IBM Global Services

Securing your IT with open source

Vlatko Košturjak

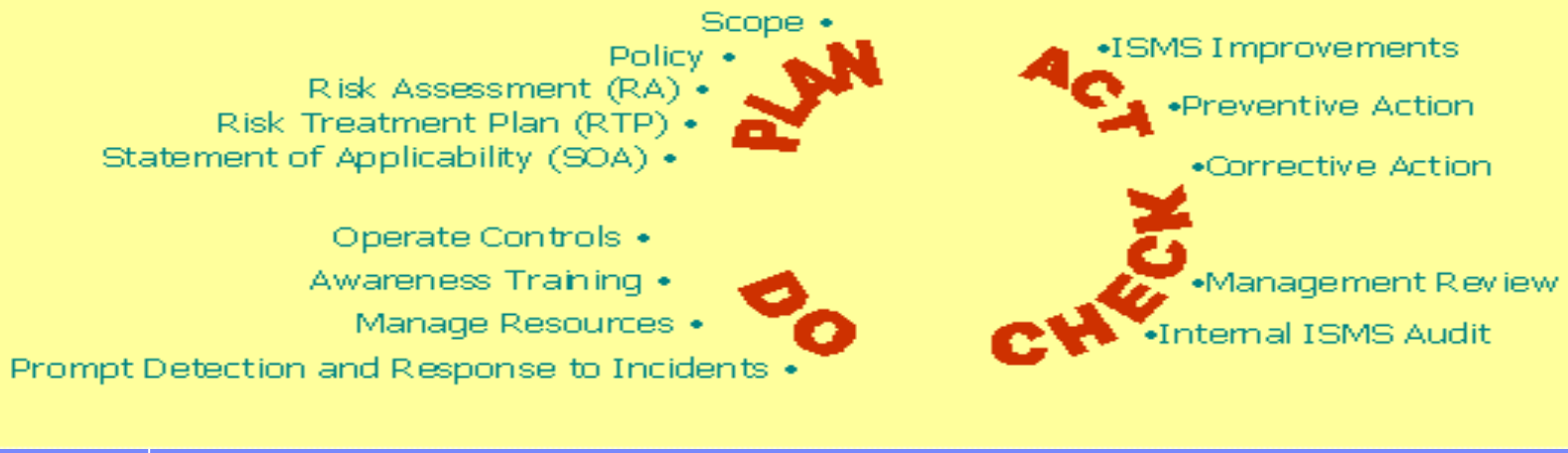
vlatko.kosturjak@hr.ibm.com

Agenda

- Hardening and Tightening
- Monitoring and preventing
- Forensic
- Future

Security policy
Security standards
Security procedurs
Physical security
...

TOTAL: 30 minutes



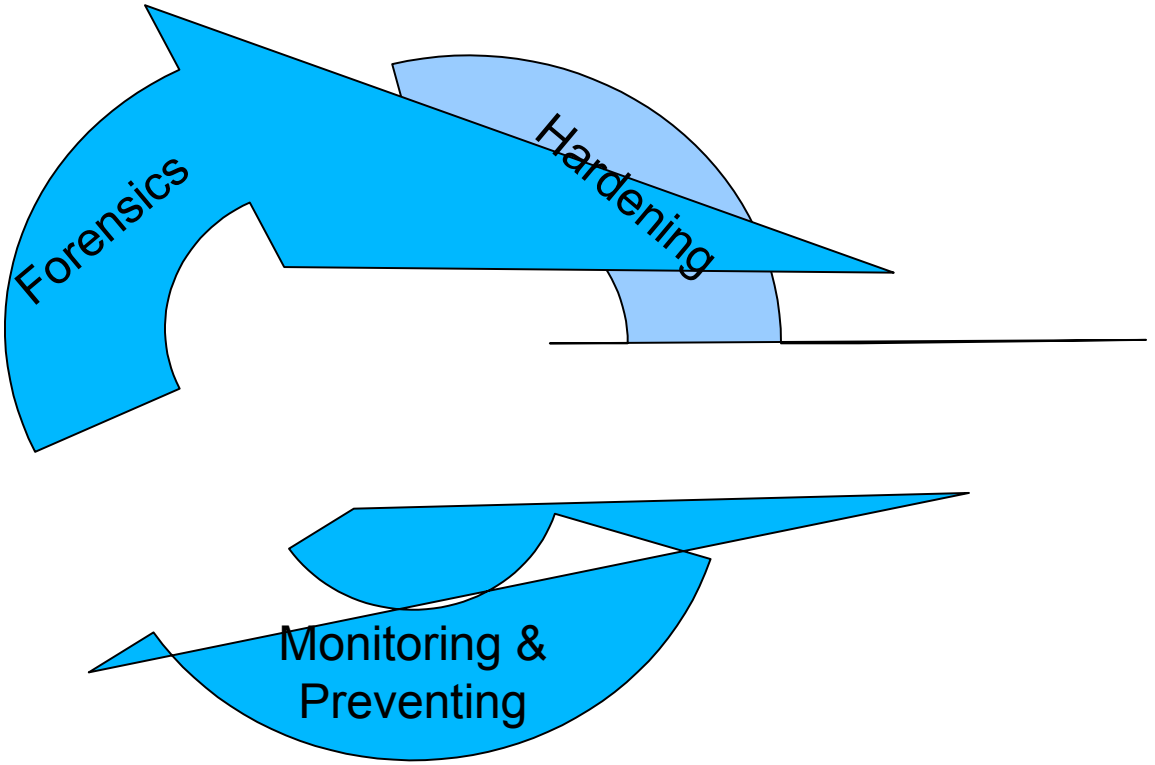
Security

Secure

Useable

Cheap

Security



Tightening your system

- Tightening according to organization policies and standards
- Basic stuff
  - Update/Patch
  - Remove unneeded services
  - Remove unneeded components
  - Least privilege principle
  - Implement strong passwords
  - Deny all, allow specific
- ...

Hardening

- Bastille
- Linux
  - SELinux
  - Grsecurity
  - Openwall project
  - Hardened debian
- Firewalls
  - Shorewall
  - FWbuilder
  - Falcon firewall project

Backup

- Amanda
  - www.amanda.org
  - Advanced Maryland Automatic Network Disk Archiver
- Bacula
  - www.bacula.org
  - Multiplatform network backup tool
- BackupPC
  - backuppc.sourceforge.net
  - High-performance backup of workstations to server's disk
- Dirvish
  - www.dirvish.org
  - Fast, disk based, rotating network backup system

Monitoring

- Multi Router Traffic Grapher (MRTG)
- SmokePing
- Big Brother
- Ntop
- Mon
- OpenNMS
- Nagios
- rrdtool

E-mail

- Amavis
- Spamassasin
- pop3proxy
- postprox
- Proxsmtp
- Anti-Spam SMTP Proxy
- Mailstore
- smtpfilter
- Clamav
- ...

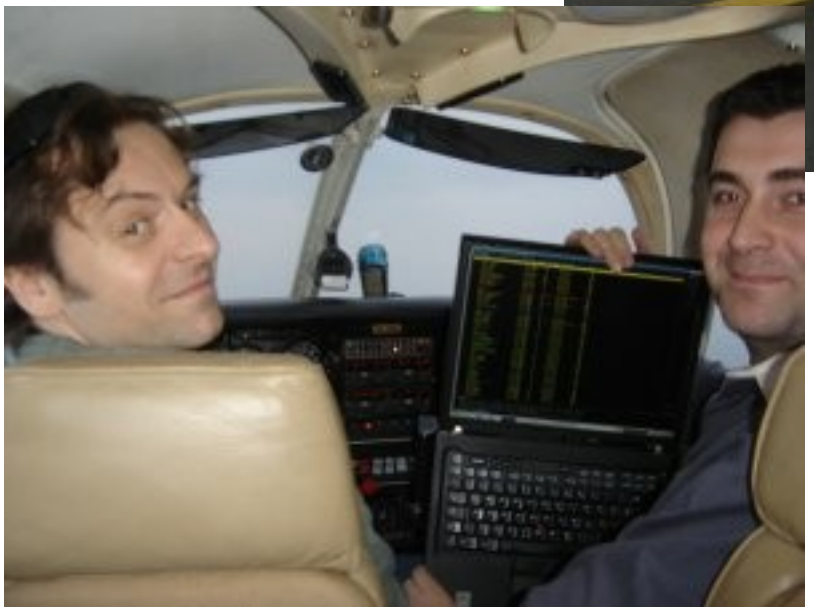
Intrusion and Prevention

- Host Intrusion Detection Systems (HIDS)
  - Tripwire
  - AIDE
- Network Intrusion Detection Systems (NIDS)
  - Snort
  - Argus
  - BroIDS
- Hybrid Intrusion Detection Systems (HyIDS)
  - Prelude
- Prevention
  - Blockit
  - Snort2pf

Integration:
OS-SIM
Demarc

Wireless

- WIDZ
- Kismet
- FakeAP
- ...



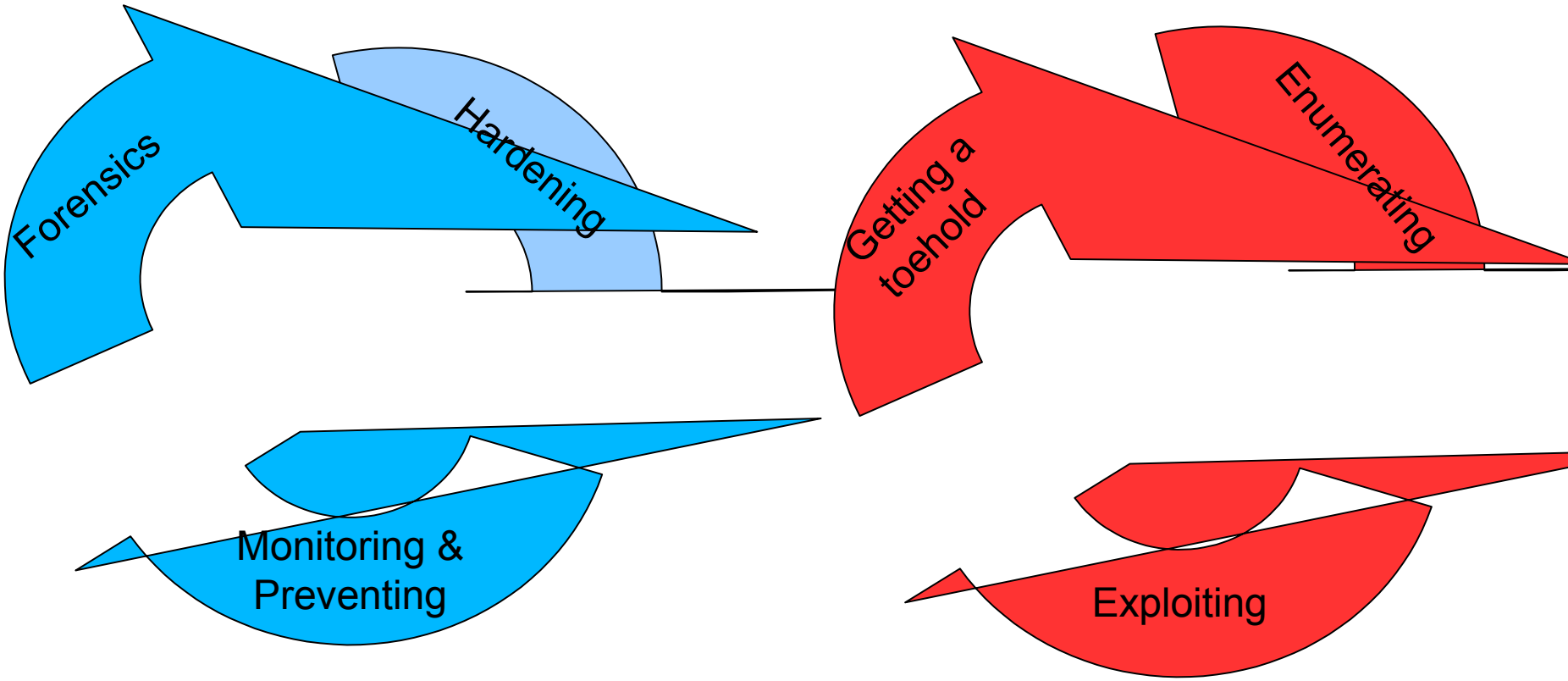
Test yourself

- Nmap
- Amap
- Hping2
- Nessus
- Nikto
- Paros
- Ike-scan
- Fragrouter
- Firewalk
- ...

Forensic

- Coroner's Toolkit
- Sleuth
- File System Investigator
- FLAG
- Bootable CD's
  - DMSZ-Fire
  - Freesbie
  - Knoppix
  - ...

Attacker and Defender methodology



Open standards

- Open standards
  - IDMEF
  - Common Base Event format
  - ANML
  - SIML
  - SDML

"An autonomic computing system cannot exist in a hermetic environment. While independent in its ability to manage itself, it must function in a heterogeneous world and implement open standards -- in other words, an autonomic computing system cannot, by definition, be a proprietary solution."
- Autonimic Computing manifesto

The end

QUESTIONS

Vlatko Košturjak <vlatko.kosturjak@hr.ibm.com>