TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari 2.1 verrattuna versioon 2.0

29.05.2022

Sisältö

- Miksi muutokset tehtiin
- Muutokset Kybermittarin rakenteeseen
- Muutokset osioittain
- Muutokset raportointiin
- Käytettävyys
- Siirto versioiden välillä

Miksi muutokset tehtiin

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Muutokset Kybermittarin taustalla oleviin viitekehyksiin

- Kybermittarin 10 osiota ja osioiden käytännöt perustuvat suurelta osin C2M2-malliin. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
  - Kybermittari V1 pohjautui C2M2 V2 luonnokseen.
  - Kybermittari V2.0:n pohjana on C2M2 V2.0.
  - Kybermittari V2.1:n pohjaksi tuli C2M2 versio V2.1. https://c2m2.doe.gov/resources
- Lisäksi kehitetty kriittisten palveluiden suojaamisen osio (CRITICAL)
- Merkittävimmät sisällölliset muutokset työkaluun
  - Käytäntökohtaiset tulkintaohjeet C2M2-mallista (englanniksi)
  - Selkeämpi kieliasu, muutoksia käytäntöihin sekä käytettävyysmuutoksia
  - Ristiinkytkentä on viitteellinen ja Kybermittarin versiossa 2.1 se on NIST National Online Informative References (OLIR) ohjelman tarjoama: https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?frameworkVersionId=85

Muutokset työkalun laskentamalliin

- Versiossa 2.1 muutettiin NIST CSF V1.1 – C2M2 V2.1 ristiinviittausta
  - V2.0 oli Kyberturvallisuuskeskuksen tekemä ristiinviittaus
  - V2.1 sisältää NIST National Online Informative References (OLIR) ohjelman tarjoaman ristiinviittauksen (https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?frameworkVersionId=85)
  - Seurannassa toimiiko uusi ristiinviittaus ja mitä tapahtuu NIST CSF 2.0:n myötä
- **Tulevaisuudessa**
  - NIST Cybersecurity Framework uudistumassa (V2.0)
  - Muita muutoksia asiakastarpeen mukaan. Tekemisen paino todennäköisesti tukimateriaalissa, vertailutiedossa ja analyysissä sekä koulutuksessa kuin excelin viilauksessa.

Muutokset Kybermittarin rakenteeseen

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Muutokset käyttäjän näkökulmasta

Rakenne	Mallin rakenne säilyy käytännössä ennallaan
Osiot	Yksi osio nimetty uudelleen THIRDPARTY->THIRD-PARTIES. Sisällöllisesti suurehkoja muutoksia kolmessa osiossa.
Tavoitteet	WORKFORCE-osion tavoitteet uudessa järjestyksessä
Käytännöt	Käytäntöjä poistunut ja uusi käytäntöjä erityisesti kypsyystasoille 2 ja 3. Hallintatoimissa kaksi käytäntöä vaihtaneet paikkaa. Paljon pieniä muutoksia käytäntöihin. Pari muutosta kypsyystasoissa.
Raportointi	Peruslaskentamalli säilyy ennallaan, mutta Kybermittari – NIST CSF ristiinviittaus on korvattu C2M2-mallin kehittäjän (DoE) tulkinnalla.
Tuki	C2M2 2.1:n mukana tulleet tulkintaohjeet saatavilla

! Versiolla 1 ja 2.0 tehdyn arvioinnin tulokset on mahdollista siirtää versioon 2.1 Tästä on erillinen ohje ja työkalut. !

Kybermittari (C2M2) vs NIST CSF V1.1

- Ristiinviittaus Kybermittari/C2M2 - NIST Cybersecurity Framework on viitteellinen
  - Toteutus on näkyvillä Kybermittarin NISTmap-välilehdellä.

	Osa-alue	Viittaukset V2.0	Viittaukset V2.1
ID	Tunnistaminen	304	222
PR	Suojautuminen	315	367
DE	Havannointi	131	107
RS	Reagointi	74	92
RC	Palautuminen	21	24
	Toteutus	Traficom	Department of Energy (US)

- NIST Cybersecurity Framework V1.1 (https://www.nist.gov/cyberframework)
  - Viitekehyksestä ei ole saatavilla virallista, suomenkielistä käännöstä.
- NIST CSF 2.0 kehitystyö on jo aloitettu

Versioiden välinen, tilastollinen vertailu.

	Kybermittari 1.0	Kybermittari 2.0	Kybermittari 2.1
Osiot	11 (10 + CRITICAL)	11 (10 + CRITICAL)	11 (10 + CRITICAL)
Tavoitteet	42 (hallintatoimia 10)	46 (hallintatoimia 10)	46 (hallintatoimia 10)
Käytännöt yht.	325	369	383
Käytännöt 1 taso	60	64	66
Käytännöt 2 taso	147	162	178
Käytännöt 3 taso	118	143	139

Versioiden välinen, tilastollinen vertailu.

	Kybermittari 2.1	CRITICAL -osio	Sama	Muutos	Uusi	Pois
Osiot	**11 (10 + CRITICAL)**		kaikki			
Tavoitteet	**46 (hallintatoimia 10)**	3		43 (10) Pääosin pieniä		
Käytännöt yht.	**383**	27	210	106	40	26
Käytännöt 1 taso	**66**	10	38	15	3	
Käytännöt 2 taso	**178**	12	92	52	22	
Käytännöt 3 taso	**139**	5	80	39	15	

Muutokset osioittain

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

		Sama	Muutos	Uusi	Yhteensä
Omaisuuden, muutosten ja konfiguraation hallinta	ASSET	18	14	4	36
Uhkien ja haavoittuvuuksien hallinta	THREAT	19	8	3	30
Riskienhallinta	**RISK**	21	14	4	**39**
Identiteetin- ja pääsynhallinta	ACCESS	21	9	5	35
Tilannekuva	SITUATION	18	6	4	28
Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus	RESPONSE	23	23	3	49
Kumppaniverkoston riskien hallinta	**THIRD-PARTIES**	17	5	3	**25**
Henkilöstön johtaminen ja kehittäminen	WORKFORCE	19	8	5	32
Kyberturvallisuus-arkkitehtuuri	**ARCHITECTURE**	37	14	7	**58**
Kyberturvallisuuden hallinta	PROGRAM	20	2	2	24

Muutokset tavoitteiden järjestykseen

	Kybermittari 2.1	Kybermittari 2.0
Kyberturvallisuuden vastuiden jakaminen	WORKFORCE-1	WORKFORCE-3
Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen	WORKFORCE-2	WORKFORCE-4
Henkilöstöhallinnon prosessit	WORKFORCE-3	WORKFORCE-1
Koulutus ja kybertietoisuuden lisääminen	WORKFORCE-4	WORKFORCE-2
Yleisiä hallintatoimia	WORKFORCE-5	WORKFORCE-5

Muutokset raportointiin

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Päämuutokset raportointiin

- Kybermittari (C2M2) vs NIST CSF V1.1 ristiinviittauksen muutokset
  - R1: taustalla oleva NIST CSF – Kybermittari ristiin viittaus päivitetty
  - R3: taustalla oleva NIST CSF – Kybermittari ristiin viittaus päivitetty

Käytettävyys

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Käytettävyys muutoksia

- Languages-välilehdellä uusi sarake:”Kuvaava teksti”, jossa C2M2-mallista otettu käytäntökohtainen tulkintaohje. Lähde: https://c2m2.doe.gov/
  - Saatavilla myös erillisenä, osin sovellettavissa V2.0:aan.
- Käytäntöjen kieliasua pyritty selkeyttämään.
- Parannettu ohjeistusta ja vinkkejä välilehdillä
- Lisätty NIST CSF-välilehti, jossa ristiinkytkennän tiedot
- Poistettu migraatiovälilehdet erilliseksi työkaluksi

Esimerkki kuvaavasta tekstistä (ASSET-2g)

ASSET-2g (MIL 3) The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes

The inventory of information assets should be updated and maintained as assets change throughout their lifecycle to ensure the inventory is complete and accurate. Ensuring that the information asset inventory is current might involve change management procedures that require inventory updates any time assets are significantly altered. The organization might also conduct inventory reviews, both periodically (such as quarterly or yearly) and based on events (such as changes in organizational structure, major changes in critical systems, and the acquisition and consolidation of another business).

Related Practices

· *Progression*: This practice is part of a practice progression. Practice progressions are groups of related practices that represent increasingly complete or more advanced implementations of an activity. The practices in this progression include: ASSET-2a, ASSET-2b, ASSET-2f, ASSET-2g.

Siirto versioiden välillä

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tulosten siirto eri versioiden välillä

- Taulukot, joissa on kuvattu muutokset
  - Ks. https://www.kybermittari.fi
- Siirtotyökalut ja ohjeet löytyvät erillisinä, ei enää integroituna samaan työkaluun.
  - Ks. https://www.kybermittari.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

https://www.kybermittari.fi