Huoltovarmuusorganisaatio

Vesihuoltolaitosten kyberteemaiset harjoitukset

Vesihuoltolaitosten Yhteinen ja Yleinen Harjoituskokonaisuus

2022-2023

Loppuraportti

YRITYSLUOTTAMUKSELLINEN

Sisällysluettelo

Johdanto

- Harjoitusvalmistelu käynnistyi Vesilaitosyhdistyksen tunnistamasta tarpeesta järjestää laaja harjoituskokonaisuus vesihuoltolaitosten kyberturvallisuuden kehittämiseksi.
- Harjoitusvalmistelua varten organisoitui suunnitteluryhmä, jossa oli mukana Kyberturvallisuuskeskuksen, Huoltovarmuuskeskuksen, ELY-keskuksen, Kuntaliiton, Helsingin seudun ympäristöpalveluiden, Valkeakosken kaupungin vesihuoltolaitoksen, Vesilaitosyhdistyksen ja Instan asiantuntijoita.
- Tavoitteena oli kehittää vesihuoltolaitoksille toistettava kyberteemainen työpöytäharjoitus etätoteutuksena.
- Harjoituksen toteutuksessa hyödynnettiin Instan Trasim-harjoitusalustaa ja Microsoft Teams alustaa.
- Harjoituksen skenaario laadittiin suunnittelupalavereissa harjoituksen tavoitteiden mukaiseksi. Tämän harjoituksen suunnittelu aloitettiin 9.9.2022 ja varsinaiset harjoitukset järjestettiin tammi-toukokuussa 2023.
- Välittömästi harjoitusten jälkeen järjestettiin palautetilaisuus, jonka perusteella harjoitus- tarkkailija- ja suunnitteluryhmiltä kerättiin suullinen palaute. Tämän lisäksi harjoitukseen osallistuneille lähetettiin verkkokysely, jonka tulokset ovat tämän raportin liitteenä.

- Harjoituskokonaisuuden tavoitteet saavutettiin hyvin, palautekyselyn perusteella keskiarvo tavoitteiden saavuttamisesta oli 4,3/5.
- Lopputulokset ja tarkemmat palautteet ovat koottuna tähän raporttiin.

Vesihuoltolaitosten yhteinen ja yleinen harjoituskokonaisuus

- Vesihuoltopoolin koordinoimana toteutettiin vesihuoltolaitoksille kyberteemaisia työpöytäharjoituksia etätoteutuksena.
  - 8 harjoitusta
  - 57 vesilaitosta
  - Noin 330 harjoittelijaa
- Hankkeen tilaajana toimi Suomen Vesilaitosyhdistys ry.
- Hankkeen rahoittavat Huoltovarmuuskeskus ja Vesihuoltolaitosten kehittämisrahasto.
- Harjoitusten teemoiksi valittiin laitosten IT- ja OT-järjestelmiin ulkopuolelta kohdistuvat häiriötilanteet, fyysinen turvallisuus, ja mainehaitat.
- Harjoituskokonaisuudesta viestittiin Vesilaitosyhdistyksen ja Instan nettisivuilla.
  - Vesihuoltolaitokset varautuvat kyberuhkiin harjoittelemalla
  - En ymmärrä kyberturvallisuudesta mitään!
  - Vesilaitokset varautuvat kyberuhkiin harjoittelemalla (Insta)

Hankkeen tavoitteet

Suorat tavoitteet

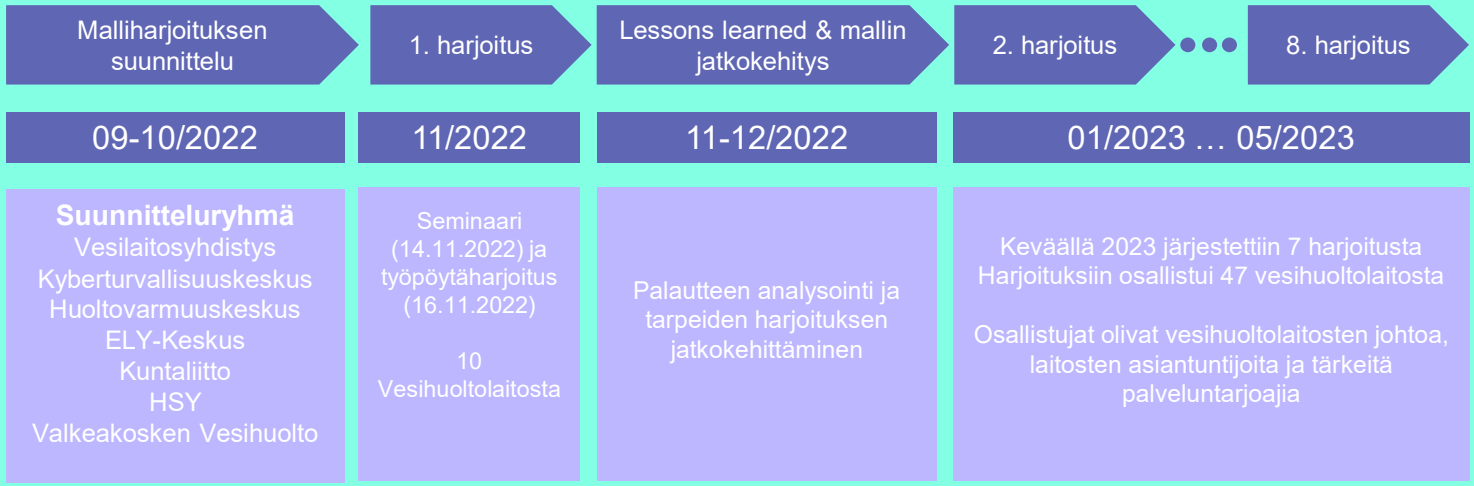
- Herättää motivaatio vesihuoltolaitosten tietoturvallisuuden varmistamiseen ja kehittämiseen.
- Edistää vesihuoltolaitosten tietoturvallisia toimintatapoja ja jakaa tietoa.
- Tukea laitosten nykyisten toimintatapojen ja osaamisen testaamista .
- Tavoittaa tehokkaasti suuri joukko vesi-huoltolaitoksia ja saada tarvittava muutos laajasti liikkeelle.

Välilliset tavoitteet

- Turvata resurssit ja osaaminen hyvään tietoturvallisuuden tasoon vesihuoltolaitoksilla.
- Kehittää valmiuksia vastata NIS2- direktiivin toimeenpanon myötä tuleviin vaatimuksiin.
- Tuottaa syötteitä ohjeiden ja työkalujen parantamiseen ja kehittämiseen.
- Yleisen tietoisuuden lisääminen IT-ja OT-turvallisuuteen liittyen.

Hankkeen ja harjoitusten toteutus

Hankkeen toteutus



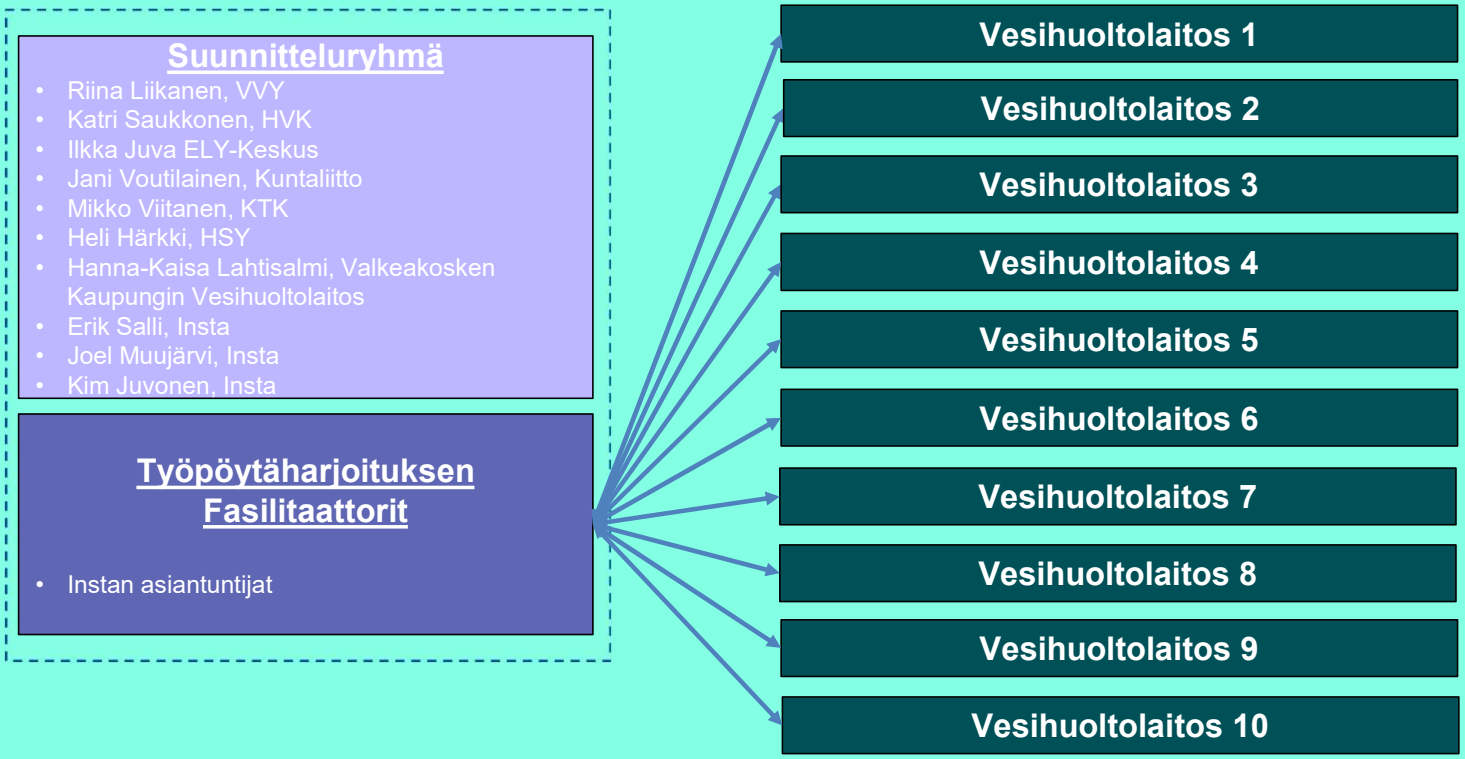
Harjoitusten toteutus

- 8 samansisältöistä harjoitusta toteutettiin talven 2022 ja kevään 2023 aikana.
    - Yksittäinen harjoitus kesti puoli päivää ja toteutustapa oli sama kaikissa kahdeksassa harjoituksessa.
- Osallistujille toimitettiin ennakkomateriaalit noin viikkoa ennen harjoitusta, sisältäen ohjeistusvideon sekä Kyberturvallisuuskeskuksen, Instan ja Vesilaitosyhdistyksen asiantuntijoiden puheenvuorot.
- Harjoituspäivänä osallistujat kirjautuivat Trasim –harjoitusalustalle sekä seurasivat Instan fasilitoimaa harjoitustapahtumaa Teams-kokouksessa.
- Harjoitusalustalla osallistujille jaettiin tilannetta kuvaavia tapahtumakuvauksia sekä tehtäviä organisaatiokohtaisia keskusteluita varten.
- Harjoituksen edetessä osallistujat pääsivät vaihtamaan ajatuksia sekä ratkomaan haasteita paitsi oman tiimin, myös muiden vesihuoltolaitosten kesken.
- Harjoitukseen osallistuneet laitokset kirjasivat havaintoja ja kehityskohteita oman toiminnan kehittämiseksi. Osallistujille tarjottiin dokumenttipohja kehityskohteiden, prioriteettien ja vastuuttamisen kirjaamiseksi.

Yksittäisen harjoituspäivän aikataulu

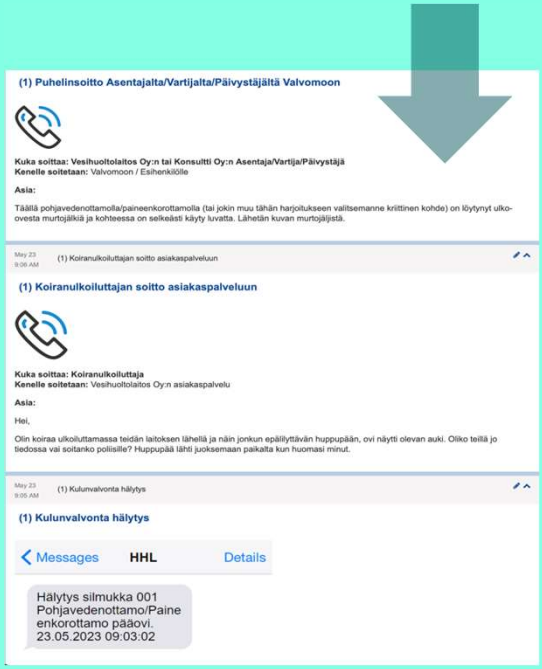
Kellonaika	Tapahtuma
08.45	Aloitustilaisuus: päivän agenda, esittäytymiset, kertaus toimintaohjeista
09.00	Syöte-erä 1
09.05	Keskustelua aiheesta organisaatiokohtaisesti + organisaatioiden yhteinen kommenttikierros
09.45	Syöte-erä 2
09.50	Keskustelua aiheesta organisaatiokohtaisesti + organisaatioiden yhteinen kommenttikierros
10.30-10.40	Tauko 10min
10.40	Syöte-erä 3
10.45	Keskustelua aiheesta organisaatiokohtaisesti + organisaatioiden yhteinen kommenttikierros
11.25	Päivän yhteenveto
12.00	Päivä päättyy (viimeistään)

Yksittäisen harjoituksen organisoituminen

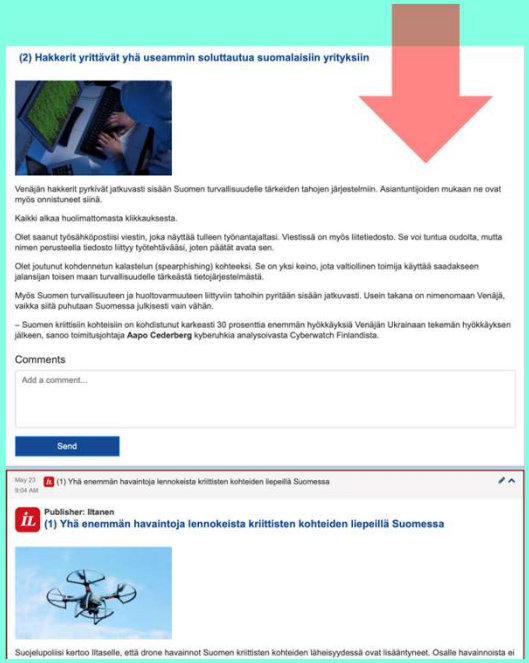


Harjoituksen aikana harjoitusalustalla julkaistiin

Tilannepäivityksiä, jotka ovat faktoja eli ne ovat tietoja ja tapahtumia, jotka ovat todella tapahtuneet harjoitustilanteessa.



Sosiaalisen ja verkkomedian päivityksiä, jotka saattavat liittyä harjoituksen tilannekuvaan. Nämä päivitykset ovat yhtä totta kuin sosiaalisen ja verkkomedian päivitykset oikeassa elämässä.



Skenaarion yhteenveto, Syöte-erä 1

- **Teema 1**, Havainto tietoturva poikkeamasta
  - Työntekijä ilmoittaa että omat käyttäjätunnukset ovat mahdollisesti päätyneet vääriin käsiin.
  - Toimittaja ilmoittaa epäilyttävästä sähköpostista.
  - Palvelutoimittajaksi tekeytyvä pyytää tietoja.
  - **Esimerkkejä kysymyksistä:**
    - Tunnistetaanko tämä tietoturvapoikkeamaksi?
    - Miten ja kenelle ilmoitetaan tietoturvapoikkeamasta oman organisaation sisällä?
    - Mille viranomaisille tulisi ilmoittaa tässä tilanteessa?
- **Teema 2**, Fyysinen turvallisuus
  - Hälytys valvomossa, yhteyskatkohälytys pohjavedenottamossa/paineenkorottamossa (laitoksen kannalta kriittinen kohde).
  - Kulunvalvonnan hälytys.
  - Epäilyttävää toimintaa havaittu kohteen lähellä ja murtojälkiä ovessa.
  - **Esimerkkejä kysymyksistä:**
    - Onko teillä prosessia tai toimintamallia fyysisen turvallisuuden poikkeamien havaitsemiselle? Ovako suunnitelmat ajan tasalla? Vastaavatko ne nykyisiin tarpeisiin?
    - Mitkä ovat ensimmäiset toimet tässä tilanteessa?
    - Kenelle ilmoitetaan tapahtumasta?

Skenaarion yhteenveto, Syöte-erä 2

- **Teema 1**, Haittaohjelma havaitaan toimistoverkossa
  - Office-tuotteet eivät käytössä haittaohjelman takia
  - Estää normaalien työkalujen toiminnan. S-posti, Teams
  - **Esimerkkejä kysymyksistä:**
    - Onko laitoksella selvästi määritellyt vastuut kyberturvallisuuden hallintaan?
    - Varajärjestelmien käyttö (Virve tai vastaavat varajärjestelmät) .
    - Tilannekuvan muodostaminen, ulkoinen/sisäinen kommunikointi.

- **Teema 2**, Pumppaamon murrossa havaitaan mahdollista tunkeutumista järjestelmiin
  - Kytkimeen liitetty tuntematon laite.
  - **Esimerkkejä kysymyksistä:**
    - Onko pääsy kriittisiin laitteisiin rajattu henkilötasolla?
    - Miten toimitaan tilanteessa?
    - Onko omien laitteiden dokumentointi kunnossa?

Skenaarion yhteenveto, Syöte-erä 3

- **Teema 1**, OT-Häiriö
  - Etäyhteys kriittiseen automaatiojärjestelmään katkeaa.
  - **Esimerkkejä kysymyksistä:**
    - Mitkä ovat välittömät toimenpiteet jos etäyhteys kriittiseen kaukovalvonta- ja ohjausjärjestelmään menetetään? Varmuuskopiot, palauttaminen?
    - Onko teillä suunnitelma toiminnan ylläpitämiseksi jos näkyvyys järjestelmään menetetään?
    - OT-järjestelmien/verkkojen turvallisuus, kriittisten kohteiden tietoliikenne varmistettu, palveluntarjoajan kanssa olemassa olevat sopimukset.
    - Onko järjestelmiä mahdollista ajaa käsiohjauksella ja onko tälle toimintamalli?

- Teema 2, Viestinnällinen elementti
  - Toimittaja soittaa vesihuoltolaitokselle ja pyytää haastattelua, spekuloi veden saannin vaarantumisella.
  - **Esimerkkejä kysymyksistä ja keskusteluista:**
    - Mitkä ovat organisaation tärkeimmät ulkoisen viestinnän kanavat? Onko näille varajärjestelyitä?
    - Onko organisaatiossa käytössä kriisiviestintäohje tai vastaava? Onko kyberuhkatilanteet huomioitu viestintäohjeessa?
    - Onko organisaatiossa viestintävastuut selkeät? Kuka tekee viranomaisilmoitukset, tiedottaa henkilöstöä?

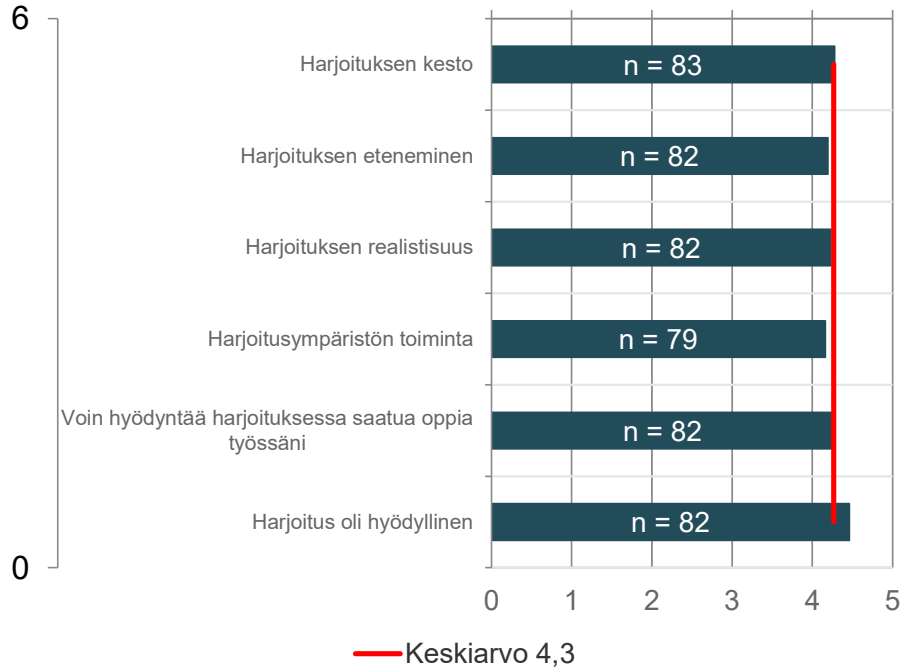
Palautekyselyn yhteenveto

Webropol-kyselyn tulokset ovat kokonaisuudessaan tämän loppuraportin liitteenä.

Palaute harjoituksen toteuttamistavasta. Mielipiteesi harjoituksesta?

Asteikko on 1-5, jossa 1 = erittäin tyytymätön, 2 = jokseenkin tyytymätön, 3 = neutraali (ei erityisen tyytymätön tai erityisen tyytyväinen), 4 = jokseenkin tyytyväinen, 5 = erittäin tyytyväinen, Jos sinulla ei ole mielipidettä / et osaa vastata johonkin kohtaan, jätä se tyhjäksi.

Vastaajien määrä: 79-83



Keskiarvo
4,3
4,2
4,2
4,2
4,3
4,5

- Harjoitus koettiin erittäin hyödylliseksi, arvosanoin 4,5/5.
- Harjoitusympäristöä (harjoitusalustaa) pidettiin havaintojen perusteella tarkoituksenmukaisena ja toimivana, arvosanoin 4,2/5.
- Osallistujat arvoivat, että voivat hyödyntää harjoituksessa saatuja oppeja omassa työssään 4,3/5.

Verkkopalautekysely lähetettiin kaikille harjoituspäiviin osallistuneille. Kyselyyn vastasi 83 henkilöä, vastausprosentti oli 25% kaikista osallistujista.

Arvio miten organisaatiosi kykeni saavuttamaan harjoitukselle asetettuja tavoitteita

Asteikko on 1-5, jossa1 = erityisen huonosti2 = jokseenkin huonosti3 = (neutraali)4 = hyvin5 = erittäin hyvinJos sinulla ei ole mielipidettä / et osaa vastata johonkin kohtaan, jätä se tyhjäksi.

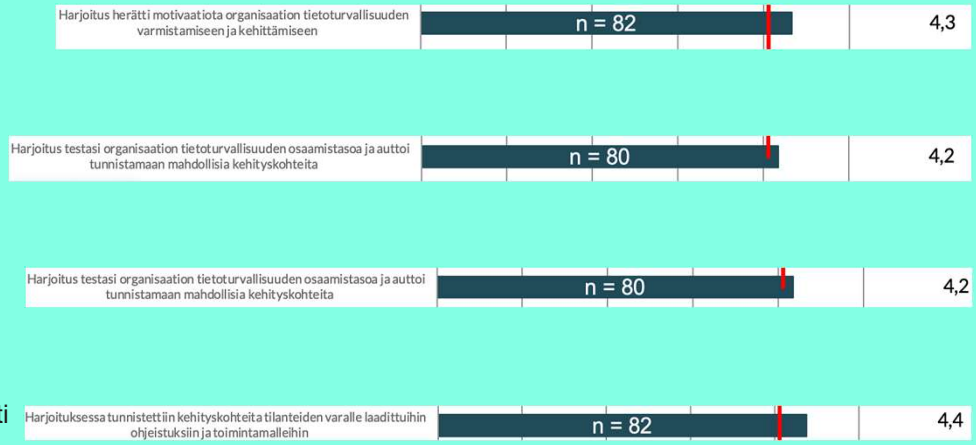
Vastaajien määrä: 75-82

Hankkeen tavoitteiden saavuttamisen arviointi

Yleiset tavoitteet

- Herättää motivaatio vesihuoltolaitosten tietoturvallisuuden varmistamiseen ja kehittämiseen.
- Edistää vesihuoltolaitosten tietoturvallisia toimintatapoja ja jakaa tietoa.
- Tukea laitosten nykyisten toimintatapojen ja osaamisen testaamista .
- Tavoittaa tehokkaasti suuri joukko vesi-huoltolaitoksia ja saada tarvittava muutos laajasti liikkeelle.

Asteikko on 1-5, jossa1 = erityisen huonosti2 = jokseenkin huonosti3 = (neutraali)4 = hyvin5 = erittäin hyvinJos sinulla ei ole mielipidettä / et osaa vastata johonkin kohtaan, jätä se tyhjäksi.



Harjoitukseen osallistui 57 vesilaitosta ja noin 330 harjoittelijaa

Palaute harjoitustoteutukseen liittyen, kehitysehdotuksia harjoituksen parantamiseksi:

”Ehkä etukäteistietona voisi suositella, että laitokselta osallistuvat keräytyisivät samaan tilaan, jos mahdollista.”

”Harjoitus eteni hyvin ja aiheet herättivät keskustelua.”

”Syötteitä oli liikaa suhteessa keskustelulle varattuun aikaan.”

“Harjoituksen vetäjä voisi pyytää ryhmiltä tiukemmin tiivistettyjä puheenvuoroja. Toisaalta tämä, että puheenvuorot olivat hiukan valmistelemattomia, johtui rajallisesta ajasta pohtia tehtäviä. “

”Hyvin toteutettu harjoitus kaiken kaikkiaan”

”Aikaa organisaation sisäiselle keskustelulle oli meidän tapauksessa vähän liikaakin. Tässä varmasti vaikuttaa osallistujaryhmän koko ja kuinka paljon asioita on tehty ja mietitty valmiiksi. Meillä oli pieni ryhmä ja varautumista tehty runsaasti, joten sisäinen keskustelu oli nopeasti käyty läpi. Varmasti suuremmalla ryhmällä lähtökohtaisesti menee enemmän aikaa yhdessä pohtia.”

“Vastaavaan harjoitteluun tulisi saada jatkoa. Kenties alueellisia harjoituksia kerran vuodessa
Konkreettisia vinkkejä olisi saanut olla enemmän kuten lopun puhelinnumerotallennukset ja tulosteet”

”Todella hyvin järjestetty harjoitus! Suur kiitokset!”

“Tuollainen tilateiden simulointi ja kehittäminen on haastava harjoitusmuoto heittäytyä. Tokikin siinä tilanteessa rajoitteet on varmaan enemmän osallistujien päässä, kun esimerkki ei ihan yksi yhteen sovi omaan toimintaan. “

“Keskustelevassa työpöytäharjoituksessa Trasimin alustan käyttö jäi vähäiselle. Pelillisessä harjoituksessa sitten enemmän syötteitä. “

Sana vapaa! Terveisiä järjestäjälle:

”Hyödyllinen ja opettavainen tapahtuma.”

”Hyvä harjoitus, näitä pitäisi pitää säännöllisesti”

” Samanlaisia koulutuksia eri teemoilla.”

”Kaiken kaikkiaan oikein onnistunut ja keskustelua oman organisaation sisällä herättelevä harjoitus.”

” Tämä harjoitus toimi erittäin hyvänä keskustelun herättäjänä ja sai meidän organisaatiossa kaikki osallistumaan keskusteluun. Koska aihe on vakava, niin heräsi ajatus siitä, että tällaisiaa harjoituksen kaltaisia lyhyitä sparraustilaisuuksia vesilaitoksille päivänpolttavista kyberturvallisuusaiheista pitäisi olla vuosittain. Konsepti 1 heräte ja osallistujia 3 vesilaitosta , tilaisuuden kesto 1-1,5h. “

“Ehdottomasti kannattaa järjestää jatkossakin useamman vesilaitoksen yhteisiä harjoituksia. Vertaistuesta ja hyvistä keskusteluista hyötyvät kaikki. “

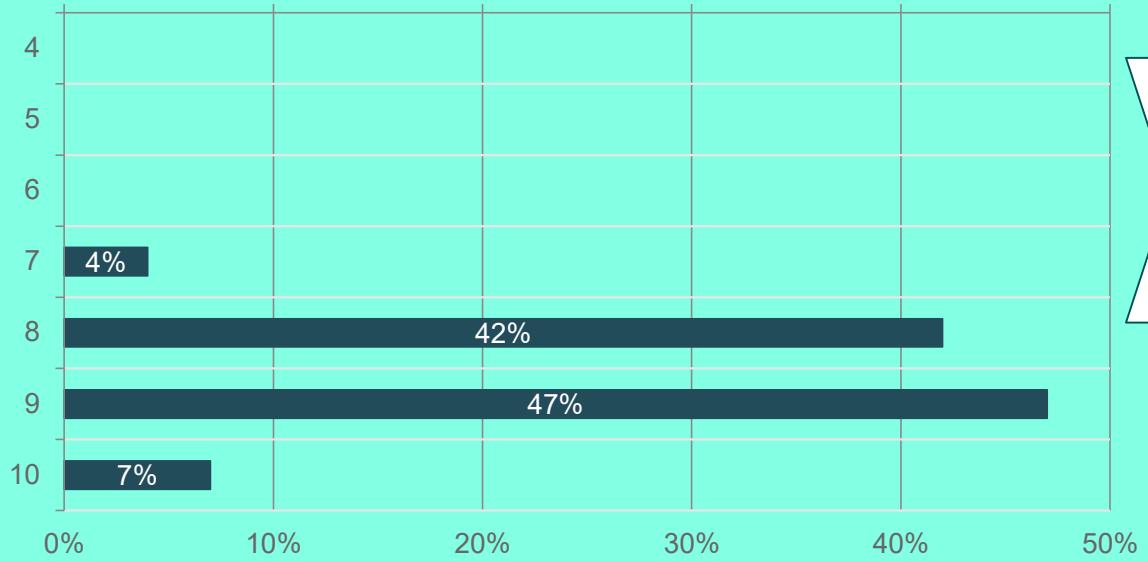
”Kiitokset hyvästä ja ajankohtaisesta tapahtuman toteutuksesta.”

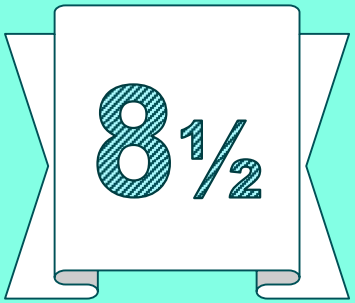
“Harjoitus oli loistava, harjoitus nosti monia asioita esille, joita ei normaalisti tule edes ajatelleeksi.
Löysimme useita parannus ideoita, kehitysideoita, ohjeistuksien puutteita yms. “

“Harjoitus oli oikein hyvä. Skenaariossa oli otettu laajasti huomioon erilaisia uhkia, joten melkoisen kattavan paketin sai sisällytettyä harjoitukseen varattuun aikaan. Olemme varautuneet useimpiin skenaariossa esiteltyihin uhkiin ja riskeihin ainakin jossain määrin, mutta oli hyvin mielenkiintoista harjoituksessa kokea minkälainen tilanne voisi olla jos joutuisi kohdennetun hyökkäyksen alle ja asiat tapahtuisivat yhtäaikaisesti. “

“Erittäin hyvä, että näitä järjestetään. Toivottavasti tämä jatkuu. “

Kokonaisarvosana harjoituksista (kouluarvosana 4-10):





Vastaajien määrä: 79

Yleiset havainnot ja kehittämisehdotukset

Yleiset havainnot harjoituksista

- Vaikka harjoituksiin osallistuneiden vesihuoltolaitosten koko vaihteli paljon, kriisinjohtamisen ja häiriötilanteiden ohjeistuksen ja dokumentaation kehittäminen nousi esille kaikissa harjoituksessa selvänä kehityskohteena.
    - Useat laitokset kommentoivat, että toimintamalleja on olemassa mutta niiden dokumentointi on puutteellista.
- VAP (Henkilövarukset) nousi keskusteluissa usein esille, ja keskustelujen perusteella vesihuoltolaitoksilla olivat omat varukset pääsääntöisesti hyvällä mallilla. Keskeisten palveluntuottajien henkilövarausten ja ajoneuvojen ja työkoneiden varausten selvittäminen kirjattiin usealla laitoksella selvitettäväksi toimenpiteeksi.
- Useat vesihuoltolaitokset kommentoivat, että yleisesti varautumiseen on panostettu viime aikoina, mutta kyberuhkiin on kiinnitetty huomiota huomattavasti vähemmän tai ei juuri ollenkaan.
- Useat vesihuoltolaitokset korostivat henkilöstön jatkuvan tietoturvakoulutuksen tarpeellisuutta.
- Ulkoisen ja sisäisen viestinnän toimintamallien puutteet ja kehittämien nousi kaikissa harjoituksissa esille.
- Harjoitus herätti usealla laitoksella tarvetta keskustella kaupungin tai keskeisen palveluntuottajan kanssa yhteistyöstä tietohallinnon ja tietoturvan näkökulmasta.
- Yleisesti harjoituksissa kiiteltiin mahdollisuudesta päästä kuulemaan ja keskustelemaan muiden laitosten kanssa.

Yleiset kehitysehdotukset harjoituksista

- Kriisinjohtamisen ja häiriötilanteiden ohjeistuksen ja dokumentaation kehittäminen/päivittämien/luominen kyberuhkien varalle.
- Keskeisten palveluntuottajien henkilövarausten sekä ajoneuvojen ja työkoneiden varausten selvittäminen ja varmistaminen.
- Keskeisten viranomaisten yhteystietojen selvittäminen ennalta, ohjeiden päivittäminen.
- Tietoturvakoulutusten aktiivinen järjestäminen ja henkilöstön tietoisuuden ylläpitäminen.
- Ulkoisen ja sisäisen viestinnän toimintamallien kehittäminen ja ohjeistusten päivittäminen.
- Keskustelun käynnistäminen tai ylläpito kaupungin tai keskeisen palveluntuottajan kanssa yhteistyön parantamiseksi tietotuvan näkökulmasta.

Huoltovarmuusorganisaatio

Fiksua huoltovarmuutta yhdessä.

Varmuuden vuoksi.

huoltovarmuuskeskus.fi varmuudenvuoksi.fi