Tietoturva järjestelmän elinkaaren hallinnassa

Markku Tyynelä

24.10.2023

Muuttuva ympäristö

Tietoturvavaatimukset ja -säädökset kehittyvät ja lisääntyvät jatkuvasti

~ 20 - 10 v - Tuotteiden tietoturva

- Kuinka perustietoturva hoidettu automaatiotuotteissa?
- Tietoturvapäivitykset (MS Windows), virustorjunta, kovennus
- Perustason ylläpitopalvelut

~ 10 - 5 v - Prosessit

- Kuinka tietoturva ja kyberturvallisuutta hallitaan Valmet Automaation prosesseissa?
- Lisääntyvät vaatimukset tuotteiden ja palvelujen kyberturvallisuuteen
- Paljon erilaisia asiakaskohtaisia vaatimuksia (kaikilla omanlaisensa tietoturvavaatimukset)

~ 5 - 2 v - Organisaation toiminta

- Kuinka Valmet yrityksenä hallitsee tietoturvaa ja kyberturvallisuutta koko organisaation laajuudella, kaikilla organisaation tasoilla?
- Vaatimuksia kuinka todistetaan että Valmet toimii niin kuin sanoo (esim. sertifikaatit)
- Liitynnät asiakkaiden omiin järjestelmiin (esim. SIEM) lisääntyvät
- Vaatimuksia yleisimpiin tietoturvastandardeihin, kuten ISO 27001 ja IEC 62443
- Tarkemmat palvelusopimukset
- Tarve riskiarviointien lisääntynyt

~ 2 v - Todistaminen

- Asiakkaat vaativat todisteita että kyberturvallisuus on asianmukaisesti hallittu kaikilla organisaation tasoilla
- Kolmansien osapuolien käyttö arvioinneissa lisääntynyt, esim. Tietoturva-arviot, todisteiden keräys (esim. Web Portaalien kautta)
- Vaatimukset IEC 62443 tietoturvatasoihin lisääntyvät
- IT/OT lähentyminen
- Assettien & Elinkaaren hallinta
- **Vaatimustenmukaisuus** Tietoturvaan liittyvät lait ja säädökset lisääntyvät jatkuvasti

Kyberturva Valmet Automationin liiketoiminnassa

Tuotteiden tietoturva

Automaation tuotteet ja palvelut kehitetty käyttäen tietoturvan parhaita käytäntöjä (best practices) ja syväsuojauksen (defense-in-depth) periaatteita. IEC-62443-4-1 sertifioidut R&D elinkaariprosessit.

Tietoturvapalvelut

Valmet Automation tarjoaa laajat tietoturvapalvelut, jotka auttavat riskienhallinnassa, sekä saavuttamaan ja ylläpitämään haluttu tietoturvataso koko laitoksen elinkaaren ajan.

Tietoturvaprosessit

Valmet Automationin Kyberturvallisuusstrategia, toiminta perustuu sertifioituun tietoturvallisuuden ISO 27001 hallintajärjestelmään (ISMS, Information Security Management System).

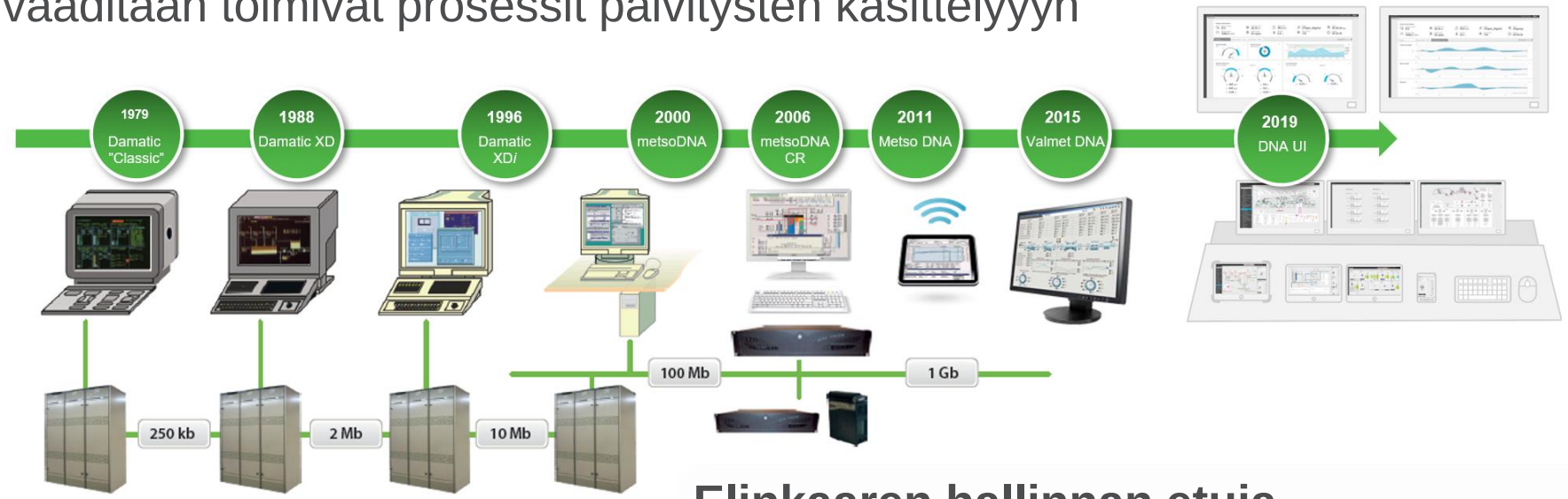
Tietoturvatietoisuus

Valmetin yleisillä ja Automaation omilla erillisillä kyberturvallisuuskoulutuksilla varmistetaan ja parannetaan yleistä tietoturvatietoisuutta.

Elinkaaren hallinta

Elinkaaren hallintaan vaaditaan toimivat prosessit päivitysten käsittelyyyn

Elinkaaren hallinta on osa riskienhallintaa



Syitä elinkaaren hallintaan

- Ikääntyvissä järjestelmissä kasvava riski häiriöihin
- Ohjelmistoversiot eivät enää tuettuja (esim. 3rd party, Windows)
- Tietoturvapäivityksiä ei enää saatavilla
- Jatkuvasti pienenevä varaosavarasto
- Ikääntyville järjestelmille ei löydy enää (erikois)osaajia
- Kasvavat ylläpitokustannukset
- Vaatimustenmukaisuutta ei enää voida taata

Elinkaaren hallinnan etuja

- Parempi luotettavuus järjestelmän toiminnalle
- Vaaditun tietoturvatason ylläpito
- Valmius tukea uusimpia/kehittyneempiä sovelluksia
- Parempi tuotantoprosessin tehokkuus
- Parempi käytettävyys
- Uusien ominaisuuksien käyttö
- Kokonaiskustannusten optimointi
- Vaatimustenmukaisuusvaatimusten täyttäminen

Automaatiojärjestelmän suojaus

Häiriötilanteisiin varautuminen ja reagointi

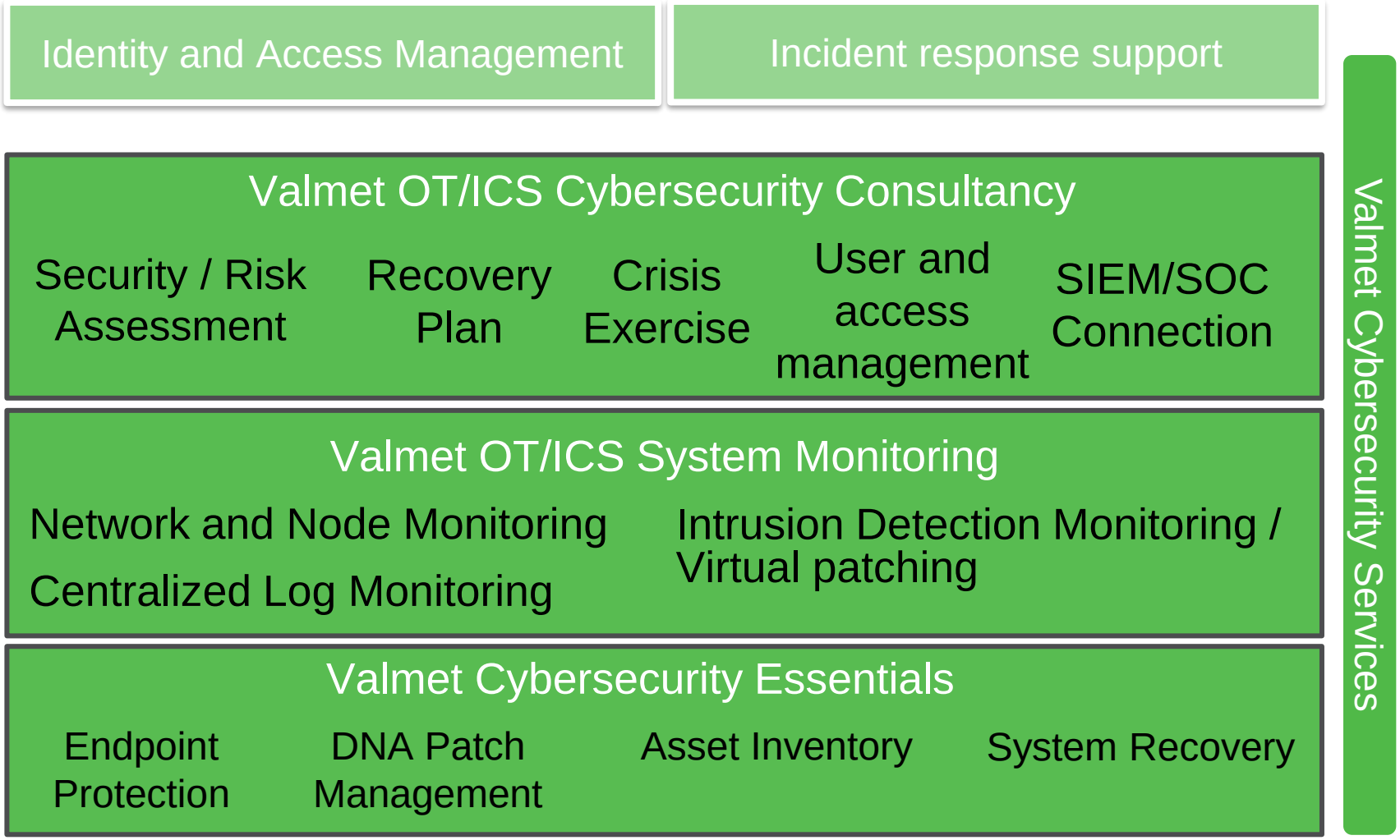
- Automaatiotoimittajan tuki ja yhteistyö asiakkaan tietoturvavalvomon (SOC) kanssa tarvittaessa
- Jatkuvuus- ja palautussuunnitelmat
- Prosessit päivitysten hallintaan
- Keskitetty käyttäjien hallinta

Verkon suojaus

- Verkon segmentointi
- Virtuaalinen suojauspäivitys (Virtual patching)
- Monitorointi
- Verkon assettien tunnistus ja havainnointi
- Tunkeutumisenestojärjestelmät OT ympäristöihin (Intrusion Prevention System, IPS + protokollien tunnistus)

Assettien suojaus

- Laitteiden suojaus (Endpoint protection)
- Suoritettavien sovellusten rajoitus (Application Whitelisting)
- Virtuaalinen suojauspäivitys



Häiriötilanteisiin varautuminen ja reagointi

Tyypillisiä haasteita

- Uusia haittaohjelmia ja yhä kehittyneempiä kyberuhkia ilmenee ja lisääntyy jatkuvasti
- Yritysten tietoturvakäytäntöjen laajentaminen myös OT puolelle takaamaan liiketoiminnan jatkuvuutta voi olla haastavaa
- Valmius OT häiriöiden havainnointiin ja erityisesti niihin reagointiin

Mahdollisia ratkaisumalleja

- Riskiarvioinnit ja tietoturva-auditit OT ympäristöön
- Automaatiotoimittajan tuki ja yhteistyö asiakkaan SOC:n kanssa
- Jatkuvuus- ja palautussuunnitelmat
- Asiantuntijaratkaisut asiakaskohtaisten OT tietoturvaratkaisujen suunnitteluun, toteutukseen ja testaukseen
- Tietoturvaharjoitukset

Keskeiset arvot ja hyödyt

- IT/OT lähentyminen - kohti uusia kyberturvakontrolleja ja toimenpiteitä
- OT assettien ja käyttäjäidentiteettien hallinta
- Alan parhaat käytännöt kyberturvauhkien havaitsemiseen
- Automaatiotoimittajan tietämys automaatiojärjestelmien teknologioista ja prosesseista, erityisesti kun häiriöihin pitää reagoida

Toipumissuunnitelma (Recovery Plan)

- Kriittisten assettien varmuuskopiointi ja palautus suunniteltu ja dokumentoitu
- Toipumisaika ja -kyky
- Tietoturvaharjoitukset ja -testaukset

Riski- ja Tietoturva-arvioinnit (Security Assessments/Audits)

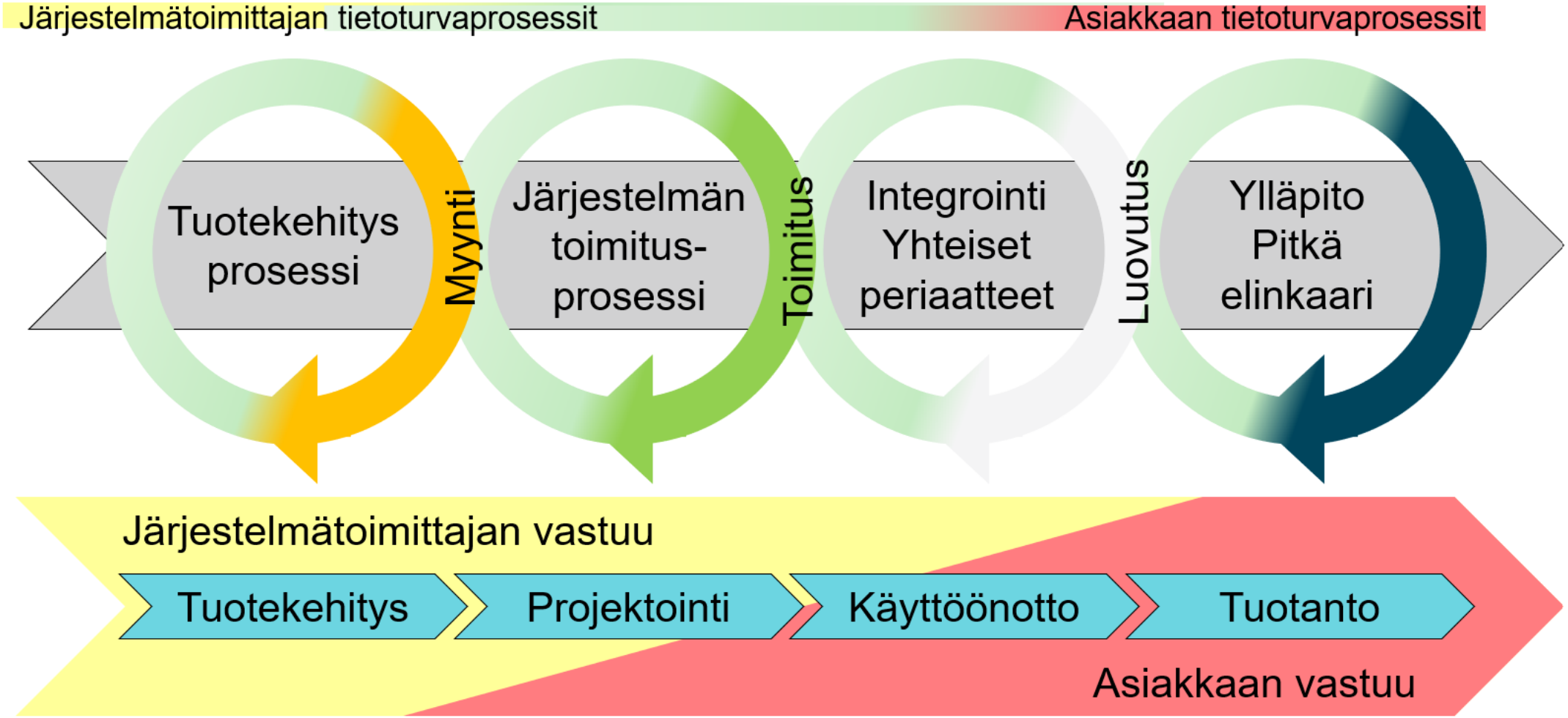
- Tärkeimpien kriittisten assettien tunnistus
- Korjaus- ja lieventämisstrategioiden parantaminen
- Varautuminen uusiin regulaatioihin, esim. NIS2 Direktiiviin

Valmet Cybersecurity Consultancy

”Automaatio edustaa vain pientä osaa laitoksen kokonaisinvestoinnista, mutta liiketoiminnan jatkuvuus, tuotannon toimivuus ja operatiiviset toiminnot ovat pääosin riippuvaisia tästä investoinnista.”

Elinkaaren hallinta

Vastuut



Elinkaaren hallinta

- OT riskienhallinta osana yrityksen liiketoiminnan jatkuvuudenhallintaa — ISO 27001, NIS2
- Riskien ja kriittisten uhkien hallinta myös OT ympäristössä — Assessment, Critical assets, Patch mgmt
- IT organisaation havainnointikyvyn laajentaminen OT järjestelmiin — Monitoring (SIEM/SOC)
- OT ympäristön käyttäjien identiteettien ja oikeuksien hallinta — AD/IAM
- OT ympäristön tietoturvatapahtumien hallinta ja palautuminen — Business Continuity Plan, Recovery Plan


Valmet
FORWARD