**Kyberharjoituksen harjoitussuunnitelma**

**TTKW0310 Kyberharjoituksen suunnittelu ja valmistelu**

Joni Ahonen

Matti Ruusupiha

Ville Sepponen

Mikko Seppänen

Tatu Viitikko  
Petteri Virtanen

Harjoitustyö

Syksy 2017

Tekniikan ja liikenteen ala

Insinööri (AMK), tieto –ja viestintätekniikan tutkinto-ohjelma

Kyberturvallisuus

# Sisältö

[Sisältö 1](#_Toc500957856)

[1 Johdanto 6](#_Toc500957857)

[1.1 Miksi kyberharjoitusten suunnitteleminen ja toteuttaminen on tärkeää? 6](#_Toc500957858)

[1.1.1 Tapahtuneita kyberhyökkäyksiä 6](#_Toc500957859)

[1.1.2 Miksi datan suojaaminen tulee yrityksen talouden kannalta tärkeämmäksi kuin koskaan? 7](#_Toc500957860)

[2 Harjoitettava organisaatio 8](#_Toc500957861)

[2.1 Taustakertomus 8](#_Toc500957862)

[2.2 Organisaatiokaavio 8](#_Toc500957863)

[3 Harjoituksen tavoitteet, harjoitusmuoto, rajaukset ja osallistujat 9](#_Toc500957864)

[3.1 Harjoituksen tavoitteet 9](#_Toc500957865)

[3.2 Harjoitusmuoto ja rajaukset 9](#_Toc500957866)

[3.3 Harjoituksen osallistujat 10](#_Toc500957867)

[4 Harjoituksen suunnittelu 10](#_Toc500957868)

[4.1 Suunnittelun aikataulu 10](#_Toc500957869)

[4.2 Suunnittelutyöryhmän tehtävät 11](#_Toc500957870)

[4.3 Suunnitteluryhmän kokoonpano 11](#_Toc500957871)

[5 Harjoituksen toteutus 11](#_Toc500957872)

[5.1 Toteutuksen ajankohta 11](#_Toc500957873)

[5.2 Toteutukseen osallistuvat joukkueet ja niiden tehtävät 12](#_Toc500957874)

[5.2.1 Puolustavan joukkueen (Blue Team) tehtävät 12](#_Toc500957875)

[5.2.2 Johtavan joukkueen (White Team) tehtävät 13](#_Toc500957876)

[5.3 Skenaario 13](#_Toc500957877)

[5.4 Uhkatoimijat 14](#_Toc500957878)

[5.4.1 Ryhmä-X 14](#_Toc500957879)

[5.4.2 Ryhmä-Y 14](#_Toc500957880)

[5.5 Harjoituksen kulku 15](#_Toc500957881)

[5.6 Harjoituksessa käytettävät syötteet 15](#_Toc500957882)

[1.1.1 White Team-syötteet 15](#_Toc500957883)

[5.6.1 Red Team-syötteet 16](#_Toc500957884)

[5.7 Vaste 18](#_Toc500957885)

[6 Harjoitusympäristö 18](#_Toc500957886)

[6.1 Harjoitusympäristön vaatimat laiteresurssit 19](#_Toc500957887)

[6.2 Harjoitusympäristön rakenne 19](#_Toc500957888)

[6.3 Harjoitusympäristön virtuaalikoneiden tiedot ja palvelut 21](#_Toc500957889)

[6.4 Harjoitettavan organisaation tietoturvakontrollit harjoitusympäristössä 22](#_Toc500957890)

[6.5 Harjoitusympäristön testaus 22](#_Toc500957891)

[7 Perehdytys 23](#_Toc500957892)

[7.1 Harjoituksen yleisjärjestelyt 23](#_Toc500957893)

[7.2 Harjoituksen yleinen aikataulutus 23](#_Toc500957894)

[7.3 Harjoitettavat organisaatioyksiköt 23](#_Toc500957895)

[7.4 Harjoituksen tekninen perehdytys 24](#_Toc500957896)

[7.5 Harjoituksen turvallisuus 24](#_Toc500957897)

[7.6 Puolustavien ja hyökkäävien joukkueiden roolitus 24](#_Toc500957898)

[7.6.1 Blue Team 24](#_Toc500957899)

[7.6.2 Red Team 25](#_Toc500957900)

[7.6.3 White Team 25](#_Toc500957901)

[7.7 Harjoituksen säännöt 25](#_Toc500957902)

[8 Harjoituksen arviointi 26](#_Toc500957903)

[Lähteet 28](#_Toc500957904)

[Liitteet 28](#_Toc500957905)

[Liite 1. Organisaatiokaavio (Täydellinen) 29](#_Toc500957906)

[Liite 2. Harjoituksen pelitapahtumat ja syötteet 30](#_Toc500957907)

[Liite 4. Harjoituksen perehdytysmateriaali 31](#_Toc500957908)

[Liite 5. Harjoitusympäristön perehdytysmateriaali (Tekninen) 36](#_Toc500957909)

[Liite 6. Arviointi ja arvostelulomake (Osallistujalle) 40](#_Toc500957910)

[Liite 7. Arviointi ja arvostelulomake (Järjestäjälle) 44](#_Toc500957911)

**Kuviot**

[Kuvio 1. Data Breach Incidents by Type of Occurrence 7](#_Toc500956067)

[Kuvio 2. Organisaatiokaavio (Organisaation harjoitukseen osallistuvat yksiköt) 9](#_Toc500956068)

[Kuvio 3. Harjoitusympäristön topologia 20](#_Toc500956069)

[Kuvio 4. Organisaation roolitus harjoituksessa 25](#_Toc500956070)

**Taulukot**

[Taulukko 1. Terminologia 5](#_Toc500956071)

[Taulukko 2. Suunnittelun aikataulu 10](#_Toc500956072)

[Taulukko 3. Harjoitukseen osallistuvat joukkueet ja niiden koostumus 12](#_Toc500956073)

[Taulukko 4. Puolustavan joukkueen (Blue Team) tehtävät 12](#_Toc500956074)

[Taulukko 5. Johtavan joukkueen (White Team) tehtävät 13](#_Toc500956075)

[Taulukko 6. Harjoituksen aikataulutus (Suppea) 15](#_Toc500956076)

[Taulukko 7. White Team-syötteet 15](#_Toc500956077)

[Taulukko 8. Red Team-syötteet 16](#_Toc500956078)

[Taulukko 9. Red Team-syötteiden kuvaus 16](#_Toc500956079)

[Taulukko 10. Vastesuunnitelma kyberpoikkeamalle. 18](#_Toc500956080)

[Taulukko 11. Harjoitusympäristön vaatimat fyysiset laiteresurssit 19](#_Toc500956081)

[Taulukko 12. Palvelu- ja konfiguraatiotaulukko (osa 1/2) 21](#_Toc500956082)

[Taulukko 13. Palvelu- ja konfiguraatiotaulukko (osa 2/2) 21](#_Toc500956083)

[Taulukko 14. Organisaation tietoturvakontrollit harjoitusympäristössä 22](#_Toc500956084)

[Taulukko 15. Harjoituksen yleinen aikataulutus 23](#_Toc500956085)

Taulukko 1. Terminologia

|  |  |
| --- | --- |
| Termi | Termin määritelmä |
| Kyberhyökkäys | Verkon välityksellä suoritettu vahingollinen teko/teon yritys |
| Kyberharjoitus | Suunniteltu tapahtuma jossa simuloidaan kyberhyökkäystä ja testata organisaation kykyä estää, lieventää, vastata ja toipua häirinnästä |
| Tietomurto | Tapaus missä arkaluontoista, suojattua tai luottamuksellista tietoa on päätynyt väärille tahoille |
| Hacking | Hacking/hakkerointi on järjestelmien heikkouksien tunnistamista ja hyväksikäyttämistä |
| Phishing | Kohdistettua tietojen kalastelua käyttäen sähköpostia, puhelinta tai muita metodeja tarkoituksena saada haltuun tärkeitä tunnistautumistietoja kuten salasanoja, naamioitumalla luotettavaksi tahoksi |
| Skimming | Transaktion aikana tapahtuva tietojen varastaminen osapuolien välistä, esimerkiksi käsittelemällä käytettäviä laitteita, kuten kortinlukijaa |
| Blue Team | Tiimi jonka tehtävänä on toimia harjoituksessa puolustavan osapuolen roolissa |
| Red Team | Tiimi jonka tehtävänä toimia harjoituksessa hyökkäävien osapuolien roolissa |
| White Team | Tiimi joka vastaa harjoituksen kulusta. Tiimi vastaa syötteiden syötöstä, valvoo osapuolten toimintaa, arvostelee toimintaa sekä selvittää mahdollisia ongelmia harjoituksen kuluessa |
| Pelitapahtuma | Tapahtumat pelin kuluessa jotka määrittävät pelin kulun |
| Syöte | Pelitapahtumaan liittyvät toimet, jotka aiheuttavat toimenpiteitä peliin osallistuvilta osapuolilta. |

1. **Johdanto**

Kyberharjoitukset ovat nykyisin, sekä tulevaisuudessa kasvavissa määrin, olennainen osa jokaisen organisaation toimintaa. Tässä dokumentissa on esitelty kuvitteelliselle organisaatiolle suunniteltu kyberharjoituksen harjoitussuunnitelma. Harjoitus on räätälöity vastaamaan kuvitteellista reaalimaailmaan skenaariota, realistisine uhkatekijöineen.

## Miksi kyberharjoitusten suunnitteleminen ja toteuttaminen on tärkeää?

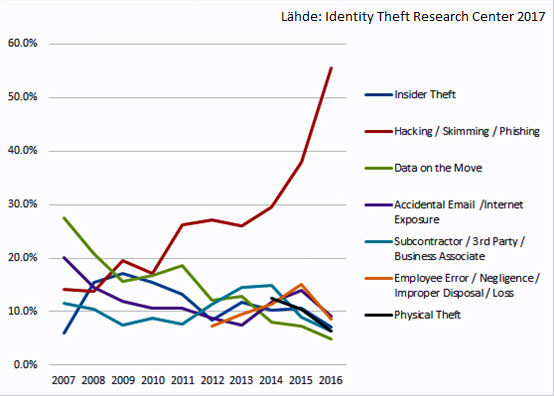
Nykyaikaisissa tietojärjestelmissä varsinaisen tiedon suojaaminen on noussut keskeiseen rooliin. Tietoverkkojen turvallisuuden ja suojaamisen sijaan yrityksillä ja yhteisöillä onkin kasvava tarve lisätä kyberturvallisuuden roolia toiminnassaan, jotta sähköinen arkaluontoinen tieto voitaisiin turvata oikein. Vaikka tiedon suojaaminen on noussut keskeiseen rooliin, sen suojaamiselle ei ole olemassa yhtä yleisesti hyväksyttyä lähestymistapaa (Kohnke, Shoemaker & Singler). Tämä luo tarpeen yrityksille ja yhteisöille luoda tietojärjestelmilleen omat yksilölliset suojausmekanismit ja menetelmät. Tietojärjestelmien kovennuksen ja suojaamisen lisäksi yrityksen on koulutettava henkilökuntaansa, jotta tietoa vaarantavilta uhkilta osattaisiin puolustautua. Kyberharjoitusten suunnittelussa ja toteutuksen tarkoituksena on siis kasvattaa yrityksen tai toimijan valmiutta turvata arkaluontoinen tieto, kun se kohtaa sitä vaarantavia uhkia.

### Tapahtuneita kyberhyökkäyksiä

Maailmalla tapahtuu jatkuvasti pieniä ja isoja tietomurtoja. Esimerkiksi vuonna 2016 tietomurrot lisääntyivät arviolta 40% edelliseen vuoteen verrattuna. (identityforce.com)

Wikipediasta löytyy vaikuttavan pitkä lista tietomurroista: <https://en.wikipedia.org/wiki/List_of_data_breaches>

Vuodesta 2007 ITCR (Identity Theft Resource Center) alkoi lisätä kategorioita tunnistamaan erilaisia tietomurtoja niiden tapahtumatyypin mukaan. Kahdeksana peräkkäisenä vuonna erilaiset hacking, phishing ja skimming-hyökkäykset olivat suurin syy tietomurtoihin, aiheuttaen yhtensä 55,5 prosenttia kaikista tietomurroista, joka on 17,7 prosentin nousu vuoden 2015 luvuista. Kuviosta 1 näkee erittäin hyvin viime vuosien suunnan. ITCR:n tilastoissa aikavälillä tammikuu 2005 vuoden 2017 syyskuu tapahtui yhteensä 7920 tietomurtoa ja paljastettujen tietueiden määrä (Number of Records Exposed) oli 1 046 870 879. (2016 Databreaches 2017)



Kuvio 1. Data Breach Incidents by Type of Occurrence

### Miksi datan suojaaminen tulee yrityksen talouden kannalta tärkeämmäksi kuin koskaan?

Vuonna 2018 astuu voimaan uusi Euroopan Unionin tietosuoja-asetus GDPR (Genera Data Protecting Regulation). Tämä asetus määrittelee muun muassa sen, miten asiakkaiden dataa tulee säilyttää ja miten asiakkaat voivat hallita omaa dataansa. Asetus koskettaa kaikkia yrityksiä, jotka prosessoivat Euroopan Unionin alueella asuvien asiakkaiden dataa, katsomatta yrityksen sijaintia. Mikäli yrityksen todetaan laiminlyövän tietoturva-asetuksen vaatimuksia, sitä voidaan sakottaa jopa 4% yrityksen liikevaihdoista tai 20 miljoonaa euroa, riippuen siitä, kumpi summa on suurempi. Myös pienempiä sakkoja voidaan antaa esimerkiksi viranomaisille datamurrosta kertomatta jättämisestä. Asetuksessa määritellään, että yritykseen on nimettävä yrityksen tietosuojavastaava, jonka päätehtävä on toimia välikätenä yhtiön ja viranomaisten välillä. On tärkeää huomata, että tämä asetus tulee koskemaan sekä datan prosessoijia, että säilyttäjiä, eli myös pilvipalveluiden oletetaan noudattavan sitä.

Asetuksen myötä yhtiön asiakkaat tulevat saamaan sekä paremman tietosuojan että enemmän oikeuksia sellaisten omien tietojensa suhteen, joita yhtiössä käsitellään tai säilytetään. Nyt on siis parempi aika kuin koskaan hoitaa yhtiön asiakkaiden datan säilyttämiseen ja käsittelyyn liittyvät asiat kuntoon. On selvää, että asetuksen tarkoituksena on tehdä datan vastuullisesta käsittelystä halvempaa kuin asetuksen laiminlyömisestä. (eugdpr.com)

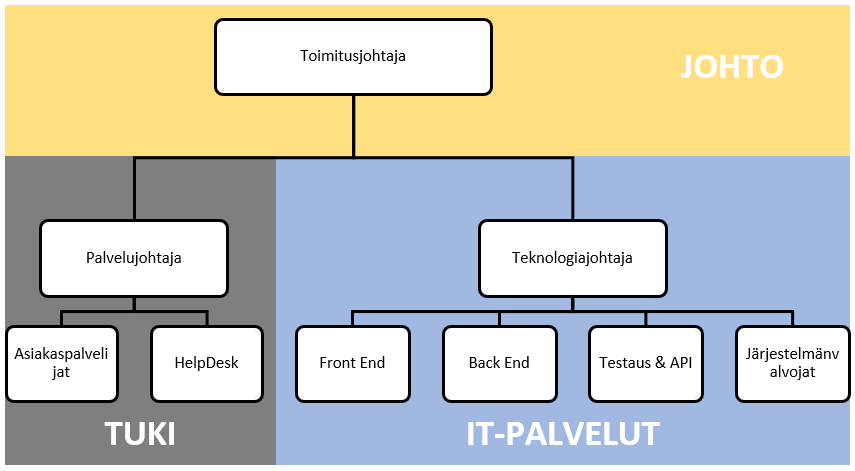
# Harjoitettava organisaatio

## Taustakertomus

DataCenter Oy on toiminut ja palvellut asiakkaitaan vasta vuoden. Organisaatio on uusi toimija alalla, eikä ole joutunut testaamaan puolustautumiskykyään todellisia kyberuhkia vastaan. Organisaation henkilöstöllä ei ole huomattavaa aikaisempaa kokemusta tietoturvauhkilta puolustautumiselta. DataCenter Oy tarjoaa tallennustilaa organisaatioille ja yksityishenkilöille, jotka eivät halua investoida omaan infrastruktuuriin. DataCenter Oy:n vastuulla on siis huolehtia asiakkaidensa arkaluontoisesta tiedosta asianmukaisella suojauksella.

## Organisaatiokaavio

DataCenter Oy:n suppea organisaatiokaavio on esitelty Kuviossa 2, johon on rajattu ainoastaan organisaation harjoitukseen osallistuvat yksiköt. Organisaatiokaavio on kokonaisuudessaan esitelty Liitteessä 1.



Kuvio 2. Organisaatiokaavio (Organisaation harjoitukseen osallistuvat yksiköt)

# Harjoituksen tavoitteet, harjoitusmuoto, rajaukset ja osallistujat

## Harjoituksen tavoitteet

Kyberharjoituksen tavoitteena on testata ja määritellä pilvitallennustilaa tarjoavan organisaation DataCenter Oy:n henkilöstön ja järjestelmien kyky vastata kyberuhkiin sekä kyky toipua kyberpoikkeamatilanteista. Harjoituksessa havainnoidaan myös työntekijöiden toimintakykyä näissä tilanteissa. Harjoituksen tavoitteena on lisäksi harjoitukseen osallistuvan organisaation henkilöstön roolien ja vastuualueiden selkiyttäminen, toiminnan kehittäminen, asiantuntijoiden osaamisen lisääminen sekä organisaation toiminnan tehostaminen. Tavoitteena on myös harjoituksen järjestäjien osaamisen kehittäminen harjoituksen ideoinnissa, suunnittelussa ja valmistelussa, toteutuksessa sekä arvioinnissa.

## Harjoitusmuoto ja rajaukset

Toteutettava harjoitus on rakenteeltaan teknillistoiminnallinen. Harjoitus on rajattu järjestelmiin, joita organisaatio käyttää palvelujensa tarjoamiseen kuluttajille sekä niihin järjestelmiin, jotka ovat kytköksissä näihin järjestelmiin.

## Harjoituksen osallistujat

Harjoitukseen osallistuu tieto- ja viestintätekniikan tutkinto-ohjelmasta, Kyberharjoituksen suunnittelu ja toteutus-opintojakson opiskelijoista muodostettuja 4-6 henkilön tiimejä, jotka toimivat harjoituksessa organisaation työntekijöiden roolissa. Opiskelijoiden lisäksi harjoitukseen osallistuu Kyberharjoituksen suunnittelu ja toteutus-opintojakson vastuuopettajat Terho Rintanen ja Karo Saharinen.

# Harjoituksen suunnittelu

## Suunnittelun aikataulu

Taulukossa 2 on esitelty harjoituksen suunnittelun aikataulu

Taulukko 2. Suunnittelun aikataulu

|  |  |
| --- | --- |
| **Viikko** | **Sisältö** |
| **35** | Suunnittelutyöryhmän muodostaminen |
| **36** | Ideointi |
| **37** | Harjoitussuunnitelman luonnostelu |
| **38** | Harjoitussuunnitelman suunnitteluosuuden valmistelu |
| **39** | Harjoitussuunnitelman suunnitteluosuuden viimeistely |
| **40** | Harjoitustekniset dokumenttiluonnokset |
| **41** | Teknisen suunnitelman toteutus (aloitus) |
| **42** | Teknisen suunnitelman toteutus (keskivaihe) |
| **43** | Teknisen suunnitelman toteutus (lopetus) |
| **44** | Teknisen osuuden testaus |
| **45** | Perehdyttämissuunnitelman ja materiaalin laatiminen ja viimeistely |
| **46** | Harjoitussuunnitelman arviointimateriaalin laatiminen ja viimeistely |
| **47** | Harjoitussuunnitelman viimeistely |
| **48** | Harjoitussuunnitelman viimeistely |
| **49** | Harjoitussuunnitelman viimeistely |
| **50** | Harjoitussuunnitelman palautus |

## Suunnittelutyöryhmän tehtävät

Suunnittelutyöryhmän tehtäviin kuuluu harjoituksen ideointi, suunnittelu ja valmistelu, harjoitukseen osallistuvien henkilöiden perehdyttäminen sekä roolien ja ryhmien jakaminen, sekä itse harjoituksen toteuttaminen, johtaminen ja arviointi.

## Suunnitteluryhmän kokoonpano

Suunnitteluryhmä koostuu kuudesta Jyväskylän Ammattikorkeakoulun kolmannen vuoden tieto -ja viestintätekniikan tutkinto-ohjelman opiskelijasta:

Joni Ahonen [h8545@student.jamk.fi](mailto:h8545@student.jamk.fi)

Matti Ruusupiha [k1889@student.jamk.fi](mailto:k1889@student.jamk.fi)

Ville Sepponen [k2335@student.jamk.fi](mailto:k2335@student.jamk.fi)

Mikko Seppänen [k2851@student.jamk.fi](mailto:k2851@student.jamk.fi)

Tatu Viitikko [k1849@student.jamk.fi](mailto:k1849@student.jamk.fi)

Petteri Virtanen [k2267@student.jamk.fi](mailto:k2267@student.jamk.fi)

# Harjoituksen toteutus

## Toteutuksen ajankohta

Harjoitus toteutetaan 14.12.2017 kello 8:00-11:15 Jyväskylän Ammattikorkeakoulun opetustiloissa, osoitteessa Piippukatu 2, 40100 Jyväskylä.

## Toteutukseen osallistuvat joukkueet ja niiden tehtävät

Taulukko 3. Harjoitukseen osallistuvat joukkueet ja niiden koostumus

|  |
| --- |
| **Red Team** |
| Harjoituksen uhkatoimijat, Ryhmät X ja Y. (Suunnitteluryhmä R1) |
| **Blue Team** |
| DataCenter Oy:n työntekijät. (Opintojaksolle osallistuvat opiskelijat) |
| **White Team** |
| Elävöittävät pelisyötteet, pelin johtaminen ja ohjaus. (Suunnitteluryhmä R1) |
| **Green Team** |
| Tarjoaa puitteet harjoituksen suorittamiseen. (vastuuopettajat Terho Rintanen ja Karo Saharinen) |

### Puolustavan joukkueen (Blue Team) tehtävät

Taulukko 4. Puolustavan joukkueen (Blue Team) tehtävät

|  |
| --- |
| **Toimitusjohtaja** |
| On vastuussa organisaation toiminnan johtamisesta. On teknologiajohtajan ja palvelujohtajan esimies ja vastaa viime kädessä organisaation päätöksenteosta |
| **Teknologiajohtaja** |
| On vastuussa organisaation IT-palveluyksikön johtamisesta ja toimii yhteyshenkilönä yksikön ja toimitusjohtajan välillä. Teknologiajohtajalla on valtuudet tehdä yksikköänsä koskevia päätöksiä, kuitenkin raportoiden toimensa toimitusjohtajalle. Teknologiajohtajalla ei ole valtuuksia tehdä organisaation toiminnan kannalta merkittäviä päätöksiä |
| **Front End** |
| Vastaavat organisaation verkkosivujen ulkoasusta ja sisällöntuottamisesta. Päätöksentekoa tarvitsevissa asioissa on yhteydessä teknologiajohtajaan |
| **Back End** |
| Vastaavat organisaation ohjelmoinnin tuottamisesta. Päätöksentekoa tarvitsevissa asioissa on yhteydessä teknologiajohtajaan |
| **Testaus & API** |
| Vastaavat organisaation uusien järjestelmien ja ohjelmistojen testauksesta ja käyttöönotosta. Päätöksentekoa tarvitsevissa asioissa on yhteydessä teknologiajohtajaan |
| **Järjestelmänvalvojat** |
| Valvoo ja ylläpitää organisaation järjestelmiä. Päätöksentekoa tarvitsevissa asioissa on yhteydessä teknologiajohtajaan |
| **Palvelujohtaja** |
| On vastuussa organisaation tuki-yksikön johtamisesta ja toimii yhteyshenkilönä yksikön ja toimitusjohtajan välillä. Palvelujohtajalla on valtuudet tehdä yksikköänsä koskevia päätöksiä, kuitenkin raportoiden toimensa. toimitusjohtajalle. Palvelujohtajalla ei ole valtuuksia tehdä organisaation toiminnan kannalta merkittäviä päätöksiä |
| **Asiakaspalvelijat** |
| Vastaavat organisaation asiakkaiden lähettämiin sähköpostiviesteihin ja puheluihin. Asiakaspalvelijat välittävät asiakkaat, joilla on ongelmia organisaatio palveluiden käytössä HelpDesk-tuelle. Päätöksentekoa tarvitsevissa asioissa on yhteydessä palvelujohtajaan |
| **HelpDesk** |
| Vastaavat asiakkaiden opastamisesta organisaation palveluiden käytössä. Päätöksentekoa tarvitsevissa asioissa on yhteydessä palvelujohtajaan |

### Johtavan joukkueen (White Team) tehtävät

Taulukko 5. Johtavan joukkueen (White Team) tehtävät

|  |
| --- |
| **DataCenter Oy:n asiakas** |
| Tallentaa tiedostoja DataCenter Oy:n tallennustilaan, jättää kommentteja ja ottaa yhteyttä DataCenter Oy:n asiakaspalveluun |
| **SoMe vastaava/yleinen tunnelma** |
| Päivittää sosiaalista mediaa, vastaa yleisen tunnelman luomisesta (videot, artikkelit, lausunnot, sähköpostit, puhelut) |
| **Konsultti** |
| Auttaa Blue Team:ia mahdollisissa ongelmatilanteissa |
| **Uhkatoimijat** |
| Johtavan joukkueen jäsenistä koostuva ryhmä hoitaa harjoituksessa uhkatoimijoiden toimenpiteet |

## Skenaario

Pilvitallennustilaa tarjoaviin organisaatioihin on viime aikoina kohdistettu uhkia. Salasanoja ja tiedostoja on varastettu useissa eri tietomurroissa ja viranomaiset ovatkin kehottaneet organisaatiota kehittämään ja suojaamaan palveluitaan kyberuhkia vastaan. Lisäksi media uutisoi aiheesta luoden yleisen mielipiteen.

DataCenter Oy on nopeasti kehittyvä tallennustilaa tarjoava organisaatio minkä suositellaan kehittävän omaa toimintaa kyberuhkaa vastaan sekä kehittävän omaa vastesuunnitelmaa kyberpoikkeamalle.

Ulkomailla sijaitsevat toimijat kohdistavat DataCenter Oy:tä kohtaan kyberuhkia. Uhka kohdistuu erityisesti DataCenter Oy:n tärkeisiin asiakasrajapintoihin. Hakkeriryhmittymät ovat suorittaneet palvelunestohyökkäyksiä kilpaileviin organisaatioihin ja ovat toimillaan estäneet asiakkaiden pääsyn tärkeisiin tiedostoihinsa. Nämä haitalliset toimijat ovat toimineet ulkopuolisen rahoituksen avustamana. Virtasen Pilvet organisaatio on syyttänyt uudempaa toimijaa DataCenter Oy:ta liiketoiminnan häiritsemisestä, ilman tarkempia tietoja ja on yrittänyt mustamaalata DataCenter Oy:n, aiheuttaen luottamuspulaa henkilöstössä.

## Uhkatoimijat

### Ryhmä-X

Ryhmä-X haluaa päästä käsiksi DataCenter Oy:n asiakkaiden tietoihin ja myydä niitä voitolla hämäräperäisillä markkinoilla. Ryhmä-X yrittää löytää takaporttia/heikkoutta DataCenter Oy:n porteissa, jotta pääsisivät käsiksi palvelimilla oleviin asiakkaiden tietoihin. Ryhmä-X:n etujen mukaista on tehdä hyökkäys piilossa pysyen. Ryhmä-X voi yrittää kerätä tietoa myös sosiaalisella tietojenkalastelulla ja fyysisellä palvelimiin/päätelaitteisiin käsiksi pääsyllä.

### Ryhmä-Y

Ryhmä-Y pyrkii häiritsemään DataCenter Oy:n toimintaa ja sotkemaan organisaation verkkosivut saadakseen mainetta ja kunniaa hämärissä piireissä. Ryhmä-Y aiheuttaa sosiaalisessa mediassa DataCenter Oy:lle haitallista mainetta. Ryhmä-Y aloittaa toimintansa myös verkkojen skannauksella. Ryhmä tavoittelee verkon häiriköintiä ja hidastamista. Toisin kuin Ryhmä-X, Ryhmä-Y ei pyri välttämättä tekemään hyökkäystään piilossa vaan se voi tehdä hyvinkin näkyvän hyökkäyksen. Ryhmä-Y käyttää hyökkäyksessään esimerkiksi DDoS:sta tai tuhrii organisaation kotisivut.

## Harjoituksen kulku

Taulukossa 6 on esitelty harjoituksen suppea aikataulutus, joka sisältää yleiskuvauksen harjoituksen kulusta. Aikataulu on joustava, joten pienet muutokset aikatauluun pelin aikana ovat mahdollisia harjoitusta johtavan joukkueen (White Team) toimesta. Harjoituksessa käytettävien syötteiden tarkka kuvaus on esitelty kappaleessa 4.7 Harjoituksen syötteet ja Liittessä 2, ja harjoituksen tarkka aikataulutus yksityiskohtineen Liitteessä 2.

Taulukko 6. Harjoituksen aikataulutus (Suppea)

|  |  |
| --- | --- |
| **Kellonaika** | **Tapahtuma** |
| **8:00** | Ympäristöön tutustuminen, Blue Team aloittaa työskentelyn |
| **8:20** | Aktiivivaihe alkaa, Uhkatoimijoiden syötteet ja puolustavan joukkueen vasteet |
| **10:45** | Aktiivivaihe päättyy, Harjoitus päättyy |
| **11:00** | Tilannekatsaus |

## Harjoituksessa käytettävät syötteet

* + 1. White Team-syötteet

Johtavan joukkueen syötteet ovat syötteitä, joita ei luokitella uhkaaviksi eli ne ovat luokiteltavissa tavanomaiseksi verkkoliikenteeksi. Nämä peliä elävöittävät syötteet on esitelty Taulukossa 7.

Taulukko 7. White Team-syötteet

|  |
| --- |
| **Käytettävät White Team-syötteet** |
| Asiakas soittaa asiakaspalveluun: Dataa on hävinnyt/Kirjautuminen ei onnistu/Yhteydet on hitaat/Sivulla omituista sisältöä |
| Sähköposti DataCenter Oy:n asiakkaalta tai henkilöstöltä, jossa kysytään miksi jokin tietty asia ei toimi |
| Yhtiön palautesivuille generoidaan yleistä kommentointia automatisoidusti |

### Red Team-syötteet

Taulukossa 8 on esitelty harjoituksen uhkatoimijoiden syötteitä. Nämä syötteet ovat haitallisia organisaation toiminnalle ja ne pyritään havaitsemaan, raportoimaan ja estämään harjoituksen aikana puolustavan joukkueen toimesta. Taulukossa 9 on kerrottu uhkatoimijoiden syötteistä tarkemmin kuvaamalla niiden toimintaa, miten ne havaitaan sekä toivotuista reaktioista.

Taulukko 8. Red Team-syötteet

|  |
| --- |
| **Käytettävät Red Team-syötteet** |
| Red Team toteuttaa porttiskannauksen (Nikto/Nmap) DataCenter Oy:tä kohtaan. Red Team käyttää eri IP-osoitetta hyökkääjän tunnistamisen vaikeuttamiseksi |
| Palvelunestohyökkäys WWW-palvelinta kohtaan. Hyökkäys pitää mahdollisimman monta porttia auki ja mahdollisimman kauan |
| Yhtiön kotisivujen yhteydessä olevan RCE haavoittuvuuden hyödyntäminen. Hyökkääjä analysoi kohdetta ja mahdollisesti tuhrii yhtiön kotisivut |
| Haitallisen sähköpostin linkin avulla toteutettu järjestelmän saastuttaminen |
| Kalastelupuhelun avulla saadun tiedon hyödyntäminen organisaation järjestelmiin murtautumisessa |

Taulukko 9. Red Team-syötteiden kuvaus

|  |  |  |  |
| --- | --- | --- | --- |
| **Syöte** | **Syötteen kuvaus** | **Miten havaitaan?** | **Toivottu reaktio** |
| **Porttiskannaus** | Hyökkäävä joukkue aloittaa nmap- porttiskannauksen käyttäen Decoy flagia määrittäen eri IP-osoitteita eripuolelta maailmaa, jotta kohde ei voi helpolla tunnistaa lähdettä tai estää sitä palomuurista | Tämä näkyy DataCenter Oy:n palomuurin IDS:n Alerteissa hyvin suurena määränä merkintöjä, useista eri IP-osoitteista | Koska IP-osoitteita on mahdollisesti spooffattu, puolustava joukkue ei voi estää näitä osoitteita. Raportoitava tapahtuma |
| **Palvelunestohyökkäys** | Hyökkäävä joukkue aloittaa Slowloris-palvelunestohyökkäyksen käyttäen 1500 luotua yhteyttä | Havaitaan IDS:n Alerteista suurena määränä liikennettä yhdestä IP osoitteesta | Puolustava joukkue luo palomuurisäännön jolla kyseinen IP-osoite estetään. Raportoitava tapahtuma |
| **PHP-injektio** | Hyökkäävä joukkue suorittaa RCE hyödyntäen firman haavoittuvaista kommentointipalstaa. Mahdollistaa järjestelmän analysoinnin, firman sivujen tuhrimisen ja mahdollisesti oikeuksien kohottamisen. Hyökkäys eskaloituu, mikäli sitä ei havaita ajoissa | Kummallisen tekstin ilmestyminen kommenttipalstalle. Esimerkiksi "www-data" tai listauksia serverin tiedostokansioista. | Puolustava joukkue ilmoittaa havainnosta, jotta tarvittavat toimenpiteet hyökkäyksen estämiseksi voidaan suorittaa. Datadir kansion php-koodin suorittamisen kieltäminen .htaccess tiedoston avulla. Koodiksi luettavien merkkien poistaminen kommenteista php strip tags -funktion avulla. Raportoitava tapahtuma |
| **Haitallinen sähköposti** | Hyökkäävä joukkue lähettää organisaation asiakaspalvelijoiden sähköpostiin epämääräisiä sähköposteja, jotka sisältävät vaarallisia linkkejä | Haitallinen sähköposti havaitaan normaalin toiminnan yhteydessä | Puolustava joukkue ei avaa haitallista sähköpostia, eikä varsinkaan sen sisältämää linkkiä. Raportoitava tapahtuma |
| **Haitallinen puhelu** | Hyökkäävä joukkue soittaa DataCenter Oy:n asiakaspalvelunumeroon, ja yrittää kalastalla tietoa organisaation verkosta | Haitallinen puhelu havaitaan normaalin toiminnan yhteydessä | Puolustava joukkue ei avaa haitallista sähköpostia, eikä varsinkaan sen sisältämää linkkiä. Raportoitava tapahtuma |

## Vaste

Taulukko 10. Vastesuunnitelma kyberpoikkeamalle.

|  |  |  |
| --- | --- | --- |
| Kategoria | Raportoitavat kyberhyökkäykset | Vasteaika |
| 1 | Mikä tahansa hyökkäys organisaation kriittisiin kohteisiin. Palvelunestohyökkäykset mitkä haittaavat organisaation palveluntarjoamista. Jos luvaton henkilö pääsee käsiksi root/järjestelmänvalvojan oikeuksiin. Virushyökkäykset eristävät organisaation osa-alueita | Viimeistään 10 minuutissa |
| 2 | Luvattomat tiedustelut ja skannaukset verkossa. Useat epäilyttävät järjestelmät | Viimeistään 20 minuutissa |
| 3 | Kadonneet tiedostot/ohjelmat. Heikot tietoturvatoimet. Epäilyttävä "aukioloaikojen" ulkopuolella tapahtuva toiminta. Jatkuvat kirjautumisyritykset eri IP-osoitteista. Luvattomat oikeuksien muutokset | Viimeistään 30 minuutissa |

# Harjoitusympäristö

Harjoitusympäristössä (Kuvio 3) on yhteensä 15 tietokonetta, joista kaikki ovat virtuaalisesti toteutettuja. Harjoitusympäristön toteutus suoritetaan Jyväskylän Ammattikorkeakoulun JAMK:n tiloissa, osoitteessa Piippukatu 2, 40100 Jyväskylä. Harjoitusympäristön virtuaalikoneet ovat hajautettu fyysisille tietokoneille niin, että toteutuksessa voidaan käyttää kahta eri luokkahuonetta. Näin Red Team voi toimia eri tilassa kuin Blue Team harjoituksen aikana.

Harjoitusympäristön toteuttamiseen käytetty GitHub-repositorio:

<https://github.com/H8545/Kyberharjoituksen-suunnittelu-ja-valmistelu>

Sivusto sisältää harjoituksessa käytettävien tietokoneiden dokumentoidut konfiguraatiot. GitHub-repositorio on esitelty myös Liitteessä 3.

## Harjoitusympäristön vaatimat laiteresurssit

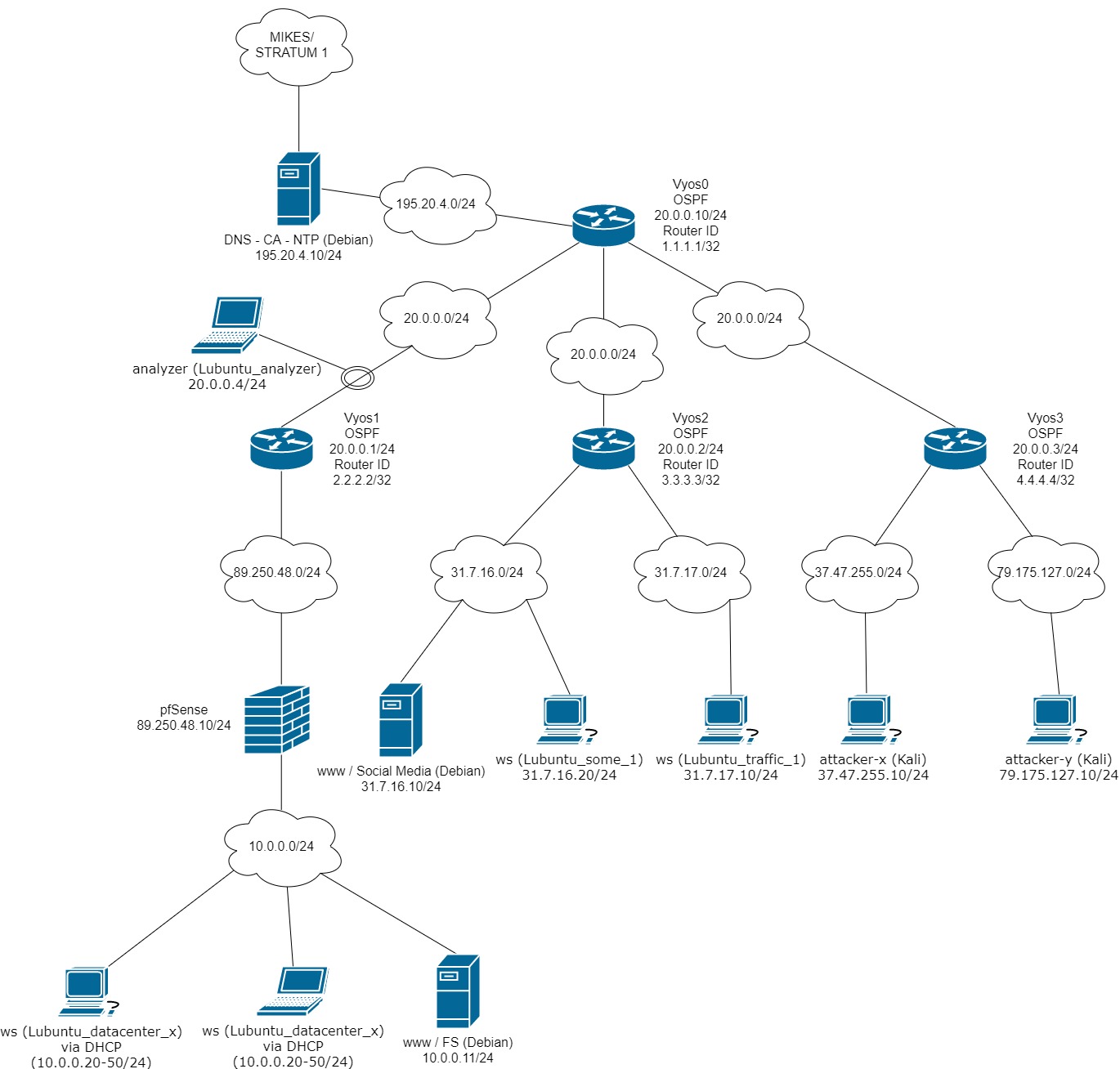
Taulukossa 11 on esitelty harjoitusympäristön vaatimat fyysiset laiteresurssit. Harjoitusympäristö on suunniteltu toteutettavaksi noin 4 fyysisellä tietokoneella.

Taulukko 11. Harjoitusympäristön vaatimat fyysiset laiteresurssit

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Virtuaalikone** | **RAM (MB)** | **HDD (GB)** | **Määrä (kpl)** | **RAM (MB)\*Määrä** | **HDD (GB)\*Määrä** |
| VyOS | 512 | 2 | 4 | 2048 | 8 |
| Kali | 1024 | 12 | 2 | 2048 | 24 |
| Debian 9 | 512 | 8 | 3 | 1536 | 24 |
| Lubuntu | 512 | 8 | 5 | 2560 | 40 |
| CentOS 7 | 512 | 10 | 1 | 512 | 10 |
| **Yhteensä** |  |  | **15** | **8704** | **106** |

## Harjoitusympäristön rakenne

Harjoitusympäristöön (Kuvio 3) on luotu virtuaalinen sisäverkko 10.0.0.0/24, joka kuvastaa mahdollisimman hyvin DataCenter Oy:n sisäverkon infrastruktuuria, ulkoverkko 89.250.48.0/24 jossa sijaitsee organisaation julkinen IP-osoite 89.250.48.10/24, ulkomaailman runkoverkko 20.0.0.0/24 joka reitittää liikennettä eri alueiden välillä, sekä useiden toimijoiden verkkoja, kuten DNS-NTP-CA 195.20.4.0/24 verkko, sosiaalisen median verkot 31.7.16.0/24 ja 31.7.16.0/24 sekä uhkatoimijoiden verkot 37.47.255.0/24 ja 79.175.127.0/24.



Kuvio 3. Harjoitusympäristön topologia

## Harjoitusympäristön virtuaalikoneiden tiedot ja palvelut

Taulukoissa 12 ja 13 on esitelty harjoitusympäristön käytettävien virtuaalikoneiden tiedot ja niiden tuottamat palvelut.

Taulukko 12. Palvelu- ja konfiguraatiotaulukko (osa 1/2)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Virtuaalikone** | **Käyttöjärjestelmä** | **Käyttäjänimi** | **Salasana** | **IP-osoite** |
| Vyos0 | Vyos | vyos | vyos | 20.0.0.10/24 |
| Vyos1 | Vyos | vyos | vyos | 20.0.0.1/24 |
| Vyos2 | Vyos | vyos | vyos | 20.0.0.2/24 |
| Vyos3 | Vyos | vyos | vyos | 20.0.0.3/24 |
| Analyytikko | Debian 9 | user | user66 | 20.0.0.4/24 |
| pfSense | CentOS 7 | user | user66 | 10.0.0.10/24 |
| www / FS | Debian 9 | root | root66 | 89.250.48.10/24  10.0.0.11/24 |
| ws | Debian 9 | user | user66 | via DHCP  (10.0.0.20-50/24) |
| ws | Debian 9 | user | user66 | via DHCP  (10.0.0.20-50/24) |
| Uhkatoimija-X | Kali | root | root66 | 37.47.255.10/24 |
| Uhkatoimija-Y | Kali | root | root66 | 79.175.127.10/24 |
| www / Sosiaalinen media | Debian 9 | user | user66 | 31.7.16.10/24 |
| ws | Lubuntu | user | user66 | 31.7.16.20/24 |
| ws | Lubuntu | user | user66 | 31.7.17.10/24 |
| DNS-CA-NTP | Debian 9 | user | user66 | 195.20.4.10/24 |

Taulukko 13. Palvelu- ja konfiguraatiotaulukko (osa 2/2)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Virtuaalikone** | **OSPF loopback** | **Palvelut** | **Käyttäjänimi** | **Salasana** |
| Vyos0 | 1.1.1.1/32 |  |  |  |
| Vyos1 | 2.2.2.2/32 |  |  |  |
| Vyos2 | 3.3.3.3/32 |  |  |  |
| Vyos3 | 4.4.4.4/32 |  |  |  |
| Analyytikko |  |  |  |  |
| pfSense |  | firewall/DHCP | admin | pfsense |
| www / FS |  | www/OwnCloud | root | root66 |
| ws |  |  |  |  |
| ws |  |  |  |  |
| Uhkatoimija-X |  |  |  |  |
| Uhkatoimija-Y |  |  |  |  |
| www / Sosiaalinen media |  | www/phpBB3 | user | user66 |
| ws |  |  |  |  |
| ws |  |  |  |  |
| DNS-CA-NTP |  | DNS/CA/NTP |  |  |

## Harjoitettavan organisaation tietoturvakontrollit harjoitusympäristössä

Harjoitusympäristössä organisaatio käyttää verkkonsa suojaamiseen Taulukossa 14 esiteltyjä tietoturvakontrolleja.

Taulukko 14. Organisaation tietoturvakontrollit harjoitusympäristössä

|  |
| --- |
| **Organisaation tietoturvakontrollit** |
| Organisaation sisäverkko 10.0.0.0/24 on palomuurin takana. Palomuurina toimii pfSense, versio 2.4. |
| Palomuurilla on yksi WAN-rajapinta sekä yksi LAN-rajapinta |
| WAN-rajapinnassa on yksi julkinen IP-osoite 89.250.48.10/24, johon tuleva liikenne ohjataan sisäverkossa olevaan palvelimeen |
| Palomuuriin on asennettu Snort IDS (Intrucion Detection System), joka on säädetty antamaan pelkkiä varoituksia, joihin Blue Team:in järjestelmänvalvojien pitää reagoida asianmukaisella tavalla |
| Palomuurista on avattuna vain HTTP (80) ja HTTPS (443) portit palveluiden mahdollistamiseksi ulkoverkkoon. Avattuihin portteihin tuleva liikenne ohjataan organisaation www/OwnCloud palvelimeen. Palomuurin GUI:hin pääsee käsiksi vain sisäverkosta |

## Harjoitusympäristön testaus

Harjoitusympäristön testaus on suoritettu viikolla 44 ja se on todettu toimivaksi ja sen toimivan halutulla tavalla.

# Perehdytys

Perehdytyksen avuksi on luotu PowerPoint-esitys (Liite 4), joka esitetään perehdytyksen yhteydessä. Perehdytysmateriaalissa kerrotaan harjoituksen taustaa ja yritetään motivoida osallistuvaa ryhmää harjoitukseen. Motivoinnin jälkeen kerrotaan harjoituksen yleisjärjestelyistä, eli missä tilassa ja milloin harjoitus pidetään. Samalla esitetään harjoituksen yleinen aikataulu. Aikataulun jälkeen kerrotaan harjoituksen tavoitteet sekä ryhmäjako. Lopuksi perehdytetään ryhmälle tekninen ympäristö ja harjoitukseen liittyvät säännöt ja turvallisuus.

## Harjoituksen yleisjärjestelyt

Ennen harjoituksen aloitusta osallistuvat henkilöt ovat tutustuneet harjoituksen kulkuun perehdytystilaisuudessa. Tiimien johdon välinen viestiminen tapahtuu harjoituksesta erillään olevan viestintäpalvelun kautta esim. Slack yms.

## Harjoituksen yleinen aikataulutus

Taulukko 15. Harjoituksen yleinen aikataulutus

|  |  |
| --- | --- |
| **Kellonaika** | **Tapahtuma** |
| **8:00** | Ympäristöön tutustuminen. Ryhmät aloittavat normaalin toiminnan |
| **8:20** | Harjoituksen aktiivivaihe alkaa |
| **10:45** | Harjoituksen aktiivivaihe päättyy |
| **11:00** | Harjoitus ohi, Tilannekatsaus |

## Harjoitettavat organisaatioyksiköt

Harjoitukseen osallistuu DataCenter Oy:n henkilöstöstä toimitusjohtaja, teknologiajohtaja, palvelujohtaja, IT-palveluyksiköiden työntekijät sekä tukiyksikön työntekijät (ks. Kuvio 2).

## Harjoituksen tekninen perehdytys

Harjoitukseen osallistuvan organisaation henkilöstön tekninen perehdytys toteutetaan teknisen perehdytysmateriaalin avulla. Tekninen perehdytysmateriaali on esitelty liitteessä Liite 5.

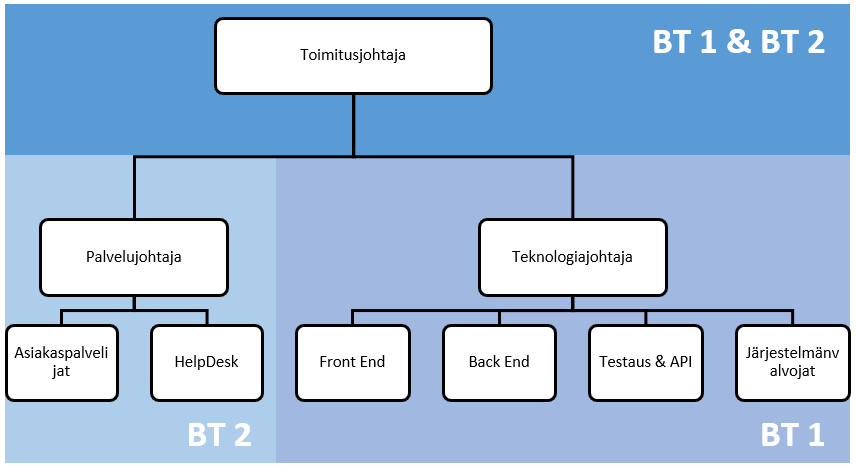
## Harjoituksen turvallisuus

Kyberharjoituksen henkilöstö toimii hätäpoistumistilanteessa rakennuksen evakuointi ohjeiden mukaisesti. Harjoituksen aikana kuvaaminen ja tiedon levittäminen harjoituksen ulkopuolelle on kielletty, johtuen organisaatiolle tärkeästä materiaalista.

## Puolustavien ja hyökkäävien joukkueiden roolitus

### Blue Team

Blue Team on jaettu harjoituksessa kahteen joukkueeseen Blue Team 1 ja Blue Team 2 (Kuvio 4). Blue Team 1 kuuluu organisaation asiakastuki ja HelpDesk, joiden tehtävänä on vastata DataCenter Oy:n palvelutoiminnasta ja sen toimivuudesta harjoituksen aikana. Jos palvelutoiminnassa ilmenee ongelmia, niistä ilmoitetaan Blue Team 1 esimiehelle eli palvelujohtajalle, joka välittää tarvittaessa viestin toimitusjohtajalle. Blue Team 2 vastaa teknillistoiminnallisista toimenpiteistä DataCenter Oy:n verkossa. Blue Team 2 toimii kyberpoikkeaman ohjeistuksen mukaisesti ja vastaa kyberpoikkeamaan tarvittavilla toimenpiteillä varmistaakseen organisaation teknisen toiminnan jatkuvuuden. Blue Team 2 esimiehenä toimii teknologiajohtaja, joka välittää tarvittaessa tietoja toimitusjohtajalle. Teknologiajohtajan ja palvelujohtajan esimiehenä toimii DataCenter Oy:n toimitusjohtaja, joka vastaa organisaation viestinnästä organisaation ulkopuolelle sekä korkeimmasta päätöksentekovallasta. Molempiin Blue Teameihin nimetään vastuuhenkilö, joka vastaa yksikkönsä johtajan kanssa kommunikoimisesta. Blue Team 1 siirtää Slackin avulla ongelmatilanteet Blue Team 2:lle.



Kuvio 4. Organisaation roolitus harjoituksessa

### Red Team

Uhkatoimijoina toimii osa harjoituksen johtavasta joukkueesta. Red Team on vastuussa organisaation tietoturvallisuutta vaarantavien syötteiden suorittamisesta. Red Teamin tarkemmasta toiminnasta ei kerrota harjoituksen puolustaville joukkueille.

### White Team

Harjoituksen johtavana joukkueena toimii harjoituksen järjestäjät. Yksi White Team:in jäsenistä toimii Blue Team:in konsulttina. Konsultti ratkaisee ongelmatilanteita, joita ei tarkoituksenmukaisesti ole luotu ympäristöön, sekä selventää mahdollisia epäselvyyksiä Blue Team:in työkaluihin ja harjoitusympäristöön liittyen.

## Harjoituksen säännöt

Harjoituksessa käytettävä materiaali on organisaatiolle tärkeää ja arkaluontoista. Näistä syistä johtuen harjoituksen aikana kaikenlainen kuvaaminen/äänittäminen on kiellettyä. Myöskään harjoituksessa mahdollisesti jaettavaa materiaalia ei saa esittää harjoituksen ulkopuolisille henkilöille. Älylaitteet on lisäksi pidettävä harjoituksen aikana lentokonetilassa. Harjoituksen aikana viestintään saa käyttää ainoastaan annettuja palveluita/kanavia. Myöskään harjoituksessa käytettävien laitteiden tai tunnusten salasanoja ei saa muuttaa ilman erillistä käskyä.

# Harjoituksen arviointi

Harjoitukseen osallistuvan organisaation henkilöstö suorittaa harjoituksen arvioinnin harjoituksen aikana tekemiensä havaintojen ja muistiinpanojen pohjalta. Harjoittelevan organisaation henkilöstölle on luotu arviointi ja arvostelulomake, joka jaetaan jokaiselle osallistujalle ennen harjoituksen alkua. Arviointi- ja arvostelulomakkeen lisäksi lomake sisältää sopimuksen harjoituksen salassapitovelvollisuudesta, jonka jokaisen harjoitukseen osallistuvan on täytettävä ennen harjoituksen alkamista ja sen arvioimista. Harjoitukseen osallistuvalla henkilöllä on mahdollista arvioida harjoituksen jokainen osa-alue pisteyttämällä se asteikolla 0 (huono) – 3 (kiitettävä) sekä kommentoimalla osuutta vapaasti. Osallistujalla on lisäksi mahdollisuus antaa harjoituksesta vapaa palaute, johon osallistuja voi kirjata harjoituksen aikana esiin tulleita kysymyksiä, kommentteja, havaintoja ja mielipiteitä harjoituksesta ja harjoitusympäristöstä.

Harjoituksen järjestäjät arvioivat harjoitukseen osallistuvan organisaation henkilöstön arvioimalla osallistuvien henkilöiden onnistumisen eri harjoituksen osa-alueissa pisteyttämällä osa-alueen onnistumisen asteikolla 0 (huono) – 3 (kiitettävä) sekä kommentoimalla onnistumista vapaasti. Harjoituksen järjestäjille annettavassa harjoituksen arviointi- ja arvostelulomakkeessa on osallistujien arvioinnin ja arvostelun lisäksi osuus, jossa harjoituksen järjestäjät arvioivat omaa onnistumistaan harjoituksen eri vaiheissa, aina ideoinnista harjoituksen toteutukseen ja arviointiin.

Harjoituksesta saatavien arvostelu- ja arviointilomakkeiden pohjalta harjoituksen järjestäjät koostavat arviointiraportin, joka esitellään harjoitukseen osallistuvalle organisaatiolle ja sen henkilöstölle kuukausi harjoituksen jälkeen järjestettävässä arviointitilaisuudessa. Arviointilaisuudessa esitettävään ja organisaation johdolle luovutettavaan arviointiraporttiin on sisällytetty harjoituksesta saadun informaation pohjalta organisaation toiminnan kehittämiskohteet korjausehdotuksineen, yleinen palaute harjoituksesta sekä arvio seuraavan harjoituksen sisällöstä ja ajankohdasta. Arviointiraportin tavoitteena on olla motivoiva ja kannustava, jotta kyberharjoituksiin osallistumisesta ja sitä kautta organisaation toiminnan tehostamisesta tulisi organisaatiolle jatkuva käytäntö.

Harjoitukseen osallistuvat organisaation henkilöt arvioivat harjoituksen Arviointi ja arvostelulomake (Osallistujalle) (Liite 6) avulla ja harjoituksen järjestäjät suorittavat harjoitukseen osallistuvien henkilöiden arvioinnin ja itsearvioinnin harjoituksesta Arviointi ja arvostelulomake (Järjestäjälle) (Liite 7) avulla.

**Lähteet**

2017 Data Breaches – The Worst So Far. Viitattu 02.10.2017. <https://www.identityforce.com/blog/2017-data-breaches>

Data Breaches Increase 40 Percent in 2016. Identity Theft Resource Center. 2017. Viitattu 3.10.2017. <http://www.idtheftcenter.org/2016databreaches>

The EU General Data Protection Regulation (GDPR). Viitattu 04.10.2017. <http://www.eugdpr.org>

List of data breaches. 2017. Viitattu 02.10.2017. <https://en.wikipedia.org/wiki/List_of_data_breaches>

Kohnke, A., Shoemaker, D., Singler, K. 2016. The Complete Guide to Cybersecurity Risks and Controls.

**Liitteet**

Liite 1. Organisaatiokaavio (Täydellinen)

Liite 2. Harjoituksen pelitapahtumat ja syötteet

Liite 3. Tekninen toteutus

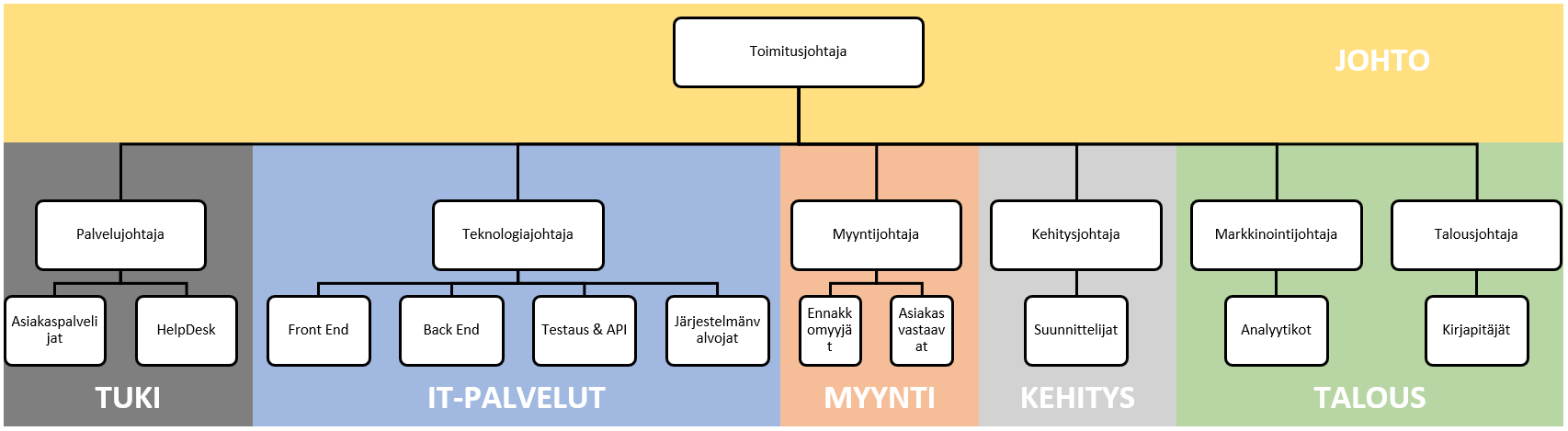
Liite 4. Harjoituksen perehdytysmateriaali

Liite 5. Harjoitusympäristön perehdytysmateriaali (Tekninen)

Liite 6. Arviointi ja arvostelulomake (Osallistujalle)

Liite 7. Arviointi ja arvostelulomake (Järjestäjälle)

### Liite 1. Organisaatiokaavio (Täydellinen)



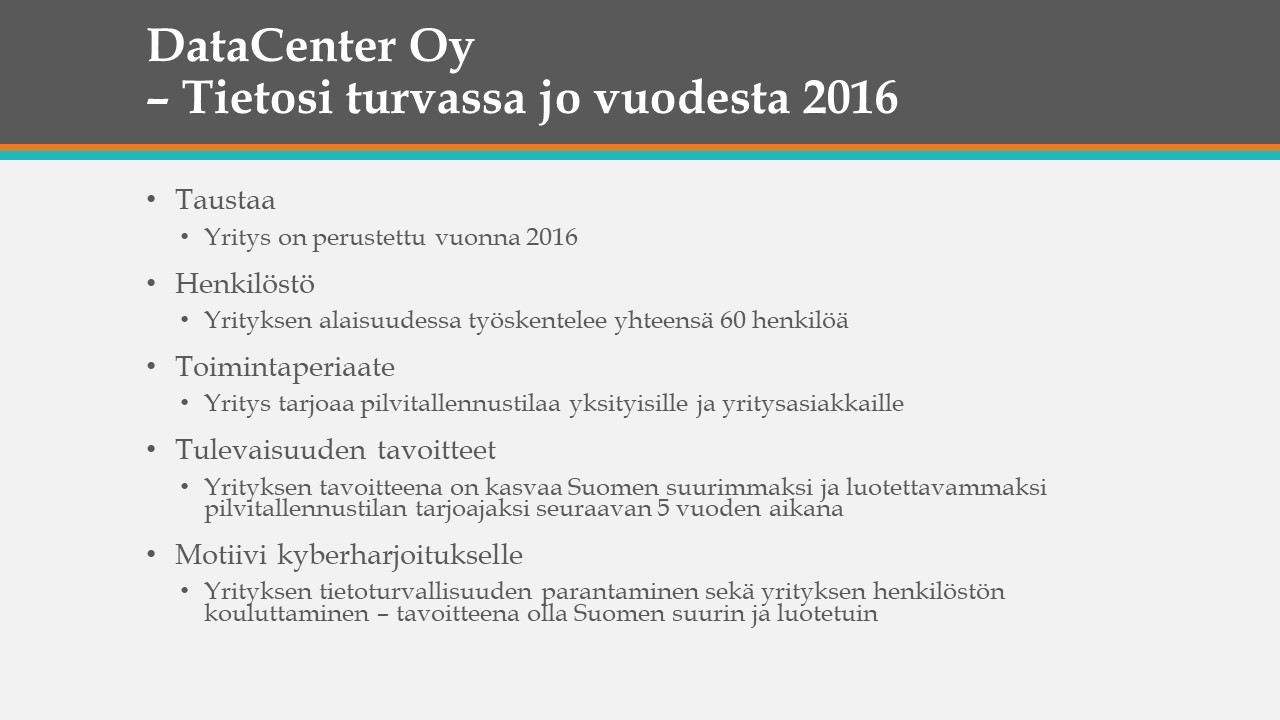
### Liite 2. Harjoituksen pelitapahtumat ja syötteet

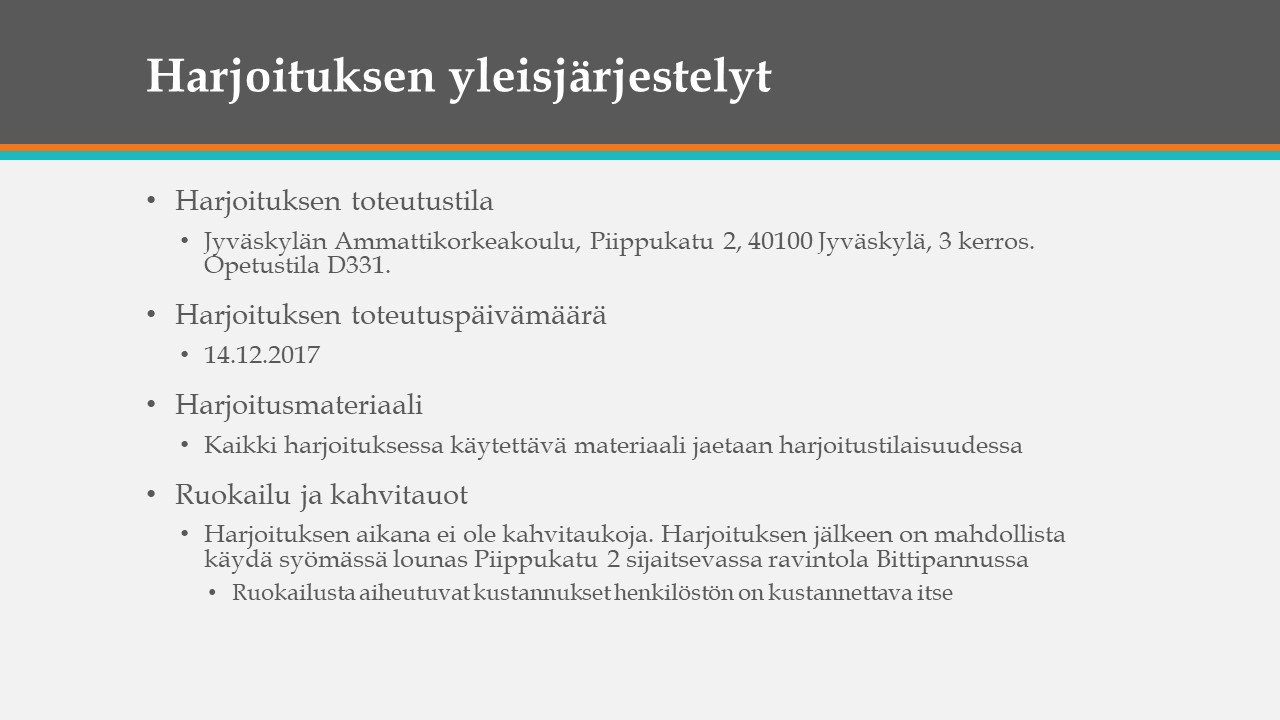


Liite 3. <https://github.com/H8545/Kyberharjoituksen-suunnittelu-ja-valmistelu>

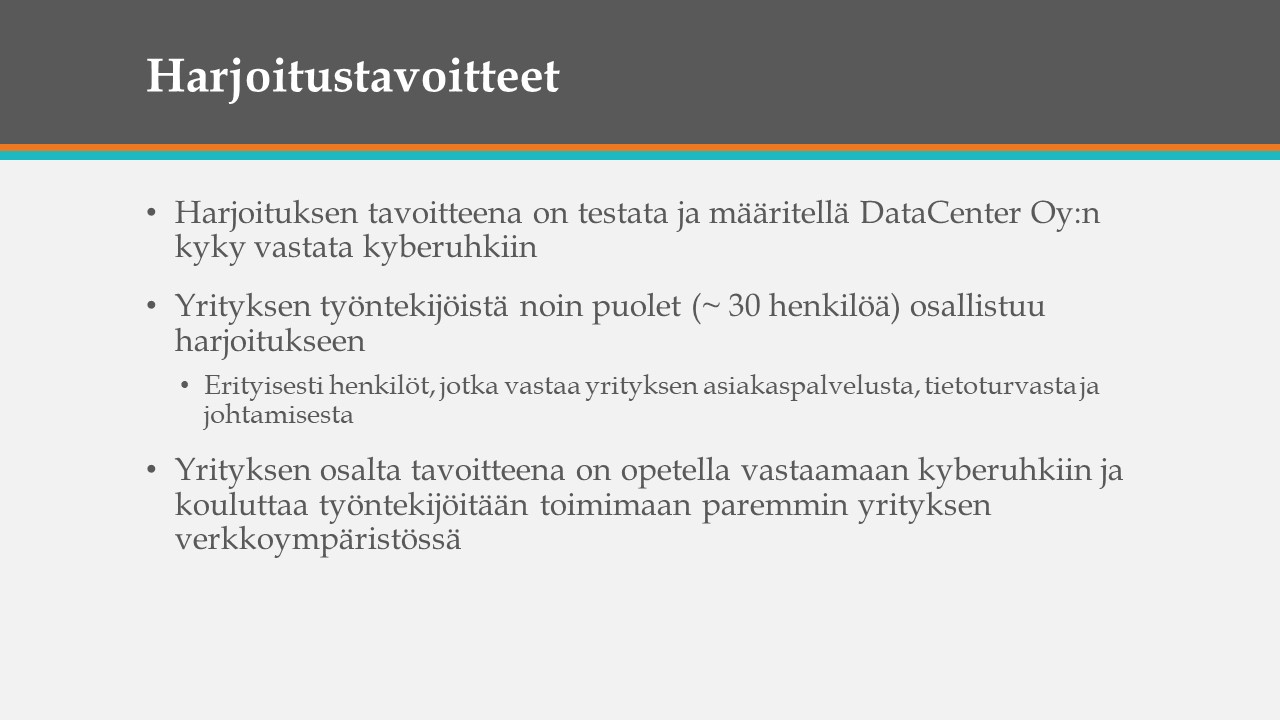
### Liite 4. Harjoituksen perehdytysmateriaali

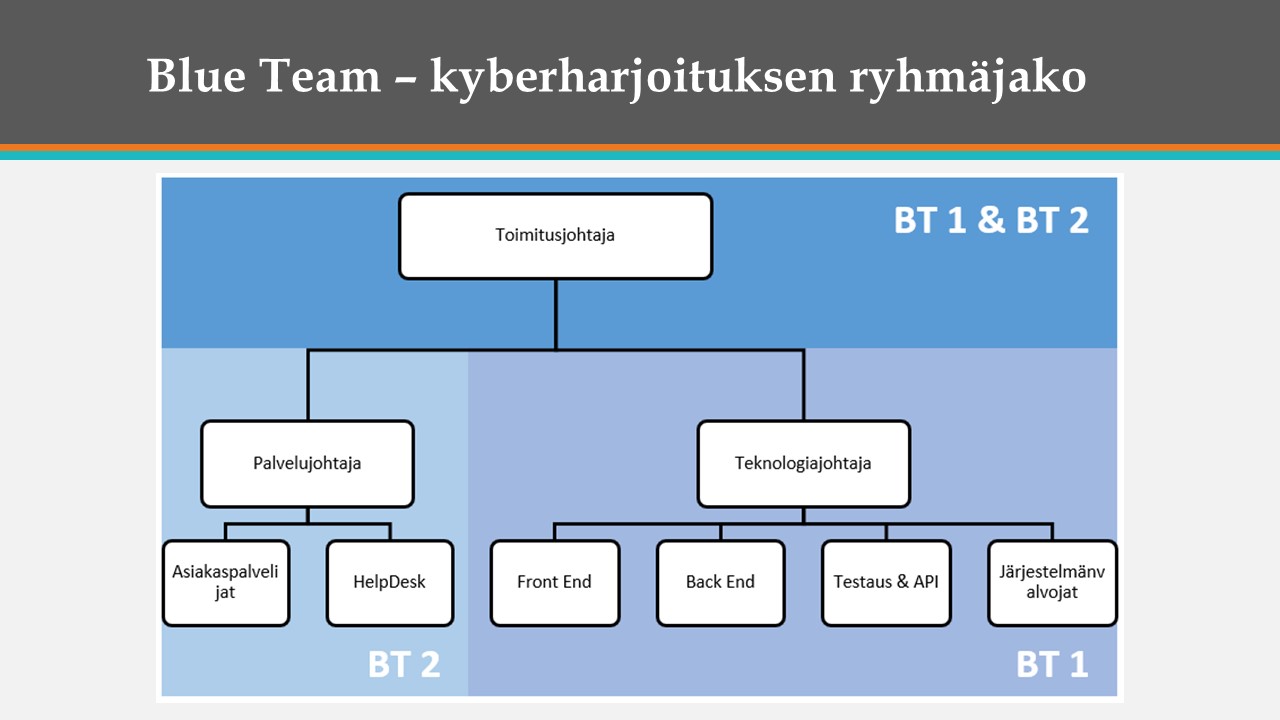


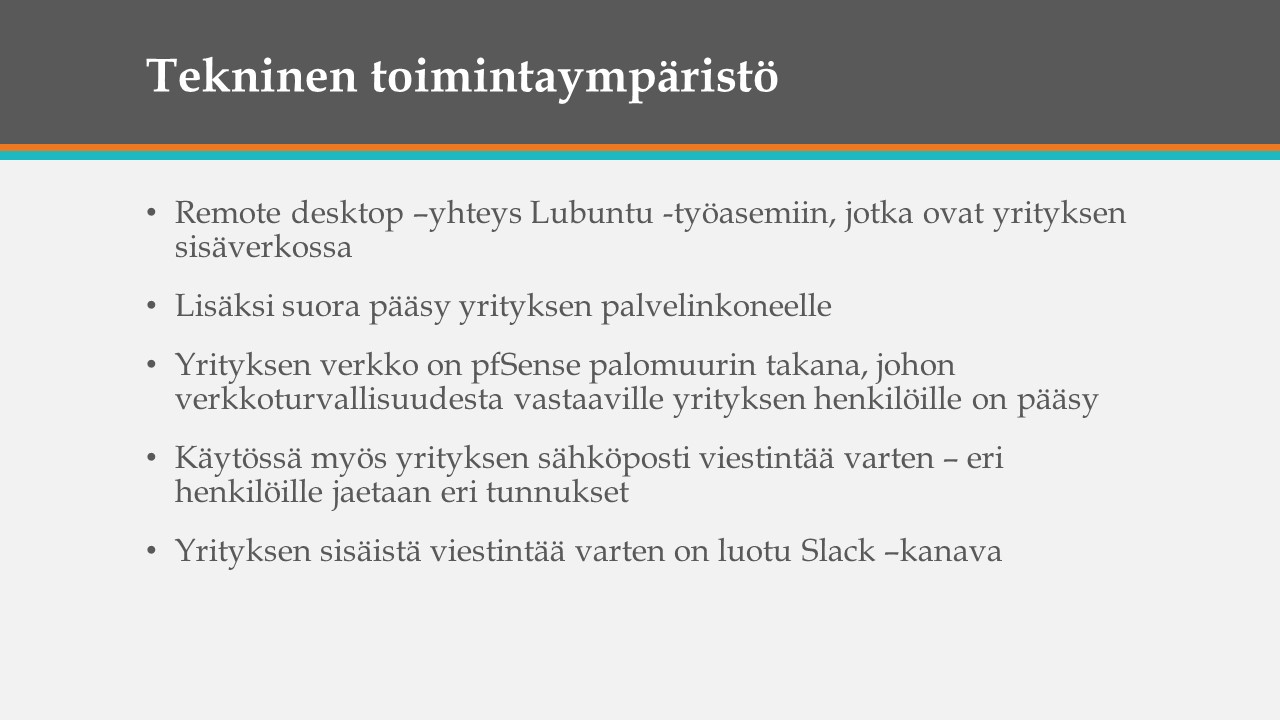


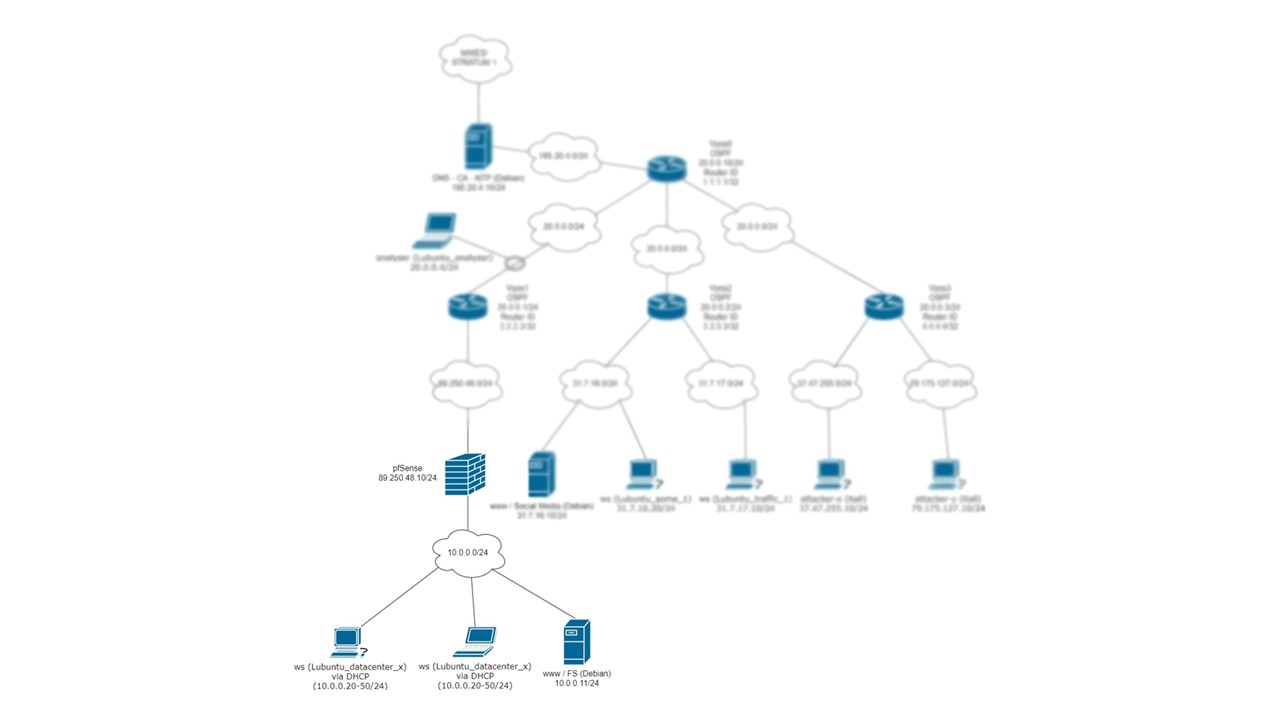




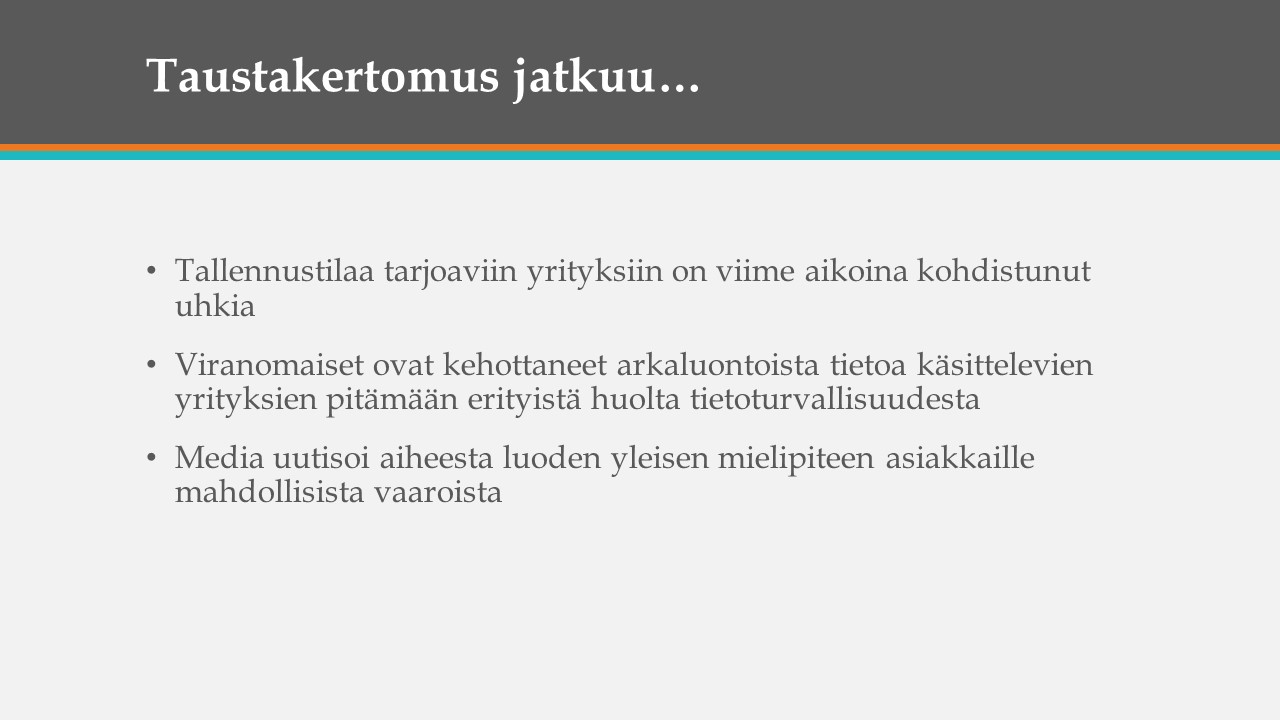


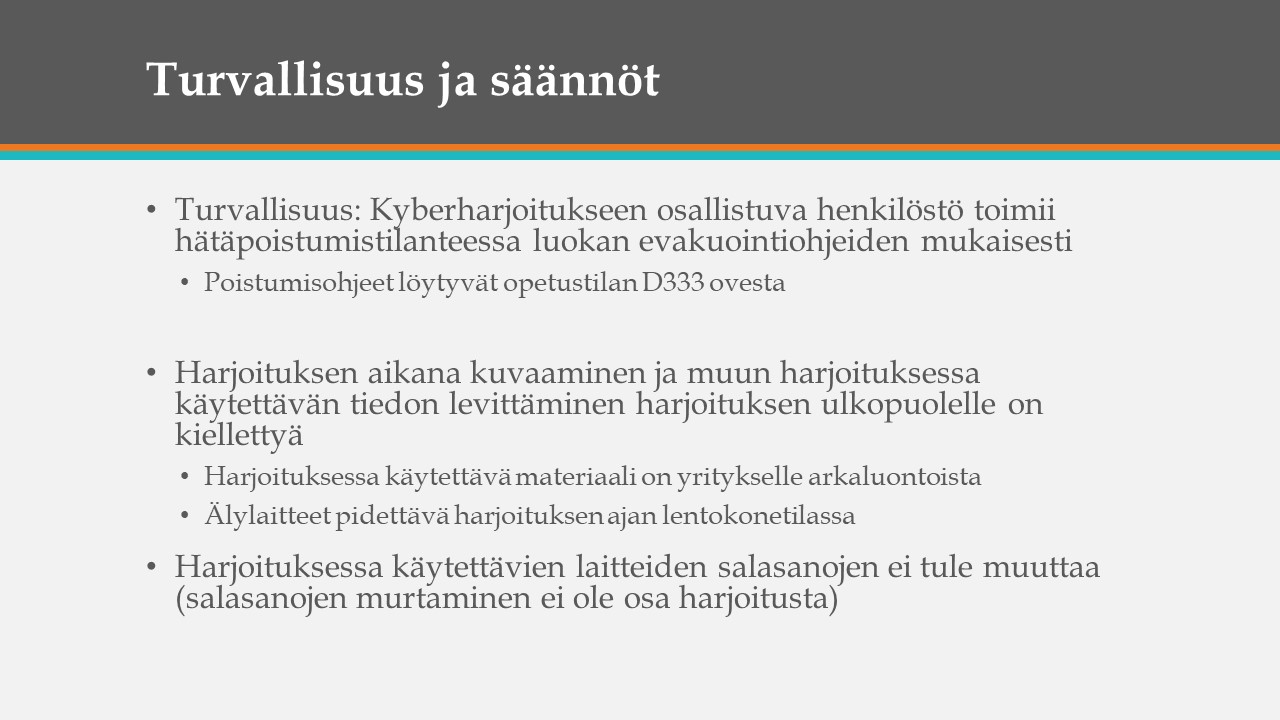












### Liite 5. Harjoitusympäristön perehdytysmateriaali (Tekninen)

Blue Team 1 vastaa asiakastuen toiminnasta. Blue Team 2 toimii harjoituksessa teknisten ongelmien ratkaisussa.

Blue Team 1 perehdytysmateriaali

Blue Team 1 vastaa asiakastuen toiminnasta. Tiimille annetaan puhelin sekä sähköpostitili, joihin tuleviin viesteihin tai puhelinsoittoihin vastataan tässä dokumentissa määritettyjen toimintaohjeiden mukaan.

Puhelimeen vastaaminen

Puhelimeen vastataan reippaalla äänensävyllä kertoen asiakaspalvelijan nimen, sekä yrityksen johon soitto tulee. esimerkiksi ”Aatu Asiakaspalvelija Datacenter Oy, kuinka voin auttaa? ☺”

Asiakkaan toiveisiin ja ongelmiin vastataan parhaan asiantuntemuksen mukaan. Mikäli ongelma on jokin jota asiakaspalvelija ei voi itse hoitaa, välitetään tieto eteenpäin Slack- kanavaa käyttäen asiantuntijatiimille.

Salasananpalautusohje

Mikäli asiakas soittaa ja pyytää salasanan palautusta, tulee toimia tämän ohjeen mukaan. Asiakkaista löytyy tietokanta, joihin asiakkaan tietoja on tallennettu. Näitä tietoja käyttäen pyritään toteamaan, onko asiakas oikeasti se henkilö joka hän väittää olevansa.

Seuraavat asiat kysytään ja näiden perusteella päätellään voiko salasanan palauttaa:

* Asuinpaikka: oltava oikein
* Milloin tili on luotu
* Milloin viimeksi kirjauduttu sisään onnistuneesti
* Arvaus viimeisestä käytetystä salasanasta: salasanan oltava lähelle nykyistä
* Erikseen määritetty tietoturvakysymys: mikäli määritetty, tähän on osattava vastata oikein
* Käytetty sähköposti

Mikäli näihin kysymyksiin vastataan riittävän tarkasti, eli jokaiseen kohtaan asiakkaan pitää osata vastata hyvin lähelle oikeaa, jotta salasana voidaan palauttaa. Palautus tapahtuu tiliin liitetyn sähköpostin perusteella. Mikäli asiakkaasta jää epäilyttävä kuva, kerrotaan että salasanaa ei voida palauttaa näillä tiedoilla, mutta asia viedään eteenpäin esimiehelle, joka tekee päätöksen jatkotoimenpiteistä ja ottaa asiakkaaseen yhteyttä myöhemmin. (ITSE PALAUTUSTA EI TARVITSE TOTEUTTAA, SANOTAAN VAIN SEN TAPAHTUVAN)

Sähköpostiin vastaaminen

Sähköpostiin vastataan hyvien asiakaspalveluperiaatteiden mukaan, jotka ovat jo varmasti kaikille tuttuja. Huomioitavia asioita:

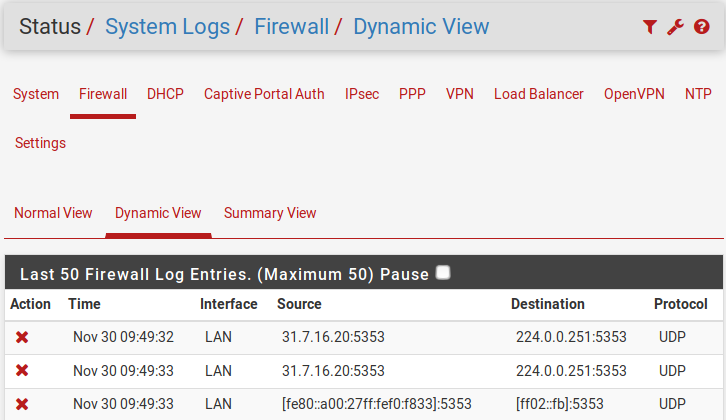
* Ei avata haitallisia linkkejä
* Ei lähetetä yksityistä dataa ulos väärille henkilöille
* Salasanan palautuskysymyksiin vastataan saman protokollan mukaan kuin puhelintiedusteluissa

Blue Team 2 perehdytysmateriaali

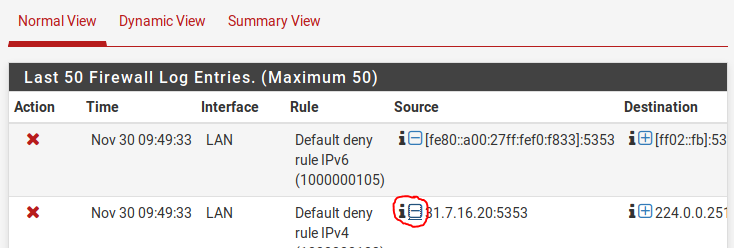
Blue Team 2 vastaa palomuurin valvonnasta ja sen teknisistä muutoksista. Blue Team 2 ottaa vastaan Datacenter Oy:n ongelma tilanteet ja etsii niihin ratkaisua.

PfSensen avulla voi estää liikenteen tietystä IP-osoitteesta nopeasti palomuurin IP-seurannasta. Menet palomuurissa **Status -> System Logs -> Firewall -> Dynamic View.**

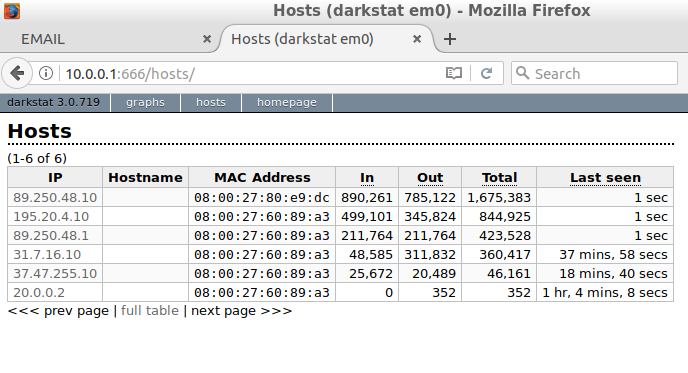
Tätä kautta voi tarkastella palomuurilla tapahtuvaa liikennettä. Vaihtoehtoina voi valita **Normal View/ Dynamic View/ Summary View.**



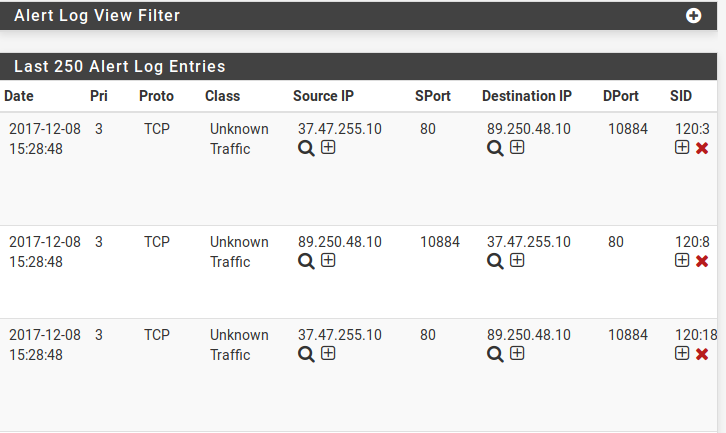
Normal View kautta voidaan estää ei haluttua liikennettä nopeasti käyttämällä: Easy Rule: Add to block list.



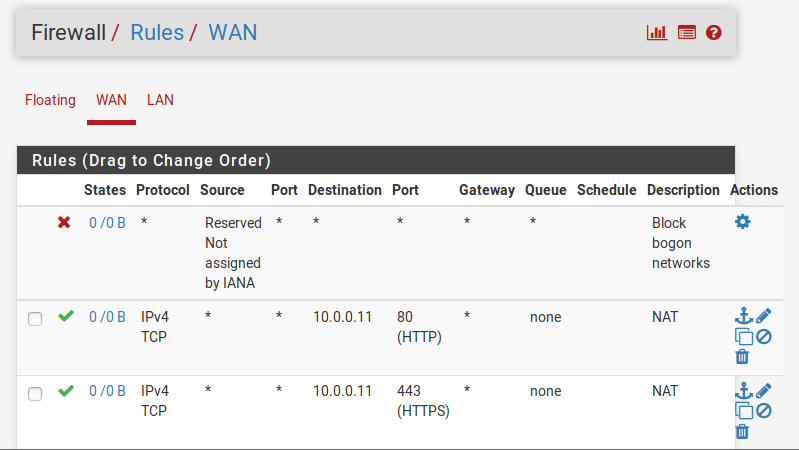
Dark statista näkee reaaliaikaisen liikenteen ja statistiikkaa. (**Diagnostics -> darkstat**)



Snortista näkee varoituksia mahdollisista hyökkäysyrityksistä. (**Services -> Snort -> Alerts**)



Palomuurin sääntöjä voidaan asettaa sekä muokatapfSenseen **Firewall -> Rules -> WAN**



**Palomuurin tehtäviin muutoksiin täytyy kysyä esimieheltä aina lupa**

Backend -tehtäviin sijoitettujen jäsenien olisi syytä tutustua firman web –palvelujen kansiorakenteeseen ja tiedostoihin. /var/www/html kansio on hyvä aloituspaikka, kannattaa myös tutkia tiedostoja.

### Liite 6. Arviointi ja arvostelulomake (Osallistujalle)

**LUOTTAMUKSELLINEN**

**Kyberharjoituksen arvostelu ja arviointilomake (Osallistujalle)**

**Osallistujalle**

Tämä lomake on tarkoitettu Ryhmän 1 järjestämän kyberharjoituksen arvosteluun ja arviointiin. Kaikki harjoituksessa ja lomakkeessa jäljempänä käsiteltävä tieto on salassapitovelvollisuuden alaista tietoa. Harjoitukseen osallistuvalta vaaditaan salassapitosopimukseen allekirjoitus ennen kuin hän voi osallistua harjoitukseen ja suorittaa harjoituksen arvostelun ja arvioinnin.

|  |  |
| --- | --- |
| **Osallistuja** | |
| Nimi |  |
| Yritys |  |
| Yrityksen osoite |  |
| Yrityksen postinumero |  |
| Yrityksen postitoimipaikka |  |
| Puhelinnumero (työ) |  |
| Sähköpostiosoite (työ) |  |

**Salassapitosopimuksen tarkoitus ja salassa pidettävä tieto**

Osallistuja käsittelee harjoitusta suorittaessaan työnantajan ja harjoituksen järjestäjän, näiden kanssa samaan konserniin kuuluvien yhtiöiden, asiakkaiden ja yhteistyökumppaneiden liike- ja ammattisalaisuuksia (myöh. ”salassa pidettävä tieto”). Tieto on salassa pidettävää tietoa riippumatta siitä, onko se kirjallisessa, sähköisessä tai muussa vastaavassa muodossa.

Salassa pidettäväksi tiedoksi katsotaan erityisesti: (esimerkiksi: harjoituksessa käsiteltävät sähköiset tiedot, pöytäkirjat, kirjeenvaihto, liiketoiminta-, markkinointi- ja muut suunnitelmat, budjetit, tiedot yhtiön tileistä ja taloudesta, yhtiön sopimukset, sopimusehdot ja sopimusneuvottelut sekä työntekijöiden, yhteistyökumppaneiden tai asiakkaiden tiedot, tekniset piirustukset, suunnitelmat, ohjeet ja menetelmät ja lisäksi kaikki materiaali, joka on merkitty ”salaiseksi” tai jonka salassapidosta on sovittu yhtiön sopijapuolen tai yhteistyökumppanin kanssa.)

**Sopimusehdot**

Osallistuja sitoutuu harjoituksen aikana pitämään salassa ja luottamuksellisena kaiken edellä mainitun tiedon ja olemaan sitä luvatta luovuttamatta tai paljastamatta ulkopuolisille sekä harjoituksen sisällä muille kuin niille, jotka tarvitsevat tiedon työtehtävien suorittamiseen. Osallistuja sitoutuu olemaan käyttämättä salassa pidettäviä tietoja muuhun kuin työtehtäviensä hoitamiseen. Osallistuja on myös välittömästi velvollinen ilmoittamaan työnantajalle tai harjoituksen järjestäjälle, mikäli salassa pidettäviä tietoja on luvatta paljastunut ulkopuolisille tai salassapito on muuten vaarantunut. Osallistuja sitoutuu välittömästi harjoituksen päättymisen jälkeen, ja milloin tahansa työnantajan tai harjoituksen järjestäjän sitä vaatiessa, palauttamaan kaiken hallussaan olevan salassa pidettävää tietoa sisältävän aineiston ja kaikki kopiot. Osallistuja sitoutuu olemaan paljastamatta tai käyttämättä mitään salassa pidettäviä tietoja niin kauan kuin tiedolla on taloudellista merkitystä, kuitenkin vähintään kahden vuoden ajan työsuhteen päättymisestä lukien. Mikäli osallistuja rikkoo tässä sopimuksessa mainittuja ehtoja ja salassa pidettävän tiedon salassapito vaarantuu, osallistuja maksaa työnantajalle tai harjoituksen järjestäjälle sopimussakkona määrän, joka vastaa osallistujan rikkomushetkeä edeltäneen kuuden kuukauden palkkaa, mahdollista bonusta ja luontoisetua. Mikäli työsuhde on päättynyt, lasketaan sopimussakko välittömästi työsuhteen päättymistä edeltäneen kuuden kuukauden palkan perusteella edellä mainituin tavoin. Lisäksi osallistujan tulee korvata työnantajalle tai harjoituksen järjestäjälle sopimusrikkomuksesta aiheutunut muu vahinko.

**Päiväys ja allekirjoitukset**

**­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Työnantaja Harjoituksen järjestäjä Osallistuja**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**HARJOITUKSEN ARVOSTELU JA ARVIOINTI**

Osallistuja täyttää harjoittelun arvostelun ja arvioinnin merkkaamalla mielestään toteutuneeseen kohtaan kuulakärkikynällä merkin ”X”. Mahdolliset lisätiedot ja kommentit osallistuja voi täyttää ”Lisätiedot”-kohtaan. Yleisen palautteen harjoituksesta osallistuja täyttää ”HARJOITUKSEN PALAUTE” – kohtaan.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yleinen** | **0 (=huono)** | **1 (=välttävä)** | **2 (=hyvä)** | **3 (=kiitettävä)** |
| 1. Harjoituksen perehdytysmateriaali |  |  |  |  |
| 2. Harjoituksen tilat ja järjestelyt |  |  |  |  |
| 3. Työpisteet |  |  |  |  |
| 4. Teknisten työkalujen toimivuus |  |  |  |  |
| 5. Harjoituksen yleinen aikataulutus |  |  |  |  |
| 6. Harjoituksen mielekkyys |  |  |  |  |

**Lisätiedot ja huomiot:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tekninen** | **0 (=huono)** | **1 (=välttävä)** | **2 (=hyvä)** | **3 (=kiitettävä)** |
| 1. Työympäristöjen selkeys |  |  |  |  |
| 2. Työympäristöjen realistisuus |  |  |  |  |
| 3. Työympäristön ohjeistus |  |  |  |  |
| 4. Käytettyjen ohjelmien realistisuus |  |  |  |  |
| 5. Käytettyjen ohjelmien ohjeistus |  |  |  |  |
| 6. Käytettyjen ohjelmien käytännöllisyys |  |  |  |  |
| 7. Harjoituksen tekninen aikataulutus |  |  |  |  |
| 8. Skenaarion realistisuus |  |  |  |  |
| 9. Pelitapahtumien järjestely |  |  |  |  |

**Lisätiedot ja huomiot:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tekninen (Yksityiskohtainen)** | **0 (=huono)** | **1 (=välttävä)** | **2 (=hyvä)** | **3 (=kiitettävä)** |
| 1. Teknisen materiaalin käytettävyys |  |  |  |  |
| 2. Arvio syötteiden realistisuudesta |  |  |  |  |
| 3. Arvio syötteiden määrät |  |  |  |  |
| 4. Arvio kyvystä vastata syötteisiin |  |  |  |  |
| 5. Arvio vasteiden onnistumisesta |  |  |  |  |

**Lisätiedot ja huomiot:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**YLEINEN PALAUTE HARJOITUKSESTA**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

### Liite 7. Arviointi ja arvostelulomake (Järjestäjälle)

**LUOTTAMUKSELLINEN**

**Kyberharjoituksen arvostelu ja arviointilomake (Järjestäjälle)**

**Järjestäjälle**

Tämä lomake on tarkoitettu Ryhmän 1 kyberharjoituksen järjestäjälle, harjoituksen osallistujien arvosteluun ja arviointiin sekä oman työskentelyn arviointiin harjoituksen ideoinnin, suunnittelun ja valmistelun, toteutuksen ja arvioinnin aikana.

|  |  |
| --- | --- |
| **Järjestäjä** | |
| Nimi |  |
| Osoite |  |
| Postinumero |  |
| Postitoimipaikka |  |
| Puhelinnumero |  |
| Sähköpostiosoite |  |

**HARJOITUKSEN OSALLISTUJIEN ARVOSTELU JA ARVIOINTI**

Järjestäjä täyttää harjoittelun osallistujien arvostelun ja arvioinnin merkkaamalla mielestään toteutuneeseen kohtaan kuulakärkikynällä merkin ”X”. Mahdolliset lisätiedot ja kommentit järjestäjä voi täyttää ”Lisätiedot ja huomiot”-kohtaan. Yleisen palautteen harjoituksen osallistujalle järjestäjä täyttää ”YLEINEN PALAUTE HARJOITUKSEN OSALLISTUJALLE” – kohtaan.

**Osallistujat ja Organisaatio:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Harjoituksen päivämäärä:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yleinen arviointi** | **0 (=huono)** | **1 (=välttävä)** | **2 (=hyvä)** | **3 (=kiitettävä)** |
| 1. Asenne ja motivaatio |  |  |  |  |
| 2. Työskentely ryhmässä |  |  |  |  |
| 3. Ohjeiden mukaan toimiminen |  |  |  |  |
| 4. Kommunikointitaidot |  |  |  |  |
| 5. Tavoitteiden saavuttaminen |  |  |  |  |

**Lisätiedot ja huomiot:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tekninen arviointi (BT 1)** | **0 (=huono)** | **1 (=välttävä)** | **2 (=hyvä)** | **3 (=kiitettävä)** |
| 1. Yleinen tekninen osaaminen |  |  |  |  |
| 2. Käyttöympäristön hallinta |  |  |  |  |
| 3. Teknisiin tilanteisiin reagoiminen |  |  |  |  |
| 4. Tekninen viestintä |  |  |  |  |
| 5. Järjestelmien asianmukainen käyttö |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tekninen arviointi (BT 2)** | **0 (=huono)** | **1 (=välttävä)** | **2 (=hyvä)** | **3 (=kiitettävä)** |
| 1. Työskentely Linux-ympäristössä |  |  |  |  |
| 2. Syötteiden havainnointi |  |  |  |  |
| 3. Syötteisiin reagointi |  |  |  |  |
| 4. Vasteiden onnistumistaso |  |  |  |  |
| 5. Työskentely palomuuri/IDS-ympäristössä |  |  |  |  |

**Lisätiedot ja huomiot:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**YLEINEN PALAUTE HARJOITUKSEEN OSALLISTUJILLE**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**HARJOITUKSEN JÄRJESTÄJÄN ITSEARVOSTELU JA -ARVIOINTI**

Järjestäjä täyttää harjoittelun itsearvostelun ja -arvioinnin merkkaamalla mielestään toteutuneeseen kohtaan kuulakärkikynällä merkin ”X”. Mahdolliset lisätiedot ja kommentit järjestäjä voi täyttää ”Lisätiedot ja huomiot”-kohtaan. Yleisen palautteen harjoituksesta järjestäjä täyttää ”YLEINEN PALAUTE HARJOITUKSESTA” – kohtaan.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Harjoituksen suunnittelu ja valmistelu** | **0 (=huono)** | **1 (=välttävä)** | **2 (=hyvä)** | **3 (=kiitettävä)** |
| 1. Ideoinnin onnistuminen |  |  |  |  |
| 2. Ajankäyttö |  |  |  |  |
| 3. Ryhmän työskentely |  |  |  |  |
| 4. Yhteistyö organisaation kanssa |  |  |  |  |
| 5. Suunnittelun ja valmistelun onnistuminen |  |  |  |  |
| 6. Perehdytyksen onnistuminen |  |  |  |  |

**Lisätiedot ja huomiot:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yleinen** | **0 (=huono)** | **1 (=välttävä)** | **2 (=hyvä)** | **3 (=kiitettävä)** |
| 1. Harjoituksen perehdytysmateriaali |  |  |  |  |
| 2. Harjoituksen tilat ja järjestelyt |  |  |  |  |
| 3. Työpisteet |  |  |  |  |
| 4. Teknisten työkalujen toimivuus |  |  |  |  |
| 5. Harjoituksen yleinen aikataulutus |  |  |  |  |
| 6. Harjoituksen mielekkyys |  |  |  |  |

**Lisätiedot ja huomiot:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tekninen** | **0 (=huono)** | **1 (=välttävä)** | **2 (=hyvä)** | **3 (=kiitettävä)** |
| 1. Työympäristöjen selkeys |  |  |  |  |
| 2. Työympäristöjen realistisuus |  |  |  |  |
| 3. Työympäristön ohjeistus |  |  |  |  |
| 4. Käytettyjen ohjelmien realistisuus |  |  |  |  |
| 5. Käytettyjen ohjelmien ohjeistus |  |  |  |  |
| 6. Käytettyjen ohjelmien käytännöllisyys |  |  |  |  |
| 7. Harjoituksen tekninen aikataulutus |  |  |  |  |
| 8. Skenaarion realistisuus |  |  |  |  |
| 9. Pelitapahtumien järjestely |  |  |  |  |
| 10. Syötteiden onnistuminen |  |  |  |  |

**Lisätiedot ja huomiot:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**YLEINEN PALAUTE HARJOITUKSESTA**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**