

Voith IT Solutions



Self defending networks?

What we do @ Voith to protect our network.

Troopers08, 23.-24.03.08 Munich, Germany

Content

Global Voith IT Organisation

Self defending networks

Best Practise @ Voith

IT Security Organisation

Technical Basis

Security Processes

Conclusion

Author

Rolf Strehle

CEO ditis Systeme

CISO Voith AG

ISO27001 Auditor

ditis Systeme

The Security Company

Carl-Schwenk-Str. 4-6

D-89522 Heidenheim

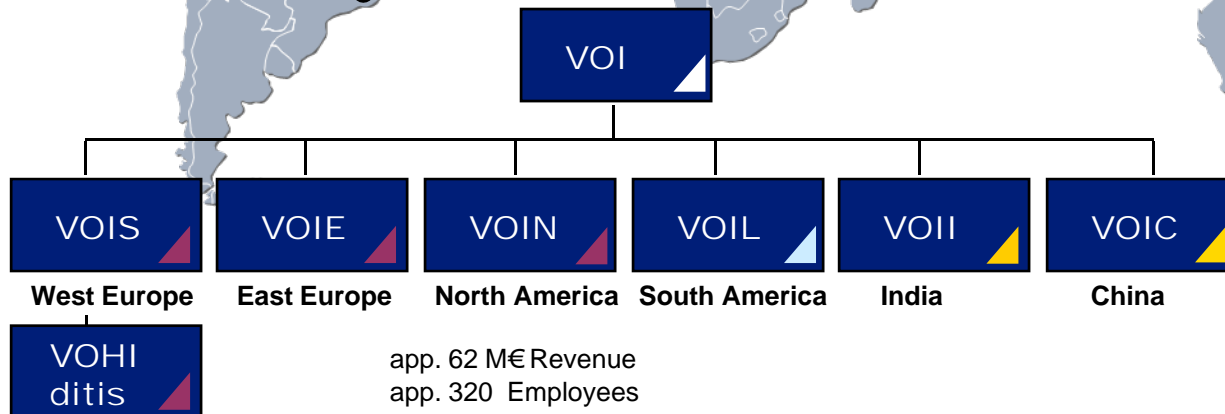
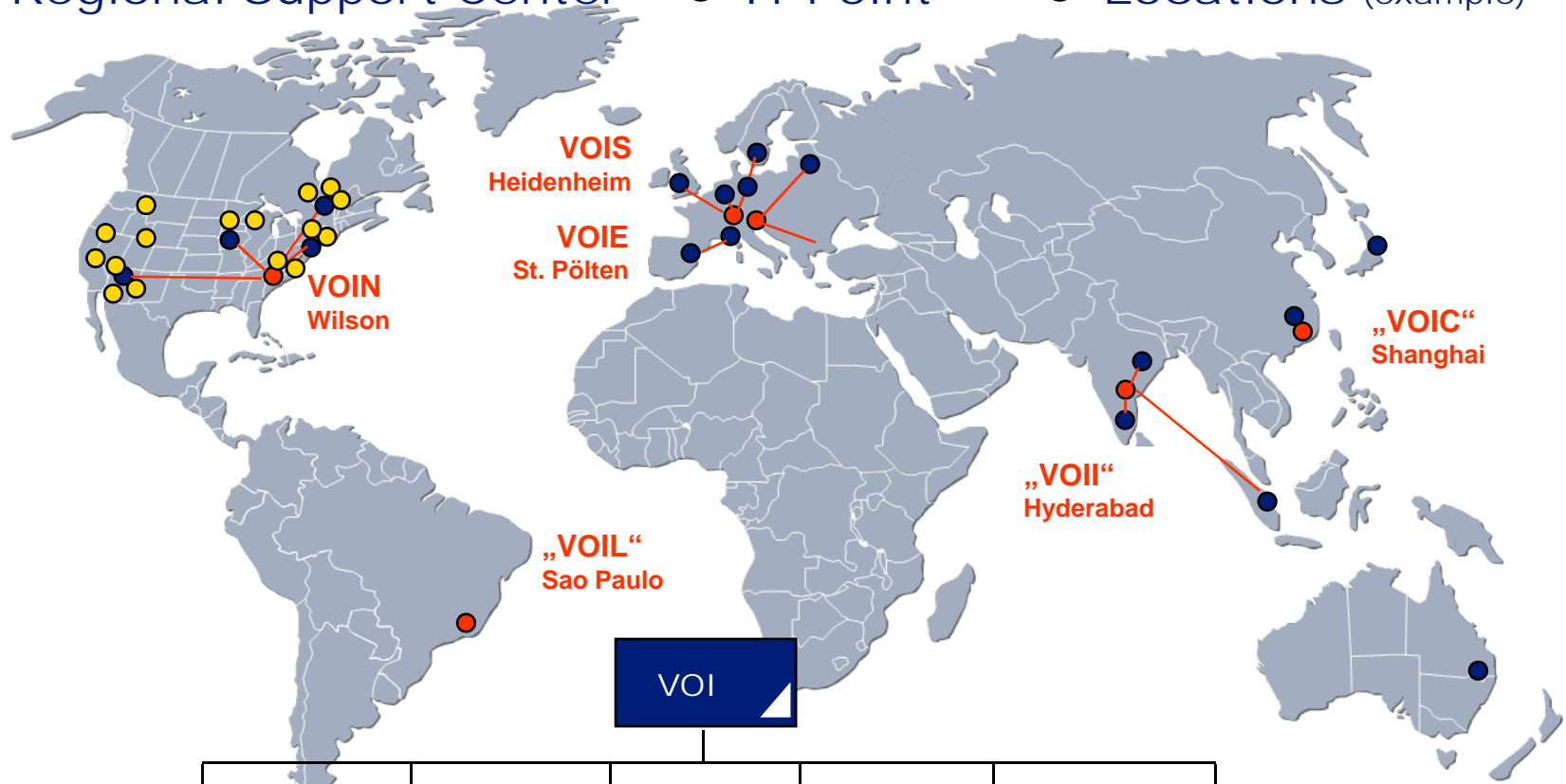
Phone: +49 7321 91770

E-Mail: rolf.strehle@ditis.de

Ein Unternehmen des Voith Konzerns

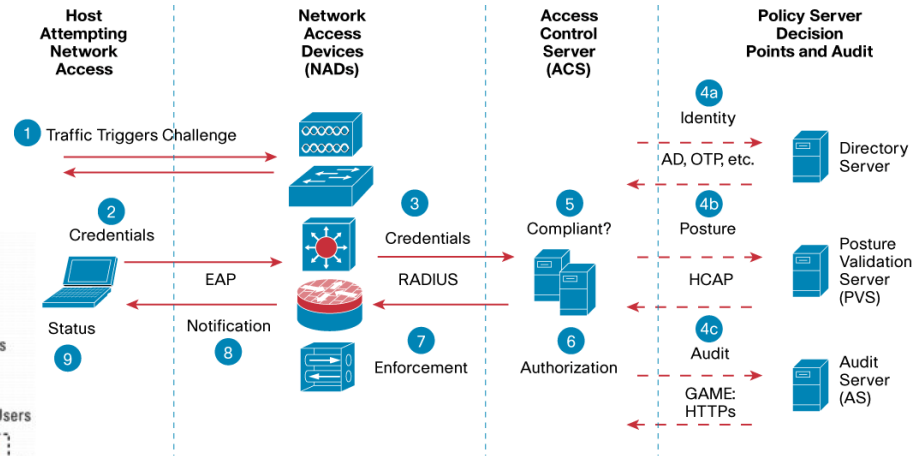
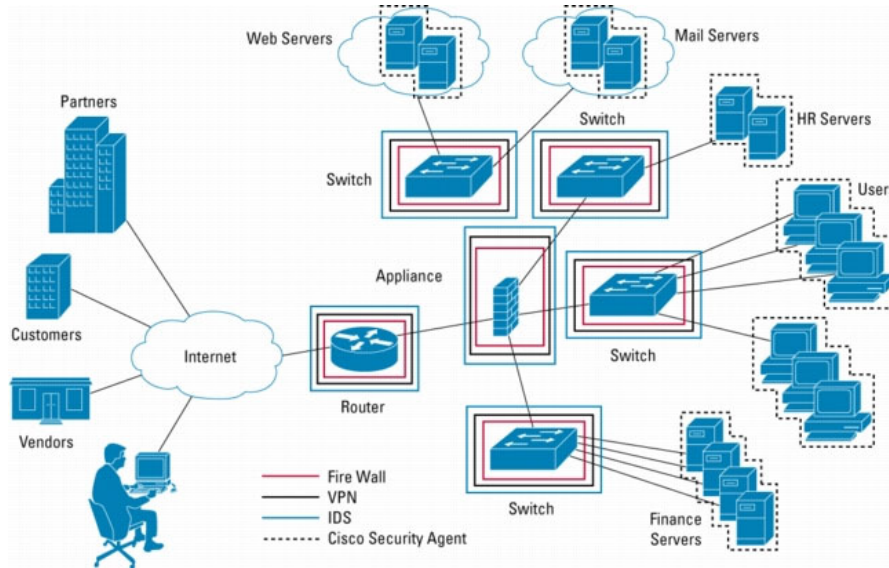
Global Voith IT Organisation

- Regional Support Center
- IT-Point
- Locations (example)



app. 62 M€ Revenue
app. 320 Employees

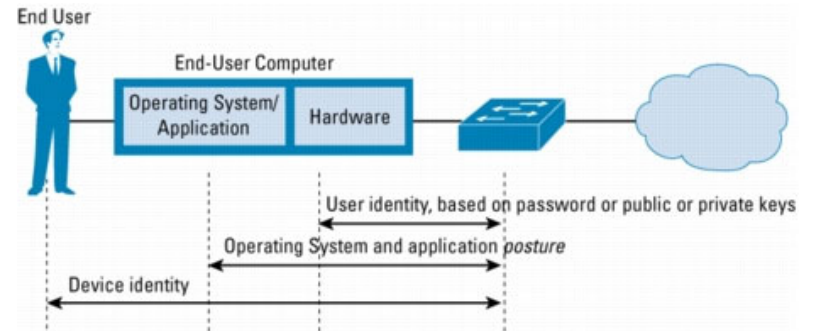
Self defending networks What and Why



Status: Result of host's interrogation determines access to network: Full access, limited access, no access, quarantined access

Cisco:
Self Defending Networks
Network Admission Control (NAC)

Microsoft:
Network Access Protection (NAP)



Because NAC represents an emerging category of security products, its definition is both evolving and controversial. The overarching goals of the concept can be distilled to:

- **Mitigation of zero-day attacks**

The key value proposition of NAC solutions is the ability to prevent end-stations that lack antivirus, patches, or host intrusion prevention software from accessing the network and placing other computers at risk of cross-contamination of network worms.

- **Policy enforcement**

NAC solutions allow network operators to define policies, such as the types of computers or roles of users allowed to access areas of the network, and enforce them in switches, routers, and network middleboxes.

- **Identity and access management**

Where conventional IP networks enforce access policies in terms of IP addresses, NAC environments attempt to do so based on authenticated user identities, at least for user end-stations such as laptops and desktop computers.

Source: Wikipedia

- **Pre-admission and post-admission**

There are two prevailing design philosophies in NAC, based on whether policies are enforced before or after end-stations gain access to the network. In the former case, called pre-admission NAC, end-stations are inspected prior to being allowed on the network. A typical use case of pre-admission NAC would be to prevent clients with out-of-date antivirus signatures from talking to sensitive servers. Alternatively, post-admission NAC makes enforcement decisions based on user actions, after those users have been provided with access to the network.

- **Agent versus agentless**

The fundamental idea behind NAC is to allow the network to make access control decisions based on intelligence about end-systems, so the manner in which the network is informed about end-systems is a key design decision. A key difference among NAC systems is whether they require agent software to report end-system characteristics, or whether they use scanning and network inventory techniques to discern those characteristics remotely.

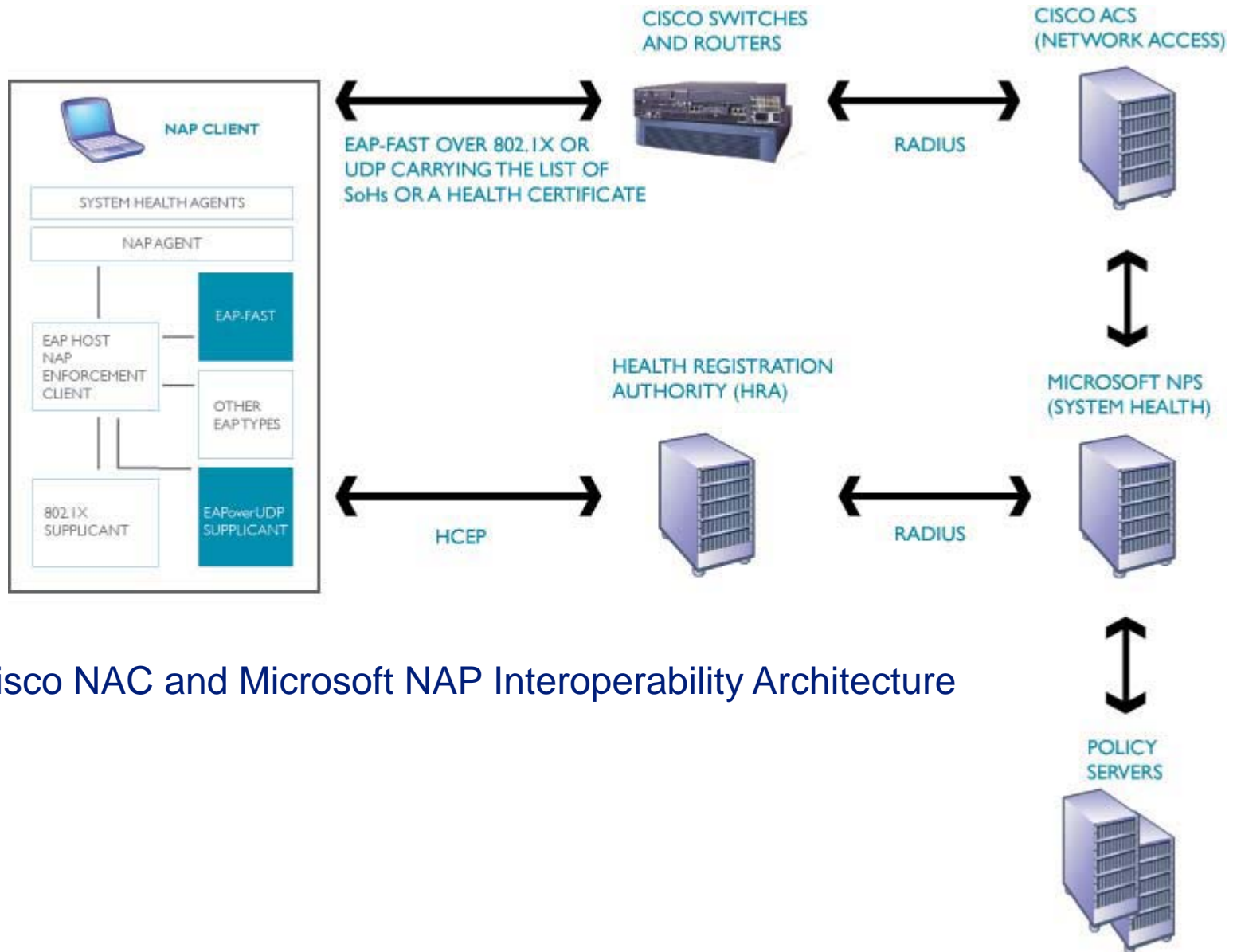
- **Out-of-band versus inline**

In some out-of-band systems, agents are distributed on end-stations and report information to a central console, which in turn can control switches to enforce policy. In contrast the inline solutions can be single-box solutions which act as internal firewalls for access-layer networks and enforce the policy. Out-of-band solutions have the advantage of reusing existing infrastructure; inline products can be easier to deploy on new networks, and may provide more advanced network enforcement capabilities, because they are directly in control of individual packets on the wire. However, there are products that are agentless, and have both the inherent advantages of easier, less risky out-of-band deployment, but use techniques to provide inline effectiveness for non-compliant devices, where enforcement is required.

- **Remediation, quarantine and captive portals**

Network operators deploy NAC products with the expectation that some legitimate clients will be denied access to the network (if users never had out-of-date patch levels, NAC would be unnecessary). Because of this, NAC solutions require a mechanism to remediate the end-user problems that deny them access.

Self defending networks Standards?



Cisco NAC and Microsoft NAP Interoperability Architecture

- We do not use NAC

As for today, there are a lot of good reasons not to rely on self defending networks:

Expensive

Incompatible

Complex

No mature technology

The “real thread” is elsewhere (Social Engineering)

- We do defend our own network

We use the combination of existing and proven technologies to defend our worldwide corporate network.

- We enable people to think “IT security”

The most complex thread is people – so we have to enable our own staff to face this reality.

So how do we achieve this?

3 Tier Security Model

IT Security Organisation

Group Directive
01/03

Voith CERT

Compliance

- ISO 27001
- BDSG
- other national regulations

Security Processes

IT Security Management

Incident Management

Change Management

Systems Monitoring

Security Audits

Risk Management

Awareness

Technical Basis

VOI Security
Toolbox

IT-Security
Infrastructure

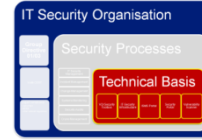
ISMS Portal

Security Portal

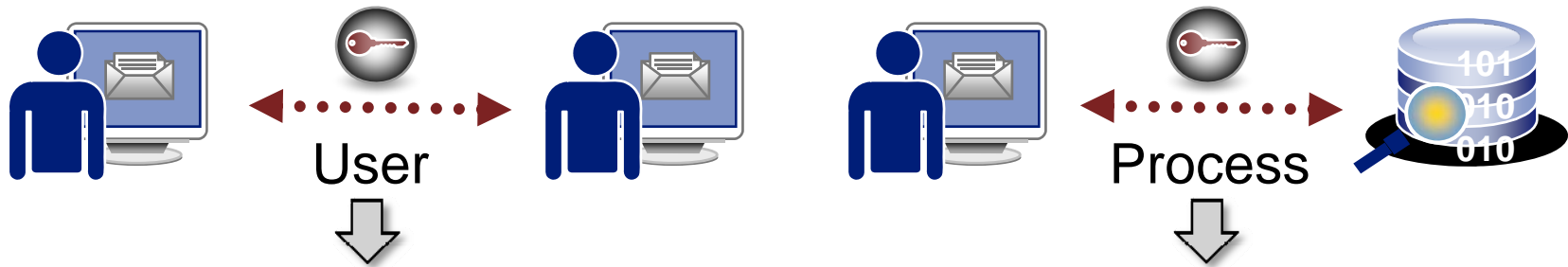
Vulnerability
Scanner

IT Security Technical Basis

Voith Security Toolbox



Voith IT Solutions



Group Directive 01/03
ISO 27001 IT-Risk Management



Secure Communication Tools

VOI E-Mail Security (PGP, S/Mime), Secure Data Exchange Portal
SFTP, SAP-cFolders, Anomaly Detection System, Citrix Secure Gateway,
Secure-Web Applications (Reverse Proxy), V-Key, VPN

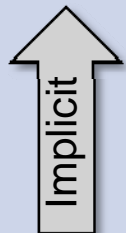
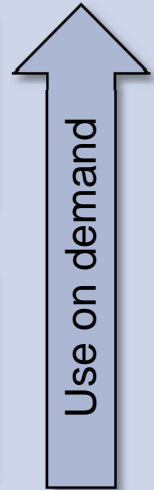


Secure Data Storage Tools

VOIS File Security, File Encryption (PGP), Digital Rights Management,
Notebook-Security (SafeGuard), CD-Encryption, USB-Stick with
Fingerprint, PDA File-Encryption

Basic Security Tools

Firewall, SPAM-Filter, Anti-Virus, Web-Content Filter, WLAN-Encryption, VPN
PSIP, ISMS
Secure Administration, Anomaly-Detection-System,
Public Key Infrastructure (PKI)

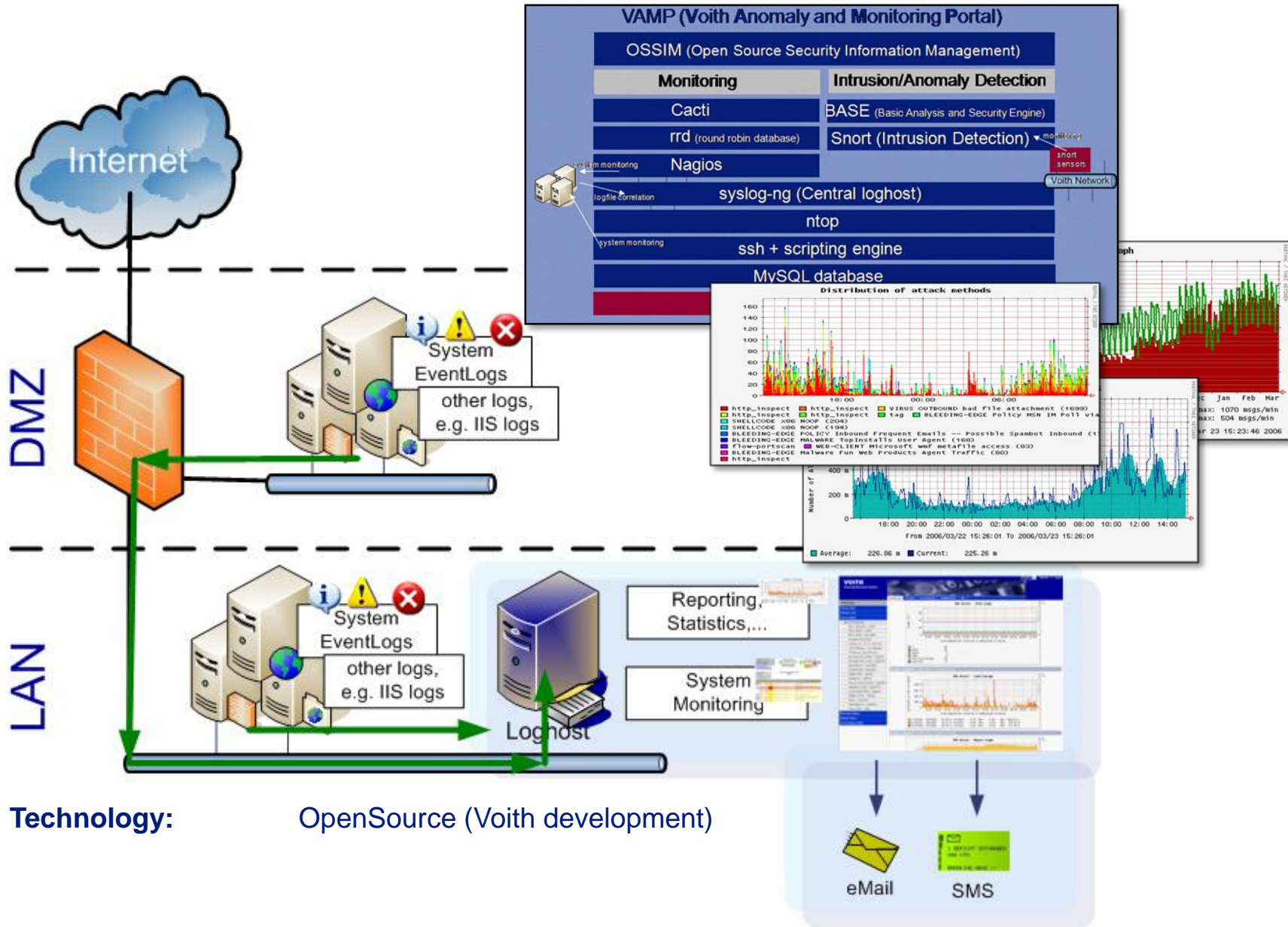


IT Security Technical Basis

Voith Anomaly Detector



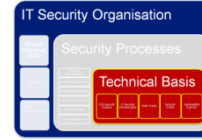
Voith IT Solutions



Technology: OpenSource (Voith development)

IT Security Technical Basis

Voith Monitoring Tool



Voith IT Solutions



Monitoring Team

The screenshot shows the 'Basic Analysis and Security Engine (BASE) vids03' interface. It includes a navigation menu on the left, a search bar, and a table of alerts. The table columns are ID, Signature, Timestamp, Source Address, Dest. Address, and Layer 4 Proto.

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(3-3640359)	[local] [snort] BLEEDING-EDGE POLICY TLS/SSL Encrypted Application Data on Unusual Port	2007-04-01 00:17:07	172.23.148.52:4867	172.21.50.94:5061	TCP
#1-(3-3640360)	[local] [snort] BLEEDING-EDGE POLICY TLS/SSL Encrypted Application Data on Unusual Port	2007-04-01 00:17:11	172.27.250.50:2381	172.21.41.155:4670	TCP
#2-(3-3640369)	[local] [snort] BLEEDING-EDGE POLICY TLS/SSL Encrypted Application Data on Unusual Port	2007-04-01 00:17:51	172.23.163.15:2381	172.21.41.155:1795	TCP
#3-(3-3640371)	[snort] xlink2state: X-Link2State length greater than 1024	2007-04-01 00:18:11	172.21.49.196:22282	172.23.187.202:25	TCP

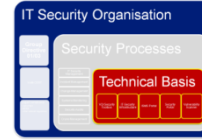
The screenshot shows a time-series chart of alerts. The x-axis is labeled 'TIME' and shows dates from 4/18 to 4/23. The y-axis shows the number of alerts, with a peak around 4/22. The chart includes a legend for 'Peak' and 'Average'.

Resource & Control Action Key:
Resource: ~ mrgu0115.euro1.voith.net

04/18/2007 02:38:00 PM to 04/23/2007 02:38:00 PM
- Edit Range...

IT Security Technical Basis

Voith Monitoring Tool



Voith IT Solutions



Monitoring Team

The screenshot shows the Nagios MRG LAN interface. On the left, there are sections for 'Platform Services Health' and 'Deployed Servers Health', both showing 'Avail' status. The 'Indicator Charts' section displays three graphs: 'Free Memory (Linux)', 'Free Memory (+ buffers/cache) (Linux)', and 'Load Average 5 Minutes (Linux)'. The 'All Metrics' section lists various metrics like Availability, Free Memory, and Swap Used.

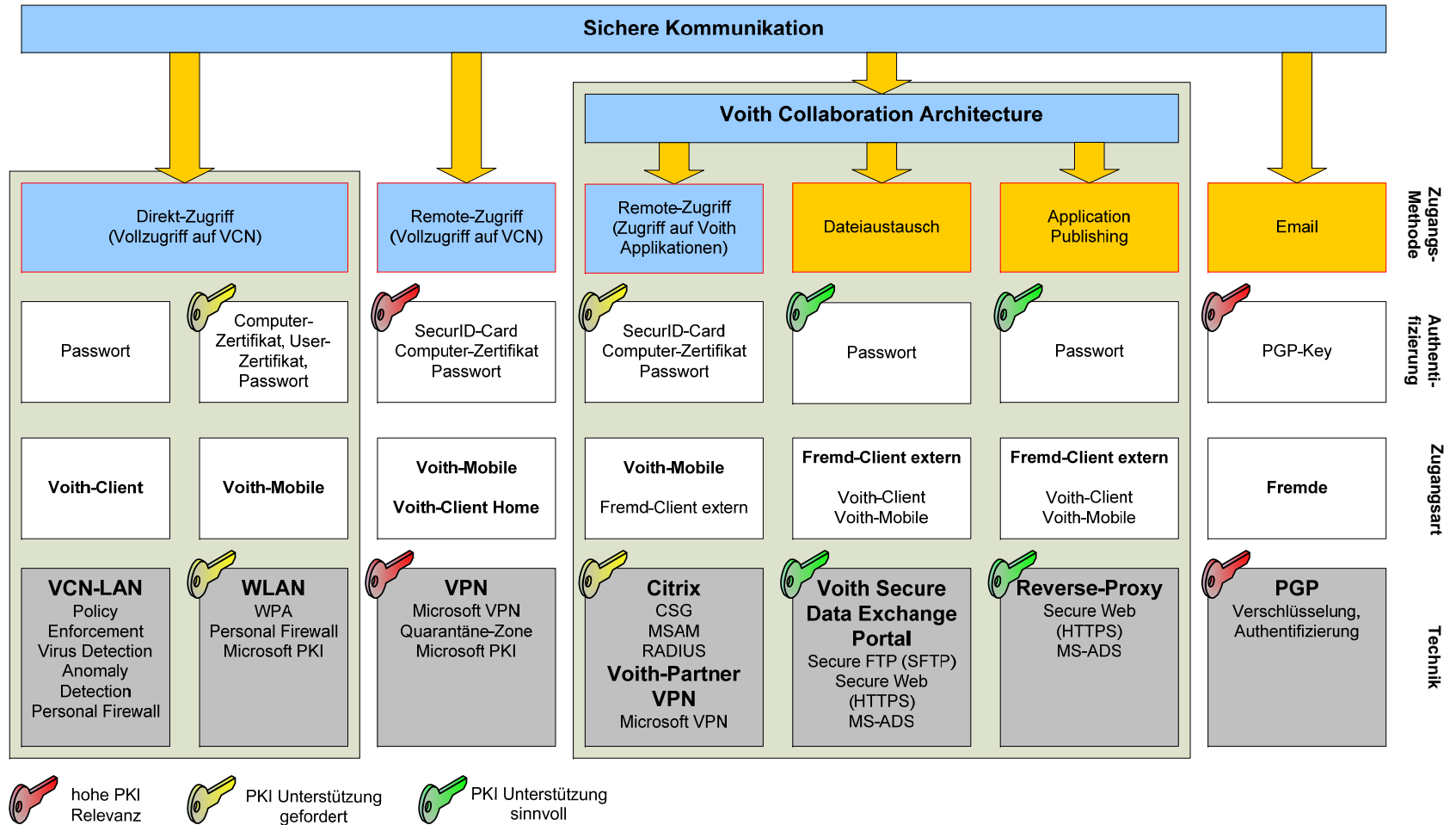
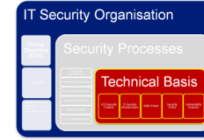
The screenshot shows the Nagios ILX prod interface. It features a 'Current Network Status' box, 'Host Status Totals' (Up: 0, Down: 0, Unreachable: 0, Pending: 3), and 'Service Status Totals' (Ok: 5, Warning: 0, Unknown: 0, Critical: 4, Pending: 11). Below these is a table of 'Service Status Details For All Hosts'.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
nbth0503	Usage Memory	CRITICAL	2007-04-23 14:29:55	0d 0h 6m 6s	3/3	CRITICAL MEM: usage 100.14 % - 3674596 Kbytes of 3669476 Kbytes
nbth0504	Usage Memory	CRITICAL	2007-04-23 14:31:27	0d 0h 0m 34s	3/3	CRITICAL MEM: usage 99.90 % - 3993108 Kbytes of 3997176 Kbytes
nbth0507	Usage Memory	CRITICAL	2007-04-23 14:30:56	0d 1h 15m 5s	3/3	CRITICAL MEM: usage 109.69 % - 3735536 Kbytes of 3405688 Kbytes
nbth0508	Usage Memory	CRITICAL	2007-04-23 14:30:37	0d 0h 31m 24s	3/3	CRITICAL MEM: usage 103.85 % - 3536840 Kbytes of 3405688 Kbytes
nbth0501	Usage Memory	WARNING	2007-04-23 14:30:57	0d 0h 1m 4s	3/3	WARN MEM: usage 98.31 % - 3607594 Kbytes of 3669476 Kbytes
nbth0502	Usage Memory	WARNING	2007-04-23 14:30:54	0d 0h 2m 7s	2/3	WARN MEM: usage 91.27 % - 3349296 Kbytes of 3669476 Kbytes
nbth0520	Diskspace hfd1 V/S	WARNING	2007-04-23 14:29:50	0d 12h 24m 25s	3/3	WARNING: diskusage on drive O: is 90%
nbth0541	Diskspace hfd1 V/S	WARNING	2007-04-23 14:30:59	0d 12h 23m 2s	3/3	WARNING: diskusage on drive O: is 94%
nbth0681	Diskspace hfd1 V/S	WARNING	2007-04-23 14:30:34	0d 2h 17m 35s	3/3	WARNING: diskusage on drive O: is 90%
nbth0222	Diskspace hfd1	OK	2007-04-23 14:31:40	5d 13h 13m 15s	1/3	OK: diskusage on drive C: is 73%
nbth0222	Ping HDH	OK	2007-04-23 14:29:55	5d 13h 22m 0s	1/3	PING OK - Packet loss = 0%, RTA = 0.77 ms
nbth0222	Process DataProtector	OK	2007-04-23 14:31:46	14d 4h 7m 9s	1/3	OK: Process Count of Omnit.exe : is 1
nbth0223	CPU Load	OK	2007-04-23 14:30:33	3d 11h 18m 14s	1/3	OK: CPU load is 0%

IT Security Technical Basis

Secure Communication

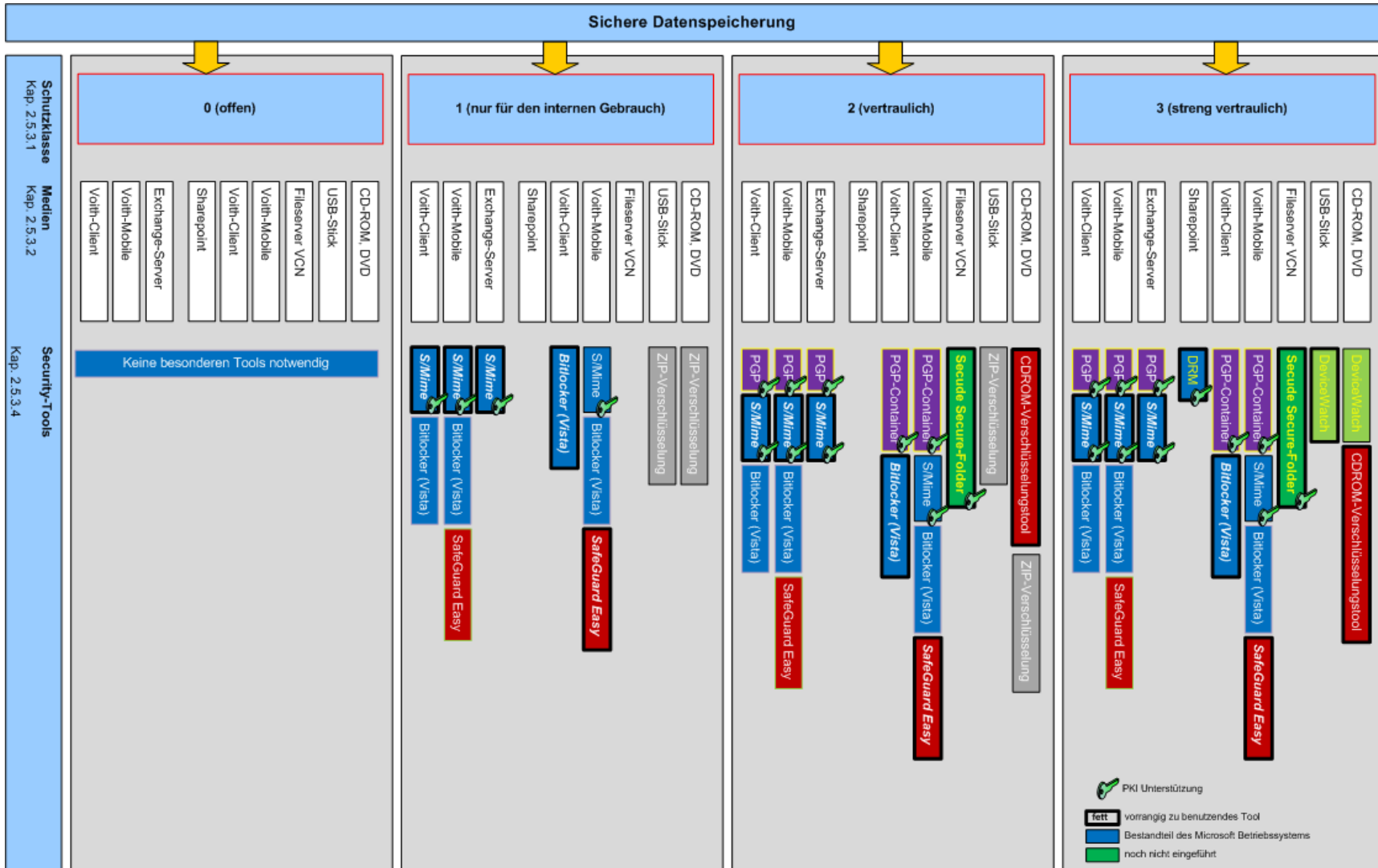
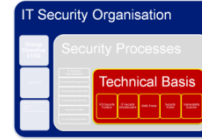
Access Management



IT Security Technical Basis

Secure Data Storage

Data Leakage Prevention



IT Security Organisation

Group
Directive
01/03

voithCERT

Legal Compliance
+ ISO 27001
+ BSI
+ other national regulations

Security Processes

IT Security
Management

Incident Management

Change Management

Systems Monitoring

Security Audits

Risk Management

Technical Basis

VOI Security
Toolbox

IT-Security
Infrastructure

ISMS Portal

Security
Portal

Vulnerability
Scanner

IT Security Processes Vulnerability Management



Voith IT Solutions

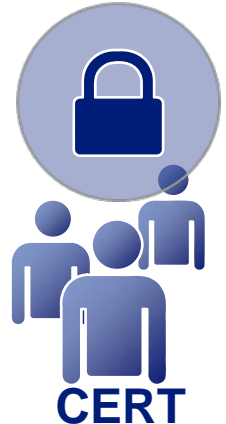
Goal:

Proactive health check of all network components in the Voith corporate net

Solution:

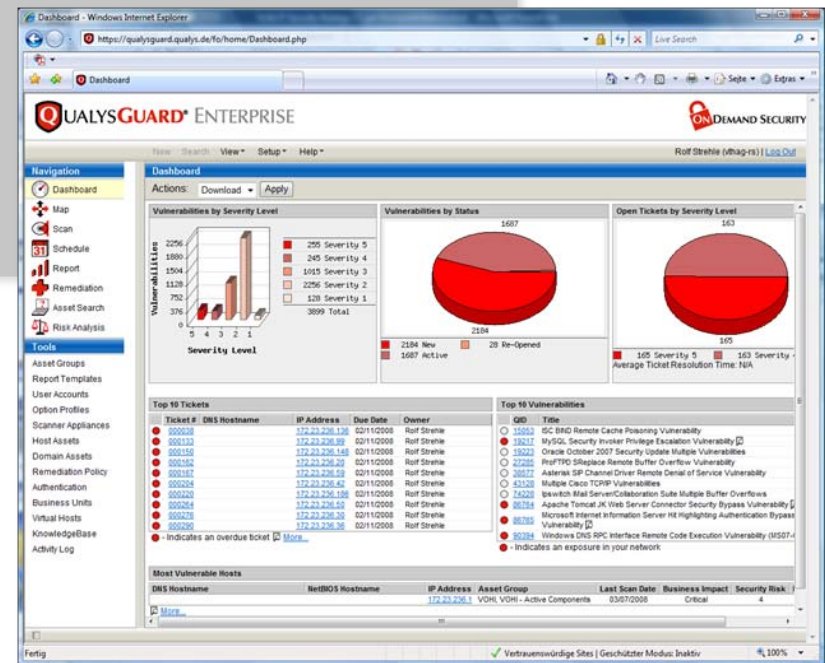
Vulnerability Scanning and Reporting

- Regular network scan (appliance based)
- Regular password quality scan (AD based)
- Integration in existing ITIL and ITSM processes
 - Monthly Reporting
 - Central Monitoring inside IT Security Team



Technology:

Qualys, Nessus



IT Security Processes

Global Monitoring



Voith IT Solutions



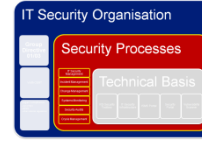
- 24x7 hours monitoring in own global support organisation
- Incident management and trouble shooting
- Pro-active management of defined SLA's

Current Network Status
 Last updated: 2007-06-21 14:30:31 CEST 2007
 Location: 100.200.0.102
 Ping: 100.200.0.102
 CPU: 100.200.0.102

Host Status Totals

Host	Service	Status	Last Check	Duration	Alertmsg	Status Information
100.200.0.102	LDAP Service	WARNING	2007-06-21 14:29:59	30.0s (30s)	CRITICAL: MEM usage 100.00 % - 36700K (80% of 36700K) (MEM)	
100.200.0.102	LDAP Service	WARNING	2007-06-21 14:29:57	30.0s (30s)	CRITICAL: MEM usage 99.76 % - 36618K (80% of 36618K) (MEM)	
100.200.0.102	LDAP Service	WARNING	2007-06-21 14:28:50	30.0s (30s)	CRITICAL: MEM usage 100.00 % - 37000K (80% of 36750K) (MEM)	
100.200.0.102	LDAP Service	WARNING	2007-06-21 14:28:37	30.0s (30s)	CRITICAL: MEM usage 100.00 % - 36888K (80% of 36720K) (MEM)	
100.200.0.102	LDAP Service	WARNING	2007-06-21 14:28:27	30.0s (30s)	WARNING: MEM usage 98.21 % - 36270K (80% of 36750K) (MEM)	
100.200.0.102	LDAP Service	WARNING	2007-06-21 14:28:16	30.0s (30s)	WARNING: MEM usage 91.27 % - 33402K (80% of 36750K) (MEM)	
100.200.0.102	LDAP Service	WARNING	2007-06-21 14:28:10	30.0s (30s)	WARNING: Mem usage 91.00 % - 33270K (80% of 36750K) (MEM)	
100.200.0.102	LDAP Service	WARNING	2007-06-21 14:28:00	30.0s (30s)	WARNING: Mem usage 91.00 % - 33270K (80% of 36750K) (MEM)	
100.200.0.102	LDAP Service	WARNING	2007-06-21 14:28:04	30.0s (30s)	WARNING: Mem usage 91.00 % - 33270K (80% of 36750K) (MEM)	
100.200.0.102	LDAP Service	OK	2007-06-21 14:29:40	30.0s (30s)	OK: Mem usage 91.00 % - 33270K (80% of 36750K) (MEM)	
100.200.0.102	LDAP Service	OK	2007-06-21 14:28:00	30.0s (30s)	OK: Mem usage 91.00 % - 33270K (80% of 36750K) (MEM)	
100.200.0.102	LDAP Service	OK	2007-06-21 14:29:40	30.0s (30s)	OK: Mem usage 91.00 % - 33270K (80% of 36750K) (MEM)	
100.200.0.102	LDAP Service	OK	2007-06-21 14:28:00	30.0s (30s)	OK: Mem usage 91.00 % - 33270K (80% of 36750K) (MEM)	

IT Security Processes Awareness Campaign



Voith IT Solutions

19 | Troopers08 – Self Defending Networks | 23.04.2008



Conclusion

- We have implemented a solid Security Basis for Voith IT worldwide
- We have a basic security framework in place (IT-Risk Management and ISMS according to ISO 27001)
- We have a very comprehensive Security Toolkit to support the business processes of our customers
- The main task is to implement the toolkit and organizational directives in the business processes of our customers
- We do not trust self defending networks – we defend our network!
- Security knowledge is very complex and rapidly changing, therefore we share the knowledge with other companies by outsourcing to www.ditis.de

Thank you!