Kehityspolut: Ohje Kehityspolkujen hyödyntäminen

Kypsyysmalli sisältää kehityspolkuja, joiden numero on merkitty jokaisen käytännön kohdalle osiovälilehtien D-sarakkeeseen. (muut paitsi CRITICAL)

Kehitys-välilehdellä voit suodatustoiminnolla myös tutkia eri polkuja ja vastauksia yksittäisiin käytäntöihin.
Kuvaus kehityspoluista:
https://c2m2.doe.gov/C2M2%20Self-Evaluation%20Guide.pdf Appendix C:Related practices, Table 7: Practice progression

Tavoitteena jatkossa sisällyttää tiedot myös koulutusmateriaaleihin. (31.10.2024)

nro	Välilehti	Kehityspolut	Subject of Progression
1	ASSET	IT- ja OT-omaisuuden rekisteri	IT and OT asset inventory
2	ASSET	Omaisuuserien priorisointi	Prioritization of inventoried assets
3	ASSET	Tietovarantojen hallinta	Information asset inventory
4	ASSET	Luetteloidun omaisuuden luokittelu	Categorization of inventoried assets
5	ASSET	Vakioitujen perusasetusten määritys ja ylläpito	Creating and maintaining configuration baselines
6	ASSET	Vakioitujen perusasetusten käyttö	Using configuration baselines
7	ASSET	Muutosten ja päivitysten tekeminen turvallisesti	Making changes to assets in a secure manner
8	ASSET	Laitteisiin, ohjelmistoihin ja tietovarantoihin tehtyjen muutosten dokumentointi	Documentation of changes to assets
9	THREAT	Kyberturvallisuuden haavoittuvuustietolähteet	Cybersecurity vulnerability information sources
10	THREAT	Kyberturvallisuuden haavoittuvuustietojen hankkiminen ja jakaminen.	Obtaining and sharing cybersecurity vulnerability information
11	THREAT	Kyberturvallisuuden haavoittuvuusarviointien tekeminen	Performing cybersecurity vulnerability assessments
12	THREAT	Kyberturvallisuuden haavoittuvuuksiin puuttuminen	Mitigating cybersecurity vulnerabilities
13	THREAT	Uhkatietolähteet	Threat information sources
14	THREAT	Uhkatietojen hankkiminen ja jakaminen	Obtaining and sharing threat information
15	THREAT	Uhkatavoitteet ja uhkaprofiilit	Threat objectives and threat profiles
16	THREAT	Uhkiin vastaaminen	Responding to threats
17	RISK	Kyberriskienhallintastrategian ja -ohjelman laatiminen	Establishing cyber risk management strategy and program
18	RISK	Kyberriskienhallintamalli ja johdon tuki.	Establishing governance and sponsorship for the cyber risk management program
19	RISK	Kyberriskien tunnistaminen	Identifying cyber risks
20	RISK	Kyberriskien organisointi ja kuvaaminen	Organizing and describing cyber risks
21	RISK	Kyberriskien priorisointi	Prioritizing cyber risks
22	RISK	Kyberriskien vaikutusten lieventäminen	Mitigating the impact of cyber risks
23	RISK	Kyberriskien analysointi	Analyzing cyber risks
24	RISK	Riskeihin reagointi	Risk responses
25	ACCESS	Identiteettien luominen	Establishing identities
26	ACCESS	Todentamisen hallinta	Managing authentication
27	ACCESS	Loogisten käyttöoikeuksien valvonta ja vaatimukset	Logical access controls and requirements
28	ACCESS	Loogiset käyttöoikeudet	Logical access privileges
29	ACCESS	Fyysisen pääsyn valvonta ja vaatimukset	Physical access controls and requirements
30	ACCESS	Fyysisen pääsyn oikeudet	Physical access privileges
31	ACCESS	Fyysisen pääsyn valvonta	Monitoring physical access
32	SITUATION	Kirjaaminen ja kirjaamisvaatimukset	Logging and logging requirements
33	SITUATION	Seuranta ja seurantavaatimukset	Monitoring and monitoring requirements
34	SITUATION	Poikkeavan toiminnan indikaattorit	Indicators of anomalous activity
35	SITUATION	Seurantatietojen yhdistäminen ja analysointi	Aggregating and analyzing monitoring data
36	SITUATION	Tietojen kerääminen tilannetietoisuutta varten	Collecting information for situational awareness
37	RESPONSE	Kyberturvallisuustapahtumien havaitseminen ja dokumentointi	Detecting and documenting cybersecurity events
38	RESPONSE	Kyberturvallisuuspoikkeamien ilmoittamiskriteerit	Cybersecurity incident declaration criteria
39	RESPONSE	Kyberturvallisuustapahtumien ja -poikkeamien analysointi.	Analyzing cybersecurity events and incidents
40	RESPONSE	Kyberturvallisuustapahtumien ja -poikkemien dokumentointi	Documentation of cyber events and incidents
41	RESPONSE	Kyberturvallisuuden poikkemanhallintasuunnitelmat	Cybersecurity incident response plans
42	RESPONSE	Kyberturvallisuuden vaaratilanteisiin reagoiminen	Responses to cybersecurity incidents
43	RESPONSE	Kyberturvallisuuden vaaratilanteisiin reagoimista koskevat harjoitukset	Cybersecurity incident response exercises
44	RESPONSE	Jatkuvuussuunnitelmat	Continuity plans
45	RESPONSE	Tietojen varmuuskopiointi	Data backups
46	RESPONSE	IT- ja OT-laitteiden varaosat	Spares for selected IT and OT assets

47	RESPONSE	Jatkuvuussuunnitelmien testaus ja harjoittelu	Continuity plans tests and exercises
48	THIRD-PARTIES	Kolmansien osapuolten tunnistaminen ja priorisointi sekä kolmansista osapuolista aiheutuvat kyberriskit	Identifying and prioritizing third parties and cyber risks arising from third parties
49	THIRD-PARTIES	Kyberturvallisuuden ja kyberriskien huomioiminen kolmansien osapuolten valinnassa	Considering cybersecurity and cyber risks in selection of third parties
50	THIRD-PARTIES	Kyberturvallisuuden ja kyberriskien huomioiminen tuotteiden ja palveluiden valinnassa	Considering cybersecurity and cyber risks in selection of products and services
51	THIRD-PARTIES	Kolmansista osapuolista aiheutuvien kyberriskien lieventäminen	Mitigating cyber risks arising from third parties
52	THIRD-PARTIES	Kyberturvallisuusvaatimukset kolmansille osapuolille	Cybersecurity requirements for third parties
53	WORKFORCE	Henkilöstötarkastukset	Personnel vetting
54	WORKFORCE	Kyberturvallisuuden huomioon ottaminen työsuhteen päättyessä ja henkilöstösiirroissa.	Addressing cybersecurity in personnel separation and transfer procedures
55	WORKFORCE	Hyväksyttävä käyttö ja muut yleiset kyberturvallisuusvastuut	Acceptable use and other general cybersecurity responsibilities
56	WORKFORCE	Kyberturvallisuustietoisuustoiminta	Cybersecurity awareness activities
57	WORKFORCE	Kyberturvallisuusvastuiden tunnistaminen ja dokumentointi	Identifying and documenting cybersecurity responsibilities
58	WORKFORCE	Kyberturvallisuusvastuiden osoittaminen	Assigning cybersecurity responsibilities
59	WORKFORCE	Kyberturvallisuuskoulutus	Cybersecurity training
60	ARCHITECTURE	Kyberturvallisuusarkkitehtuurin kehittämissuunnitelma	Cybersecurity architecture strategy
61	ARCHITECTURE	Kyberturvallisuusarkkitehtuuri	The cybersecurity architecture
62	ARCHITECTURE	Kyberturvallisuusarkkitehtuurin hallintamalli ja johdon tuki	Establishing governance and sponsorship for the cybersecurity architecture
63	ARCHITECTURE	Omaisuuserien segmentointi	Asset segmentation
64	ARCHITECTURE	Verkkojen suojaus	Network protections
65	ARCHITECTURE	IT- ja OT-omaisuuden sekä tietovarantojen turvaaminen	IT and OT asset security
66	ARCHITECTURE	Turvalliset konfiguraatiot	Asset configuration security
67	ARCHITECTURE	Turvallinen ohjelmistokehitys käytössä talon sisällä	Secure software development use in-house
68	ARCHITECTURE	Turvallinen ohjelmistokehitys käytössä toimittajilla	Secure software development use by vendors
69	ARCHITECTURE	Tietojen suojaus	Data security
70	PROGRAM	Kyberturvallisuusohjelma / strategia	The cybersecurity program strategy
71	PROGRAM	Kyberturvallisuuden hallinta / ohjelma	The cybersecurity program
72	PROGRAM	Ylimmän johdon tuki kyberturvallisuusohjelmalle.	Senior management support and sponsorship for the cybersecurity program
73	PROGRAM	Yhteistyö sisäisten ja ulkoisten sidosryhmien kanssa kyberturvallisuusohjelman hallinnassa	Collaboration with internal and external stakeholders in cybersecurity program management