NETSOL
NETWORK SOLUTIONS

Hyökkäysten havainnoinnin tulevaisuus?

Intrusion Detection,Kontakti.net, 2.6.2004

Jari Pirhonen
Tietoturvallisuuskonsultti, CISSP, CISA
Netsol Solutions – www.netsol.fi
jari.pirhonen@netsol.fi - www.iki.fi/japi/

NETSOL
NETWORK SOLUTIONS

Tietojärjestelmän elinehdot

1. Hyökkäysten vastustuskyky
   - Ennakoivat tietoturvajärjestelyt, perinteiset tietoturvaratkaisut, arkkitehtuuri.
2. Hyökkäysten ja vahinkojen laajuuden tunnistaminen
   - Tietojärjestelmän normaalitilan ymmärtäminen, hyökkäysten havainnointi, rikkomusten havainnointi, poikkeamat normaalitilanteesta, järjestelmämuutokset.
3. Hyökkäyksistä toipuminen
   - Vahinkojen rajoittaminen, rajoitetun toiminnallisuuden takaaminen, normaalitilan palauttaminen.
4. Sopeutuminen ja evoluutio
   - Hyökkäysten vaikutusten pienentäminen jatkossa, tehokkaampi toipuminen

Lähde: CERT/CC

NETSOL
NETWORK SOLUTIONS

Herkkyys vs. tarkkuus

IDS reagointi \ Tunkeutuminen	+	-
+	True Positive (tunkeutuminen havaitaan)	False Positive (väärä hälytys)
-	False Negative (tunkeutumista ei huomata)	True Negative (toimivuus todetaan)

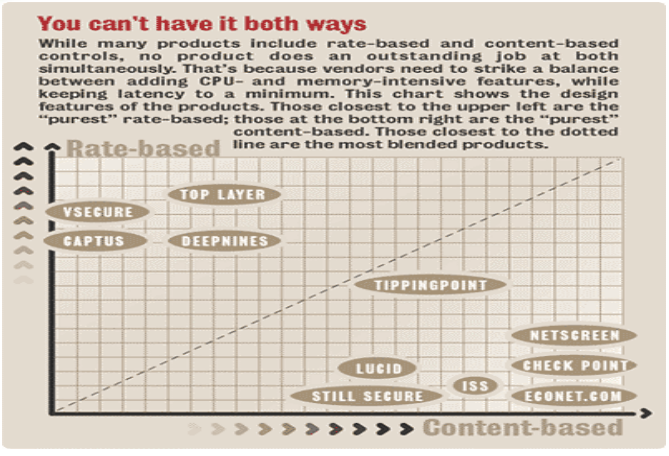
$$\text{Herkkyys} = \frac{TP}{TP + FN}$$

$$\text{Tarkkuus} = \frac{TN}{TN + FP}$$

$$\text{Virheettömyys} = \frac{TP + TN}{TP + TN + FP + FN}$$

NETSOL
NETWORK SOLUTIONS

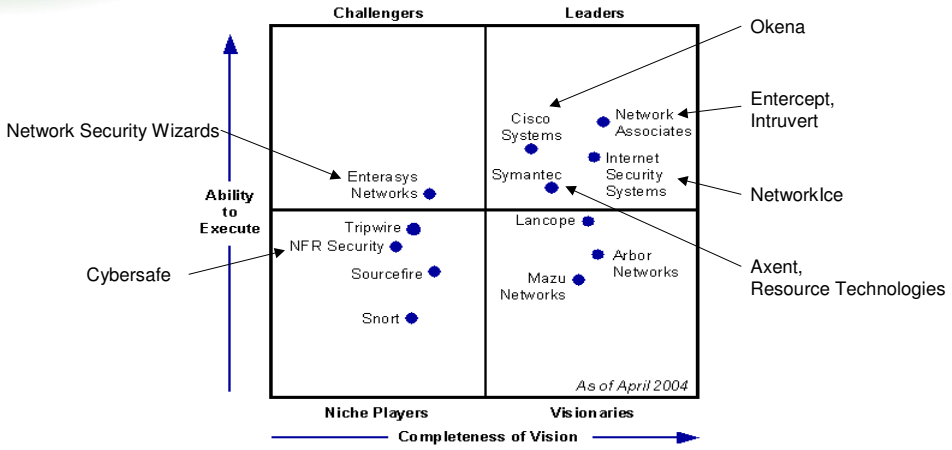
Rate- or Content-based IPS



Lähde: http://www.nwfusion.com/reviews/2004/0216ipsintro.html

NETSOL
NETWORK SOLUTIONS

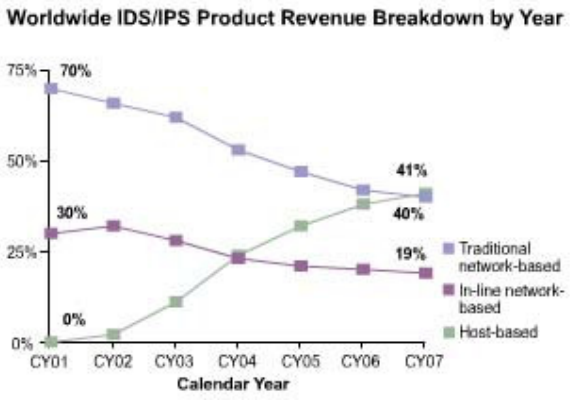
Snort vs. kaupalliset tuotteet



Lähde: Gartner Research (4/2004)

NETSOL
NETWORK SOLUTIONS

Network vs. host



Lähde: Infonetics Research 3/2004

NETSOL
NETWORK SOLUTIONS

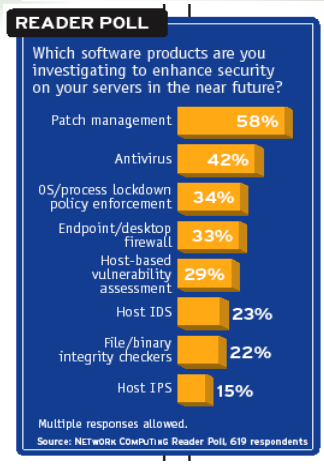
Yritysten prioriteetit

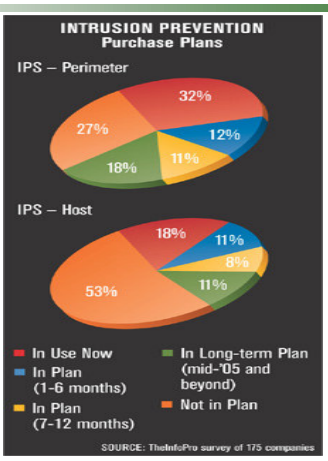
1. Identity management
2. User provisioning
3. Single Sign-On
4. *Intrusion prevention -- perimeter*
5. Wireless LAN Security
6. Patch Management
7. Vulnerability Management
8. Security Dashboard for Ops
9. *Intrusion Detection -- perimeter*
10. Secure Messaging
11. Secure Wireless Devices
12. SSL VPNs
13. Enterprise Security Management
14. *Intrusion Detection -- Host*
15. *Intrusion Prevention -- Host*

Lähde: Information Security Magazine, 4/2004

NETSOL
NETWORK SOLUTIONS

IDS/IPS hankinnat?

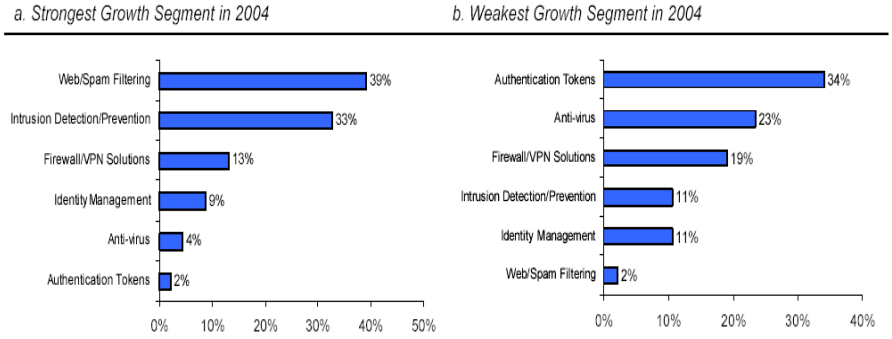




Lähteet: http://www.securitypipeline.com/howto/19300068 ja Information Security Magazine, 4/2004

NETSOL
NETWORK SOLUTIONS

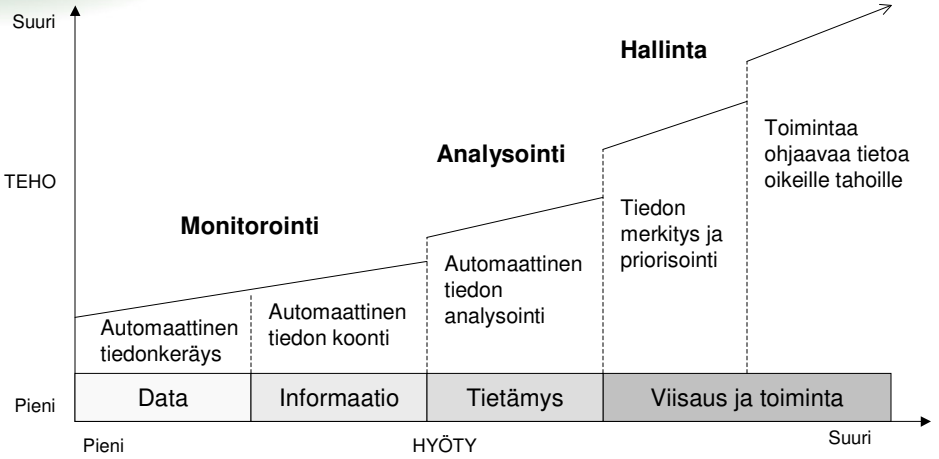
Tuotemyyjien odotukset



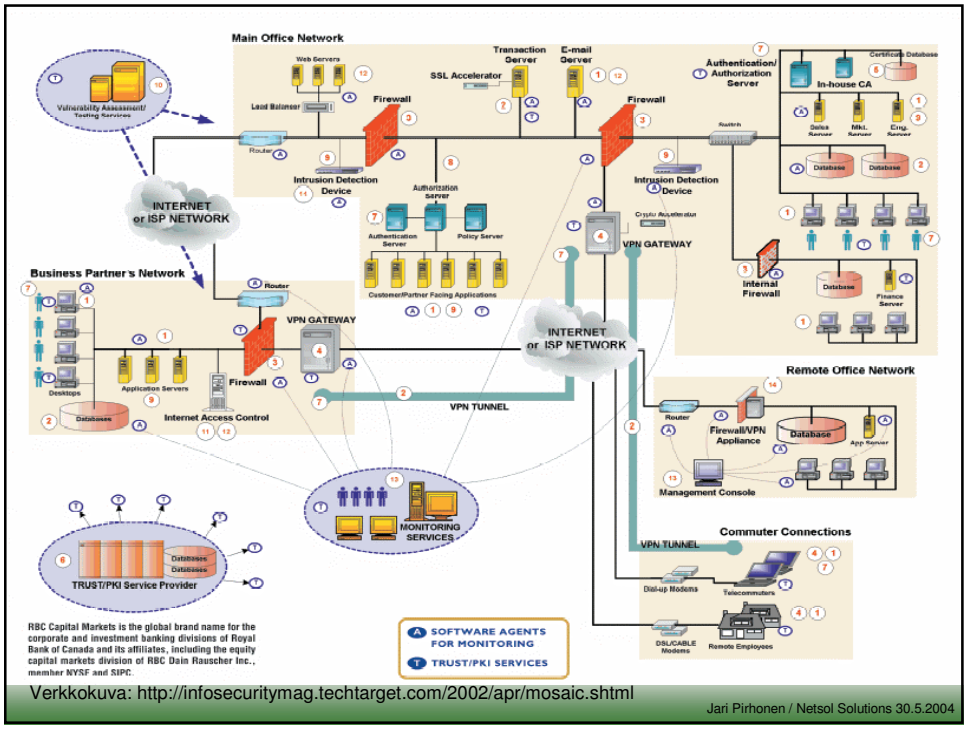
Source: SFG/Spire Security VAR Survey, March 2004.

NETSOL
NETWORK SOLUTIONS

Tiedonpalasista toimintaan

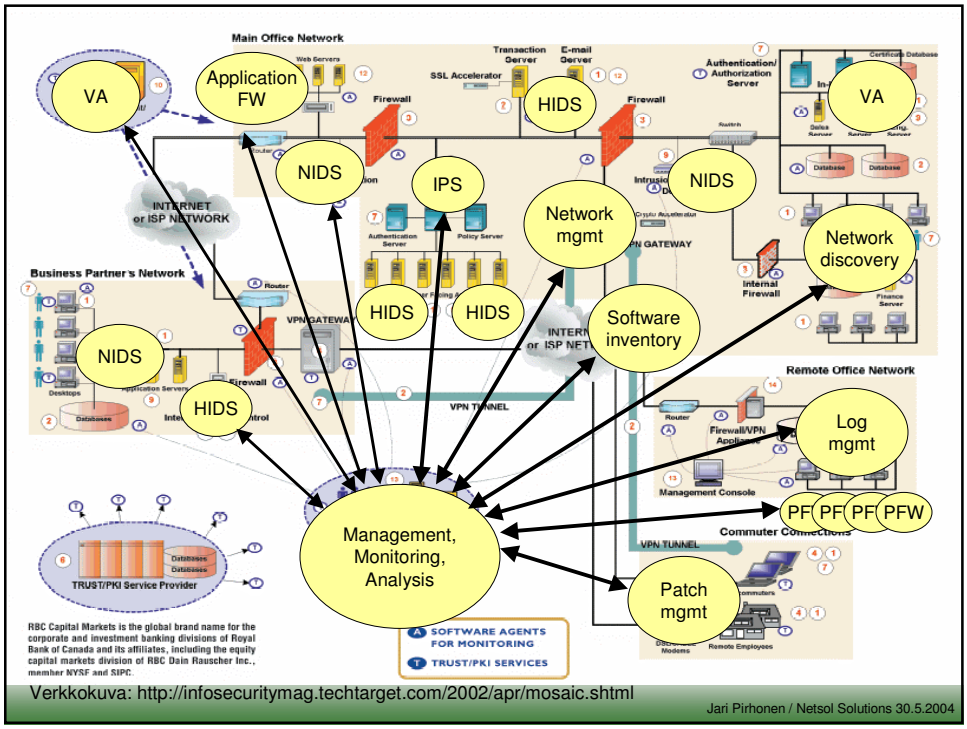


Lähde: Aberdeen Group



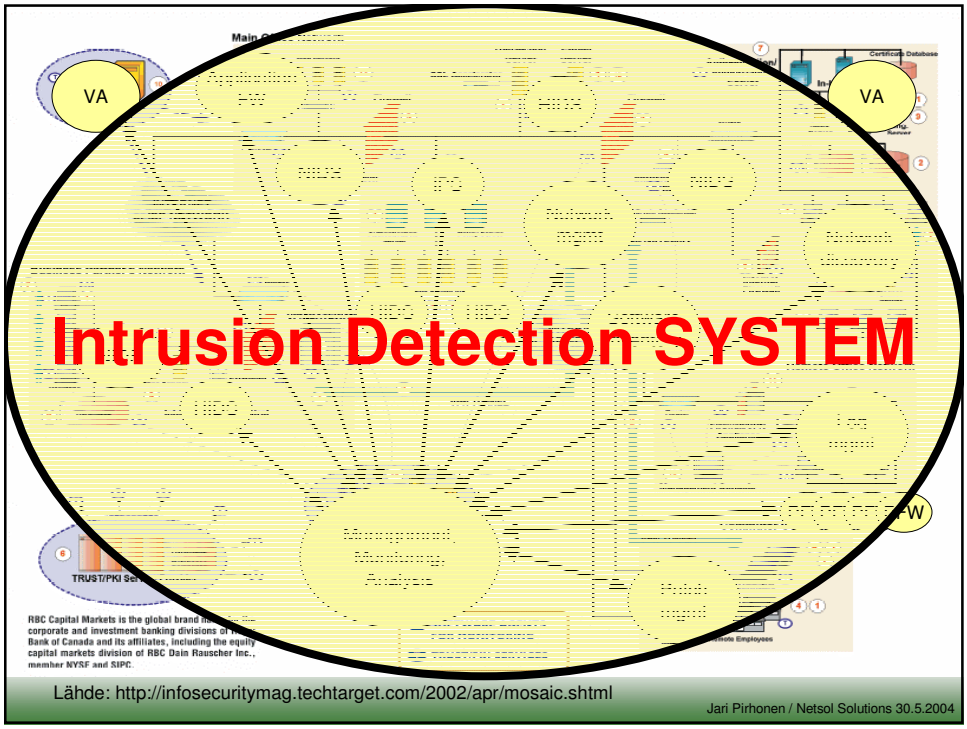
Verkkokuva: http://infosecuritymag.techtarget.com/2002/apr/mosaic.shtml

Jari Pirhonen / Netsol Solutions 30.5.2004



Verkkokuva: http://infosecuritymag.techtarget.com/2002/apr/mosaic.shtml

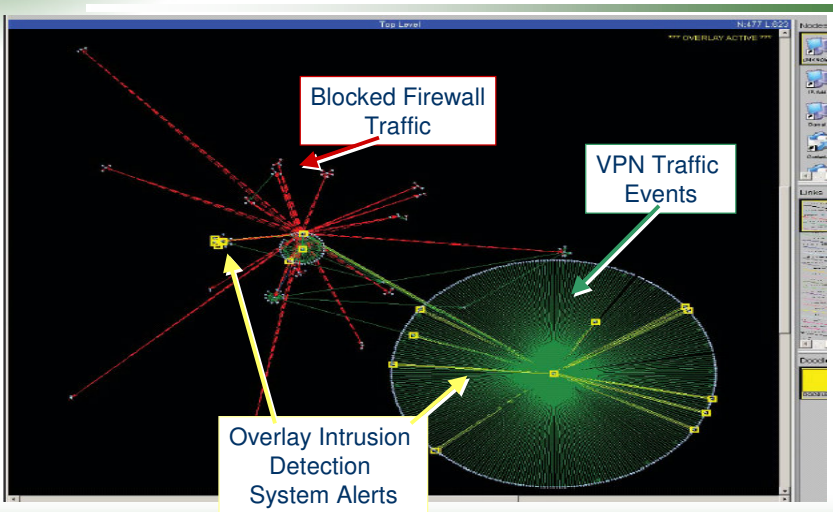
Jari Pirhonen / Netsol Solutions 30.5.2004



Lähde: http://infosecuritymag.techtarget.com/2002/apr/mosaic.shtml

NETSOL
NETWORK SOLUTIONS

Visualisointia



Lähde: CA eTrust materiaali

NETSOL
NETWORK SOLUTIONS

Tulevaisuudessa…

- Sovellusten suojaaminen korostuu
  - erikoistuneet IPS-järjestelmät yleistyvät (HTTP, SOAP,…)
- Kontekstitietoa tarvitaan, parempia ”arvausmoottoreita”
  - target-based IDS, network discovery
- IDS/IPS-tyyppisen toiminnallisuuden integroituminen jatkuu
  - palomuurit, reitittimet, kytkimet, tietokannat, middleware,…
- Myynnin helpottamiseksi IDS/IPS-tuotteista tehdään helppokäyttöisiä ja halpoja
  - rajoitettu toiminnallisuus
- Standardit
  - tietojen esitystapa, hallinta
- Mielenkiintoisia ”uusia” termejä/tapoja kehitetään
  - Meta-IDS, Sinkholes, Evil Honeypots, Network Forensics Tools, Threat mgmt,…

NETSOL
NETWORK SOLUTIONS

Skenaarioita

1. IDS-ratkaisut jäävät muiden tietoturvatoimien jalkoihin.
   - Haittaohjelmien torjunta, SSO, käyttäjätietojen hallinta, Web Services, päivitysten hallinta, PKI ja toimikortit, WLAN, roskaposti, sovellusten tietoturva, …
2. Yritykset tyytyvät erikoistuneisiin, halpoihin ja helposti käyttöönotettaviin IDS/IPS-ratkaisuihin.
   - Mato-ohjelmilta suojautuminen, web-sovellusten suojaaminen, Web Services suojaukset
   - Pistemäisiä IDS/IPS-ratkaisuja
   - Open Source - ratkaisuja
3. Itsenäiset IDS-ratkaisut häviävät ja toiminnallisuus sulautuu muihin verkkokomponentteihin.
   - Reitittimet, kytkimet, palomuurit, käyttöjärjestelmät, tietokannat,…

Jari Pirhonen / Netsol Solutions 30.5.2004

NETSOL
NETWORK SOLUTIONS

Skenaarioita

4. Yritykset rakentavat IDS-järjestelmän yhden tuotetoimittajan kokonaisratkaisun (suite) varaan.
   - Hyvä integrointi
   - Vahva sitoutuminen kaupalliseen toimittajaan
5. IDS-toiminta käsitetään koko yritystä kattavana toimintona. IDS-tuotteet vain yksi monista tiedonkeruumenetelmistä.
   - IPS-toiminnallisuus valituissa pisteissä
   - Open Source ja kaupalliset työkalut
   - Standardit tiedonvaihtoon ja hallintaan, työkalujen yhteen
   - Hyvät työkalut analysointiin ja tiedonlouhintaan
   - Panostus resursseihin ja prosesseihin