					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P40					Asiakirjan nimi: **Tietoturvatestauksen ja red team -harjoitusten politiikka**							
Versio: 1.0		Voimaantulopäivä: 01.01.2025			Asiakirjan omistaja:							
X	Politiikka		Standardi		Menettely		Lomake		Rekisteri		Muu	

Muutoshistoria				
Muutosnumero	**Muutospäivä**	**Muutokset**	**Tarkistanut**	**Prosessin omistaja**

Hyväksynnät			
Nimi	**Tehtävänimike**	**Päivämäärä**	**Allekirjoitus**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/säädös	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
EU:n GDPR	Art. 32(1)(d)	
EU:n NIS2-direktiivi	Art. 21(2)(f)	
EU:n DORA-asetus	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Tarkoitus

1 Määrittää jäsennelty ohjelma organisaation verkkojen, järjestelmien ja sovellusten säännölliseen tietoturvatestaukseen, mukaan lukien haavoittuvuusarvioinnit, penetraatiotestaus ja red team -harjoitukset, jotta täytetään EU:n NIS2-direktiivin 21 artiklan 2 kohdan f alakohdan vaatimukset kyberturvallisuustoimenpiteiden tehokkuuden arvioinnista.

1.1 Varmistaa, että teknisten ja organisatoristen toimenpiteiden heikkoudet tunnistetaan ja korjataan ennakoivasti hallitun testauksen avulla sekä että organisaation tietoturvan taso paranee jatkuvasti.

2. Soveltamisala

2 Tämä politiikka kattaa kaikki organisaation omistamat tai ylläpitämät kriittiset tietojärjestelmät, sovellukset ja niitä tukevan infrastruktuurin. Se kattaa myös toimitilojen fyysisen tietoturvatestauksen siltä osin kuin se on kyberturvallisuuden kannalta merkityksellistä (esimerkiksi sosiaalisen manipuloinnin testit tai fyysiset tunkeutumistestit, jos ne kuuluvat red team -harjoituksen soveltamisalaan).

2.1 Tätä politiikkaa sovelletaan sisäisiin tietoturvatiimeihin, kaikkiin sopimussuhteessa oleviin ulkoisiin tietoturvatestausyrityksiin sekä asiaankuuluviin järjestelmä- ja sovellusomistajiin. Kaikkien testaustoimien on oltava valtuutettuja ja tässä politiikassa kuvattujen menettelyjen mukaisia tahattomien häiriöiden välttämiseksi.

3. Tavoitteet

3 Varmistaa toteutettujen kyberturvallisuuskontrollien (teknisten, operatiivisten ja organisatoristen) tehokkuus säännöllisen testauksen ja simulaatioiden avulla EU:n NIS2-direktiivin tehokkuuden mittaamista koskevien vaatimusten mukaisesti.

3.1 Tunnistaa haavoittuvuudet ja puutteet, jotka voivat jäädä tavanomaisissa operatiivisissa prosesseissa havaitsematta, mukaan lukien zero-day-haavoittuvuudet ja konfiguraatiovirheet, realistisissa hyökkäysskenaarioissa (red teaming) ennen kuin uhkatoimija hyödyntää niitä.

3.2 Tuottaa johdolle varmuutta ja toimeenpantavia suosituksia raportoimalla testien auditointihavainnot ja mahdollistamalla siten perustellut riskienkäsittelyä koskevat päätökset sekä tietoturvaohjelman jatkuvan parantamisen.

4. Roolit ja vastuut

4 Tietoturvatestauksen koordinaattori (STC): tietoturvajohtajan (CISO) nimeämä henkilö, joka vastaa kaikkien tietoturvatestaustoimien suunnittelusta ja valvonnasta. Varmistaa, että testien

soveltamisala määritetään, ne valtuutetaan asianmukaisesti ja että tulokset raportoidaan sekä niihin reagoidaan.

4.1 Sisäinen tietoturvatiimi (Blue Team): osallistuu testaukseen yhteistyössä (esimerkiksi toimittaa tietoja soveltamisalan määrittelyä varten ja valvoo järjestelmiä testauksen aikana). Red team -harjoituksissa Blue Team reagoi simuloituihin hyökkäyksiin, ja sen havaitsemis- ja reagointikykyä arvioidaan.

4.2 Red Team / penetraatiotestaajat: voi olla sisäinen hyökkäävään tietoturvaan keskittyvä tiimi tai ulkoisia konsultteja. Toteuttavat testit sovittujen toimintasääntöjen mukaisesti, dokumentoivat kaikki havaitut haavoittuvuudet ja hyödyntämisketjut sekä ylläpitävät luottamuksellisuutta.

[... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ...]

9. Seuranta ja auditointi

9 STC ylläpitää kalenteria ja lokia kaikista toteutetuista tietoturvatestaustoimista. Lokin on sisällettävä päivämäärä, soveltamisala, testin suorittaja ja yhteenveto tuloksista. Lokia katselmoidaan sen varmistamiseksi, että vaadittua aikataulua noudatetaan (esimerkiksi ettei yksikään kriittinen järjestelmä jää testaamatta vuosikierron yli).

9.1 Testien auditointihavaintojen korjaavien toimenpiteiden etenemistä seurataan ja siitä raportoidaan kuukausittain. Avoimet korkean vakavuuden ongelmat katselmoidaan johdon kokouksissa, kunnes ne on suljettu.

9.2 Sisäinen tarkastus tai riippumaton auditoija katselmoi tietoturvatestausohjelman vuosittain varmistaakseen, että testit on asianmukaisesti valtuutettu, toteutettu ja raportoitu, kriittisiin auditointihavaintoihin on puututtu ja ohjelma täyttää sääntelyn odotukset (esimerkiksi auditoijat voivat tarkistaa, että penetraatiotestaus on tehty ennen uuden verkkopalvelun käyttöönottoa vaatimusten mukaisesti). Kaikki poikkeamat johtavat korjaavien toimenpiteiden suunnitelmiin.

10. Katselmointi ja ylläpito

10 Tämä politiikka ja kokonaisvaltainen testaussuunnitelma katselmoidaan vähintään kerran vuodessa. Katselmoinnissa huomioidaan uhkaympäristön muutokset (esimerkiksi uudet hyökkäystekniikat, joita nykyinen testaus ei kata) ja soveltamisaloja tai testauksen tiheyttä mukautetaan tarvittaessa.

10.1 Jokaisen merkittävän kyberturvallisuuspoikkeaman tai tietomurron jälkeen tämä politiikka on tarkistettava sen arvioimiseksi, olisiko lisätestaus tai tiheämpi testaus voinut estää tapahtuman tai mahdollistaa sen havaitsemisen aiemmin. Politiikka päivitetään tämän jälkeen vastaavien muutosten sisällyttämiseksi siihen (esimerkiksi lisäämällä uusi skenaario red team -harjoituksiin havaittujen hyökkäysmallien perusteella).

10.2 Tämän politiikan muutokset on hyväksyttävä tietoturvajohtajan (CISO) toimesta ja saatettava hallituksen tietoon. Kaikille asiaankuuluville henkilöille tiedotetaan muutoksista, ja ulkoisille testauskumppaneille ilmoitetaan, jos muutos vaikuttaa heidän toimeksiantonsa ehtoihin.

11. Liittyvät politiikat ja yhteydet

11.1 P06 – Riskienhallintapolitiikka. Testauksen tuotokset ohjaavat riskien arviointia ja riskienkäsittelyä.

11.2 P22 – Lokitus- ja valvontapolitiikka. Varmistaa havaitsemisen kattavuuden harjoitusten aikana.

11.3 P24 – Turvallisen kehityksen politiikka. Sisällyttää testauksen auditointihavainnot ohjelmistokehityksen elinkaaren (SDLC) kontrolleihin.

11.4 P25 – Sovellusturvallisuusvaatimusten politiikka. Varmistaa, että vaatimukset heijastavat testauksesta saatuja oppeja.

11.5 P30 – Tietoturvapoikkeamien hallintapolitiikka. Red team -skenaariot tarkentavat toimintapelikirjoja ja reagointia.

11.6 P31 – Todisteiden keräämisen ja forensiikan politiikka. Mahdollistaa artefaktien turvallisen keräämisen testauksen aikana.

11.7 P32 – Liiketoiminnan jatkuvuus- ja katastrofipalautuspolitiikka. Harjoitukset varmentavat häiriönsietokyvyn hyökkäystilanteissa.

11.8 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka. Varmistaa tietoturvatestausohjelman tehokkuuden riippumattoman valvonnan.

12. Viitteet

12.1 NIS2-direktiivi (EU 2022/2555), 21 artiklan 2 kohdan f alakohta (kyberturvallisuusriskien hallintatoimenpiteiden tehokkuuden arviointia koskevat politiikat ja menettelyt)

12.2 Komission täytäntöönpanoasetus (EU) 2024/2690, liitteen 7 jakso (kyberturvallisuustoimenpiteiden seurannan, testauksen ja arvioinnin tehokkuutta koskevat vaatimukset)

12.3 ENISAn tekninen ohjeistus (2025) – liite tietoturvatestauksesta ja auditoinnista (suuntaviivat kyberturvallisuusharjoitusten ja teknisten testien toteuttamiseen)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Toimialan parhaat käytännöt: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (rahoitusalan red team -viitekehykset viitteellisessä käytössä)