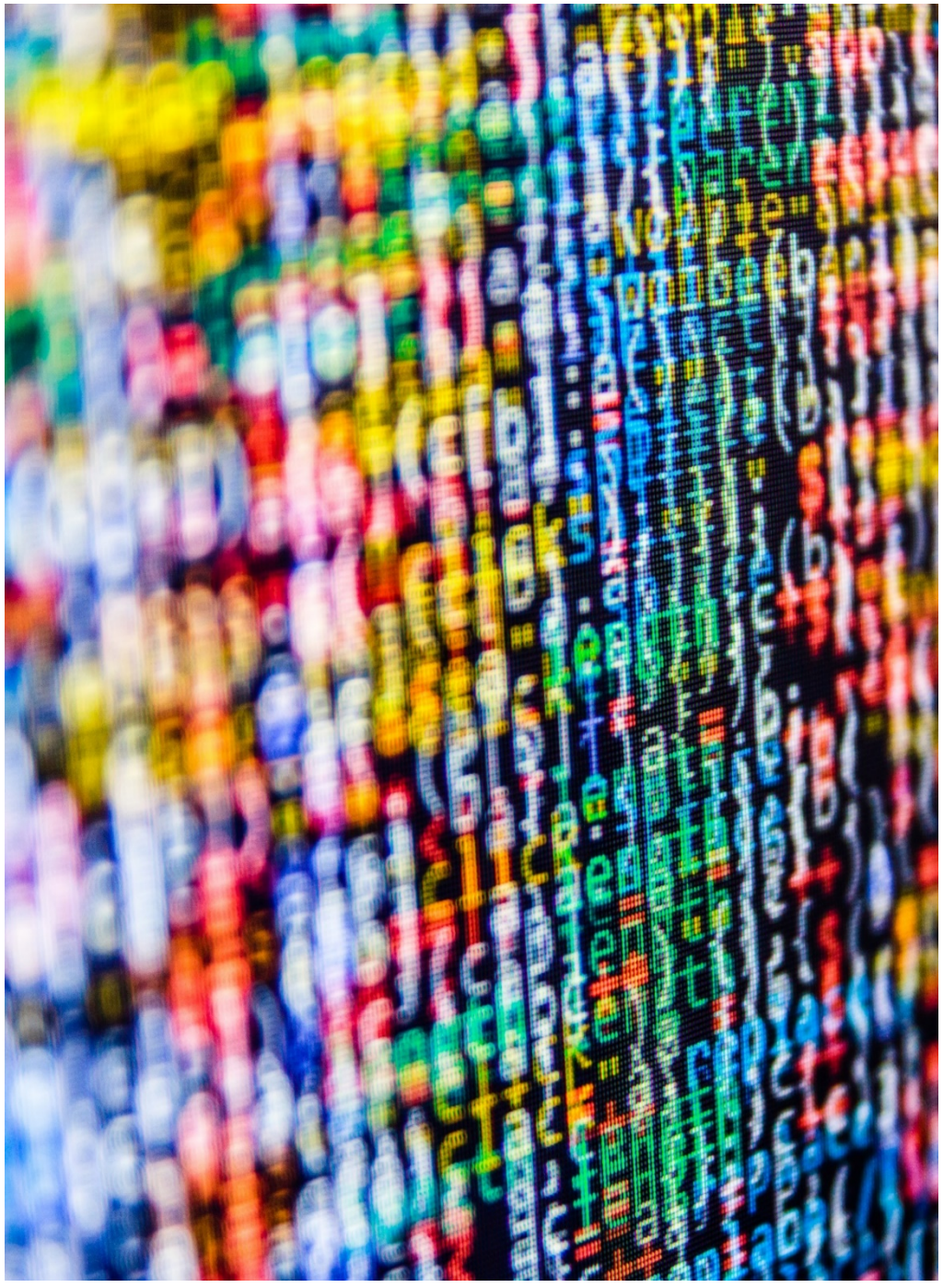
TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Operatiivinen kyberturvallisuus

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisväline (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.



Opintojaksot

- **Operatiivinen kyberturvallisuus (5 op)**
- Kyberuhkatiedon hyödyntäminen (5 op)

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Operatiivinen kyberturvallisuus

5 op

Opiskelijoiden odotetaan laajentavan tietämystään tietoturvakeskuksen käsitteestä ja toiminnoista, kokeilemaan, vertailemaan ja edistämään tietoturvakeskuksen toimintaan sopivia teknisiä ratkaisuja sekä toteuttamaan uhkanmetsästystä teknisin välinen osana tietoturvakeskuksen tehtäviä ja prosesseja.

Kurssin suoritettuaan opiskelijoilla on valmiudet suunnitella, johtaa ja toteuttaa erilaisia kyberpoikkeamien käsittely- ja uhkanmetsästystoimia sekä monitorointiratkaisuja ICT-järjestelmien kokonaisvaltaisen turvallisuuden parantamiseksi.

Kurssi keskittyy erityisesti verkotetun infrastruktuurin valvonnan rakentamiseen ja tehostamiseen osana organisaatioiden operatiivisia toimintoja. Poikkeamien havainnointiin ja niiden käsittelyyn liittyvissä valvontaprosesseissa painopisteenä on reaktiivisuus.

Operatiivinen kyberturvallisuus

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OSAAMISALUEET

- Tietoturvan hallinta
- Erilaisten tietomallien rakenteistaminen
- Luo kyvykkyyksiä poikkeamien ja korreloitujen kyberuhkien visualisointiin ja seurantaan
- Kyberturvallisuuden poikkeamahallinnan prosessien sekä niiden työnkulun suunnittelu, optimointi ja dokumentointi
- Uhkanmetsästys kybertiedustelutietoa hyödyntämällä

Operatiivinen kyberturvallisuus

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

TIETÄMYS

- Kyberturvallisuuden politiikat ja parhaat käytänteet
- Häiriönkäsittelystandardit, menetelmät ja viitekehykset
- Häiriönkäsittelyn työkalut ja viestintämenettelyt
- Tietoturvakeskuksen (SOC) toiminta
- CSIRT toiminta
- Kyberturvallisuuteen liittyvät teknologiat
- Tietojärjestelmien haavoittuvuudet

Operatiivinen kyberturvallisuus

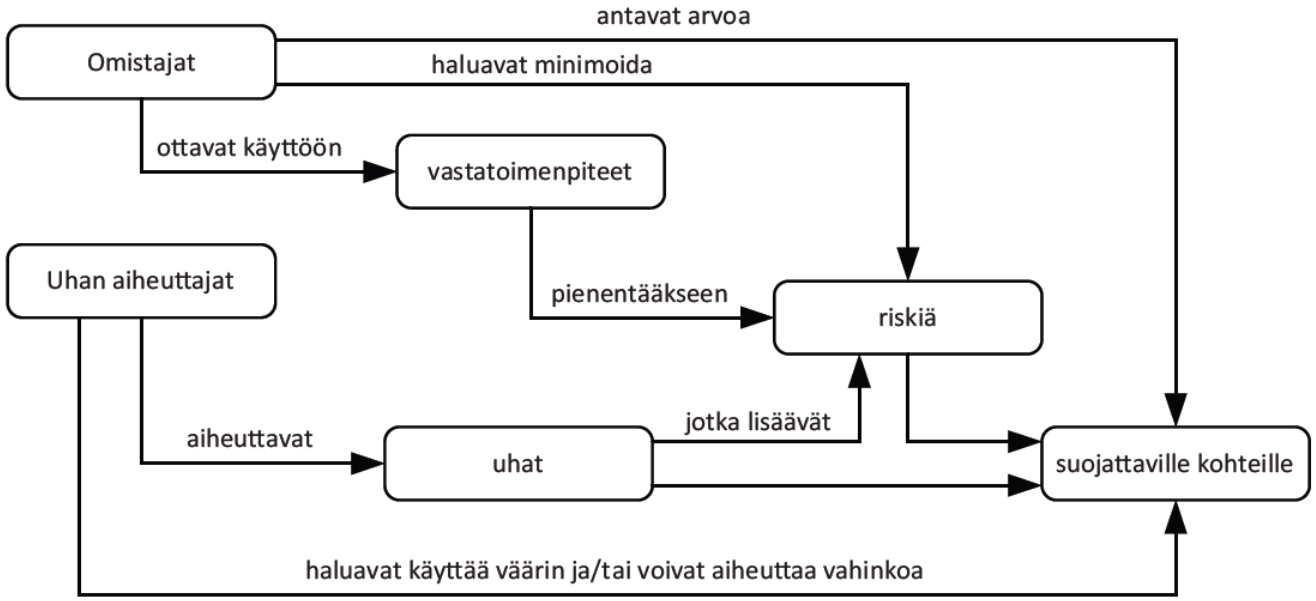
TAIDOT

- Kyberturvallisuuden häiriönkäsittelyn teknisten ja operatiivisten toimintojen suunnittelu ja harjoittelu
- Kyberuhkatiedon hyödyntäminen uhkanmetsästyksessä
- Teknisten kyberturvallisuusratkaisujen integroiminen osaksi valvontaympäristöä
- Havaitsemis- ja reagointijärjestelmän (XDR) käyttö uhkanmetsästyksessä

Tietoturva-asiayhteys

ISO/IEC 62443-1-1

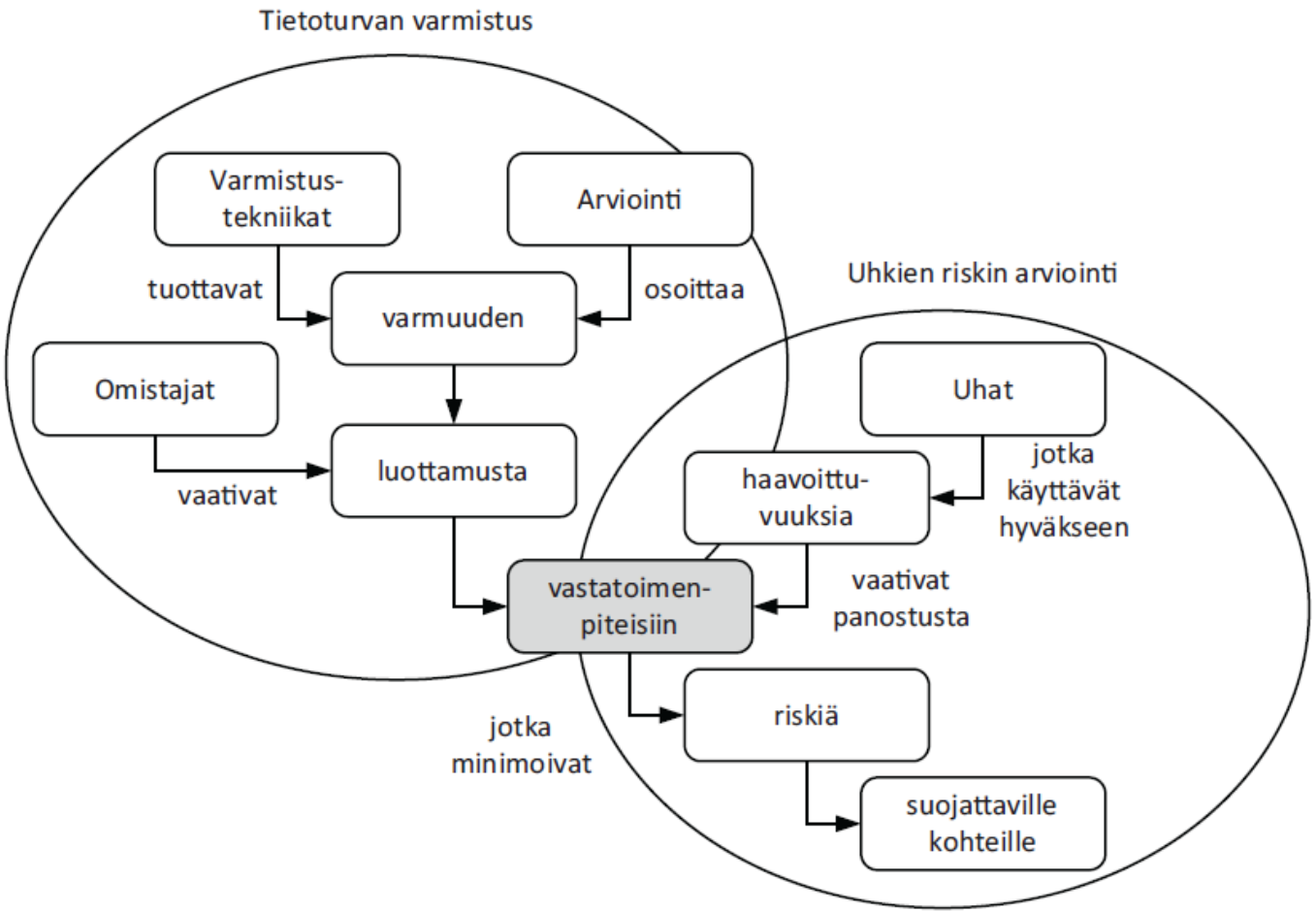
Tietoturva-asiayhteys perustuu uhkien, riskien ja vastatoimenpiteiden käsitteisiin ja niiden välisiin suhteisiin. Näiden käsitteiden suhteet voidaan esittää yksinkertaisella mallilla. Yksi tällaisista malleista, joka esitetään ISO/IEC 15408-1:ssä (Yhteiset kriteerit), on kopioitu viereiseen kuvaan.



Tietoturva-asiayhteys

ISO/IEC 62443-1-1

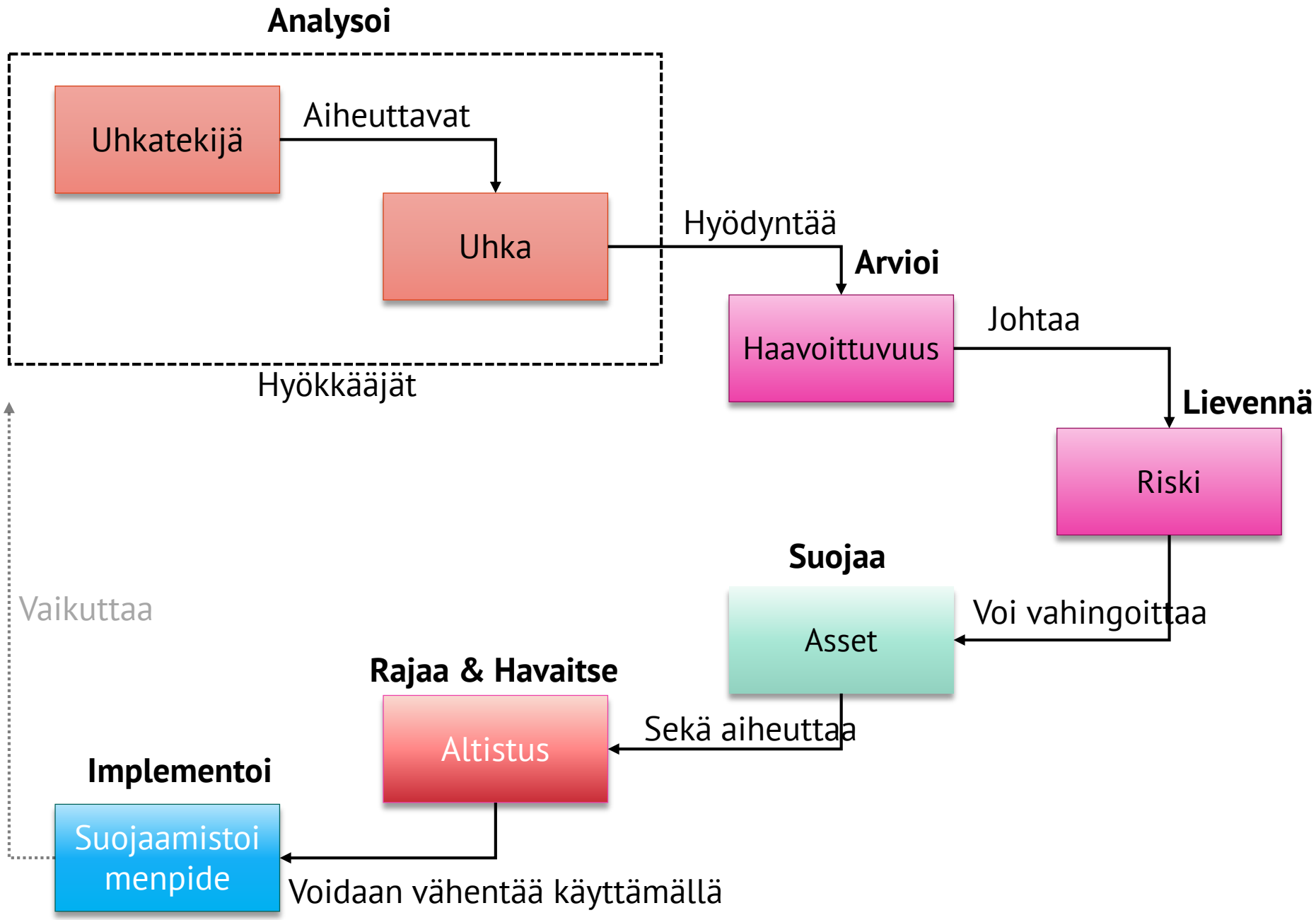
Oheisen kuvan kontekstimallissa esitetään toinen näkemys uhkien, riskien ja vastatoimien käsitteiden suhteista. Se osoittaa, miten laajennettu käsitejoukko liittyy kahteen toisiinsa liittyvään prosessiin, tietoturvavarmuuteen ja riskien arviointiin.



Operatiivinen kyberturvallisuus

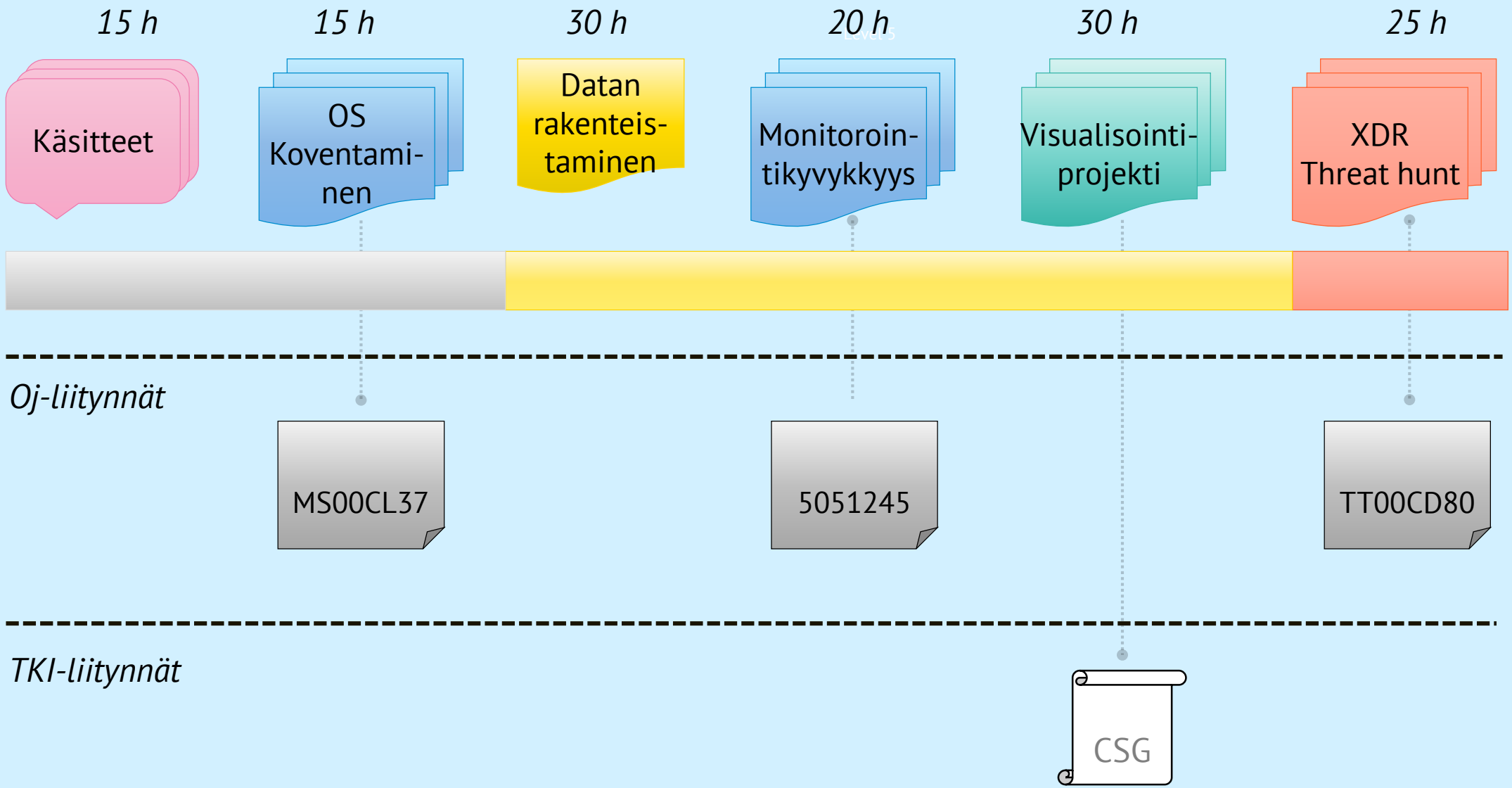
johdetut teemat

- Kybertoimintaympäristön tilannekuvan täydentäminen
  - hallinnollisista määräyksistä käytännön vaatimuksenmukaisuuteen
  - havainnointi/monitorointikyvyn rakentaminen ja käytännön implementointi
  - Uhkanmetsästys - ennakoiva lähestymistapa aiemmin tuntemattomien, selvittämättömien tai yhä jatkuvien uhkien tunnistamiseksi organisaation verkossa


Analysoi
Uhkatekijä
Aiheuttavat
Uhka
Hyökkääjät
Hyödyntää
Arvioi
Haavoittuvuus
Johtaa
Lievennä
Riski
Suojaa
Asset
Voi vahingoittaa
Vaikuttaa
Rajaa & Havaitse
Altistus
Sekä aiheuttaa
Implementoi
Suojaamistoi menpide
Voidaan vähentää käyttämällä

Suunnitelmanmukainen tehtävä- ja teemajaottelu

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES



Tehtäväpisteytys ja arvosanarajat (vahvistamatta)

- Koti- ja labratehtävät
  - ryhmätehtävät 2 x 10 p
  - yksilötehtävät 6 x 5 p
- Visualisointiprojekti 30p
- Vertaisarvioidut esitykset 2 x 10p

- Arvosanarajat
  - 0 0..39 p
  - 1 40..49 p
  - 2 50..59 p
  - 3 60..74 p
  - 4 75..89 p
  - 5 90..100 p