Open source nadzor sustava

Vlatko Košturjak
kost at linux dot hr

Agenda

- Uvod
- Zašto nadzirati
- Vrste nadzora
- Software za nadzor
  - Snort
  - Prelude
  - Nagios
  - ...
- Budućnost

45 minuta

Zašto nadzirati?

- Sigurnost
  - Praćenje incidenata
  - Danas korisnik vidi problem prije nego mi
- Praćenje
  - Zauzetost resursa
  - Opterećenje
  - Anomalije
  - Raspoloživost
- Troubleshooting
  - Olakšava troubleshooting

Razine nadziranja

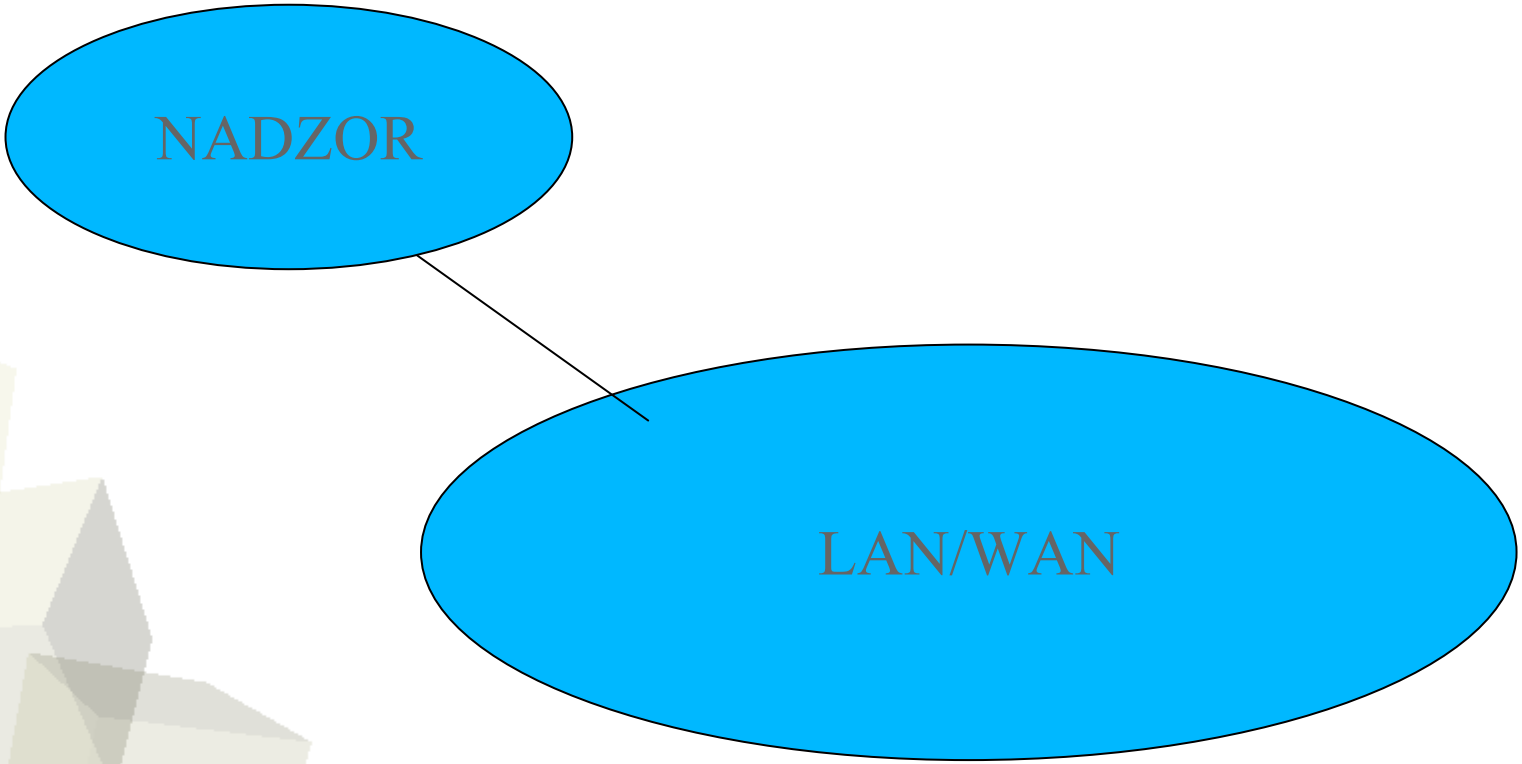
- Zapisivanje
  - Prati stanje sustava
  - Zapisuje statistike
  - Korisnik prepoznaje i rješava probleme
- Prepoznavanje problema
  - Prati stanje sustava, te prepoznaje probleme
  - Korisnik se obavještava o problemima
  - Korisnik rješava probleme
- Prepoznavanje i rješavanje problema
  - Prati stanje sustava, prepoznaje probleme i rješava ih, te samo obavještava korisnika

Nadzor

- S obzirom na ulogu korisnika
  - Aktivni
  - Pasivni
- S obzirom na stvar nadzora
  - Nadzor mreže
  - Nadzor poslužitelja
- S obzirom na tip nadzora
  - Intrusion detection System(IDS)
  - Intrustion Prevention System (IPS)
  - ...

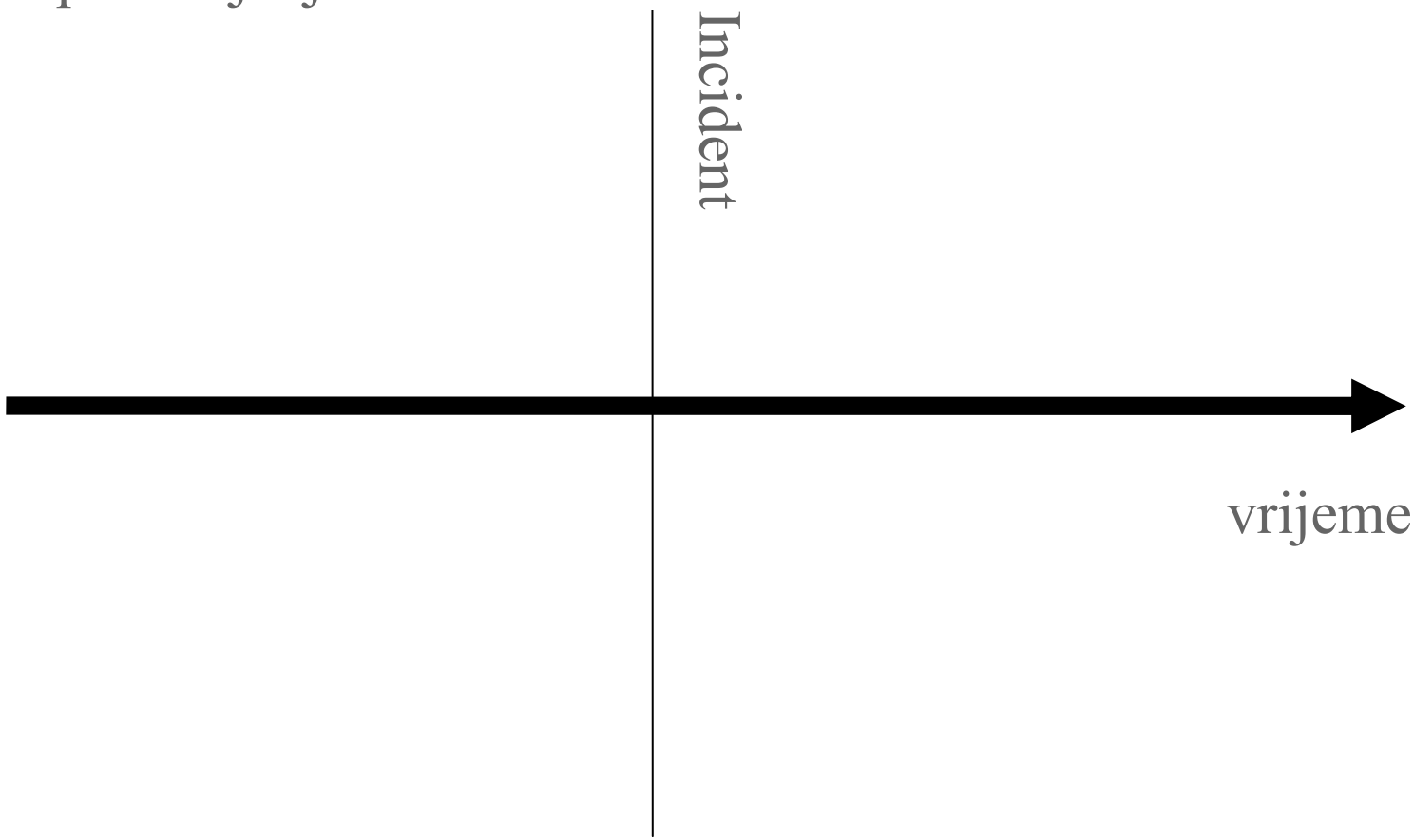
Gdje postaviti nadzor?

- Posebno zaštićen dio mreže
- Samo fizički pristup?



Nadzor i vrijeme

Pravovremenost postavljanja nadzora



Kakvo je normalno stanje?

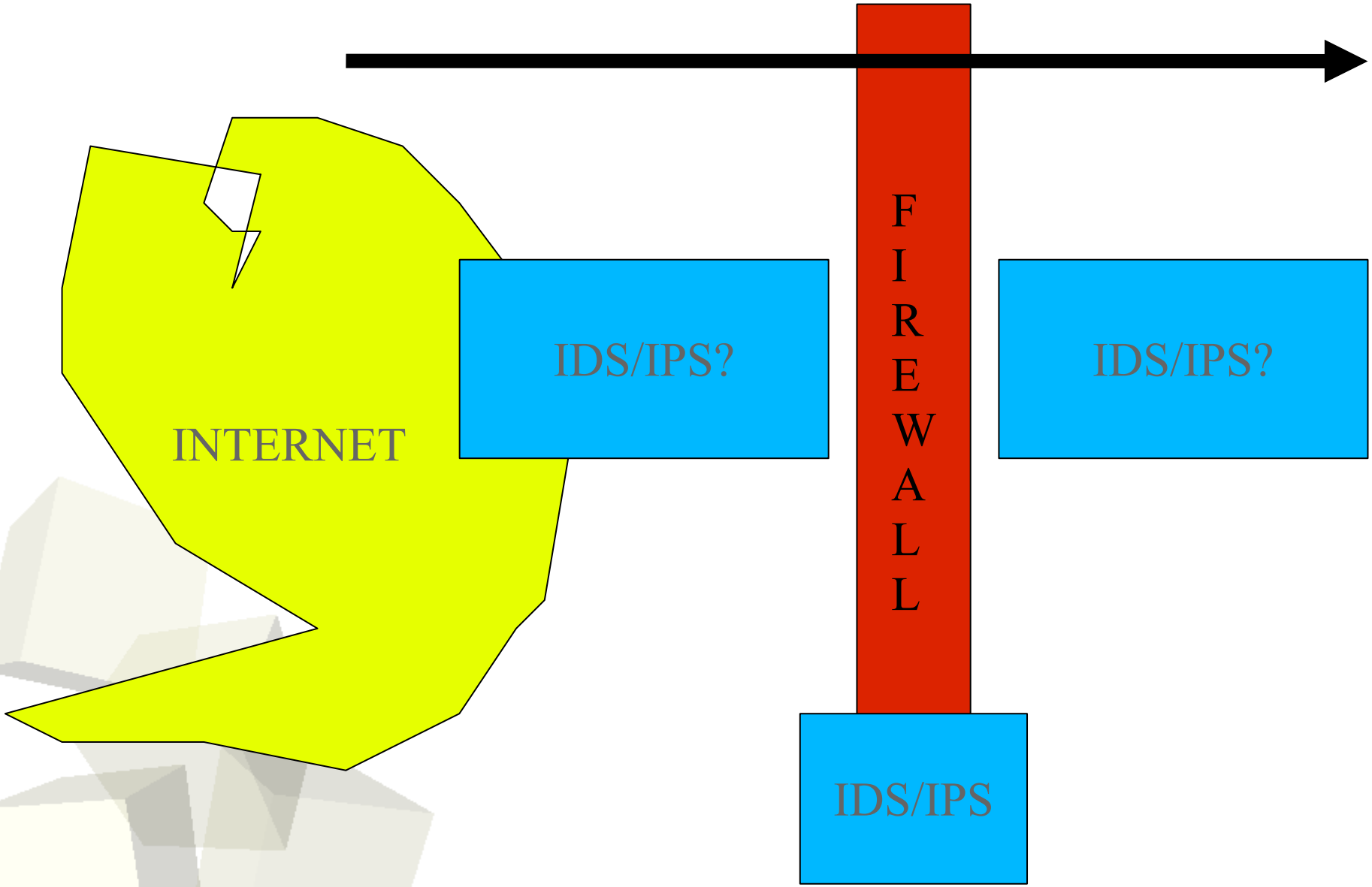
Sinhronizacije vremena

- Sinhronizacija vremena izrazito važna
  - Korelacije i sekvenca događanja interno
  - Korelacije i sekvenca događanja eksterno
- Time sinhronizacija
  - Linux
    - ntpdate,
    - xntpd,
    - chrony....
  - Windows
    - Postoji podrška za sinhronizaciju

IDS / IPS

- Vrste
  - Intrusion detection system (IDS)
  - Intrusion prevention system (IPS)
- Način prepoznavanja
  - Baziran na potpisima (signature based)
  - Baziran na statističkoj analizi (statistical)
  - Baziran na praćenju ponašanja (heuristic)
- Predmet nadziranja
  - Network intrusion detection system (NIDS)
  - Host intrusion detection system (HIDS)
  - Hybrid intrusion detection system (HyIDS)

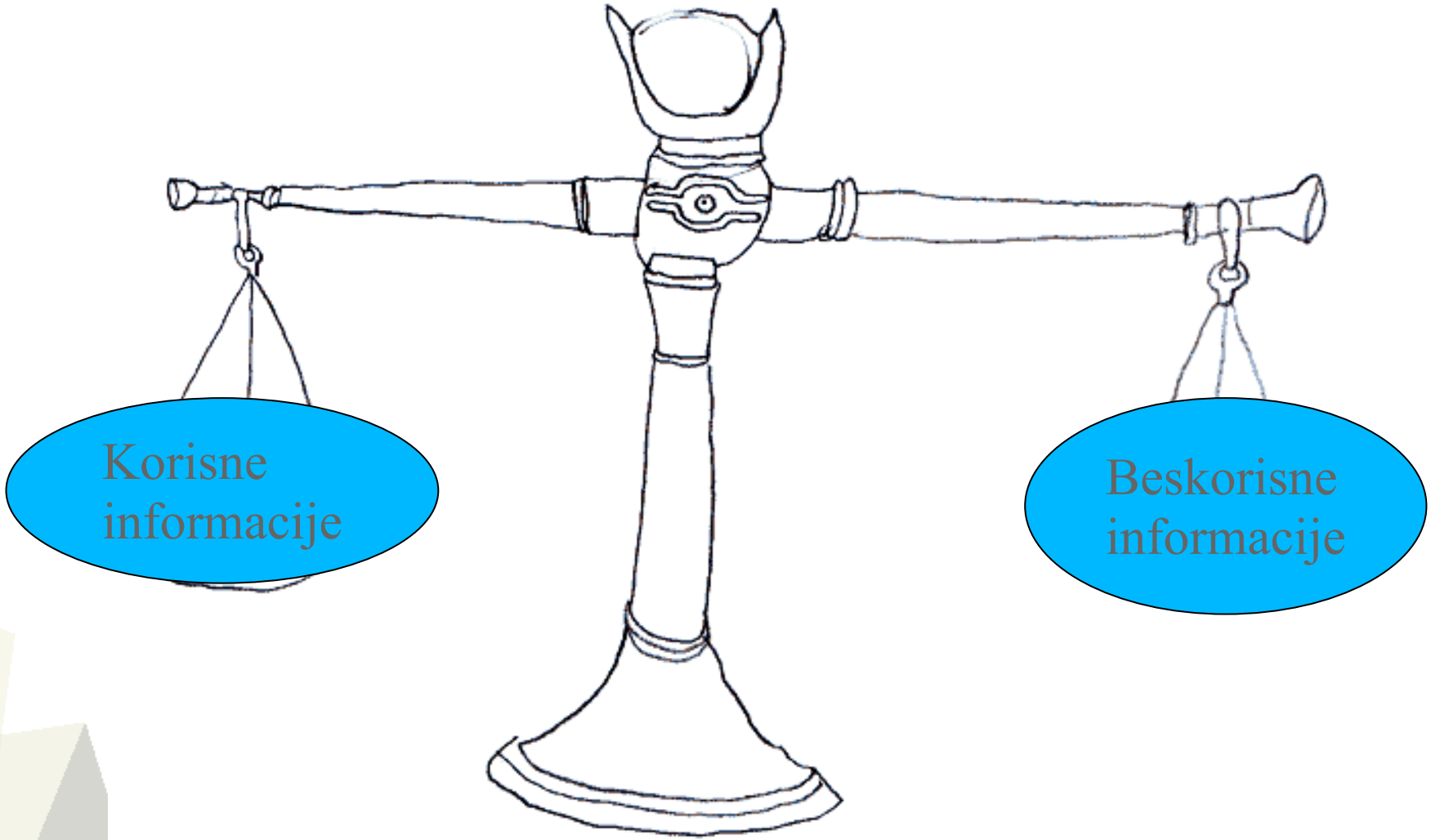
IDS / IPS postavljanje



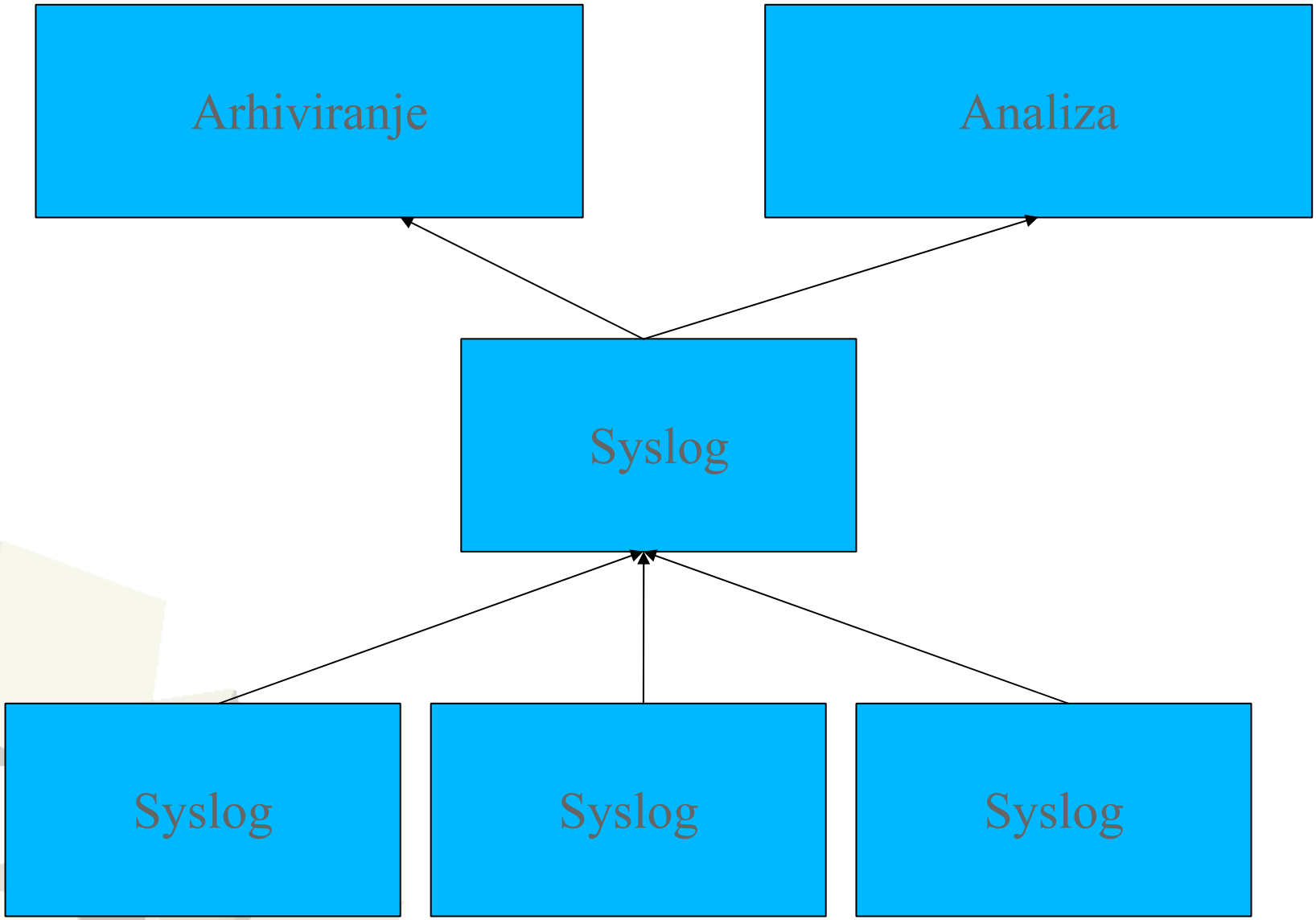
Logovi

- Logovi izrazito važni
  - Linux: /var/log
  - Windows: syslog mogućnost
- Log parseri
  - Bojanje logova
  - Različiti alati da izvlače što je bitno
- Skripte
  - Grep? :)
  - Vlastite skripte za izvadak bitnoga
  - Vlastite skripte za korelaciju

Prava razina logova



Centralni syslog poslužitelj



MRTG

- http://oss.oetiker.ch/mrtg/
- Multi Router Traffic Grapher (MRTG)
- Pisan u PERL-u
- Unix/Linux/Windows
- Informacije
  - Koristi SNMP
  - Izlaz(output) od određene komande
- Kreira HTML stranice za prikaz dobivenih informacija
- Dizajniran za mrežne uređaje (input/output)
- Podržava osnovnu dojavu
  - Ako vrijednosti pređu određenu granicu

RRDtool

- http://oss.oetiker.ch/rrdtool/
- Round-robin database tool
- Alat za rukovanje podacima u vremenskom periodu
- Optimiziran za praćenje različitih podataka u vremenskoj dimenziji
  - Zauzeće diska
  - Zauzeće procesora
  - Temperatura
  - ...
- Alati za prikazivanje navedenih podataka putem različitih grafova

ntop

- http://www.ntop.org
- Prati korištenje mreže
- Unix/Linux/Windows
- IPv4/IPv6/IPX/NetBIOS/...
- Koristi se RRD za zapisivanje
- Podržava prepoznavanje peer2peer protokola
- Pasivno prepoznavanje operativnih sustava
- Podrška za WAP

SmokePing

- http://oss.oetiker.ch/smokeping/
- Prati odziv mreže i izgubljene pakete
- Podrška za dinamički IP
- Koristi se RRD za zapisivanje podataka
- Pisan u PERL-u (cgi/speedycgi/mod_perl)
- Unix/Linux
- Podrška za pluginove

Cacti

- http://www.cacti.net/
- Cacti (Cactus)
- Frontend za RRDtool
- Unix/Linux/Windows
- Podatke sprema u MySQL
- PHP/MySQL frontend za web
- Informacije
  - Koristi SNMP
  - Izlaz(output) od određene komande
- Podržava ograničavanje pristupa podacima putem korisnika

Snort

- http://www.snort.org
- Tri namjene
  - Sniffer opće namjene
  - Intrusion detection system (IDS)
  - Intrusion prevention system (IPS)
- Pisan u C-u
- Unix/Linux
- Podrška za pluginove
- Stabilan, dugi niz godina razvoja
- Imao nekoliko sigurnosnih problema u prošlosti

Snort kao sniffer

- Postavljanje
  - Kao gateway
  - Monitor mode
- Mogućnost zapisivanja paketa u datoteku
- Primjeri
  - ./snort -v
  - ./snort -vd
  - ./snort -vde
  - ./snort -dev -l /tmp/snort
  - ./snort -dev -l /tmp/snort -h 192.168.0.0/24

Snort kao IDS

- Postavljanje
  - Kao gateway
  - Monitor mode
- Na mrežama 1000 Mbps preporučljivo koristiti unified logging i barnyard
- Mogućnost pisanja novih pravila
- Mogućnost zapisivanja događaja
  - Log zapis
  - MySQL
  - ODBC

Snort kao IPS

- Snort in-line
- Postavljanje pomoću iptables
  - Koristi se ip_queue modul
  - Target QUEUE
  - Šalje pakete u user space
  - iptables -A OUTPUT -p tcp --dport 53 -j QUEUE
  - snort_inline -QDc /etc/snortd.conf -l /var/log/snort
- Mogućnost proizvoljnog mjenjanja paketa
  - Ograničenje: paket mora biti iste veličine

ACID

- http://acidlab.sourceforge.net/
- Analysis Console for Intrusion Databases (ACID)
- Razvoj nije aktivan (2003)
- PHP/MySQL
- Prikaz snort događaja putem weba
  - Različite mogućnosti sortiranja
  - Grafovi
  - Sortiranje događaja
  - Filtriranje događaja
- Nedostaci:
  - Nemogućnost interaktivne zabrane/konfiguriranje

BASE

- http://base.secureideas.net/
- Basic Analysis and Security Engine (BASE)
- Nastavak razvoja ACID-a
- PHP/MySQL
- Prikaz snort događaja putem weba
  - Različite mogućnosti sortiranja
  - Grafovi
  - Sortiranje događaja
  - Filtriranje događaja
- Nedostaci:
  - Nemogućnost interaktivne zabrane/konfiguriranje

Tripwire

- http://sourceforge.net/projects/tripwire/
- HIDS sustav
- Unix/Linux
- Potpisana baza promjena
- Prati promjene
  - Na datotečnom sustavu
- Osnovna mogućnost dojave
- Dodaci
  - FICC
    - → Olakšava praćenje više tripwire instalacija
    - → http://www.firsttracks.net/ficc/

AIDE

- http://aide.sourceforge.net
- HIDS sustav
- Unix/Linux
- Enkriptirana/potpisana baza promjena
- Prati promjene
  - Na datotečnom sustavu
- Osnovna mogućnost dojave
- RFC
  - master/slave koncept
  - Remote filesystem checker
  - http://rfc.sourceforge.net/

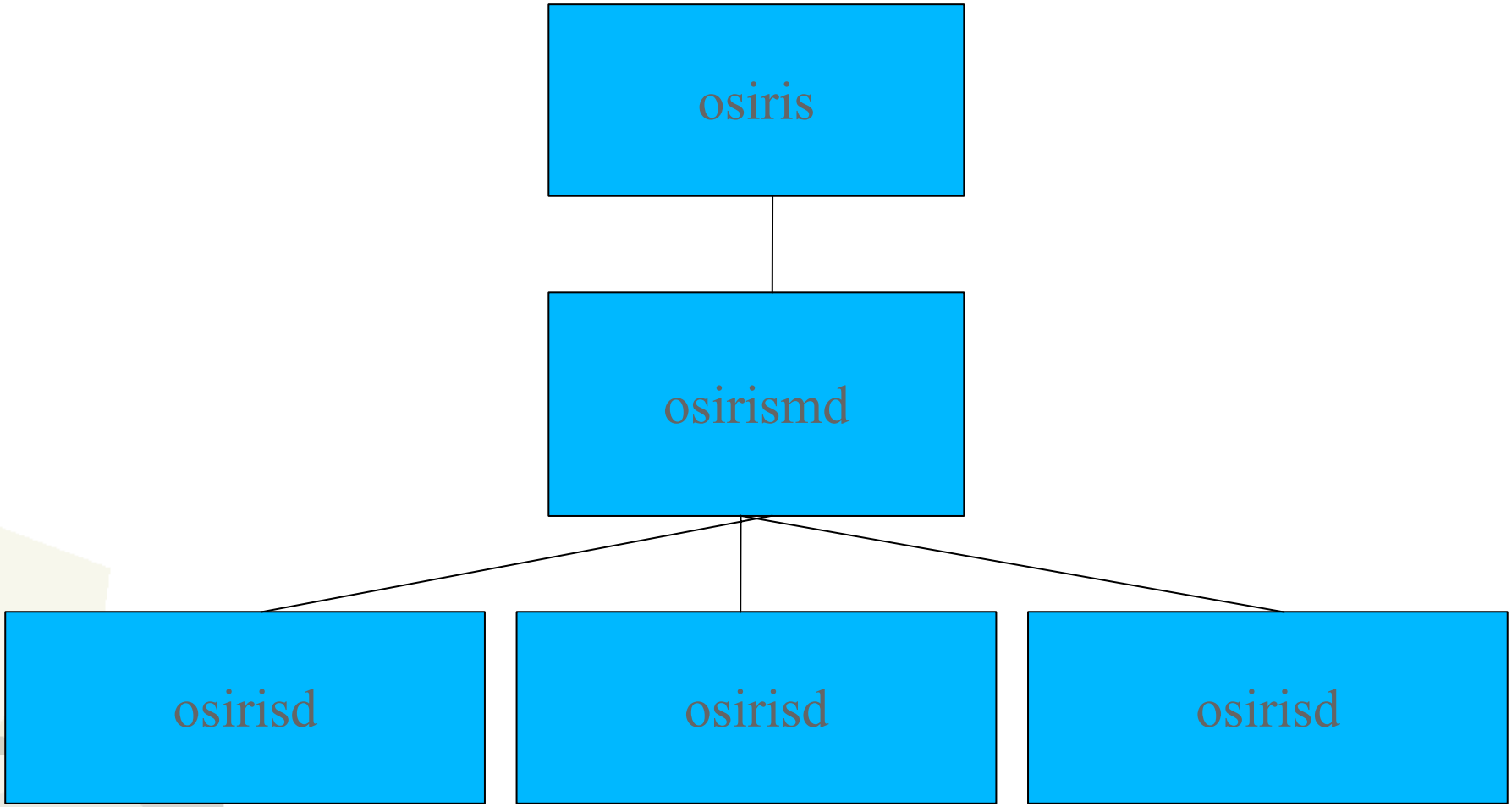
SAMHAIN

- http://www.la-samhna.de/samhain/
- HIDS sustav
- Unix/Linux/Windows
- Client/server sustav
- Podrška za centralno upravljanje
- Potpisana baza promjena
- Prati promjene
  - Na datotečnom sustavu
  - Kernel modul rootkitove (samo Linux)
- Osnovna mogućnost dojave

Osiris

- http://osiris.shmoo.com/
- Osiris
- HIDS sustav
- Baziran na potpisima (Signature based)
- Unix/Linux/Windows
- Prati promjene
  - Na datotečnom sustavu
  - Konfiguracijskih datoteka
  - Popis korisnika i grupa
  - Aktivnih kernel modula
- Osnovna mogućnost dojave

Osiris



OSSEC HIDS

- http://www.ossec.net/
- HIDS sustav
- Baziran na potpisima (Signature based)
- Unix/Linux
- Windows (samo agent)
- Prati promjene
  - Na datotečnom sustavu
  - Konfiguracijskih datoteka (uključujući registry na Win)
  - Snort logove
  - NMAP
- Osnovna mogućnost dojave

Prelude Hybrid IDS

- http://www.prelude-ids.org/
- Hybrid IDS
- Unix/Linux
- Koristi:
  - Snort, Nessus, samhain, ...
- Pregled log datoteka
- Automatska korelacija
- Mogućnost centralnog upravljanja
- IETF IDMEF (Intrusion Detection Message Exchange Format)

Munin

- http://munin.projects.linpro.no/
- Praćenje stanja poslužitelja, servisa itd.
- Unix/Linux
- Cilj: jednostavno pisanje pluginova
- Koristi RRD za zapisivanje
- Pisan u PERL-u
- Arhitektura na razini plugina
  - Veliki izbor pluginova
  - Bilo koji programski jezik za pluginove
- “Plug and play”

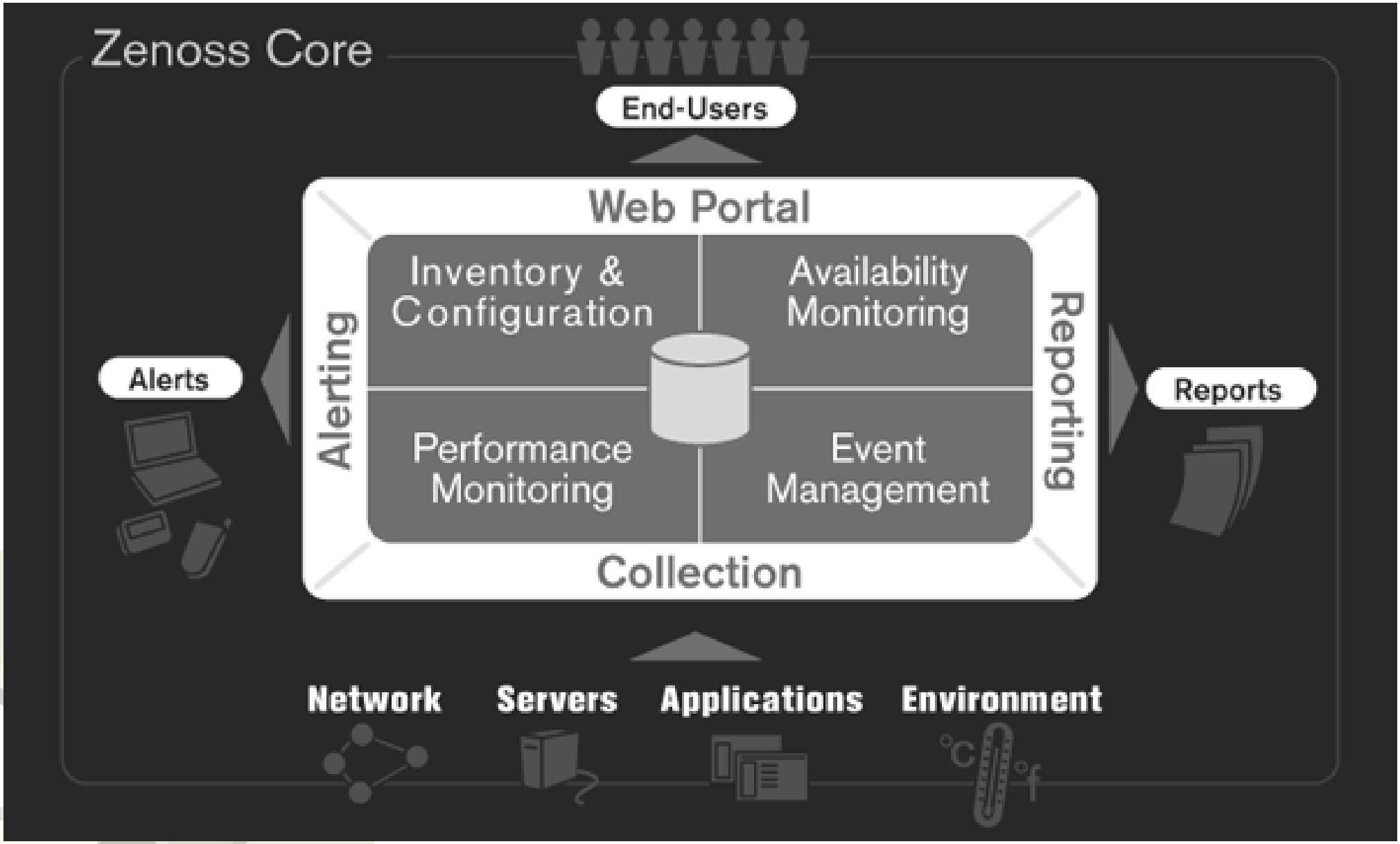
Nagios

- http://nagios.org/
- Nagios
  - Nekada netsaint
- Praćenje stanja mrežnih računala i servisa
- Dojava problema na različite načine
  - E-mail
  - SMS/pager
- Pisan u C-u
- Arhitektura na razini plugina
  - Veliki izbor pluginova
- Mogućnost pregledavanja putem WEB/WAP

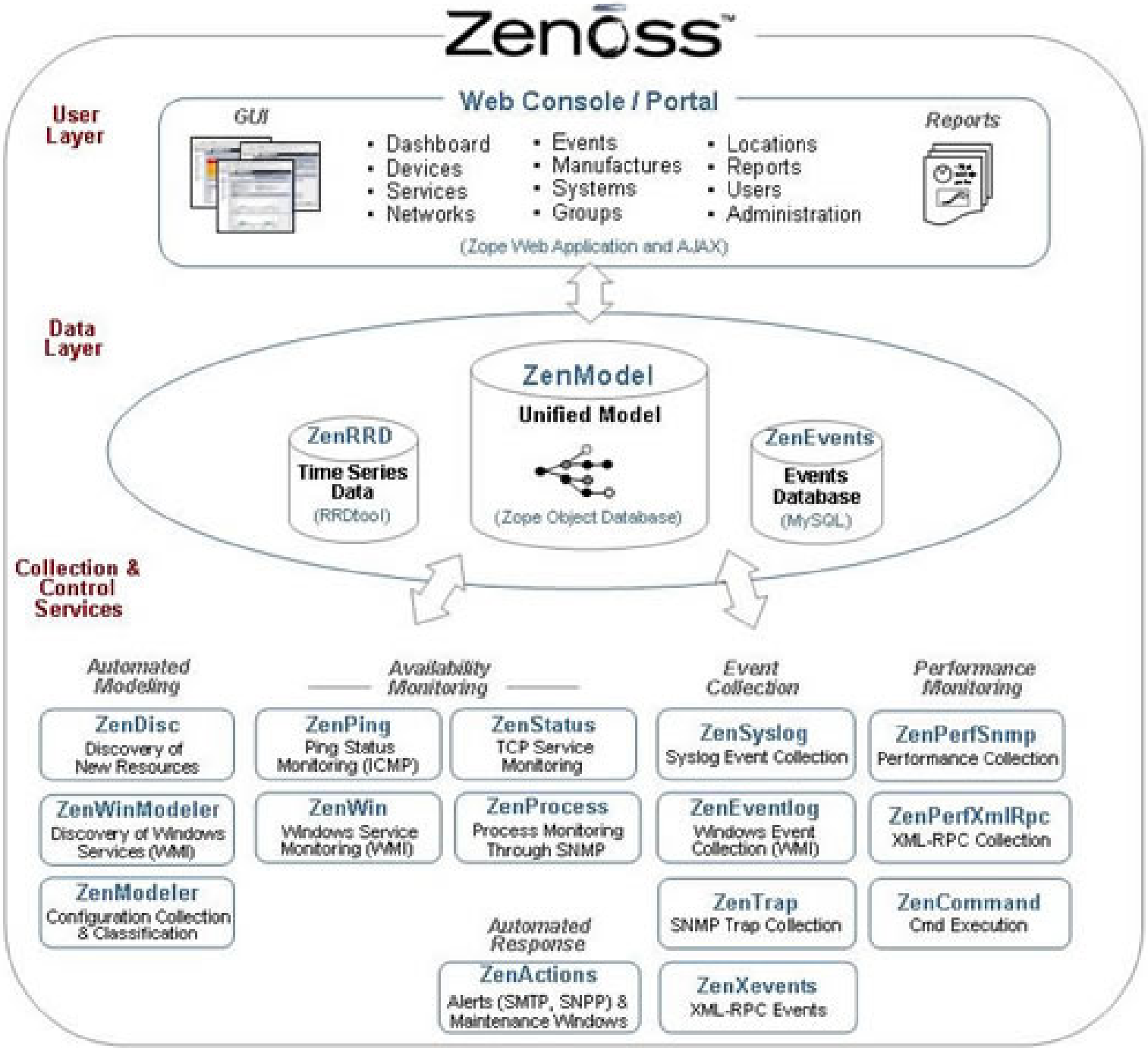
Zenoss

- http://www.zenoss.com
- Zenoss
  - Podrška od strane Zenoss Inc.
- Praćenje stanja i performansi mrežnih računala i servisa
- Potpuni system management
- Python/Zope/MySQL
- Koristi se RRD za zapisivanje
- Arhitektura na razini plugina
  - Veliki izbor pluginova
- Pregled/konfiguracija putem weba

Zenoss


Zenoss Core
End-Users
Web Portal
Inventory & Configuration
Availability Monitoring
Performance Monitoring
Event Management
Alerting
Reporting
Collection
Alerts
Reports
Network
Servers
Applications
Environment

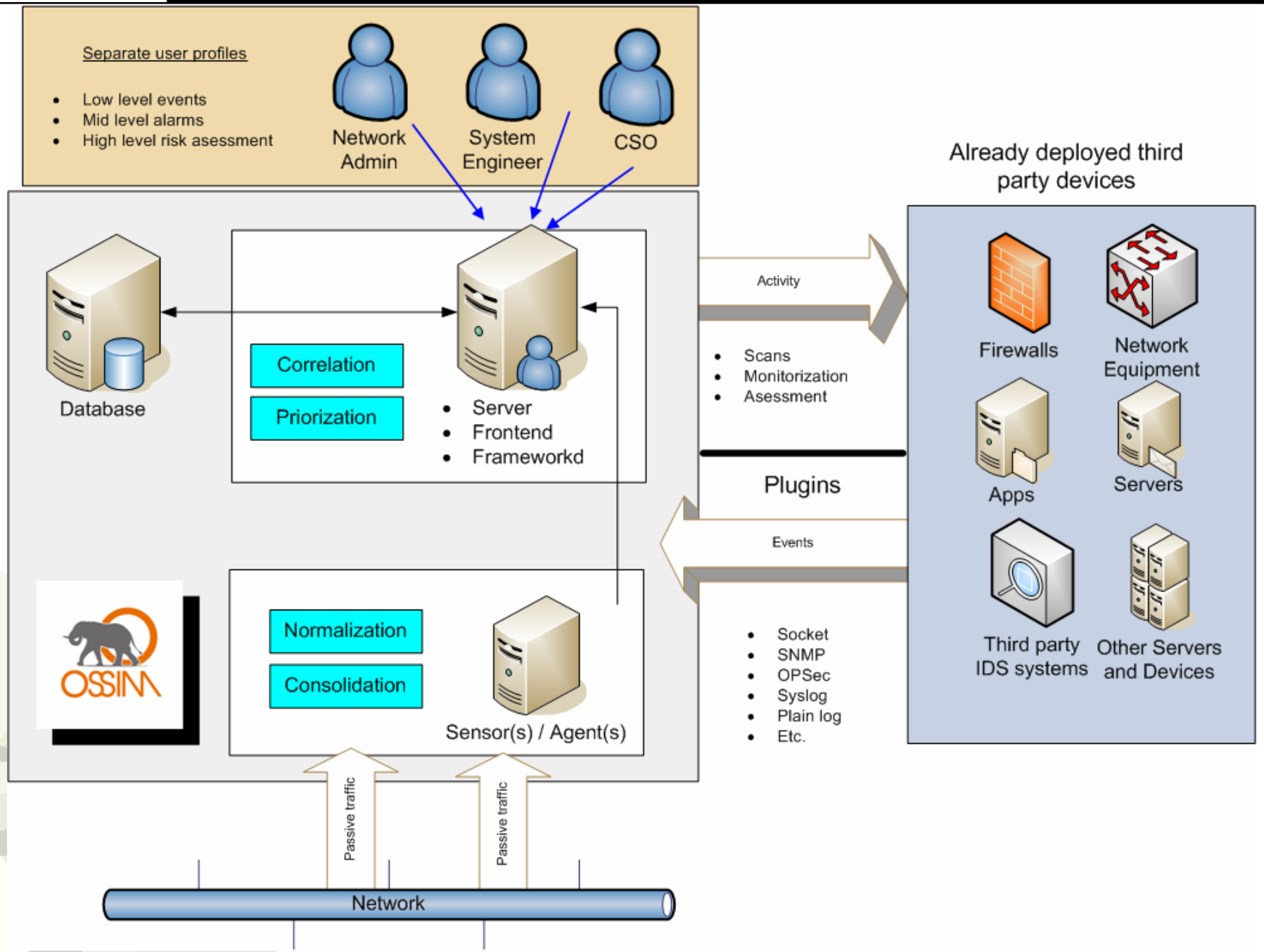
Zenoss


Zenoss
User Layer
Web Console / Portal
GUI
Dashboard
Devices
Services
Networks
Events
Manufactures
Systems
Groups
Locations
Reports
Users
Administration
Reports
(Zope Web Application and AJAX)
Data Layer
ZenModel
Unified Model
(Zope Object Database)
ZenRRD
Time Series Data
(RRDtool)
ZenEvents
Events Database
(MySQL)
Collection & Control Services
Automated Modeling
Availability Monitoring
Event Collection
Performance Monitoring
ZenDisc
Discovery of New Resources
ZenPing
Ping Status Monitoring (ICMP)
ZenStatus
TCP Service Monitoring
ZenSyslog
Syslog Event Collection
ZenPerfSnmp
Performance Collection
ZenWinModeler
Discovery of Windows Services (WMI)
ZenWin
Windows Service Monitoring (WMI)
ZenProcess
Process Monitoring Through SNMP
ZenEventlog
Windows Event Collection (WMI)
ZenPerfXmlRpc
XML-RPC Collection
ZenModeler
Configuration Collection & Classification
ZenTrap
SNMP Trap Collection
ZenCommand
Cmd Execution
Automated Response
ZenActions
Alerts (SMTP, SNPP) & Maintenance Windows
ZenXevents
XML-RPC Events

OS-SIM

- http://www.ossim.net/
- Open Source Security Information Management
- Centralni softver za nadzor
- Može raditi kao IPS
- Koristi sljedeće alate:
  - Arpwatch, P0f, Pads
  - Nessus, Snort
  - Spade, Tcptrack
  - Ntop
  - Nagios
  - Osiris

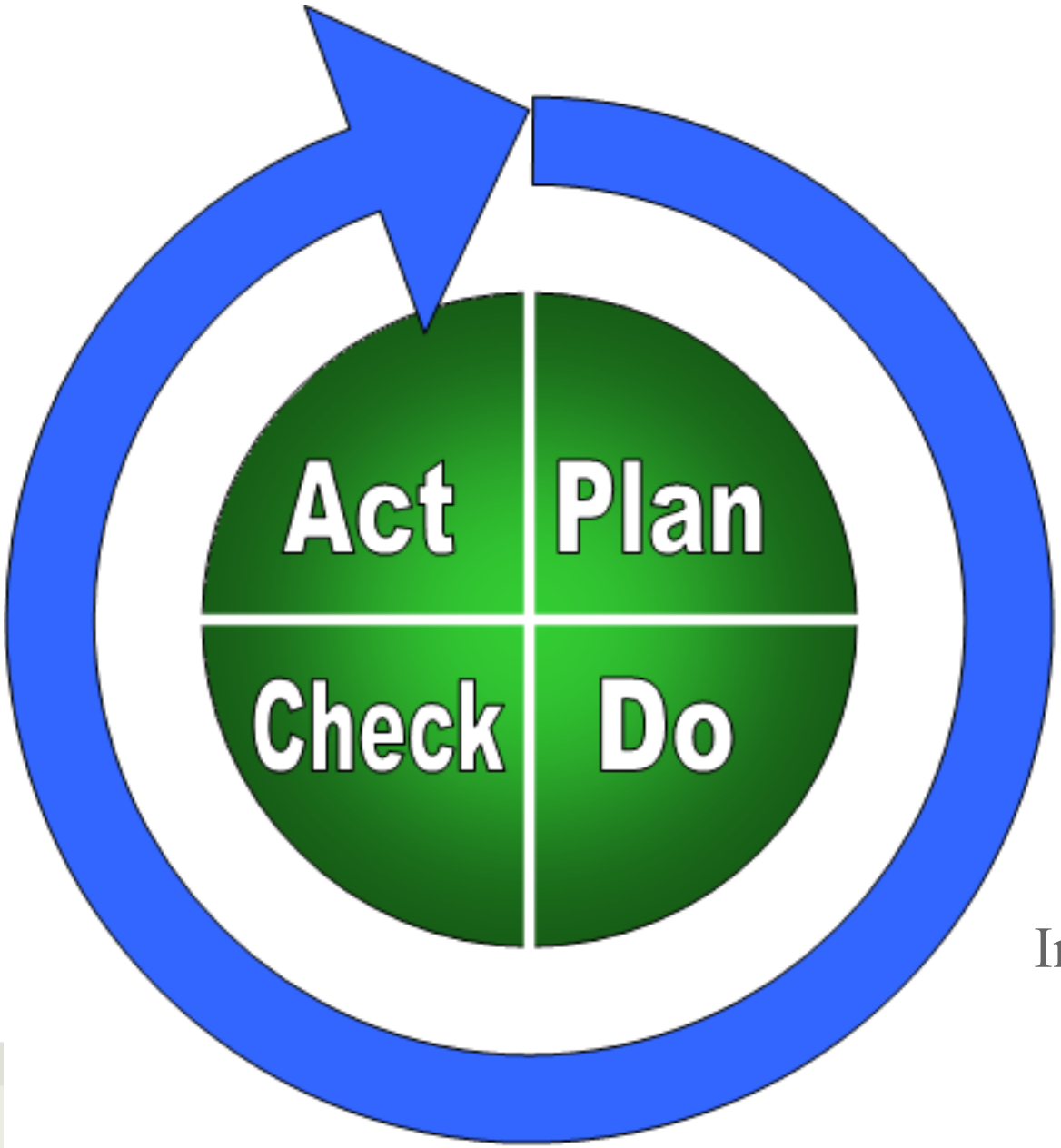
OS-SIM


Separate user profiles
Low level events
Mid level alarms
High level risk asessment
Network Admin
System Engineer
CSO
Already deployed third party devices
Database
Correlation
Priorization
Server
Frontend
Frameworkd
Activity
Scans
Monitorization
Asessment
Plugins
Events
Socket
SNMP
OPSec
Syslog
Plain log
Etc.
Firewalls
Network Equipment
Apps
Servers
Third party IDS systems
Other Servers and Devices
OSSIM
Normalization
Consolidation
Sensor(s) / Agent(s)
Passive traffic
Passive traffic
Network

Budućnost

- Problem kompleksnosti sustava
- Autonomic computing – self managing computer system
  - Self Configuration
  - Self Healing
  - Self Optimization
  - Self Protection
- Razine
  - Level 1 – trenutno stanje
  - Level 2-4 – različite razine
  - Level 5 – pravi autonomic computing
- 2001. godine

PDCA/PIPD način



Djelovanje

Planiranje

Provjera

Implementacija

Pitanja

Vlatko Košturjak (**kost** at **linux** dot **hr**)