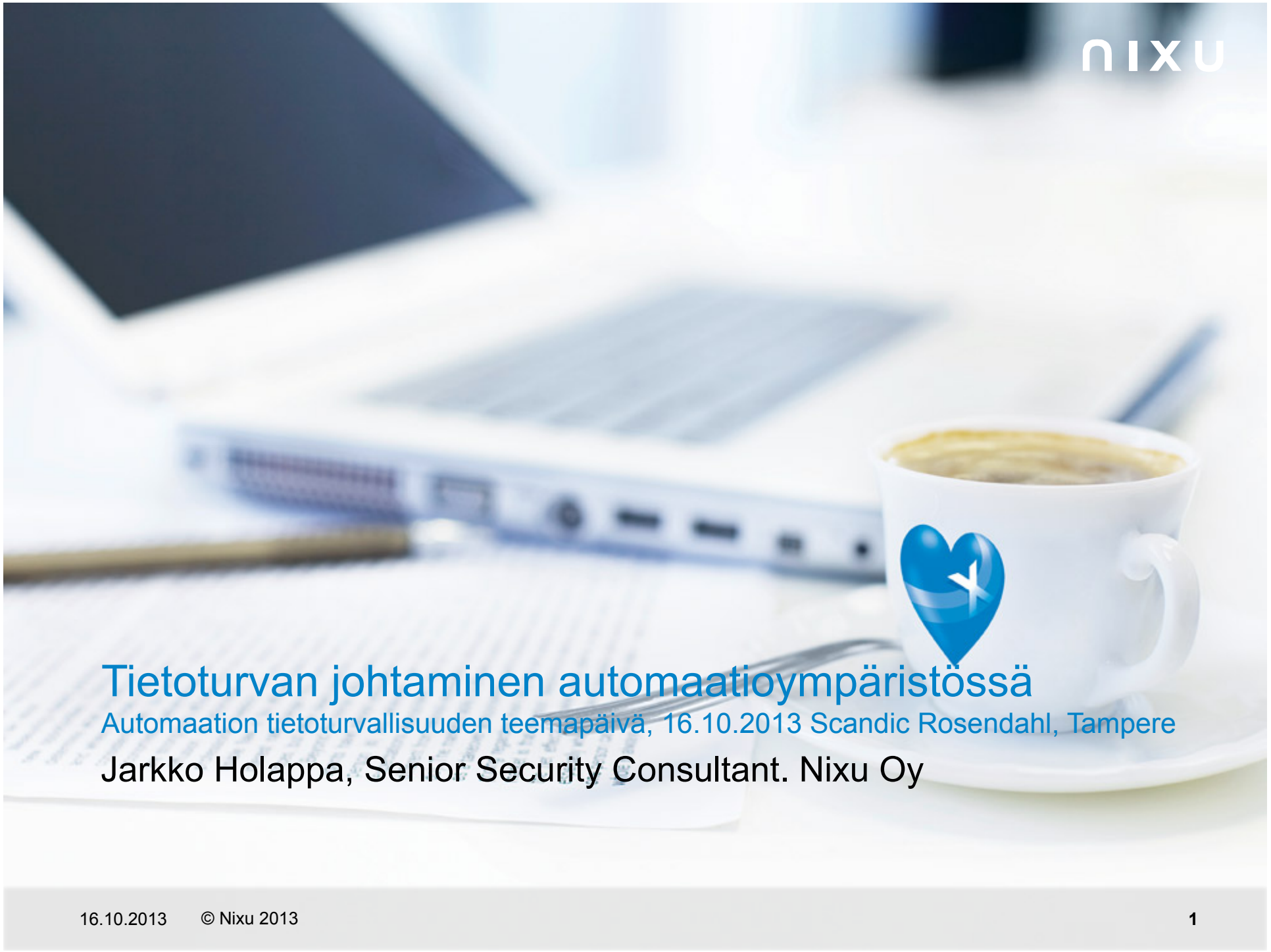
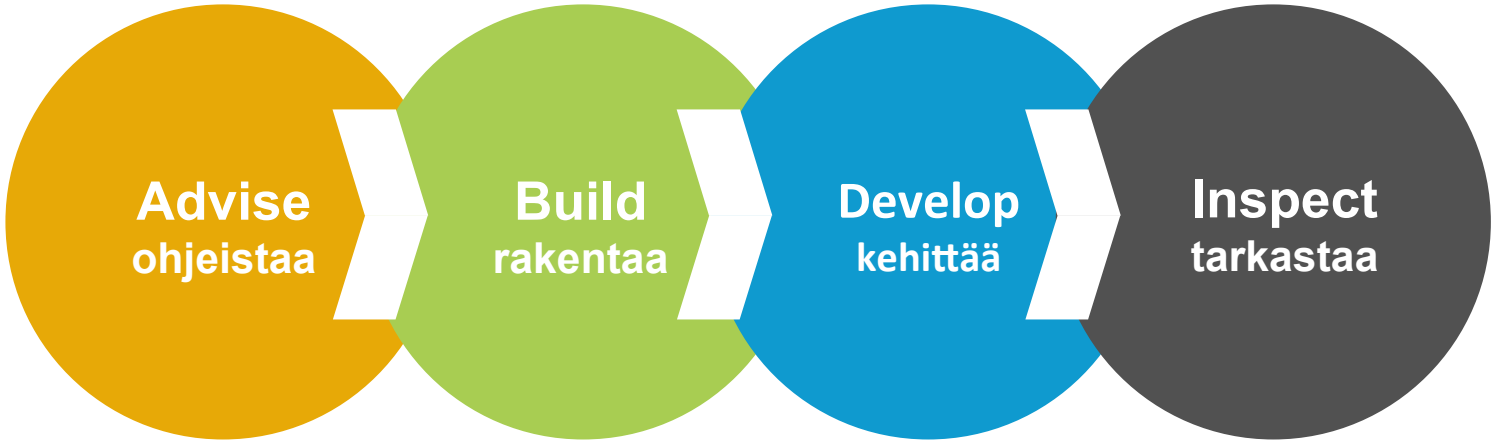


Tietoturvan johtaminen automaatioympäristössä

Automaation tietoturvallisuuden teemapäivä, 16.10.2013 Scandic Rosendahl, Tampere

Jarkko Holappa, Senior Security Consultant. Nixu Oy

Nixu - Palvelualueemme



- Tietoturvastrategia
- Riskienhallinta
- Jatkuvuussuunnittelu
- Tietoturvapolitiikat ja ohjeistot
- Tietoturvakulttuurin luonti ja jalkautus
- Vaatimustenmukaisuus

- Identiteetinhallinnan konsultointi ja toteutus
- Pääsynhallinta (SSO)
- Tilannekuva (GRC&SIEM)
- Lokienhallinta
- Sisällön suojaaminen
- PKI kehitys
- Turva-arkkitehtuuri

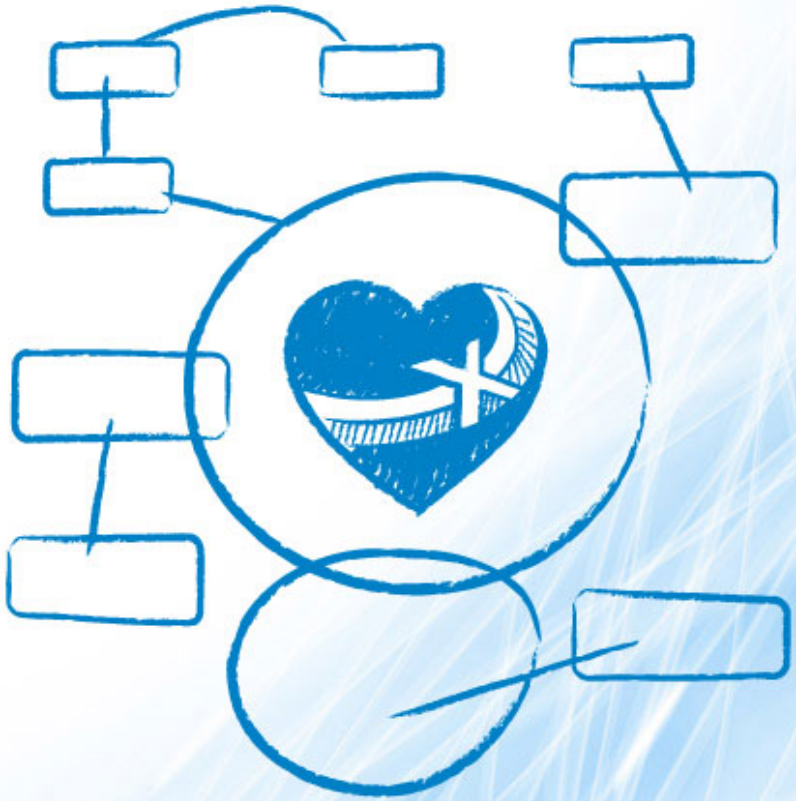
- Turvakriittinen ohjelmistokehitys
- Linux/embedded ohjelmistokehitys
- Secure Software Development Life Cycle
- Teollisuus-automaation tietoturva

- Tietoturva-arvioinnit
- Web-sovellusten murtotestaus
- Verkon penetraatiotestaus
- PCI DSS auditoinnit
- Forensiikka ja tietoturvaloukkausten hallinta
- Haavoittuvuuksien-hallinta

Agenda

- Automaatiojärjestelmien tietoturvallisuuden erityispiirteitä
- Tietoturvan johtaminen automaatiojärjestelmissä
- Toimittajahallinta elinkaaren eri vaiheissa

Automaatiojärjestelmien tietoturvallisuuden erityispiirteitä



Automaatiojärjestelmien tietoturvan nykytila

- Digitalisaatio ja verkottuminen
- Safety-kulttuuri vahva, tietoturva vasta heräämässä
- Ympäristöt eivät ole staattisia, tarvitaan päivityksiä ja muutosten hallintaa
- Suorituskykyvaatimukset voivat poissulkea salauksen ja autentikoinnin käyttämisen
- Hyökkääjän näkökulmasta ero perinteiseen IT-maailmaan ei ole suuri:
  - Järjestelmässä on Windows-pohjaisia tiedosto- ja tulostinpalvelimia. Reitittimet ja palomuurit perus IT-tuotteita
  - Ero: päivitysten hallinta ja tietoturvallinen konfigurointi lapsenkengissä
- Suurin osa ICS-järjestelmistä löydetyistä haavoittuvuuksista on IT-tietoturva-ammattilaisten löytämiä – ilman mitään automaatiotaustaa (Läh. ICS-CERT, Department of Homeland Security)
- Stuxnet todisti, että ilmarako verkkojen välissä ei riitä turvaamaan ympäristöä.

Uhkat

- Mobiilijärjestelmät
  - Tuotantokatkosten hallinta
  - Kunnossapito
  - Työmääräykset
  - BYOD

- Langattomuuden suosion kasvu (kustannuskysymys)
- Nollapäivä-haittaohjelmien lisääntyminen (antivirus-ratkaisut eivät toimi)

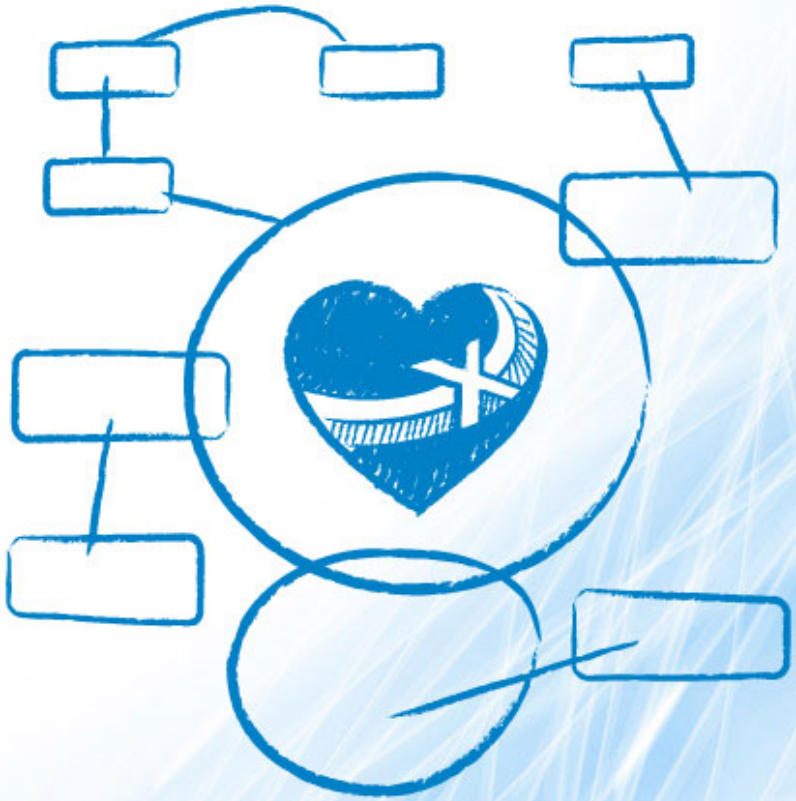
Automaatioverkon tietoturva vs. Perinteinen tietoturva

- Ohjausjärjestelmässä mielenkiinto on *kestävyydessä* (robustness) ja toiminnan varmistamisessa, ei tietoturvallisuudessa
  - Mutta: Jos järjestelmä on tietoturvaton, se ei ole kestävä eikä toimintavarmuudesta ole takeita
- Haavoittuvuuksia ei voida käyttää hyökkäysten ennakoimiseen
  - Tietoturvattomuus ja kykenemättömyys selvitä prosessissa tapahtuvasta vaihtelusta ovat järjestelmän ominaisuuksia
  - Järjestelmässä tapahtuu asioita, joita ei ole suunniteltu
- Automaatio-insinööri ei puhu luottamuksellisuudesta, eheydestä, saatavuudesta, riskien todennäköisyyksistä,…
  - Tavoite on saada prosessi toimimaan ilman tuotantokatkoja

Tyypillisiä havaintoja automaatioympäristöistä

- Toimittajien (vendor) oletus käyttäjätunnukset ja salasanat käytössä (osassa järjestelmiä ei mahdollisuutta edes vaihtaa)
- Jaettuja salasanoja
- Käyttämättömiä ohjelmistoja ja palveluita järjestelmissä
- Ei lokienhallintaa
- Tyypillisiä IT-tietoturvakontrolleja ei käytössä (palomuurit, IDS,..), tai niitä ei voida käyttää
- ICS järjestelmien riippuvuus muista yritysverkon palveluista (DNS,..)
- Suoria VPN yhteyksiä
- Ei turvallisuussopimuksia toimijoiden välillä
- Ei tietoturvavaatimuksia toimittajille
- Päivitysten hallinta olematonta
- Ei kokonaiskuvaa ympäristöstä (laitteet, ohjelmistoversiot, kunnossapidon ohjelmistot, yhteydet)

Tietoturvan hallinta automaatioympäristössä



Tietoturvan hallinta

•Tavoitteet
•Resurssit
•Riskien hallinta

•Riskienhallinta – kontrollit
•Osaaminen, koulutus
•Dokumentaation ylläpito

•Raportointi
•Auditointi
•Mittaaminen

•Toiminnan kehittäminen mittarien ja auditointien ohjaamana

Tietoturvan hallinta automaatioympäristössä

- Hankintakäytännöt
  - Kaikki oleellinen tulee olla dokumentoituna
  - Tietoturvavaatimukset sopimuksissa
  - Toimittajien auditointi ja hallinta
- Jäljitettävät muutoksen- ja konfiguraationhallintakäytännöt
- Politiikat ja toimintakäytännöt
  - Roolit ja vastuut määriteltävä
  - Auditoitava
  - Dokumentoitava ja ylläpidettävä
- Tilannekuva
  - Prosessit
  - Järjestelmän toiminta, lokit
  - Vaatimustenmukaisuus
  - Seuranta

Tietoturvan hallinta automaatioympäristössä: dokumentoinnin merkitys

- Dokumentaatio ja politiikat ovat perusta järjestelmän tietoturvaamisessa (ja robustisuuden parantamisessa)
- Jos järjestelmän toimintaa ei ymmärretä, se ei voi olla tietoturvallinen
- Kaikki laitteistot ja ohjelmistot on tunnistettava ja dokumentoitava
- Verkot ja tietovuot on dokumentoitava
- Dokumentaatiota on ylläpidettävä

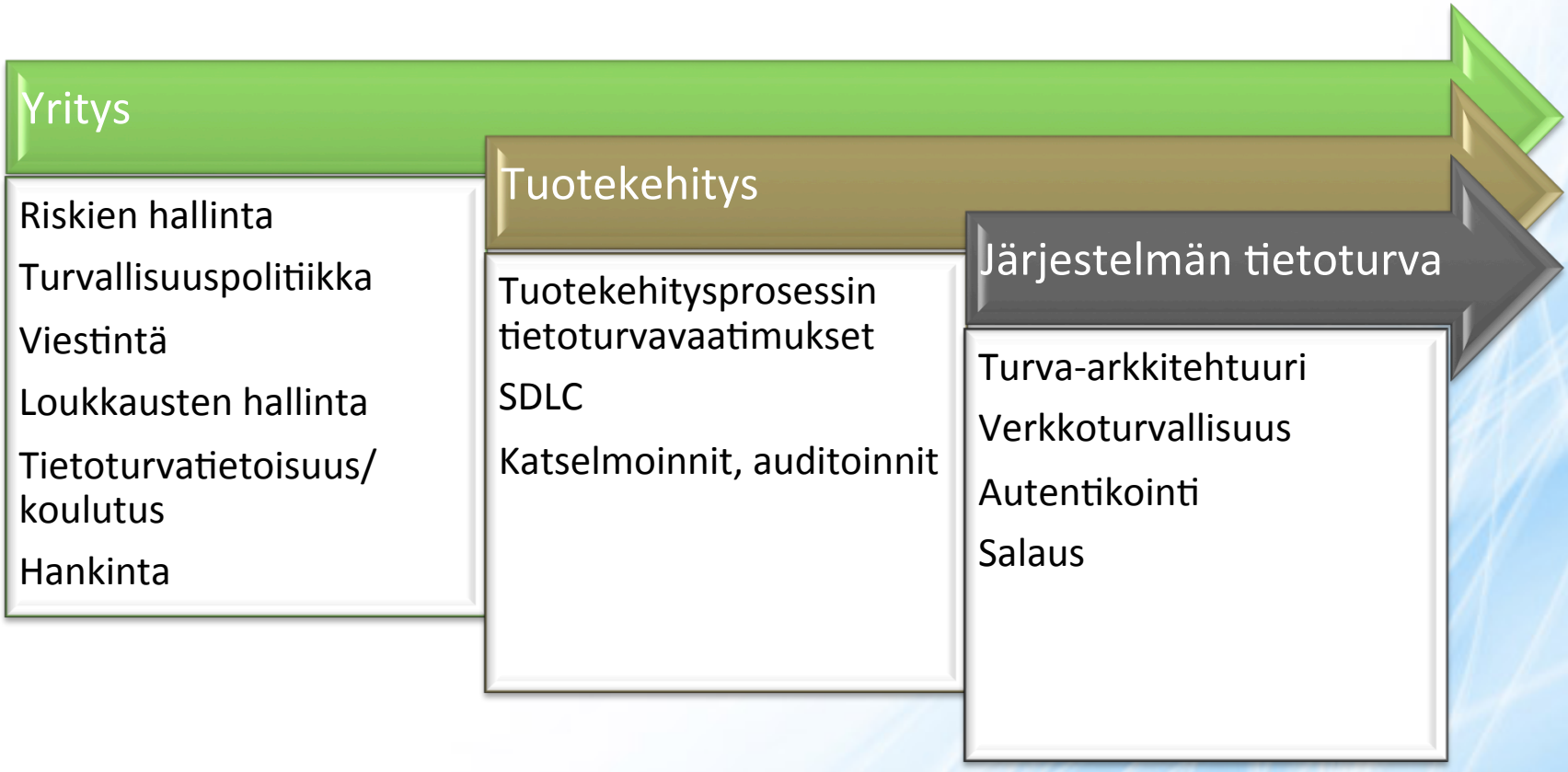
Toimiva tietoturvallisuuden hallinta on…

- Jatkuvaa
- Mitattavissa olevaa
- Huomioi hankinnan
- Johdon tukemaa

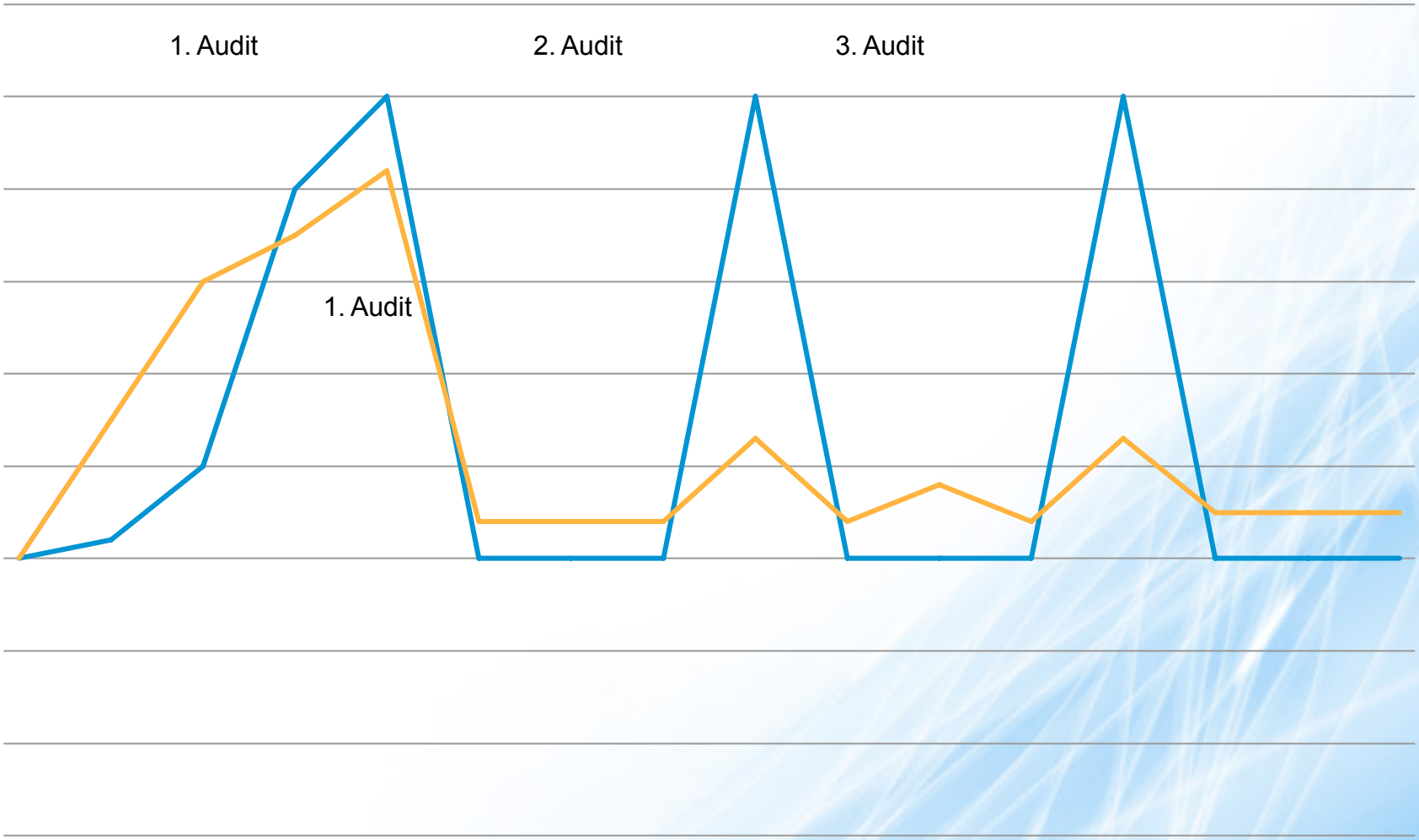
Tietoturvanhallintajärjestelmän kehittäminen ja ylläpito

- Johdon sitoutuminen yrityksen laajuisella ohjelmalla
- Tuotantoautomaatioympäristön liittäminen osaksi yrityksen tietoturvakäytäntöjä
  - ICS-spesifisiä standardeja ja toimialakohtaisia vaatimuksia yrityksen olemassa olevien kontrollien ja politiikkojen lisäksi
  - Erityisvaatimukset hankinnoille

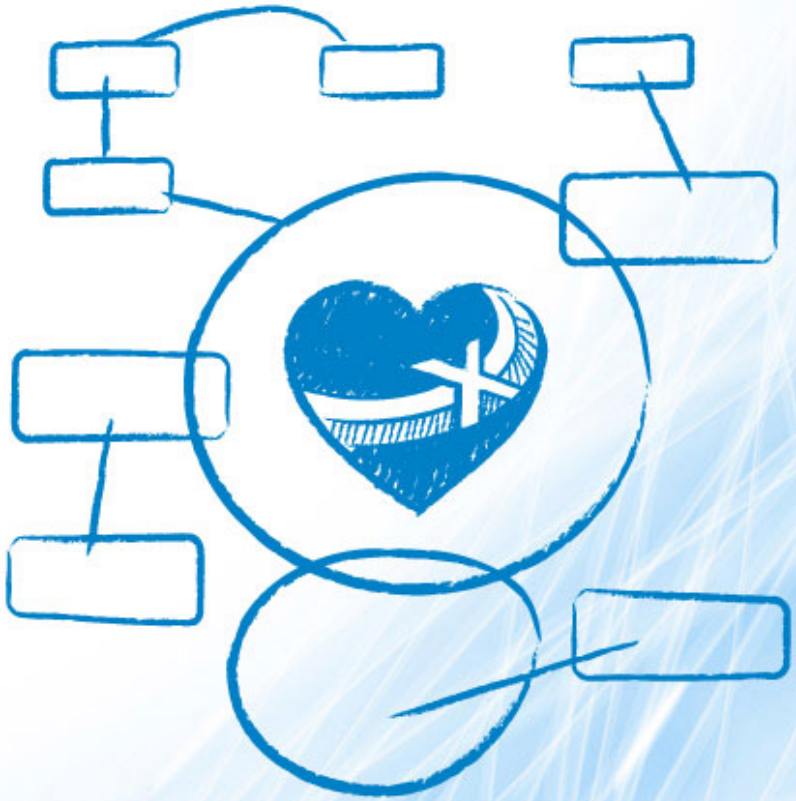
Yrityksen tietoturvallisuuden hallinta on kokonaisuus



Tehokkuus: Jatkuva parantaminen vs projektit



Toimittajanhallinta elinkaaren eri vaiheissa



Vaatimukset hankinnan kohteen mukaan

Lähde: VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje

Suunnitteluvaihe

- Tehtäviä:
  - Projektin laajuuden määrittely
  - Roolien ja vastuiden määrittely
  - Riskien tunnistaminen ja arviointi
  - Tietoturvavaatimusten määrittely ja dokumentointi (mm. riskiarvion pohjalta)
  - Tietoturvatestauksen suunnittelu
- Toimittajahallinta
  - Sopimukset:
    - Vastuut eri vaiheissa
    - Vaatimuksenmukaisuus
  - Katselmoinnit

Toteutusvaihe

- Tehtäviä
  - Kehittäjien kouluttaminen (turvalliset ohjelmointikäytännöt, tietoturvaohjeistus, politiikat)
  - Katselmoinnit
  - Turvakontrollien toteuttaminen:
    - Pääsynhallinta
    - Liikenteensuodatus
    - Haittaohjelmasuojaus
    - …
  - Tietoturvatestaus

- Toimittajahallinta:
  - Toteutusvaiheen tietoturvasta raportointi
  - Auditointioikeus sekä järjestelmään että kehitysprosessiin ja –ympäristöön
  - Hyväksymiskäytännöt

Ylläpitovaihe

- Tehtäviä:
  - Tietoturvan seuranta
    - Lokienhallinta
    - Tilannekuva
  - Muutosten hallinta
  - Tietoturvapäivitykset
  - Tietoturvaloukkausten hallinta
  - Säännölliset tarkastukset, auditoinnit
  - Jatkuva riskien hallinta

- Toimittajahallinta:
  - Raportointikäytännöt
  - Auditoinnit
  - Huollon tietoturvalliset työskentelytavat
  - Pääsyoikeuksien hallinta

Käytöstäpoisto

- Tehtävät:
  - Järjestelmien ja tietoaineiston turvallinen käytöstäpoisto ja hävittäminen

- Toimittajahallinta
  - Toimittajan hallussa olevan tietoaineiston palauttaminen/tuhoaminen
  - Käyttö- ja kulkuoikeuksien poisto

Tietoturvavaatimuksia toimittajalle

- Riittävä dokumentaatio
  - Laitteet, ohjelmisto, verkot → Kokonaiskuva ympäristöstä
- Konfiguraation hallinta
  - Järjestelmän kovennus
  - Versionhallinta
- Testauskäytännöt
  - FAT, SAT
  - Haavoittuvuusskannaukset
- Pääsynhallinta
  - Salasanat, käyttöoikeudet, käyttöoikeuksien hallinta
- Toimittajan tietoturvakäytännöt
  - Turvallinen järjestelmäkehitysprosessi (auditoinnit, katselmoinnit, testaus)
  - Laadunhallinta
  - Tietoaineiston käsittely
  - Tietoturvaloukkausten hallinta ja kommunikointi

Oikeat tietoturvan arviointimenetelmät oikeaan paikkaan

Kohde	Tarkastuksen luonne	Esimerkkejä suoritettavista arvioinneista
Automaatiojärjestelmä	Laaja tarkastus, riskilähtöinen	✓Riskianalyysi ✓Arkkitehtuurin katselmointi ✓Tietoturvan hallinnan prosessien arviointi ✓Sovellustason tarkastus ✓Alustatarkastus
Sovellus (black box)	Sovellustason tarkastus: toiminnallisuus	✓Haavoittuvuusskannaus ✓Manuaaliset testausmenetelmät ✓Hyväksikäyttömenetelmien kehittäminen
Sovellus (white box)	Sovellustason tarkastus: laatu, vaatimuksenmukaisuus	✓Arkkitehtuurin katselmointi ✓Lähdekoodin analysointi
Verkko		✓Verkon haavoittuvuuksien arviointi
Alustat		✓Palvelimen tai työaseman käyttöjärjestelmätason konfiguraation arviointi.

Yhteenveto

- Automaatioympäristön tietoturvatyön on oltava jatkuvaa ja johtamisen perustuttava määriteltyihin (ja dokumentoituihin!) käytäntöihin ja sen on oltava linjassa koko yrityksen tietoturvanhallinnan periaatteiden kanssa (liiketoimintariskit, jatkuvuus).
- Tietoturvallisuus on tuotava automaatioympäristöön toimintavarmuutta ja prosessin ennustettavuutta parantavana tekijänä.
- Toimittajahallinta ulotettava läpi elinkaaren ja valvottava toteutumista.

Kiitos!

Jarkko.Holappa@nixu.com, mobile +358 40 766 3203

Nixu Oy

www.nixu.fi/blogi - www.tietovastuu.fi - twitter: @nixutigerteam

P.O. Box 39 (Keilaranta 15), FI-02150 Espoo, Finland

Tel +358 9 478 1011, Fax +358 9 478 1030, nixu.sales@nixu.com

