagointikyvyn testaamisen ja vaihtoehtoisten analyysien tuottamisen. Tämä laajempi rooli tukee palvelukonseptia, joka ylittää perinteisen penetraatiotestauksen rajat.

Menetelmäosaaminen ja psykologinen ymmärrys ovat erottautumistekijöitä. Hoffmanin (2017) ja Zenkon (2015) mukaan red teamingin arvo syntyy strukturoidusta haastamisesta ja kognitiivisten vinoumien tunnistamisesta — ei pelkästä teknisestä osaamisesta. Social engineering -menetelmien hallinta edellyttää sekä teknistä että inhimillistä osaamista, mikä nostaa palvelun asiantuntijavaatimuksia.

Sääntely-ympäristö luo pysyvää kysyntäpohjaa. DORA, NIS2, CRA ja TLPT muodostavat yhdessä sääntely-ympäristön, jossa kyberturvallisuuden testaus ei ole enää vapaaehtoista vaan lakisääteistä yhä useammalle organisaatiolle. Yli 160 tuhatta EU-organisaatiota kuuluu NIS2:n piiriin, ja DORA edellyttää finanssialan toimijoilta uhkatietopohjaista testausta.

Tekoäly muuttaa sekä uhkakenttää että palvelumalleja. AI madaltaa hyökkäysten kynnystä merkittävästi: AI-avusteinen tietojenkalastelu kasvoi 1 265 % vuodesta 2024 (CrowdStrike 2026), ja ENISA:n (2025) mukaan yli 80 % havaituista social engineering -hyökkäyksistä hyödynsi tekoälyä alkuvuonna 2025. Samanaikaisesti AI muuttaa myös puolustusta ja testausta: agenttinen red teaming mahdollistaa pienemmille palveluntarjoajille suuremman skaalan ja nopeamman testaussyklin. Pk-yrityksille tilanne on erityisen kriittinen: ne ovat kolme kertaa todennäköisemmin kyberhyökkäyksen kohteita kuin suuryritykset, mutta WEF:n (2026) mukaan 2,5 kertaa todennäköisemmin riittämättömän kyberkestävyyden tasolla. Tekoälyn kaksoisrooli — sekä uhkien tuottaja että puolustuksen skaalaaja — tekee siitä elementin, jonka varaan palvelumalli kannattaa rakentaa alusta alkaen, ei jälkikäteisenä lisänä. Tekoälyn integrointia case-yrityksen palvelumalliin käsitellään luvussa 5.5 ja laajempaa markkinavaikutusta luvussa 6.2.

5 Liiketoimintakonseptin muodostaminen

Luvuissa 3 ja 4 kartoitettiin toimialan nykytila ja teoreettinen perusta. Tässä luvussa yhdistetään nämä havainnot liiketoimintakonseptiksi, joka kuvaa case-yrityksen keskeiset elementit. Luku rakentuu Galbraithin (2002) tähtimallin mukaisesti. Tähtimalli on organisaatiosuunnittelun viitekehys, joka varmistaa viiden ulottuvuuden (strategian, rakenteen, prosessien, palkitsemisen ja osaamisen) keskinäisen linjauksen. Luku jakautuu strategiaan ja asemointiin (5.1), palvelumalliin ja arvolupaukseen (5.2), rakenteeseen ja prosesseihin (5.3) sekä osaamiseen ja sertifiointeihin (5.4). Palkitsemista ei käsitellä erillisenä kokonaisuutena, koska case-yritys on esiselvitysvaiheessa eikä palkitsemisjärjestelmän suunnittelu ole vielä ajankohtaista.

5.1 Strategia ja asemointi

Luvussa 4.1 tunnistettiin, että kyberturvallisuus- ja riskiarviointitoimiala on intermediating-muutoksessa ja markkinalla on kaksi kilpailematonta aluetta: strateginen red teaming ja PK-sektori. Tässä alaluvussa määritetään, miten case-yritys asemoituu näille markkinoille.

Porterin (1985) mukaan yritys voi saavuttaa kilpailuedun kustannusjohtajuudella, erottautumisella tai fokusoimalla tiettyyn markkinasegmenttiin. Case-yrityksen strategia yhdistää erottautumisen ja fokusoinnin: palvelu kohdistetaan kapeisiin segmentteihin (strateginen red teaming, PK-sektori), joissa kilpaillaan osaamisella, ei hinnalla. Asiantuntijapalveluissa kustannusjohtajuus on harvoin kestävä strategia, koska palvelun arvo syntyy osaamisesta, ei volyymista. Case-yrityksen strategia perustuu erottautumiseen kolmella tasolla:

- Strateginen red teaming — organisaation päätöksenteon ja toimintamallien haastaminen Hoffmanin (2017) ja Zenkon (2015) kuvaamilla menetelmillä. Tämä palvelutaso on käytännössä kilpailuton, koska nykyiset toimijat keskittyvät tekniseen testaukseen.
- Kyberturvallisuuden red teaming — TIBER-EU- ja DORA-vaatimusten mukainen uhkatietopohjainen testaus finanssi- ja kriittisen infrastruktuurin toimijoille. Tällä markkinalla kilpaillaan vakiintuneiden

toimijoiden kanssa, mutta erottaudutaan yhdistämällä tekninen testaus strategiseen näkökulmaan.

- PK-sektorin tuotteistettu palvelu — NIS2:n piiriin tulevien organisaatioiden tarpeisiin suunniteltu kevyempi palvelupaketti. Luvussa 3.2 tunnistettu kysyntä ja luvussa 4.6 todettu Pk-yritysten kyberhaavoittuvuus tukevat tätä valintaa.

Kolmiportainen palvelumalli mahdollistaa toimitusketjuasemoinnin, jossa case-yritys toimii eri rooleissa asiakkaan koon ja tarpeen mukaan: strategisena kumppanina suurille organisaatioille ja tuotteistettuna palveluntarjoajana PK-sektorille. Alustamalliin ei lähdetä, koska asiantuntijapalveluissa jokainen asiakkuus vaatii räätälöintiä ja yksittäisten vaativien asiakkaiden palvelukustannus on korkea — toisin kuin alustamalleissa, joissa yksikkökustannus lähestyy nollaa (Osterwalder; Pigneur; & Clark 2010).

Porter (1985) korostaa, että erottautumisstrategia edellyttää tietoista valintaa siitä, mitä yritys ei tee. Case-yritys ei kilpaile hinnalla, ei tarjoa geneeristä penetraatiotestausta eikä rakenna alustapalvelua. Sen sijaan se keskittyy palveluihin, joissa menetelmäosaaminen ja asiakassuhteen syvyys luovat kilpailuetua, jota on vaikea kopioida.

5.2 Palvelumalli ja arvolupaus

Palvelumallin jäsentämiseen käytetään Osterwalderin, Pigneurin ja Clarkin (2010) Business Model Canvas -viitekehystä (taulukko 7). BMC kuvaa liiketoiminnan yhdeksän osa-alueen väliset riippuvuudet ja soveltuu hyvin uuden liiketoimintakonseptin hahmottamiseen.

Taulukko 7 Business Model Canvas -viitekehys

BMC-osa-alue	**Kuvaus**
Kumppanit	- Kyberturvallisuuden konsulttivälitysalustat (CyberDo) - IT-palveluyritykset alihankintakanavana (Digia) - Sertifiointielimet (CREST, OffSec)

BMC-osa-alue	Kuvaus
	- Alan verkostot ja yhteisöt
Ydintoiminnot	- Red team –harjoitusten suunnittelu ja toteutus - Haavoittuvuusanalyysit ja testiraportit - Asiakasorganisaation riskienhallintaprosessien validointi - Asiakkaiden neuvonta - Uhkaympäristön seuranta ja testausmenetelmien kehittäminen
Arvolupaus	- Asiakasorganisaation toimintakyvyn ja jatkuvuuden varmistaminen - Strateginen red teaming: päätöksenteon laadun parantaminen - Kyberturvallisuustestaus: haavoittuvuudet löydetään ennen todellisia hyökkääjiä - PK-sektorin palvelu: vaatimustenmukaisuus kustannustehokkaasti
Asiakassuhde	- Pitkäaikaiset kumppanuudet kertaluonteisten toimeksiantojen sijaan - Henkilökohtainen palvelu erottautumistekijänä - Avainasiakkuuksien tunnistaminen ja projektisalkun hallinta
Asiakasryhmät	- Finanssiala ja kriittinen infrastruktuuri (DORA/TIBER-EU) - Suuret organisaatiot (strateginen red teaming) - NIS2:n piiriin tulevat Pk-yritykset (tuotteistettu palvelu)
Resurssit	- Asiantuntijat omassa yrityksessä sekä yhteistyöverkostossa - Testaustyökalut ja -infrastruktuuri - Osaaminen, sertifioinnit ja jatkuva kehittyminen
Kanavat	- Suorat B2B-myyntikanavat - CyberDo välitysalustana - Digia alihankintakanavana - Alan verkostot, konferenssit ja yhteisöt
Kulurakenne	- Palkat ja asiantuntijapalkkiot - Sertifikaatit

BMC-osa-alue	Kuvaus
	- Testausinfrastruktuurin ylläpito - Markkinointi - Verkostoituminen (ajallinen panostus)
Tulovirrat	- Retainer-sopimukset eli jatkuvaa palvelua koskevat pysyväissopimukset (ennustettavuus) - Projektimyynti (testaus- ja arviointitoimeksiannot) - PK-sektorin tuotteistettu palvelu (jatkuva tulovirta) - Koulutuspalvelut - Läpilaskutus (testausinfrastruktuuri)

Arvolupaus on asiakasorganisaation toimintakyvyn ja jatkuvuuden varmistaminen. Luvussa 5.1 kuvattu kolmiportainen palvelumalli tuottaa arvoa eri tavoin: strategisessa red teamingissä arvo syntyy päätöksenteon laadun parantamisesta, kybertestauksessa haavoittuvuuksien löytämisestä ennen todellisia hyökkääjiä ja PK-sektorin palvelussa vaatimustenmukaisuuden saavuttamisesta kustannustehokkaasti.

Asiakasryhmät jakautuvat palvelutasojen mukaisesti. Finanssialan ja kriittisen infrastruktuurin toimijat tarvitsevat DORA- ja TIBER-EU-vaatimusten mukaista testausta. Suuret organisaatiot, joiden toimintaympäristö on monimutkainen, hyötyvät strategisesta red teamingistä. NIS2:n piiriin tulevat Pk-yritykset tarvitsevat tuotteistettua ja saavutettavaa palvelua.

Asiakassuhteet ovat pitkäaikaisia. Asiantuntijapalvelussa henkilökohtainen palvelu on erottautumistekijä — pyritään jatkuvaan kumppanuuteen kertaluonteisten toimeksiantojen sijaan. Avainasiakkuuksien tunnistaminen ja projektisalkun hallinta ovat tärkeitä johtamisen työkaluja.

Ydintoiminnot kattavat asiakasorganisaation riskienhallintaprosessien validoinnin, red team -harjoitusten suunnittelun ja toteutuksen, haavoittuvuusanalyysien ja testiraporttien tuottamisen sekä asiakkaiden neuvonnan. Jatkuva uhkaympäristön seuranta on edellytys palvelun ajantasaisuudelle.

Kumppanit ja kanavat. Luvussa 3.3 tunnistetut kumppanuudet, CyberDo välitysalustana ja Digia alihankintakanavana, täydentävät suoria B2B-myyntikanavia. Alan verkostot, konferenssit ja yhteisöt ovat asiantuntijapalvelussa tärkeitä luottamuksen rakentajia.

Resurssit ovat ensisijaisesti inhimillisiä: kokeneet asiantuntijat, joilla on ajantasainen menetelmäosaaminen ja alan sertifioinnit. Teknisiä resursseja ovat testaustyökalut ja -infrastruktuuri. Osaamisen suunnittelua käsitellään tarkemmin luvussa 5.4.

Kulurakenne muodostuu pääosin palkoista ja asiantuntijapalkkioista, sertifikaateista, testausinfrastruktuurin ylläpidosta sekä markkinoinnista. Hallinnollisen henkilöstön osuus pidetään pienenä, koska asiantuntijaorganisaatiossa ihmiset ovat itseohjautuvia. Verkostoituminen on huomattava ajallinen panostus, joka ei näy suoraan kuluissa mutta on edellytys asiakashankinnalle ja näkyvyydelle.

Tulovirrat muodostuvat useasta lähteestä. Pitkäaikaiset retainer-sopimukset, joissa asiakas maksaa jatkuvasta palveluvalmiudesta kiinteää kuukausikorvausta, tuovat kassavirtaan ennustettavuutta. Projektimyynti yksittäisissä testaus- ja arviointitoimeksiannoissa täydentää retainer-tuloja. PK-sektorille suunnattu tuotteistettu palvelu tuottaa jatkuvaa tulovirtaa pienemmällä henkilöstöpanoksella, ja koulutuspalvelut laajentavat tarjontaa edelleen. Testausinfrastruktuurista voidaan lisäksi sopia asiakkaan kanssa läpilaskutuksesta, mikä mahdollistaa raskaammat testausympäristöt ilman kiinteää investointia.

5.3 Rakenne ja prosessit

Galbraithin (2002) tähtimallissa rakenne ja prosessit määrittävät, miten organisaatio toteuttaa strategiaansa käytännössä. Case-yrityksen kaltaiselle asiantuntijaorganisaatiolle kevyt rakenne on etu: pieni ydintiimi täydennettynä verkostomaisella yhteistyöllä mahdollistaa skaalautumisen ilman raskaita kiinteitä kustannuksia.

Keskeiset prosessit ovat toimeksiantojen hallinta (scoping, Rules of Engagement, raportointi), laadunvarmistus (ISO 27001 -käytäntöjen noudattaminen omassa toiminnassa) ja asiakkuuksien hallinta. Luvussa 4.4 käsitellyt laatujärjestelmät koskevat myös palveluntarjoajaa itseään — uskottavuus edellyttää, että omat prosessit täyttävät samat vaatimukset, joita asiakkailta edellytetään.

Taulukossa 8 esitetään liiketoiminnan keskeiset riskit ja niiden hallintakeinot.

Taulukko 8 Liiketoiminnan keskeiset riskit ja niiden hallintakeinot

Riski	**Vaikutus**	**Hallintakeino**
Toimeksiannon hallinta ja riippumattomuus	Yhteyshenkilöiden välinen kitka voi tehdä toimeksiannosta kestämättömän. Tilaaja voi myös pyrkiä ohjaamaan löydöksiä — jos palveluntarjoaja taipuu, harjoitus menettää arvonsa (Hoffman 2017; Zenko 2015).	Selkeästi määritellyt testausalueet ja vastuut, testausympäristöjen huolellinen valinta sekä jatkuva raportointi. Riippumattomuus varmistetaan sopimuksellisesti ja palveluntarjoajan ammattietiikka on neuvottelematon.
Juridiset ja eettiset riskit	Laittomaksi tulkittava toiminta voi johtaa oikeudellisiin seuraamuksiin.	Tarkat sopimukset ja lailliset valtuutukset (Rules of Engagement). Toiminta kansainvälisten ja kansallisten säädösten mukaisesti.
Tietovuodot ja asiakastiedon suojaaminen	Tietovuoto voi tapahtua kummassakin päässä: asiakkaan haavoittuvuustiedot toimittajan hallussa tai asiakkaan toimittajalle luovuttama pääsy. Molemmissa tapauksissa seuraukset ovat mainehaittaa ja oikeudellisia.	Tiukat tietoturvakäytännöt, joita valvotaan jatkuvasti — ei kertaluonteisesti. Salassapitosopimukset (NDA), tietojen salaus ja rajattu pääsy. Suurilla asiakasorganisaatioilla valvonta kytkeytyy tyypillisesti laatujärjestelmän mukaisiin auditointeihin (ks. 4.4).
Toimeksiannon operatiiviset riskit	Asiakas voi tulkita testauksen haitalliseksi, jos viestintä epäonnistuu.	Selkeästi määritellyt testausalueet, testausympäristöjen huolellinen

Riski	Vaikutus	Hallintakeino
	Testauksen aikana järjestelmät voivat häiriintyä.	valinta, jatkuva raportointi ja vastuiden dokumentointi.
Epäpätevät tai epäeettiset työntekijät	Sisäiset tietoturvarikkomukset tai mainehaitta.	Huolellinen rekrytointi, turvaselvitykset, jatkuva koulutus ja sisäinen valvonta.
Nopeasti kehittyvät kyberuhat	Uudet hyökkäysmenetelmät ja erityisesti AI-avusteiset hyökkäykset (ks. 4.6) voivat tehdä testausmenetelmistä vanhentuneita nopeasti.	Jatkuva koulutus ja alan kehityksen seuraaminen. Alalla osaamisen ylläpito edellyttää asiantuntijoilta omatoimisuutta. Tekoälyn hyödyntäminen omissa testausmenetelmissä on sekä kilpailuetu että välttämättömyys.
Markkina-asema ja asiakaspysyvyys	Erottautuminen on vaikeaa ja ilman pitkäaikaisia asiakkuuksia liiketoiminta on epävakaata	Luvussa 5.1 kuvattu erottautumisstrategia, jatkuvat palvelut ja strateginen kumppanuus (ks. 5.2)

5.4 Osaaminen ja sertifioinnit

Galbraithin (2002) tähtimallin viimeinen ulottuvuus on ihmiset. Kyberturvallisuus- ja riskiarviointitoimialalla osaaminen on sekä palvelun raaka-aine että keskeisin erottautumistekijä — taulukossa 7 tunnistettu osaamisen vanhentumisriski korostaa jatkuvan kehittymisen merkitystä.

Tekninen ydinosaaminen rakentuu tunnustettujen sertifiointien varaan. OSCP (Offensive Security Certified Professional) ja OSEP (Offensive Security Experienced Penetration Tester) ovat alan vakiintuneita pätevyyksiä, jotka osoittavat käytännön hyökkäysosaamisen. Kansainvälisen tietoturvatestauksen sertifiointielin CREST:in (Council of Registered Ethical Security Testers) sertifiointi on erityisesti TIBER-EU-toimeksiannoissa edellytys. Näiden lisäksi MITRE

ATT&CK-viitekehyksen tuntemus on keskeistä, koska se on sekä testauksen suunnittelun työkalu (ks. 4.4) että yhteinen kieli asiakkaan kanssa.

Teknisen osaamisen rinnalla tarvitaan strategista ajattelukykyä ja vahvaa ammattietiikkaa. Luvussa 4.3 kuvattu Hoffmanin (2017) devil's advocacy -menetelmä edellyttää kykyä haastaa asiakkaan oletuksia. Luvussa 5.3 todettu riippumattomuusvaatimus edellyttää rohkeutta pitää kiinni löydöksistä paineen alla.

Osaamisen suunnittelu on skaalautumisen edellytys. Ensimmäisten asiantuntijoiden profiili määrittää, mitä palvelutasoja (ks. 5.1) yritys voi tarjota käynnistysvaiheessa, ja rekrytointisuunnitelma tulee kytkeä suoraan liiketoiminnan kasvutavoitteisiin.

5.5 Tekoäly palvelumallissa

Tekoäly ei ole case-yritykselle pelkkä ulkoinen markkinavoima, vaan osa palvelumallin ydintä. Luvussa 4.6 todettiin, että agenttinen red teaming ja tekoälyavusteiset työkalut muuttavat toimialan palvelutuotantoa. Tässä alaluvussa kuvataan, miten tekoäly istuu case-yrityksen palvelumalliin käytännössä.

Tiedustelu- ja analyysivaiheessa tekoälyä voidaan hyödyntää laajamittaiseen avoimen lähteen tiedustelutietoon (OSINT) ja haavoittuvuuksien priorisointiin. Raportointivaiheessa tekoäly tukee löydösten jäsentämistä asiakkaalle ymmärrettävään muotoon. Toteutusvaiheessa agenttinen testaus, jossa tekoälyagentti suorittaa testaustoimenpiteitä itsenäisesti, mahdollistaa raskaan infrastruktuurin kartoituksen, joka olisi käsin tehtynä sekä hidasta että virhealtista.

Agenttisen testauksen etu korostuu toistettavuudessa. Sama testitapaus voidaan ajaa uudelleen vähäisin valmisteluin esimerkiksi asiakkaan tekemien muutosten jälkeen, mikä tekee jatkuvasta tietoturvan arvioinnista taloudellisesti kannattavaa. Yhdistelmä vapauttaa asiantuntijat keskittymään monimutkaisiin skenaarioihin, hyökkäyspolkujen rakentamiseen ja strategiseen analyysiin.

Tekoälymallien saatavuus on itsessään muotoutumassa omaksi markkinakseen. Anthropic julkaisi huhtikuussa 2026 Claude Mythos Preview -mallin osana Project Glasswing -aloitetta, jossa malli on saatavilla vain kutsusta valituille kumppaneille kriittisten ohjelmistojen suojaamiseen. (Anthropic 2026a; Anthropic 2026b.) Mallia on käytetty tuhansien aiemmin tuntemattomien haavoittuvuuksien, niin sanottujen nollapäivähaavoittuvuuksien, joihin ei ole olemassa korjausta, tunnistamiseen. Mallin vakavuusarviot ovat osuneet 89 prosentissa tapauksista täsmälleen oikein asiantuntijavalidoinnin kanssa (Anthropic 2026a). OpenAI julkaisi viikon viiveellä GPT-5.4-Cyber-mallin, jonka pääsy on rajattu Trusted Access for Cyber -ohjelman kautta tunnistautuneille puolustajille (OpenAI 2026). OpenAI:n Preparedness Framework luokittelee GPT-5.4:n korkean kyberkyvykkyyden tasolle (OpenAI 2025).

Kaksi lähestymistapaa edustaa eri liiketoimintamalleja: Anthropicin Glasswing on tiukasti rajattu kumppaniverkosto, kun OpenAI:n Trusted Access for Cyber pyrkii laajempaan verifioitujen puolustajien ekosysteemiin. Molemmissa pääsy malliin toimii kilpailuetuna, jota ei voi kopioida pelkällä yleisellä API-pääsyllä. Case-yritykselle tämä tarkoittaa, että tekoälyn hyödyntäminen palvelussa edellyttää pääsyä asianmukaisiin työkaluihin; suhteiden rakentaminen malliekosysteemien hallinnoijiin on osa palveluntarjoajan strategista pääomaa.

Kaupallisten mallien rinnalle on kehittymässä avoimen lähdekoodin ja paikallisesti ajettavien mallien ekosysteemi. Niiden suorituskyky ei vielä vastaa parhaita kaupallisia malleja, mutta niillä on kaksi etua: pääsy ei vaadi kumppanuussopimuksia, ja mallit voidaan ajaa asiakkaan omassa ympäristössä, mikä sopii erityisen hyvin arkaluontoisten toimeksiantojen tietoturvavaatimuksiin. Alkuvaiheen palveluntarjoajalle avoimet mallit tarjoavat kyvykkyysalustan ennen kuin pääsy rajoitettuihin kaupallisiin malleihin on auki. Euroopan unionin digitaalisen autonomian tavoite tukee tätä kehitystä. Pidemmällä aikavälillä case-yritys voi myös osallistua avointen mallien kehittämiseen tai jalostaa niistä omiin tarpeisiinsa soveltuvan version, mutta mallikehitys rajautuu tämän työn ulkopuolelle.

Tekoäly ei kuitenkaan korvaa asiantuntijaa. Hoffmanin (2017) kuvaama devil's advocacy, Zenkon (2015) korostama riippumattomuus ja luvussa 5.4 todettu strateginen ajattelukyky ovat inhimillisiä kyvykkyyksiä, joita tekoäly ei tavoita. Haavoittuvuuksien löytäminen on vain osa arvoketjua; niiden tulkinta liiketoimintariskien valossa, korjaustoimenpiteiden priorisointi asiakkaan toimintaympäristöön sopivasti ja päätöksenteon haastaminen edellyttävät ihmisen harkintaa.

Korjauskapasiteetti on case-yritykselle erityinen kilpailuetu. Koska yritysryhmässä on myös sovelluskehitys- ja pilvi-infrastruktuuriosaamista, haavoittuvuuksien löytäminen voidaan tarvittaessa sitoa korjaustoimenpiteiden suunnitteluun ja toteutukseen. Tämä vastaa toimialaa koskevaan kritiikkiin, jonka mukaan tekoälyavusteinen löytäminen voi ylittää organisaatioiden korjauskapasiteetin ja jättää haavoittuvuudet käytännössä hyödyntämättä.

Tekoälyn rooli kyberturvallisuus- ja riskiarviointialalla kehittyy nopeasti. Tässä alaluvussa kuvattu tilanne vastaa huhtikuun 2026 asetelmaa, ja uudet mallit tai niiden jakelumallit voivat muuttaa kilpailukenttää lyhyelläkin aikavälillä.

5.6 Avainlöydökset liiketoimintakonseptissa

Erottautuminen rakentuu osaamiselle, ei hinnalle. Porterin (1985) erottautumisstrategian mukaisesti case-yritys asemoi itsensä kolmiportaisella palvelumallilla, jossa strateginen red teaming, kyberturvallisuustestaus ja PK-sektorin tuotteistettu palvelu palvelevat eri asiakassegmenttejä eri logiikalla.

Korjauskapasiteetti sovelluskehitys- ja pilviosaamisen kautta erottaa case-yrityksen pelkästä testauksesta.

Alustamalli ei sovellu asiantuntijapalveluun. Asiakkuuksien räätälöintitarve ja vaativien toimeksiantojen korkea yksikkökustannus tekevät volyymiin perustuvasta mallista kannattamattoman — retainer-pohjainen kumppanuusmalli tuottaa paremman katteen ja ennustettavamman kassavirran.

Auditointikelpoisuus on kilpailuetu, ei kustannus. Kun omat prosessit täyttävät ISO 27001 -vaatimukset ensimmäisestä toimintapäivästä alkaen, palveluntarjoaja on valmiiksi hyväksyttävissä suurten asiakasorganisaatioiden toimittajaksi ilman lisätyötä.

Riippumattomuus on palvelun arvo. Red teamingin uskottavuus edellyttää, että palveluntarjoaja ei taivu tilaajan paineeseen — ammattietiikka on neuvottelematon ja se varmistetaan sopimuksellisesti.

Osaamisen suunnittelu ratkaisee skaalautumisen. Ensimmäisten asiantuntijoiden profiili määrittää, mitä palvelutasoja yritys voi tarjota, ja rekrytointi tulee kytkeä suoraan kasvutavoitteisiin.

6 Liiketoimintakonseptin arviointi

Luvussa 5 muodostettiin liiketoimintakonsepti yhdistämällä nykytila-analyysin ja kirjallisuuskatsauksen havainnot Galbraithin (2002) tähtimallin mukaiseksi liiketoimintakonseptiksi. Tässä luvussa arvioidaan liiketoimintakonseptin toteuttamiskelpoisuutta, tarkastellaan tekoälyn vaikutusta palvelumalliin ja määritetään jatkotoimenpiteet liiketoiminnan käynnistämiseksi.

6.1 Johtopäätökset

Tämän työn erityispiirteenä on tekijän kaksoisrooli: tutkijana ja case-yrityksen toimitusjohtajana. Liiketoimintakonsepti on muodostettu esiselvityksenä liiketoiminnan käynnistämispäätöksen tueksi, ja sen arviointi perustuu luvussa 3 kartoitettuun markkinatilanteeseen, luvun 4 teoreettisiin viitekehyksiin ja tekijän toimialakokemukseen. Kaksoisrooli mahdollistaa syvällisen toimialatuntemuksen hyödyntämisen, mutta edellyttää tulosten kriittistä tarkastelua.

Markkinavalidointi tukee konseptia. Luvussa 3.1 tunnistettu kilpailutilanne osoittaa, että strategisen red teamingin ja PK-sektorin yhdistelmää ei nykyisin tarjoa yksikään suomalainen toimija. Luvussa 3.2 tunnistettu asiakastarve —

erityisesti NIS2:n piiriin tulevien organisaatioiden kasvava testausvelvoite — luo kysyntää, joka ei ole suhdanneriippuvaista. Kumppaniverkosto (CyberDo, Digia) tarjoaa kanavan markkinoille pääsyyn ilman suuria alkuinvestointeja myyntiin.

Teoreettinen perusta on johdonmukainen. McGahanin (2004) intermediating-malli selittää, miksi toimialan palvelumallit muuttuvat vaikka ydinosaaminen säilyy. Porterin (1985) erottautumisstrategia osoittaa, miksi kustannuskilpailu ei ole kestävä vaihtoehto asiantuntijapalveluissa. Osterwalderin ym. (2010) BMC jäsentää liiketoimintamallin elementit, ja Galbraithin (2002) tähtimalli varmistaa, että strategia, rakenne, prosessit ja osaaminen ovat linjassa keskenään.

Toimialakokemukseen perustuva arvio vahvistaa, että konseptin riskit ovat hallittavissa. Taulukossa 7 tunnistetut riskit, erityisesti riippumattomuuden varmistaminen ja tietovuotojen kaksisuuntaisuus, ovat todellisia, mutta hallittavissa sopimuksellisesti ja prosessien kautta. Auditointikelpoisuuden rakentaminen alusta alkaen (ks. 5.6) madaltaa suurten asiakasorganisaatioiden ostokynnystä.

Konseptin suurin rajoite on skaalautuminen. Asiantuntijapalvelu on riippuvainen osaajista, joita alalla on niukasti. ISC2:n (2024) mukaan kyberturvallisuusalan osaajapula on 4,8 miljoonaa henkilöä maailmanlaajuisesti. Tämä korostaa luvussa 5.4 käsitellyn osaamisen suunnittelun merkitystä ja tekee rekrytoinnista strategisen pullonkaulan.

6.2 Tekoälyn vaikutus markkinaan

Luvussa 5.5 kuvattiin, miten tekoäly integroituu case-yrityksen palvelumalliin. Tässä alaluvussa tarkastellaan tekoälyn laajempaa vaikutusta markkinadynamiikkaan ja sitä, miten kehitys vaikuttaa liiketoimintakonseptin toteuttamiskelpoisuuteen.

Kysynnän kasvu on selkeä. CrowdStriken (2026) raportoima 1 265 prosentin kasvu AI-avusteisessa tietojenkalastelussa vuodessa osoittaa, että uhkatoimijat hyödyntävät tekoälyä jo laajasti. Tämä kasvattaa testauspalveluiden

rakenteellista kysyntää, sillä organisaatioiden puolustuksen on vastattava AI-avusteisiin hyökkäyksiin. WEF:n (2026) raportoima kyberkestävyyden epätasapaino suurten ja pienten organisaatioiden välillä laajentaa kysyntää erityisesti PK-sektoriin, jota nykyiset palveluntarjoajat palvelevat heikosti.

Tekoäly muuttaa myös kilpailuasetelmaa pienemmän toimijan eduksi. Aiemmin skaalautuminen edellytti suurta asiantuntijakapasiteettia, jonka hankkiminen oli pienelle yritykselle hidasta ja kallista. Agenttinen testaus (ks. 4.3.3) mahdollistaa pienemmälle toimijalle suuremman testausskaalan, minkä seurauksena konsolidoituneiden suuryritysten kokoedut heikkenevät osassa palveluita.

Tekoälyn hyödyntäminen kyberturvallisuudessa ei ole ongelmatonta. Julkisessa keskustelussa on esitetty kritiikkiä siitä, että tekoälyavusteinen haavoittuvuuksien löytäminen voi ylittää organisaatioiden korjauskapasiteetin: haavoittuvuuksia löydetään nopeammin kuin niitä ehditään korjata. Case-yrityksen kannalta tämä kriittinen näkökulma tukee korjauskapasiteetin (ks.5.5) nostamista palvelumallin erottautumistekijäksi; pelkkä löytäminen ei enää erotu markkinalla, vaan arvo syntyy löytämisen ja korjauksen yhdistelmästä. Suuret toimijat voivat periaatteessa yhdistää nämä kaksi, mutta niiden nykyinen organisaatiorakenne erottelee testauksen ja kehityksen tyypillisesti eri yksiköihin tai eri toimittajien vastuulle. Case-yrityksen yritysryhmärakenne tarjoaa yhdistelmän luontevasti ja välittömästi, mikä antaa aikaedun ennen kuin suuret toimijat ehtivät järjestää toimintaansa uudelleen.

Ajoitus on case-yritykselle otollinen. Sääntelyvelvoitteet tuovat pakollisen kysynnän, tekoäly mahdollistaa skaalautumisen, ja suurten toimijoiden konsolidaatio jättää tilaa erikoistuneille palveluntarjoajille. Riskinä on, että pääsy edistyneimpiin kaupallisiin malleihin pysyy rajoitettuna vain harvoille; tätä riskiä lieventää avointen mallien nopea kehitys ja case-yrityksen mahdollisuus rakentaa palvelumalli useampien malliekosysteemien varaan.

6.3 Jatkotoimenpiteet

Tämä insinöörityö tuottaa liiketoimintakonseptin, ei valmista liiketoimintasuunnitelmaa. Konseptista liiketoimintaan siirtyminen edellyttää seuraavia toimenpiteitä:

Palvelun pilotointi voidaan aloittaa ennen täyden palveluvalikoiman rakentamista. Ensimmäiset toimeksiannot, esimerkiksi olemassa olevien kumppanuuksien (ks. 3.3) kautta, toimivat sekä tulorahoituksena että palvelumallin validointina. Pilotointivaiheessa testataan erityisesti hinnoittelumallia ja asiakasprosessien toimivuutta.

Hinnoittelumallin tarkentaminen edellyttää markkinatestausta. Luvussa 5.2 kuvatut tulovirrat, retainer, projekti ja tuotteistettu palvelu, tarvitsevat konkreettiset hintapisteet, jotka syntyvät ensimmäisten toimeksiantojen kautta.

Markkinointi- ja myyntisuunnitelma tulee laatia erikseen. Yhteisönäkyvyyden suunnittelu, sisältömarkkinointi ja B2B-myyntiprosessin rakentaminen ovat laajuudeltaan oman suunnitelman arvoisia.

Kustannusarvio ja rahoitussuunnitelma tarvitaan ennen merkittäviä investointeja. Sertifiointikustannukset, testausinfrastruktuuri ja ensimmäisten asiantuntijoiden palkkaus muodostavat alkuvaiheen suurimmat menoerät.

Eettisen ohjeistuksen ja prosessikuvausten laatiminen on edellytys toiminnan käynnistämiselle. Luvussa 5.3 kuvattu auditointikelpoisuuden vaatimus tarkoittaa, että prosessit on dokumentoitava ennen ensimmäistä asiakastoimeksiantoa.

7 Yhteenveto

Tämän insinöörityön tavoitteena oli muodostaa liiketoimintakonsepti kyberturvallisuus- ja riskiarviointipalveluita tarjoavalle case-yritykselle. Työ eteni nykytila-

analyysistä (luku 3) kirjallisuuskatsauksen (luku 4) kautta liiketoimintakonseptiin (luku 5), jonka toteuttamiskelpoisuutta arvioitiin luvussa 6.

Nykytila-analyysi osoitti, että markkinalla on tilaa uudelle toimijalle. Strateginen red teaming ja PK-sektori ovat käytännössä kilpailuttomia markkina-alueita, ja NIS2:n laajeneminen yli 160 000 EU-organisaatioon luo sääntelystä kumpuavaa kysyntää. Kirjallisuuskatsaus vahvisti, että toimiala on McGahanin (2004) intermediating-muutoksessa: palvelumallit muuttuvat, mutta ydinosaaminen säilyttää arvonsa.

Liiketoimintakonsepti rakennettiin Galbraithin (2002) tähtimallin mukaisesti. Case-yrityksen strategia perustuu Porterin (1985) erottautumisstrategiaan kolmiportaisella palvelumallilla, jonka arvolupaus on asiakasorganisaation toimintakyvyn ja jatkuvuuden varmistaminen. Keskeisinä löydöksinä nousivat auditointikelpoisuus kilpailuetuna, riippumattomuus palvelun arvona ja osaamisen suunnittelu skaalautumisen edellytyksenä. Yritysryhmän sovelluskehitys- ja pilviosaaminen mahdollistaa korjauskapasiteetin, joka erottaa case-yrityksen pelkästä testauksesta.

Työn rajaus koskee liiketoimintakonseptin muodostamista, ei sen käytännön toteutusta. Konsepti perustuu kirjallisuuteen, toimiala-analyysiin ja tekijän toimialakokemukseen. Varsinainen liiketoiminnan käynnistäminen edellyttää luvussa 6.3 kuvattuja jatkotoimenpiteitä, erityisesti pilotointia, hinnoittelun markkinatestausta ja kustannusarvion laatimista.

Tekoälyn nopea kehitys sekä uhka- että puolustuspuolella tekee ajoituksesta otollisen: pieni, ketterä toimija voi hyödyntää AI-avusteista testausta skaalautuakseen nopeammin kuin perinteiset kilpailijat. Samalla sääntely-ympäristön tiukentuminen varmistaa, ettei kysyntä ole ohimenevää.

Tekoälyn rooli kyberturvallisuuden palvelumalleissa muuttuu nopeasti, ja aihe ansaitsee syvemmän tutkimuksen. Tekijä aikoo jatkaa aiheen parissa tulevissa opinnoissaan, erityisesti avointen mallien hyödyntämisen ja niiden jatkokehittämisen osalta case-yrityksen tarpeisiin.

Insinöörityö osoittaa, että liiketoimintakonsepti on toteuttamiskelpoinen. Seuraava askel on siirtyminen konseptista toimintaan.

Lähteet

Anthropic. 2026a. Mythos Preview System Card. Verkkoaineisto. <https://red.anthropic.com/2026/mythos-preview/>. Luettu 19.4.2026.

Anthropic. 2026b. Project Glasswing. Verkkoaineisto. <https://www.anthropic.com/glasswing>. Luettu 19.4.2026.

CrowdStrike. 2026. 2026 Global Threat Report. Verkkoaineisto. <https://www.crowdstrike.com/en-us/global-threat-report/>. Luettu 24.3.2026.

Cyberday Oy. 2025a. DORA: Esittely, soveltamisala ja keskeiset vaatimukset. Verkkoaineisto. <https://www.digiturvamalli.fi/blogi/dora-esittely-soveltamisala-ja-keskeiset-vaatimukset>. Luettu 24.3.2025.

Cyberday Oy. 2025b. ISMS:n toteuttaminen: dokumenttien, wikien, ISMS-työkalujen ja GRC:n vertailu. Verkkoaineisto. https://www.digiturvamalli.fi/blogi/isms-n-toteuttaminen-dokumenttien-wikien-isms-tyokalujen-ja-grc-n-vertailu. Luettu 10.4.2025.

Cyberday Oy. 2025c. ISO 27001 ja ISO 9001: erot, yhteistyö ja yhdistämisen hyödyt. Verkkoaineisto. <https://www.digiturvamalli.fi/blogi/iso-27001-ja-iso-9001-erot-yhteistyo-ja-yhdistamisen-hyodyt>. Luettu 23.3.2025.

Cyberday Oy. 2025d. Kyberturvallisuuslaki (NIS2) tulee voimaan 8.4.2025. Verkkoaineisto. <https://www.digiturvamalli.fi/blogi/kyberturvallisuuslaki-nis2-tulee-voimaan-8-4-2025->. Luettu 4.4.2025.

Cyberday Oy. 2025e. Vaatimuskehikkokatsaus, SUPO:n turvallisuuskatsaus & ja roolienhallinta: Digiturvamallin tuote- ja uutiskooste 3/2025. Verkkoaineisto. <https://www.digiturvamalli.fi/blogi/digiturvamallin-tuote-ja-uutiskooste-3-2025>. Luettu 10.4.2025.

Delizonna, L. 2017. High-Performing Teams Need Psychological Safety. Here's How to Create It. Harvard Business Review.

European Central Bank. 2025. More than 100 TIBER tests conducted. Verkkoaineisto. <https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews230427.en.html>. Luettu 21.3.2025.

European Commission. 2026. Commission strengthens EU cybersecurity resilience and capabilities. Verkkoaineisto. <https://digital-strategy.ec.europa.eu/en/news/commission-strengthens-eu-cybersecurity-resilience-and-capabilities> . Luettu 16.3.2026.

European Insurance and Occupational Pensions Authority. 2025. Digital Operational Resilience Act (DORA). Verkkoaineisto. <https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en>. Luettu 22.3.2025.

Galbraith, J. 2002. Designing Organizations: An Executive Guide to Strategy, Structure, and Process. Jossey-Bass.

Harland, C.; Brenchley, R. & Walker, H. 2003. Risk in supply networks. Journal of Purchasing and Supply Management, vol. 9, nro 2, s. 51–62.

Hoffman, B. G. 2017. Red Teaming: How Your Business Can Conquer the Competition by Challenging Everything. Crown Business.

ISC2. 2026. 2025 Cybersecurity Workforce Study. Verkkoaineisto. <https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study>. Luettu 24.3.2026.

Kim, C. W. & Mauborgne, R. 2004. Blue Ocean Strategy. Harvard Business Review.

Manuj, I. & Mentzer, J. T. 2008. Global Supply Chain Risk Management. Journal of Business Logistics, vol. 29, nro 1, s. 133–156.

McGahan, A. M. 2004. How industries change. Harvard Business Review, October 2004, s. 87–94.

Mitchell, V.-W. 1995. Organizational Risk Perception and Reduction: A Literature Review. British Journal of Management, vol. 6, nro 2, s. 115–133.

Mordor Intelligence. 2026. Finland Cybersecurity Market Size & Share Analysis. Verkkoaineisto. <https://www.mordorintelligence.com/industry-reports/finland-cybersecurity-market>. Luettu 22.3.2026.

OpenAI. 2025. Preparedness Framework (Version 2). Verkkoaineisto. <https://cdn.openai.com/pdf/18a02b5d-6b67-4cec-ab64-68cdfbddebcd/preparedness-framework-v2.pdf>. Luettu 15.4.2025.

OpenAI. 2026. Trusted access for the next era of cyber defense. Verkkoaineisto. <https://openai.com/index/scaling-trusted-access-for-cyber-defense/>. Luettu 19.4.2026.

Osterwalder, A.; Pigneur, Y. & Clark, T. 2010. Business model generation: A handbook for visionaries, game changers, and challengers. Hoboken, New Jersey: John Wiley & Sons.

Porter, M. E. 1985. Kilpailuetu: Miten ylivoimainen osaaminen luodaan ja säilytetään. Espoo: Weilin + Göös.

Talamantes, J. 2014. The Social Engineer's Playbook: A Practical Guide to Pretexting.

The European Union Agency for Cybersecurity, ENISA. 2024. ENISA Threat Landscape 2024. Verkkoaineisto.

<https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf>. Luettu 7.4.2025.

The European Union Agency for Cybersecurity, ENISA. 2025. ENISA Threat Landscape 2025. Verkkoaineisto. <https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf>. Luettu 19.4.2026.

Vaadata. 2025. What is Red Teaming? Methodology and Scope of a Red Team Operation. Verkkoaineisto. <https://www.vaadata.com/blog/what-is-red-teaming-methodology-and-scope-of-a-red-team-operation/>. Luettu 21.3.2025.

Verizon. 2024. 2024 Data Breach Investigations Report (DBIR). Verkkoaineisto. <https://www.verizon.com/business/resources/reports/dbir/>. Luettu 19.4.2026.

World Economic Forum. 2026. Global Cybersecurity Outlook 2026. Verkkoaineisto. <https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf>. Luettu 16.3.2026.

Zenko, M. 2015. Red Team: How to Succeed By Thinking Like the Enemy. Basic Books.