Pilve kaitsmas

Excellent Business Solutions AS Security Software OÜ

Sven Karuse ja Ronnie Jaanhold / 10.05.2017

Excellent Business Solutions Eesti AS

- HansaWorldi distribuutor Eestis
- Tegutseme alates 2002. a.
- 5 500 lepingulist klienti

HansaWorldi tooteseeria Eestis

Standard ERP by HansaWorld

Enterprise by HansaWorld

Books by HansaWorld

Standard Hansa by HansaWorld

HansaRaama by HansaWorld

HANSAWORLD SBE

Office/2

FIRSTOFFICE

excellent

security SOFTWARE

HANSAWORLD AUTHORISED DISTRIBUTOR

Pilveteenus

- Pilveteenus alates 2014
- 150+ virtuaalserverit
- 1 600+ ERP andmebaasi meie pilves
- 15 000 ettevõtte majandusandmed

SIEMi eesmärgid

- Serverite suur hulk ja planeeritav kasv
- Efektiivsus ja kvaliteet
- Vajadus vastata GDPR’ile.
- Ülevaade serverites toimuva osas
- Turvalisus

SIEMi eesmärgid

- Oluliseks indikaatoriks on Soovitusindeks (NPS)
- Liikuda reaktiivsest proaktiivseks
- Lisada klientidele teenuseid/võimalusi
- Mitte üle maksta teenusepakkujale serveriressursside kasutuse eest

Tarne

Lisaväärtused

SIEM = Faktid

Kummutab automaatselt:

- „Ma arvan, et see on nii“
- „Mul on kõvem hääl kui sul“
- Soovmõtlemise

Arhitektuuri põhikomponendid

Books by HansaWorld

Hansa

- Rakenduste logid
- Kasutajate aktiivsus
- Rakenduse seis ja töö
- Tervise indikaatorid
- Turvalisuse indikaatorid

OS

- Süsteemi tervis
- Autentimisinfo (audit)
- Muutused süsteemis
- Ründe tuvastus
- Platvormi tugevdamine
- Turvameetmete rakendamine

Võrk

- Flow data (liiklusseire)
- Haavatavuste skänneerimine
- Ründe tuvastus / reaktsioon
- Rakendusele juurdepääs

Väärtuspunktid

- Operatsioonitiimile (Pilvikud)
  - Operatiivinfo rakenduste hingeelu kohta
  - Operatiivinfo kasutajakogemuste kohta
  - Operatiivinfo koormuste kohta
  - Regulaarsed raportid kogu infrastruktuuris toimuvast
- Turvatiimile (Security Software)
  - Rünnakute tuvastamine erinevatel kihtidel
  - Ebareeglipärane kasutus (anomaaliad, ekstreemid)
  - Kehtestatud reeglite jälgimine (teine silmapaar, politsei)
  - Login data, audit data

Väärtuspunktid

- Ärile
  - Lisateenuste kujundamine, pakkumised
  - Ressursside parem planeerimine (optimeerimine)
  - Big-data pealt konkreetsete pakkumiste tegemine kitsamatele gruppidele
- Reaktiivsest liikumine proaktiivseks
  - Klientide murede ennetamine (positiivne üllatamine)
  - Jooksvate probleemide lahendamine enne kliendi reaktsiooni
- Protsesside automatiseerimine
  - Väga erinevate infosüsteemide logide korrelleerimine ja SIEM'i kasutamine automatiseerimise ajuna
- Turvariskide maandamine + logide tõendusväärtus

excellent

security SOFTWARE

HANSAWORLD
AUTHORISED DISTRIBUTOR

Sven Karuse

Arendusjuht
sven@excellent.ee
tel (+372) 669 1111
info@excellent.ee
www.excellent.ee

Local ESM - ERC-ELM

Ebaõnnestunud Sisselogimised Hansade...

Previous Week

Distribution

7,143 (100%)

360 300 240 180 120 60 0

04/25/2017 04/26/2017 04/27/2017 04/28/2017 04/29/2017 04/30/2017 05/01/2017

04/24/2017 00:00:00 — 05/01/2017 00:00:00

Source Geolocation by Country

Bound to Distribution — 7,139 (100%)

Estonia	6,992
United St	34
Japan	33
Netherlan	12
Norway	11
Spain	9
Greece	9
Morocco	9
United Ki	8
Denmark	5
Sweden	5

Page 1

Source IPs

Bound to Source Geolocation... — 7,139 (100%)

368 213 188 103 96 93 74 62 62 60 57 55 54 52 52 51 49 49 49 47

Page 1

Hosts

Bound to Source IPs — 7,139 (100%)

628 272 261 253 248 191 180 178 169 163 147 141 140 130 126 123 121 119 115 112

Page 1

Company

Bound to Hosts — 7,139 (100%)

477 191 180 134 123 109 102 99 92 88 88 83 80 80 77 74 74 71 69 66

Page 1

Source User

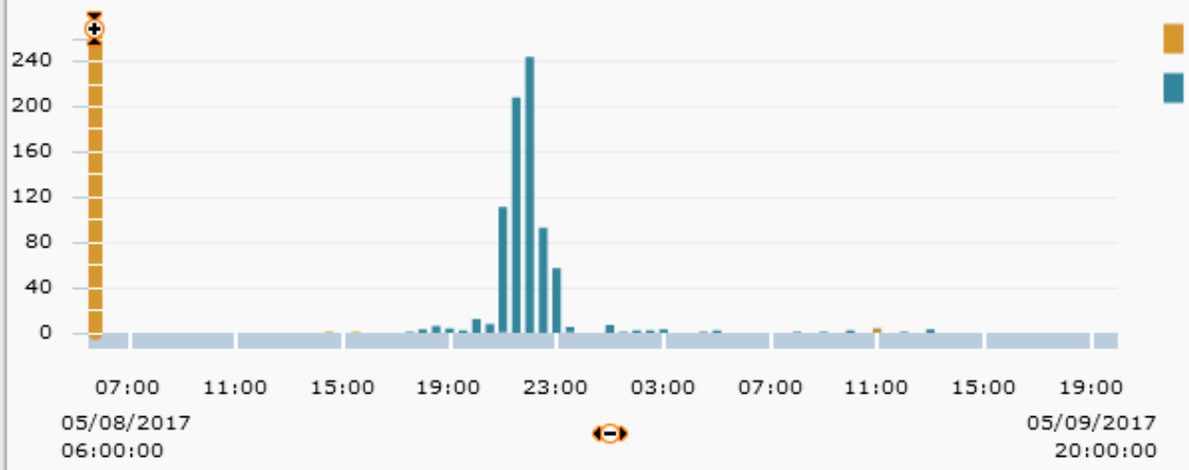
Bound to Company — 104 (1.46%)

104 74 67 60 53 50 50 48 46 45 45 44 44 43 42 42 40 40 34 33

Page 1

Distribution

786 (100%)

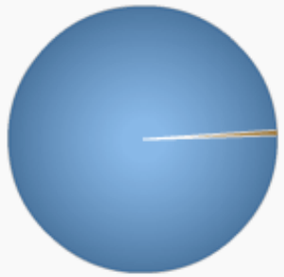


SS - Viimane tekstikoopia ebaõnnestus

SS - Tekstikoopia edukalt eksporditud

Signature IDs

Bound to Distribution 5 (0.64%)



49190-5000078	781
49190-5000067	5

Page 1

Events

Bound to Signature IDs

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
195	SS - Viimane tekstikoopia ebaõnnestus	3		::	n/a	05/09/2017 11:24:29	failure
65	SS - Viimane tekstikoopia ebaõnnestus	1		::	n/a	05/08/2017 15:35:42	failure
65	SS - Viimane tekstikoopia ebaõnnestus	1		::	n/a	05/08/2017 14:59:20	failure

Details | Advanced Details | Geolocation | Description | Notes | Custom Types | Packet | ELM Archive

Packet Format: Auto Auto get packet

Find text:

```
<158>May  8 14:59:20 books47 elukool: 2017-05-08 14:59:11 Viimane tekstikoopia ebaõnnestus
```

Page 1 All events

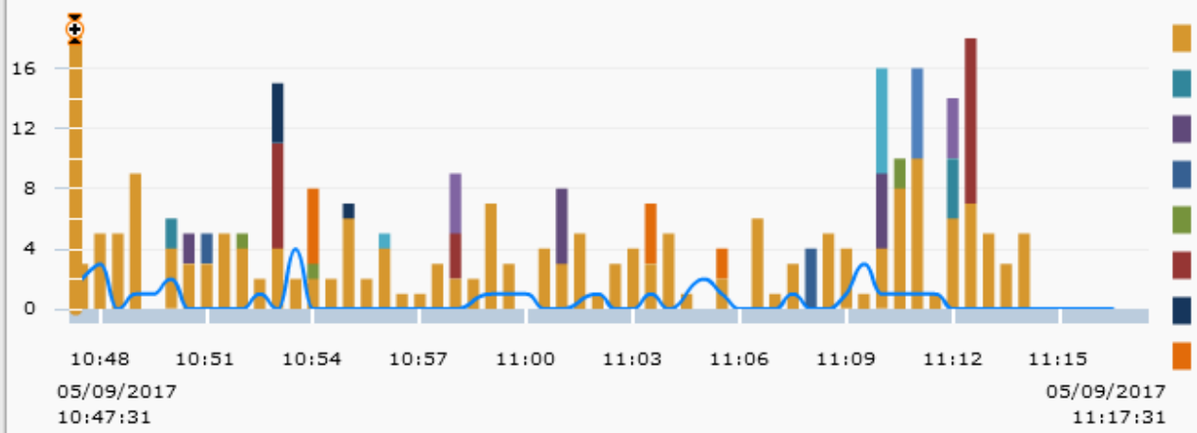
Local ESM - ERC-ELM

Õnnestunud Sisselogimised Hansadesse

Last 30 Minutes

Distribution

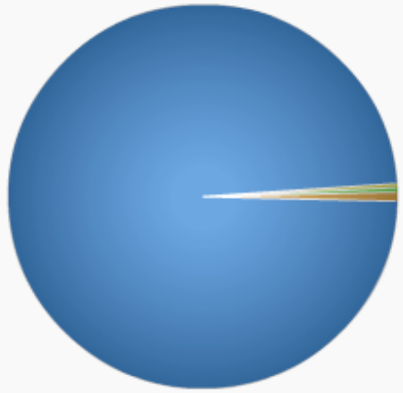
271 (100%)



Source Geolocation by Country

Bound to Distribution

271 (100%)



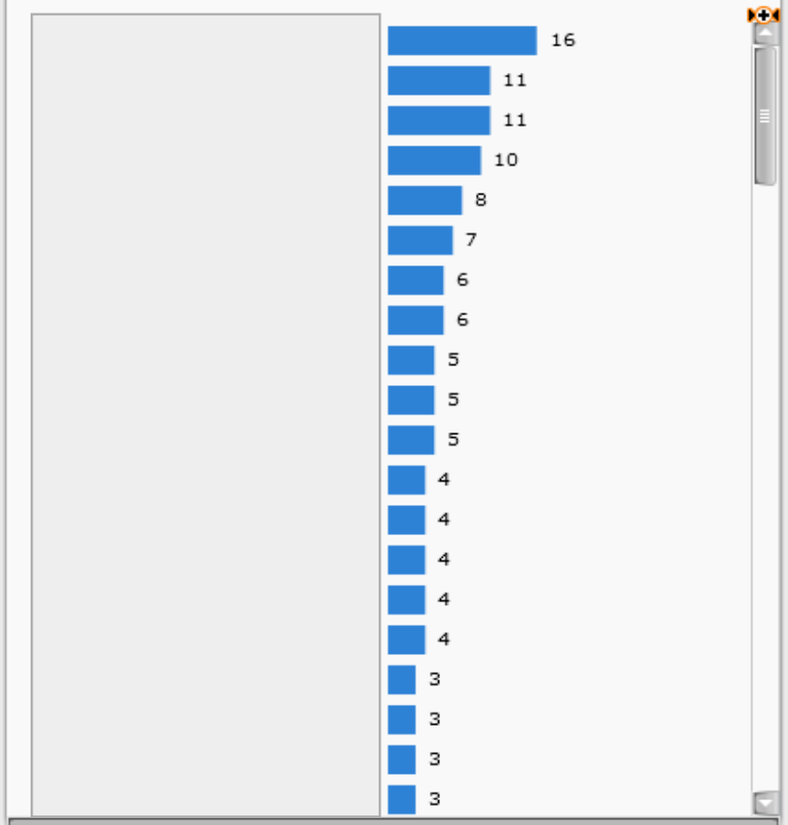
Estonia	267
Finland	2
Netherland	1
Sweden	1

Page 1

Source IPs

Bound to Source Geolocation by Country

271 (100%)

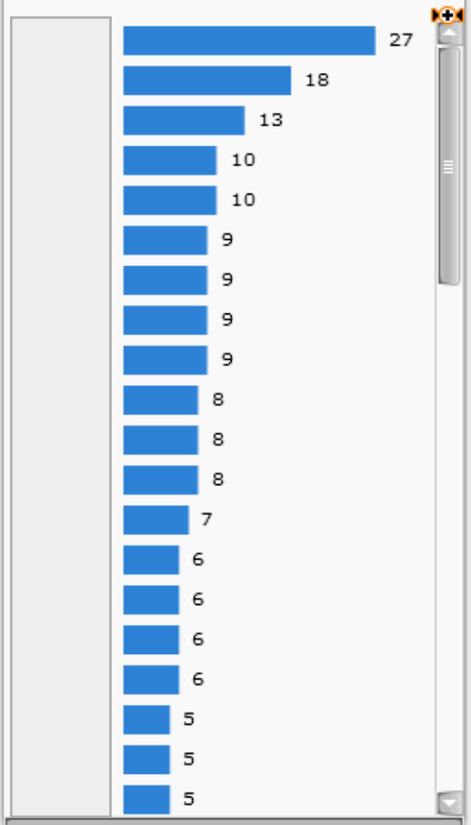


Page 1

Hosts

Bound to Source IPs

271 (100%)

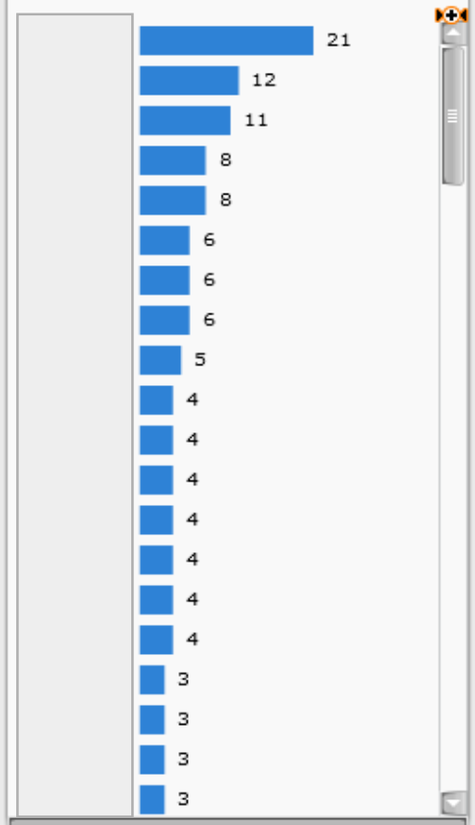


Page 1

Company

Bound to Hosts

271 (100%)

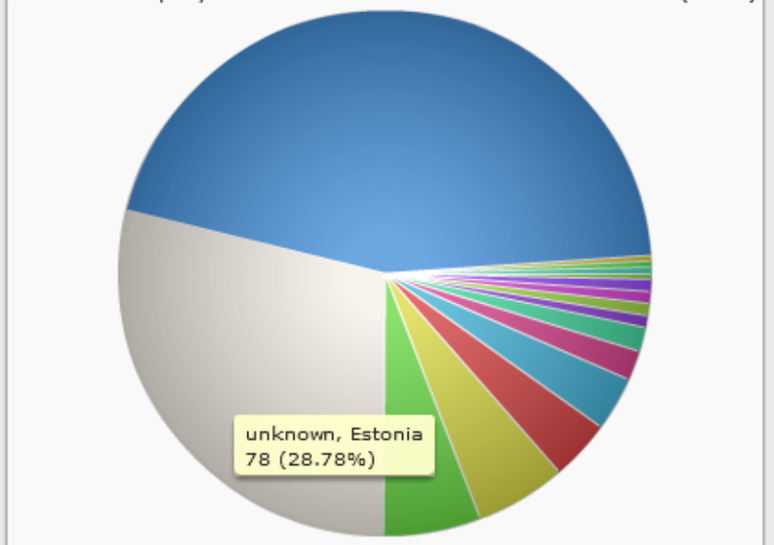


Page 1

Source Geolocation by City

Bound to Company

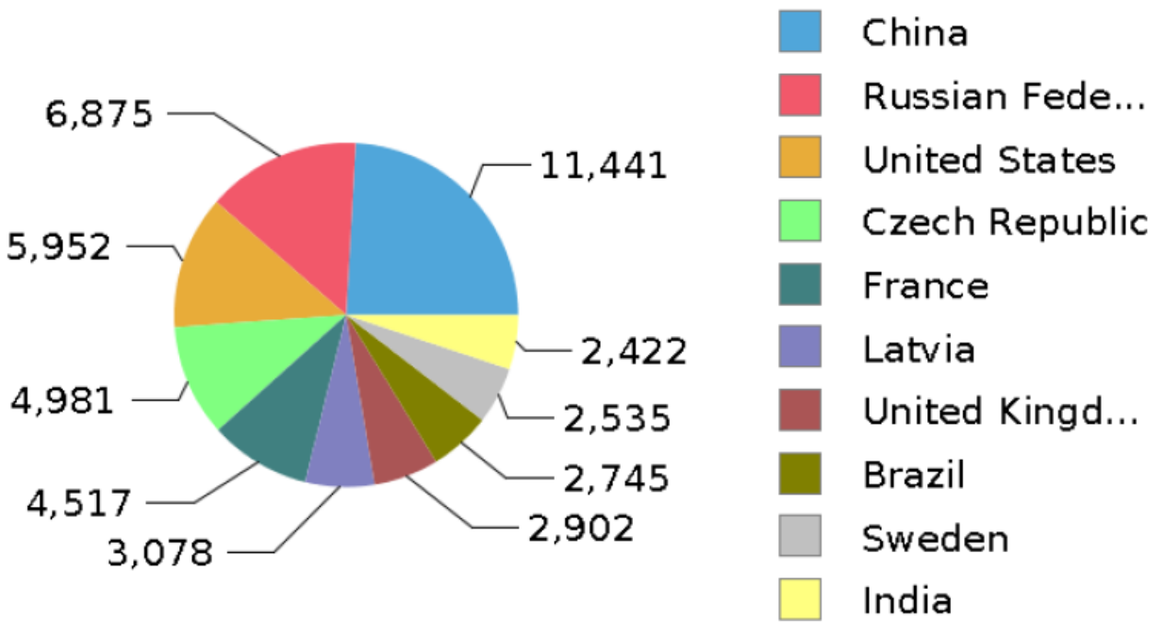
271 (100%)



Tallinn, Harjumaa, Estonia	122
unknown, Estonia	78
Viimsi, Harjumaa, Estonia	16
Tartu, Tartumaa, Estonia	15
Rakvere, Laane-Virumaa, Estonia	10
Ülenurme, Tartumaa, Estonia	9

Page 1

Source Geolocation by Country



Hosts