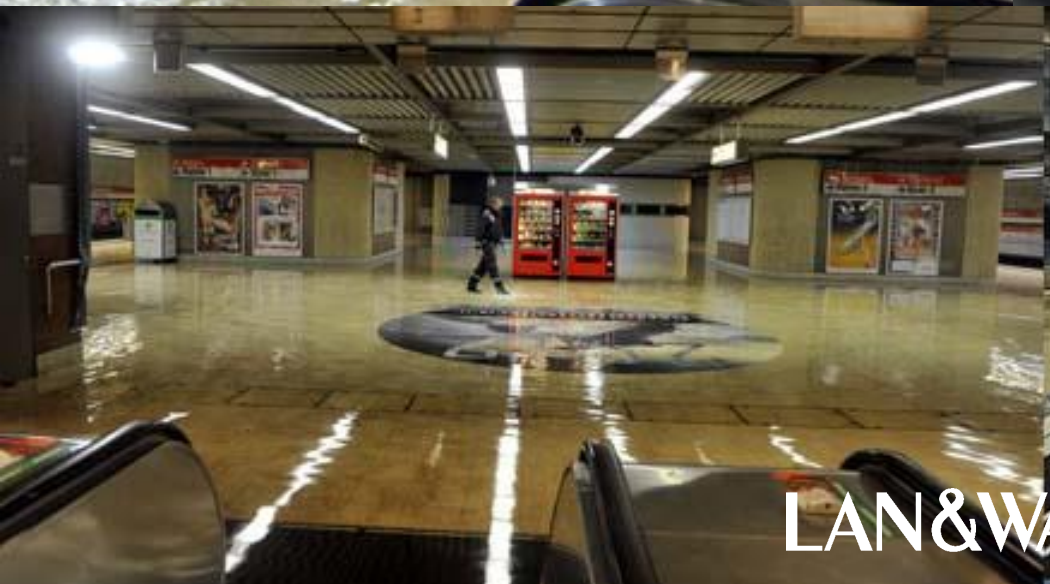
VALVO JA VARAUDU PAHIMPAAN

Erkki Sivonen
Senior Account Manager
Nordic LAN&WAN Communication
erkki.sivonen@lanwan.fi

LAN&WAN


HS613
HS613




KOE LOPUN ALKU

27 February 2014 Last updated at 00:26 GMT

Share

Energy firm cyber-defence is 'too weak', insurers say

By Mark Ward
Technology correspondent, BBC News

1.10.2013 UUSI SÄHKÖMARKKINALAKI

YLEISET

JATKUVUUDENHALLINNA KYSYMYKSET 1-7

1. Johtaminen
2. Toimintasuunnitelmat
3. Henkilöstö
4. Resurssit ja kumppanit
5. Prosessit
6. Mittarit

7. Kyberturvallisuus

UUSI SÄHKÖMARKKINALAKI: KYSYMYKSET 5.10.-5.17

1. Yhtiön varautumissuunnittelun perustiedot
2. Häiriötilanteiden hallinnan vastuut ja järjestelyt
3. Kriittisiin häiriötilanteisiin ja poikkeusoloihin varautuminen
4. Teknisten resurssien ja järjestelmien käytettävyyden varmistaminen
5. Palvelutuottajien käytettävyyden varmistaminen
6. Toiminta häiriötilanteissa
7. Alueellinen yhteistyö häiriötilanteissa
8. Yhtiön varautumisen mittarit

Sähkömarkkinalain velvoitteet varautumiselle

- **Verkkojen toimitusvarmuuden tason nostaminen (SML 19§)**
- **Verkonhaltijan varautumisvelvoite (SML 28§)**
- **Verkonhaltijan yhteistyövelvoite (SML 29§)**
  - Häiriötilannekuvan kokoaminen
- **Jakeluverkon asiakkaiden varautumisen ohjaaminen (SML 58§)**
  - Ohjeistus viranomaisille ja yrityksille
  - Ohjeistus kansalaisille
- **Häiriötilannekuvan välittäminen (SML 59§)**

Standardeja

- Teknologiastandardit
- ISO 27001
- Säädökset
- Tietosuojalainsäädäntö (EU, kansallinen)
- PCI-DSS
- Payment Card Industry Security Standards Council
- HIPAA (US)
- The Health Insurance Portability and Accountability Act of 1996 USA
- FedRamp (US)

BS 7799 (ISO 17799)

British Standard 7799: Code of Practice for Information Security, josta on julkaistu myös ISO-standardi 17799.BS 7799 on Iso-Britannian standardointi-instituutin julkaisema suositus organisaation tietoturvallisuuden hallintajärjestelmäksi.


TIEDON PIRSTALOITUMINEN
LAN&WAN

VARAUTUMISEN JA VALVONNAN POSITIO

LAN&WAN

Kokonaisvaltainen valvonta

- IT-infra
- Tuotanto-järjestelmät
- Kiinteistö-järjestelmät
- Tietoturva

NÄIN SE RAKENTUU
CASE: FINNAIR

KÄYTTÄJÄ

LAITE

YHTEYS

- Internet
- Lähiverkko
- Langattomat yhteydet
- Operaattoriyhteydet

SUOJAUS

- Käyttäjän tunnistaminen
- Laitteiden suojaus ja hallinta
- Yhteyden suojaus ja hallinta
- Tiedon ja palvelun eheys ja suojaus

SEURANTA

- Palvelun käytettävyys
- Trendin seuranta
- Valvontatieto
- Analyysi
- parannusehdotukset

PALVELU (sovellus, portaali, ohjelmisto)

TIETO, METADATA, BIG DATA, ”ARVOPÄÄOMA”

TIETOTURVAUHKA VOI OLLA LÄHEMPÄNÄ KUIN USKOTKAAN

Joka päivä uusia uhkia

Kyberturvallisuu
julkaissut varoit
sisällönhallintajä
haavoittuvuudes

21.11.2014 klo 08:28

**Wordpress on suosittu www-julk
ohjelmisto. Sitä käytetään yleise
Ohjelmistosta on löydetty vakav
päivitystarpeista on Kyberturvall**

Julkaisujen sisällönhallintaan tarkoite
vakava haavoittuvuus. Haavoittuvu
lukemisen, m

Viestintäviras
suositellaan
välittömästi.

Julkaistu: 3.12.2014 11:45

Suosittele Jaa 152

TIETOTURVA **F-Secure
salasanoista, lapsen ti**

F-Securen tutkimusjohtaja
Reddit-verkkosivustolla av
Kyselijät esittivät kysymyk

Tietoturvagurua tentattiin
chatista kiinnostavimmat

K: Mitä ihmiset tekevät ti
tietoturvasyistä tehdä?

MH: Käyttävät Internet E

K: Mikä on analysoimistasi
monimutkaisin ja miksi?

MH: Stuxnet. Regin. Rutla
Heillä on paljon rikollisia pa

Mediuutiset

ETUSIVU KESKUSTELUT TYÖPAIKAT » TAPAHTUMAT YHTEYSTIEDOT

Viikon uutiset | **Uutisarkisto** | Kirjat | Rytmihäiriö | Sairaalavierailut | Sa

Hyvä juttu | Lähetä | Tulosta | A | A

TIETOTURVA Erpo Pakkala, 11.3.2015, 15:03

Virus livahti potilastietojärjestelmään - Varsinais-Suomen sairaanhoitopiiri kielsi Facebookin käytön

Varsinais-Suomen sairaanhoitopiiri havaitsi tietoverkossaan tietokoneviruksen viime perjantaina ja tämän viikon maanantaina. Virus pääsi verkkoon kummassakin tapauksessa yhden työaseman kautta.

Viruksen epäillään päätyneen työasemalle Facebook-sivuston ja Internet Explorer -selaimen kautta ja siksi Facebookin käyttö on varotoimenpiteenä toistaiseksi kielletty ja pääosin estettykin sairaanhoitopiirin tietoverkossa.

Työasemat paikallistettiin nopeasti ja otettiin pois käytöstä, mikä esti viruksen leviämisen muihin työasemiin. Virus ehti vahingoittaa potilastietojärjestelmän kutsukirjepohjia ja niiden liitteitä sekä yleisellä levyalueella noin 20 000–30 000 tiedostoa.

Viruksen takia potilaiden suunniteltuja kutsukirjeitä ei voitu lähettää useaan tuntiin perjantaina sekä vajaaseen tuntiin tiistaina. Kirjepohjia ja -liitteitä on voitu korjausten jälkeen taas käyttää normaalisti.

Virus oli tyypiltään niin sanottu Cryptolocker-haittaohjelma, jollaisia on parhaillaan liikkeellä paljon eri puolilla maailmaa. Aktivoitunut haittaohjelma salaa tiedostoja sekä saastuneen koneen paikallisilla levyasemilla että siihen kytkeytyneillä verkkolevyasemilla. Ohjelma vaatii kohteeltaan maksua salauksen purkuavainten toimittamisesta. Sairaanhoitopiiri ei maksuun suostunut.

Yleisellä levyalueella sijaitsevat vahingoittuneet tiedostot on korvattu varmuuskopioilla.

– Tällä kertaa selvittiin potilashoidon näkökulmasta vain kutsukirjeiden lähettämisen viivästymisellä, eivätkä potilastiedot olleet vaarassa, toteaa sairaanhoitopiirin tietohallintoylilääkäri **Pirkko Kortekangas** tiedotteessa.

ta löytyi tietokonevirus
o-laite on riski"

KIMMO TASKINEN HS

oittuvuus
elainistunnon

äyksen avulla

**löydetty haavoittuvuus mahdollistaa
sen purkamisen, jos hyökkääjä pääsee
aan uhrin ja palvelimen välistä**

lynnettävästä SSL 3.0 -salausprotokollasta on
hdollistaa salatun tietoliikenteen osittaisen
dle"-nimen saanut haavoittuvuus koskee
Erittäin harva selain tai verkkosivu hyödyntää
utta edelleen suurin osa tukee sitä taaksepäin
ksi.

uu siihen, että selainliikenne pakotetaan
otokollaa uudempien TLS-protokollien sijaan.
s. välimiesasemaa (Man-in-the-Middle), jossa
ja muokkaamaan uhrin ja palvelimen välistä
e saattaa syntyä esimerkiksi suojaamatonta
essä.

Tietoturvauhka isossa organisaatiossa

Joka **viides sekunti** havaitaan uusi tuntematon tietoturvauhka

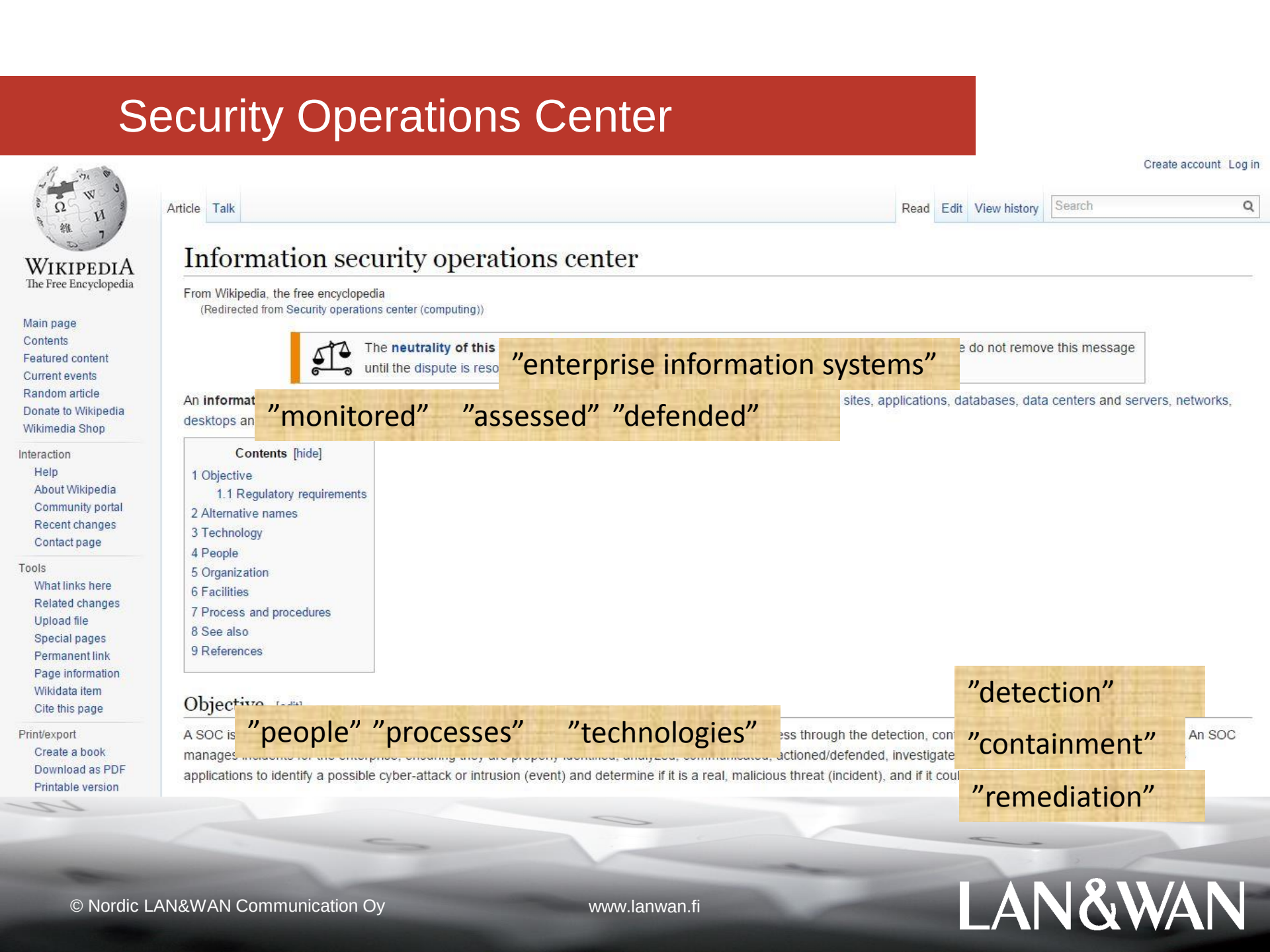
Joka **minuutti** joku käyttäjä selaa jotain haitallista sivustoa

Joka **27. minuutti** käyttäjä lataa tuntemattoman haittaohjelman omalle koneelleen

Tiedot perustuvat tietoturvayhtiöiden tekemiin tutkimuksiin vuosien 2012-2014 aikana.

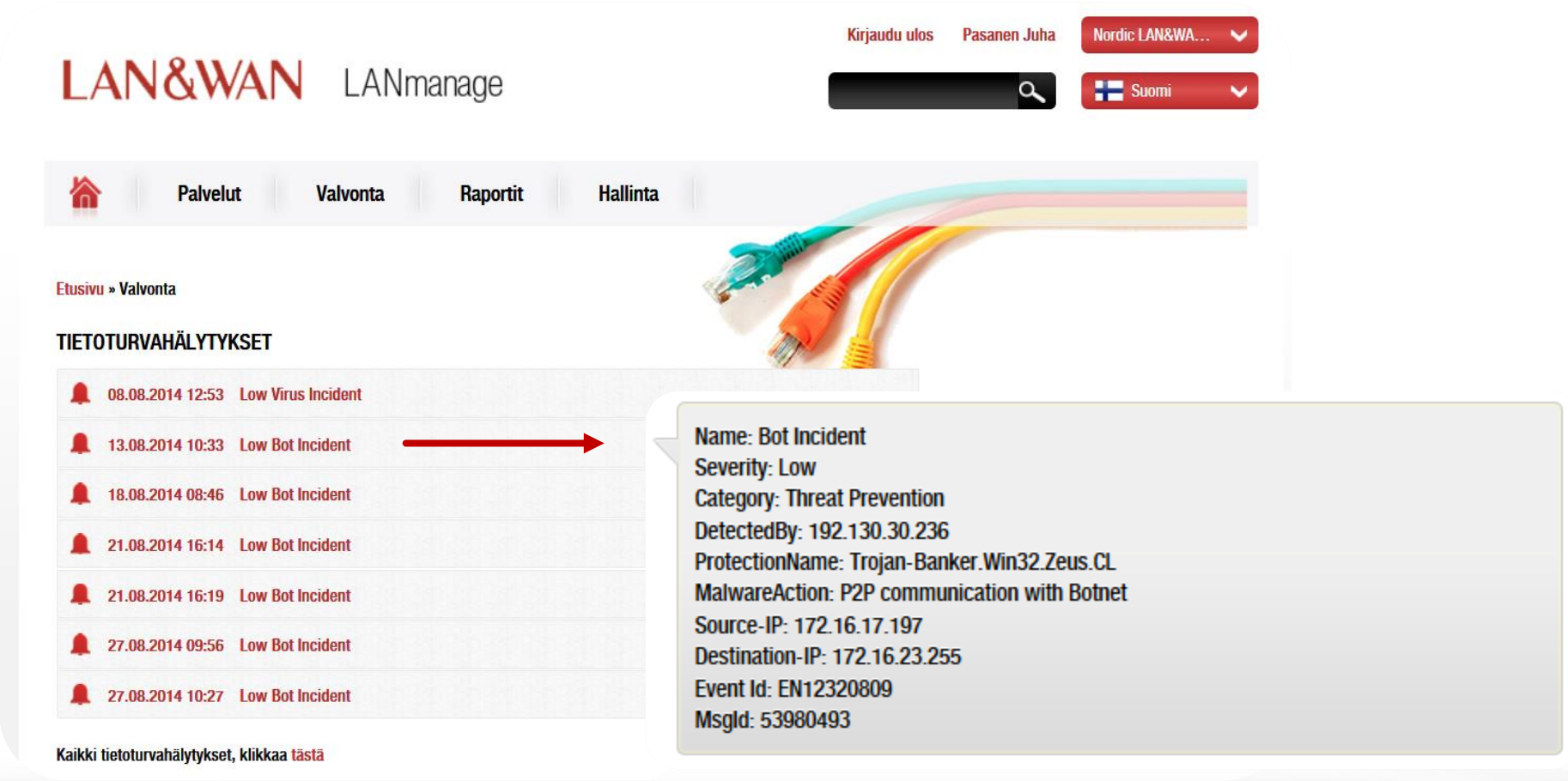
LAN&WAN

Security Operations Center



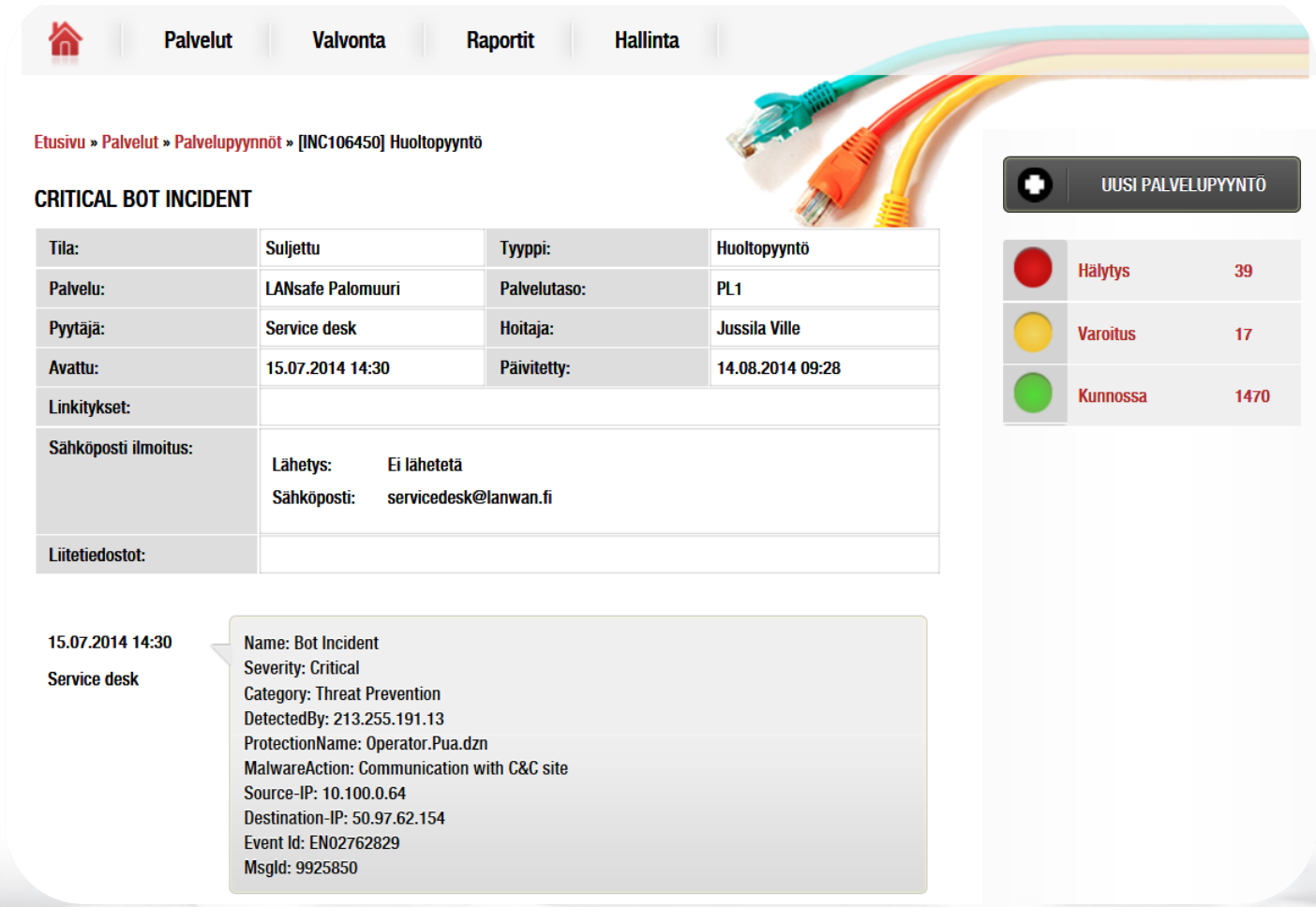
LAN&WAN

Havainnointi tuottaa tapahtumia ..



LAN&WAN

.. jotka käsitellään ennalta suunnitellun prosessin mukaan



Tietoturva ei ole välineurheilua

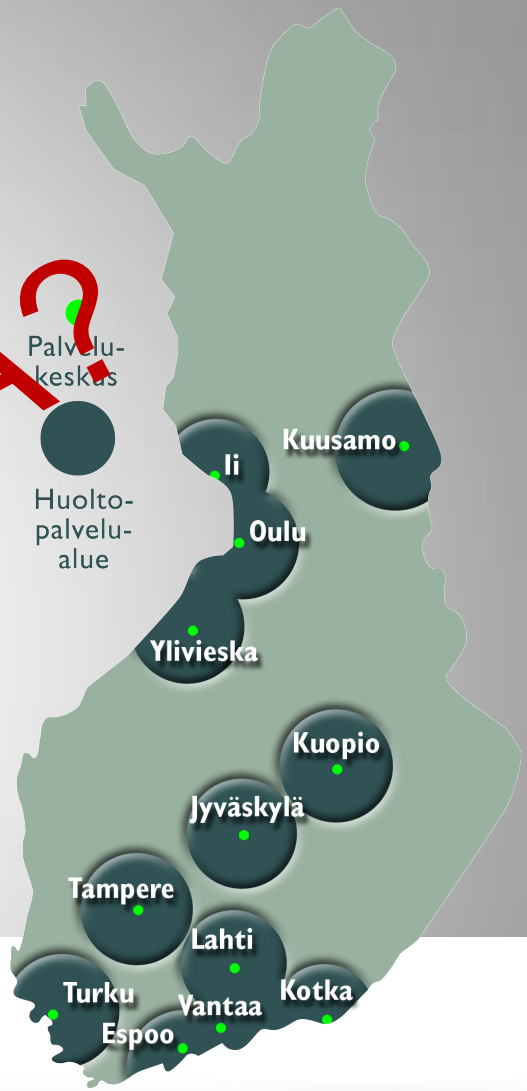
- 80 % tietoturvakustannuksista on työtä
- Tietoturvan toteuttamiseen tarvitaan laaja-alaista osaamista ja riittävää resursointia
- Palomuuripalvelu ei ole sama asia kun SOC
- SOC:ia ei voi korvata laitteilla

LAN&WAN

KIITOS

Nordic LAN&WAN Communication Oy
Erkki Sivonen & Kari Salmela
Senior Account Manager
erkki.sivonen@lanwan.fi

KYSYMYKSIÄ?



LAN&WAN