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

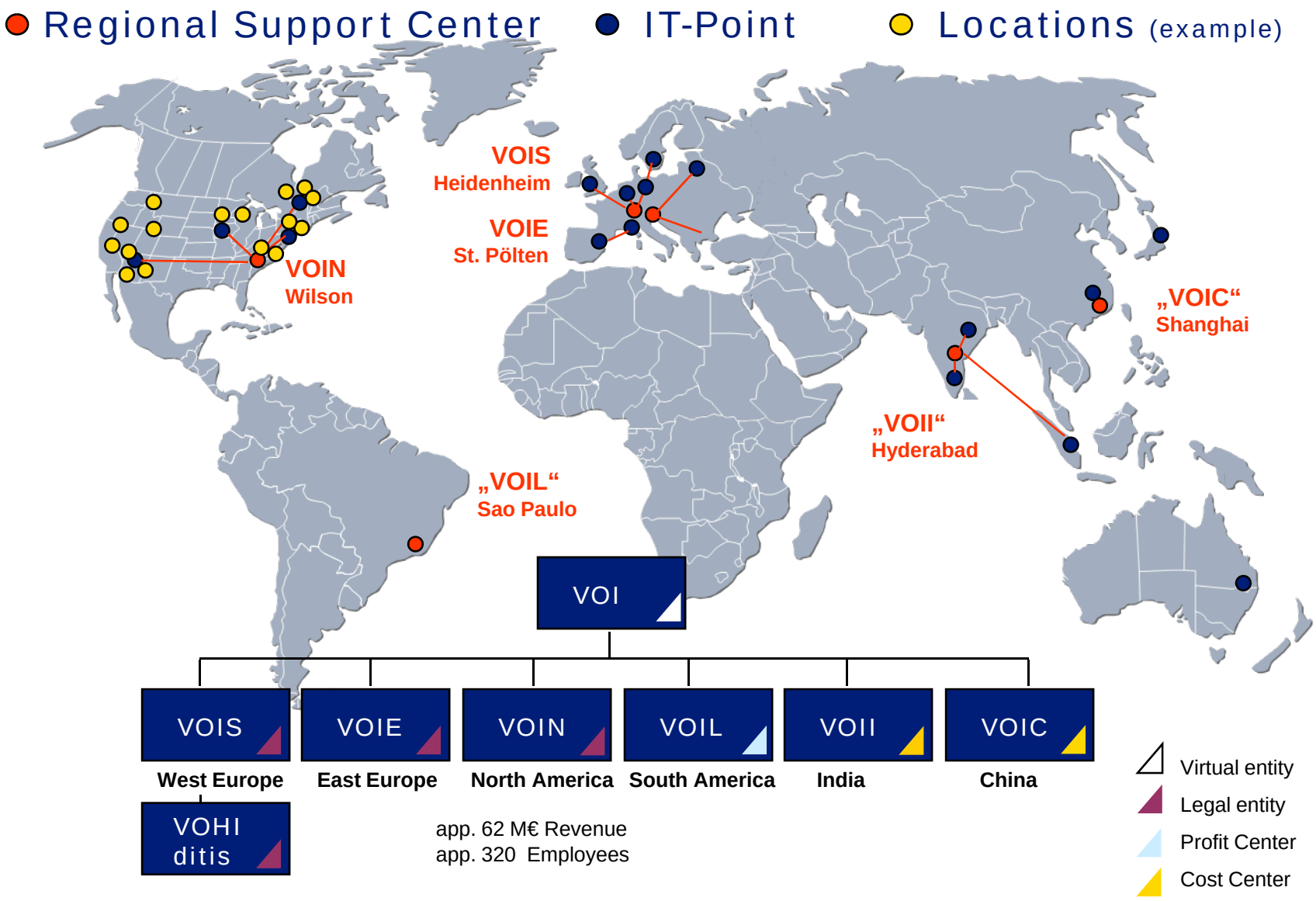
Rolf Strehle
CEO ditis Systeme
CISO Voith AG
ISO27001 Auditor

ditis Systeme
The Security Company
Carl-Schwenk-Str. 4-6
D-89522 Heidenheim

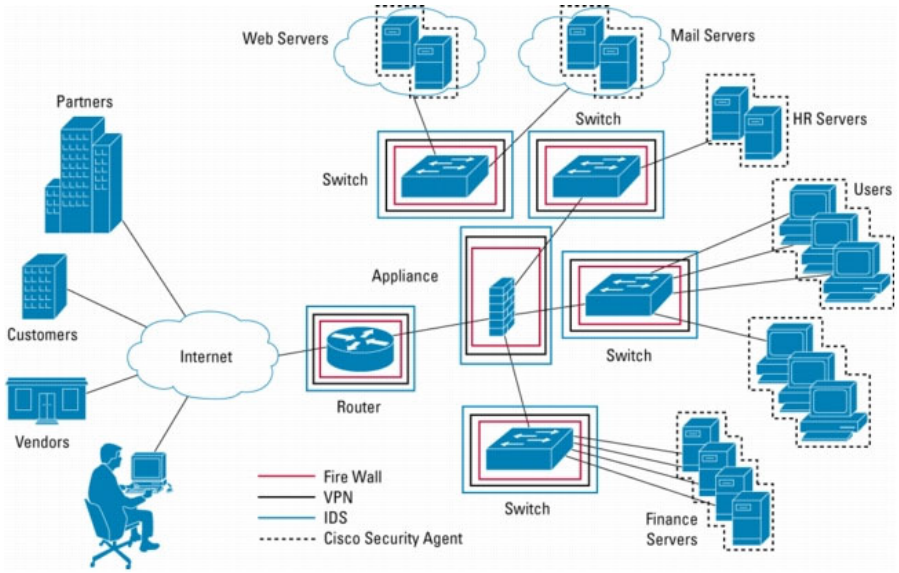
Phone: +49 7321 91770
E-Mail: rolf.strehle@ditis.de

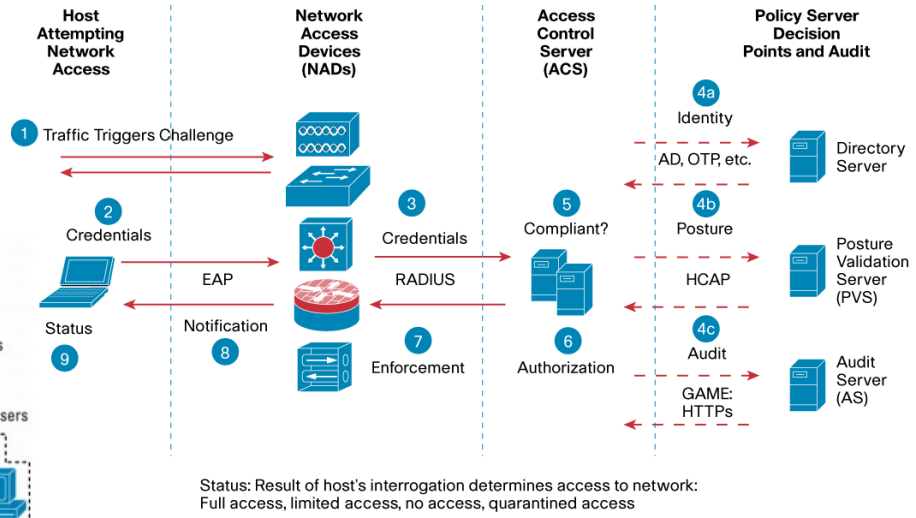
Ein Unternehmen des Voith Konzerns

Global Voith IT Organisation



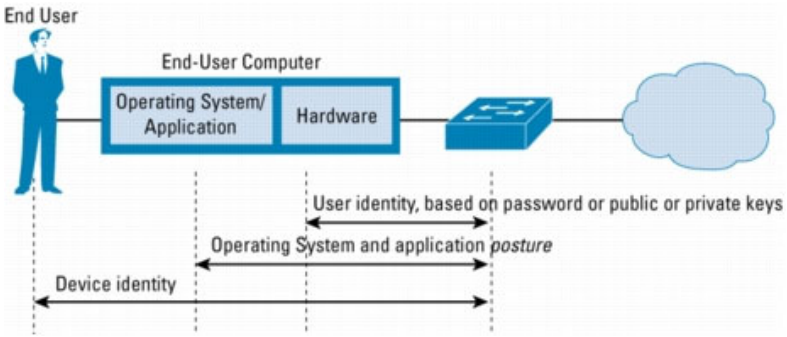
What and Why





Cisco:
Self Defending Networks
Network Admission Control (NAC)

Microsoft:
Network Access Protection (NAP)



Source: Cisco

Goals of NAC

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

Concepts

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.

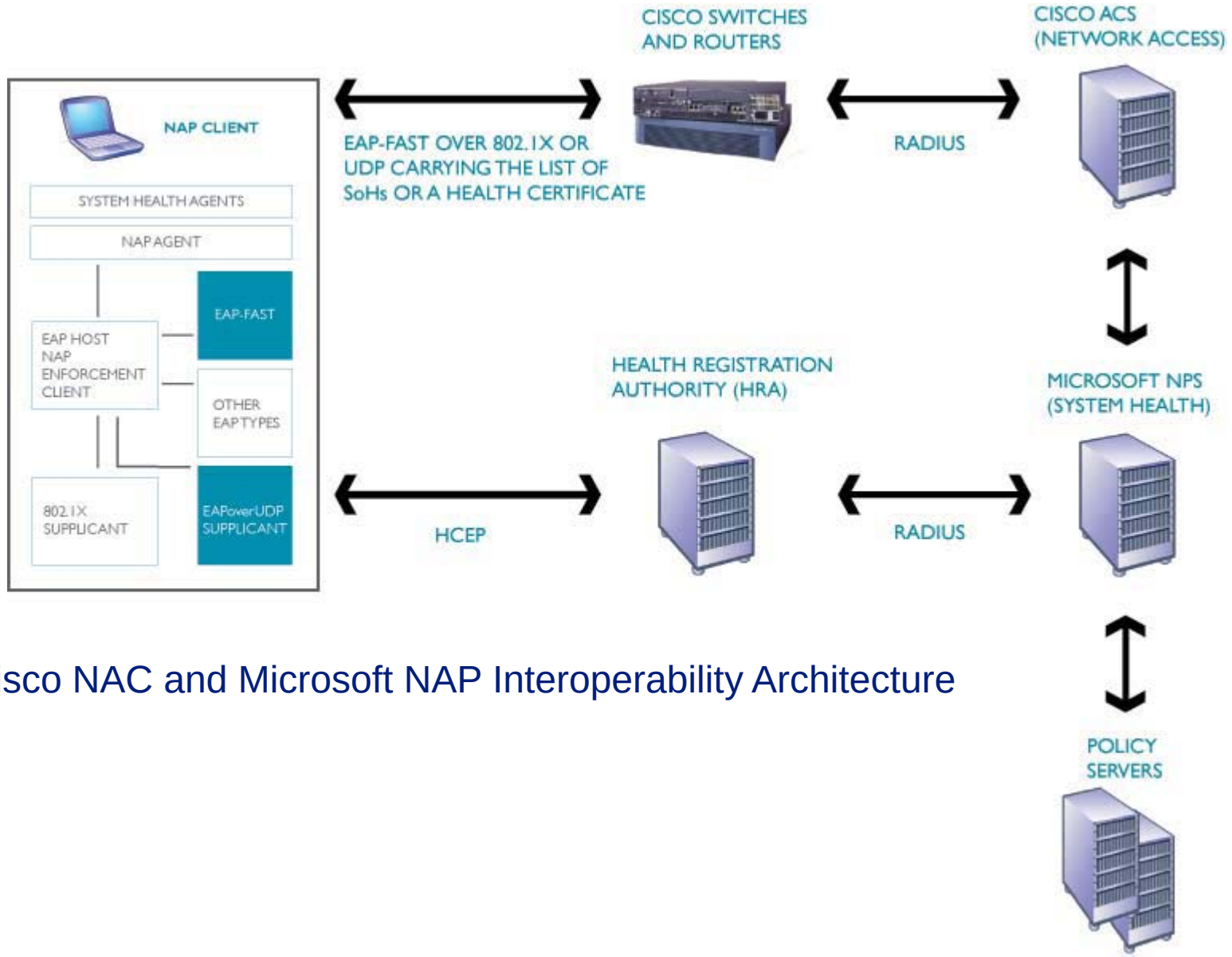
Out-of-band versus inline

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.

Standards?



Cisco NAC and Microsoft NAP Interoperability Architecture

Best Practise @ Voith

- 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.

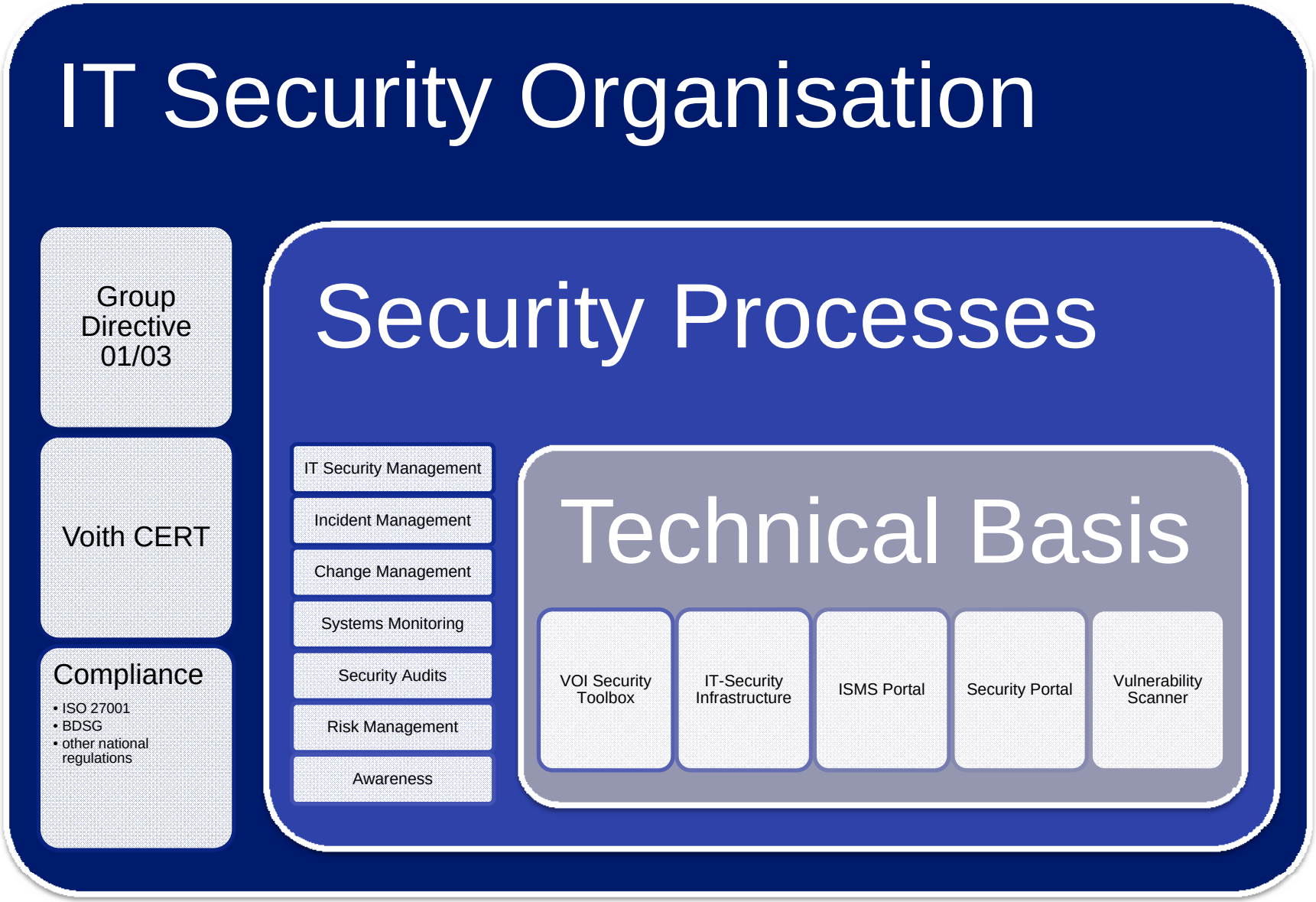
- We enable people to think “IT security”

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

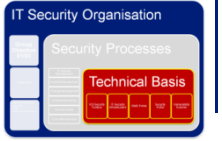
.

So how do we achieve this?

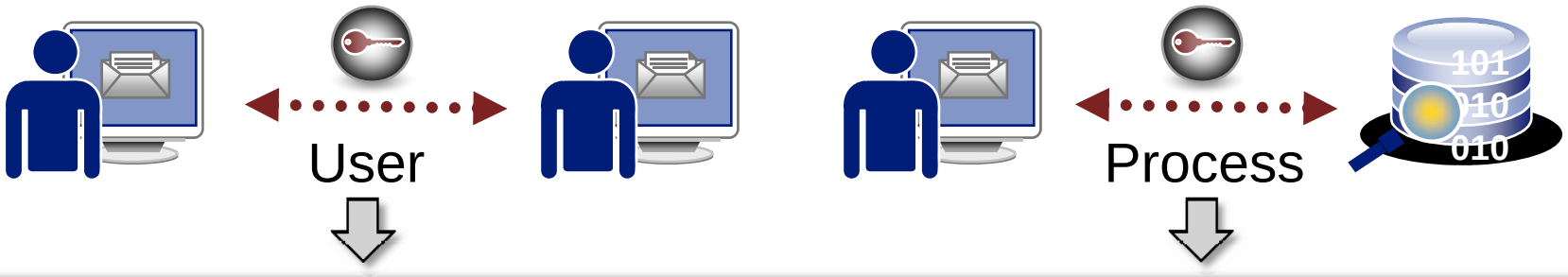
3 Tier Security Model



Voith Security Toolbox



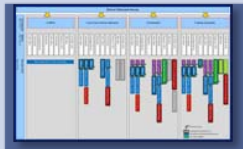
Voith IT Solutions



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

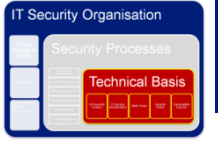
Basic Security Tools

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

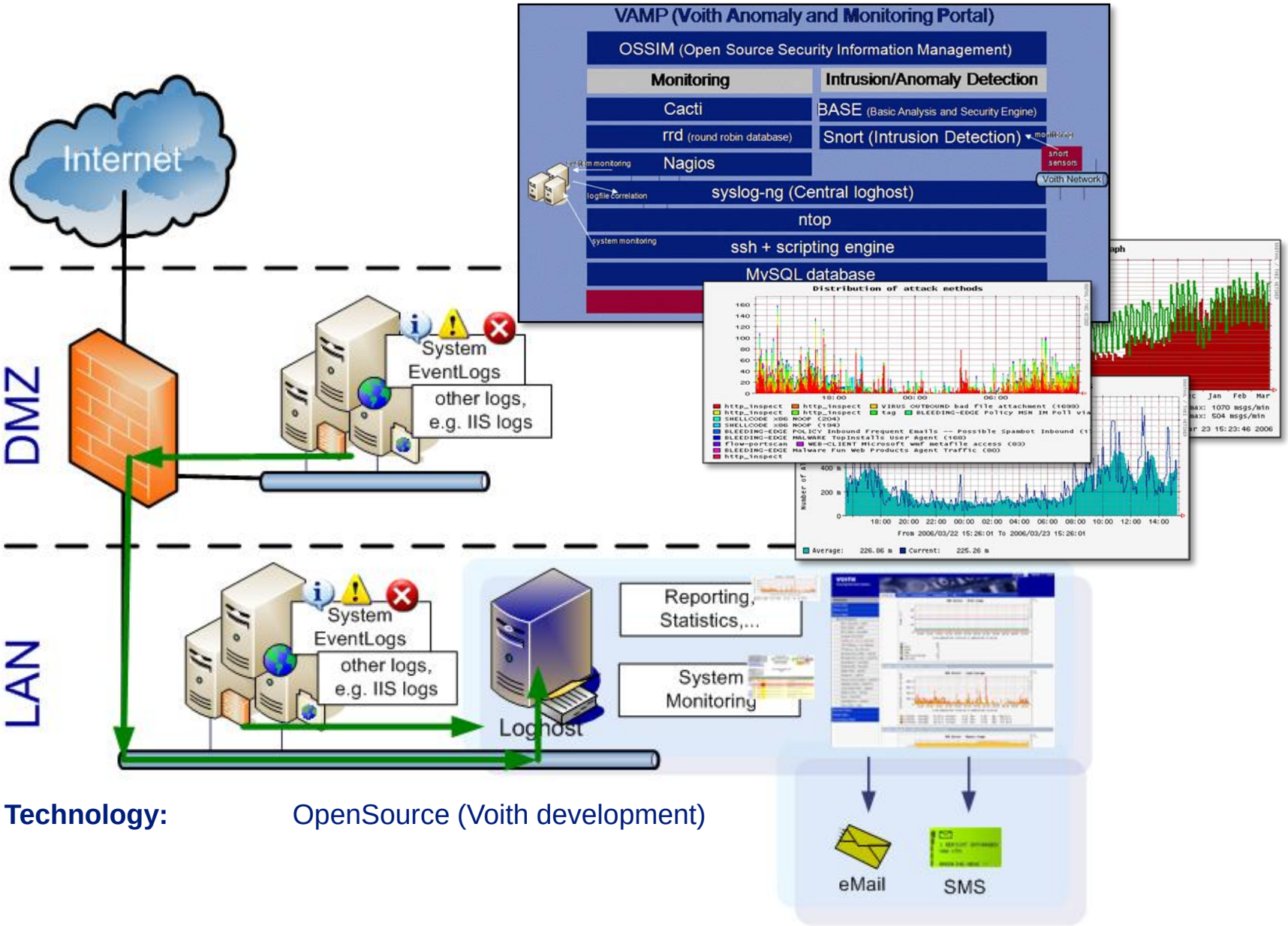
Use on demand

Implicit

Voith Anomaly Detector

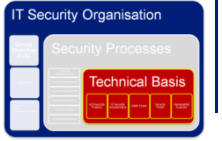


Voith IT Solutions



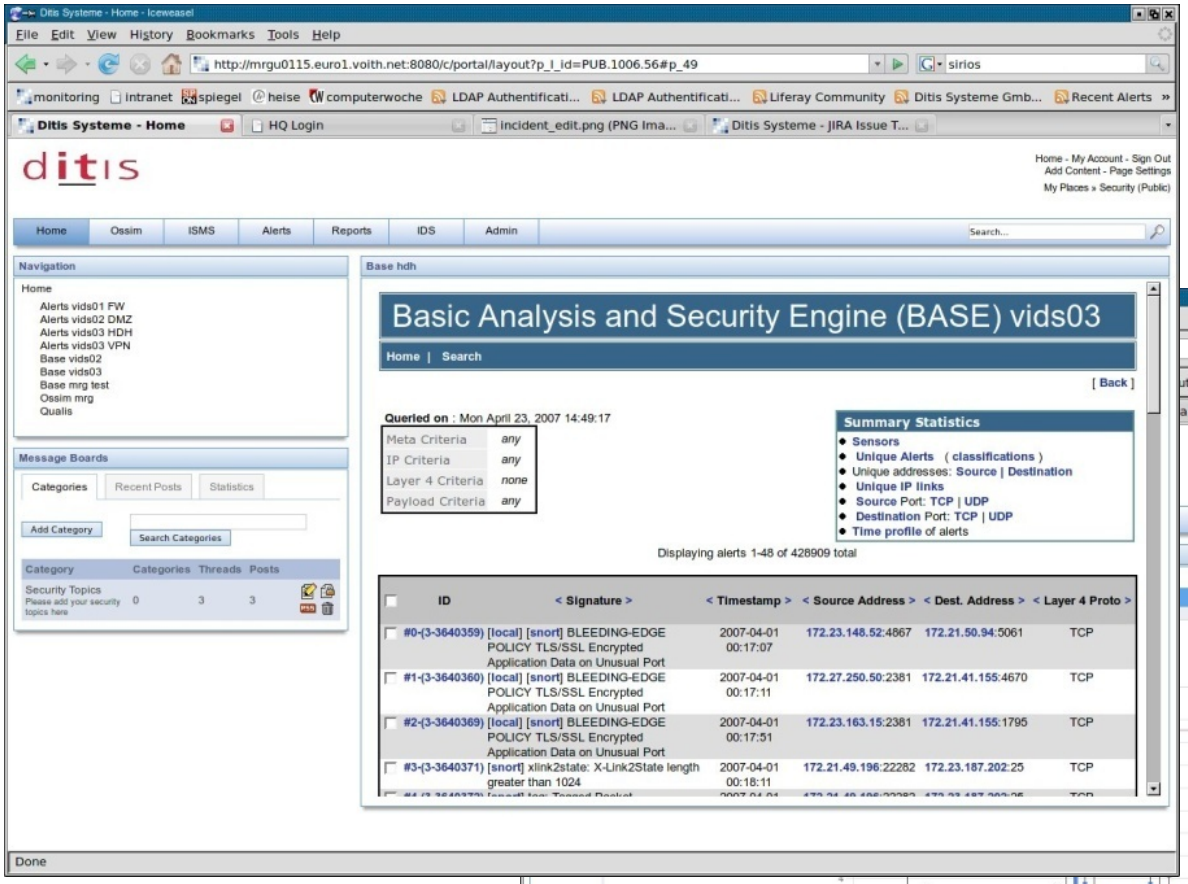
Technology: OpenSource (Voith development)

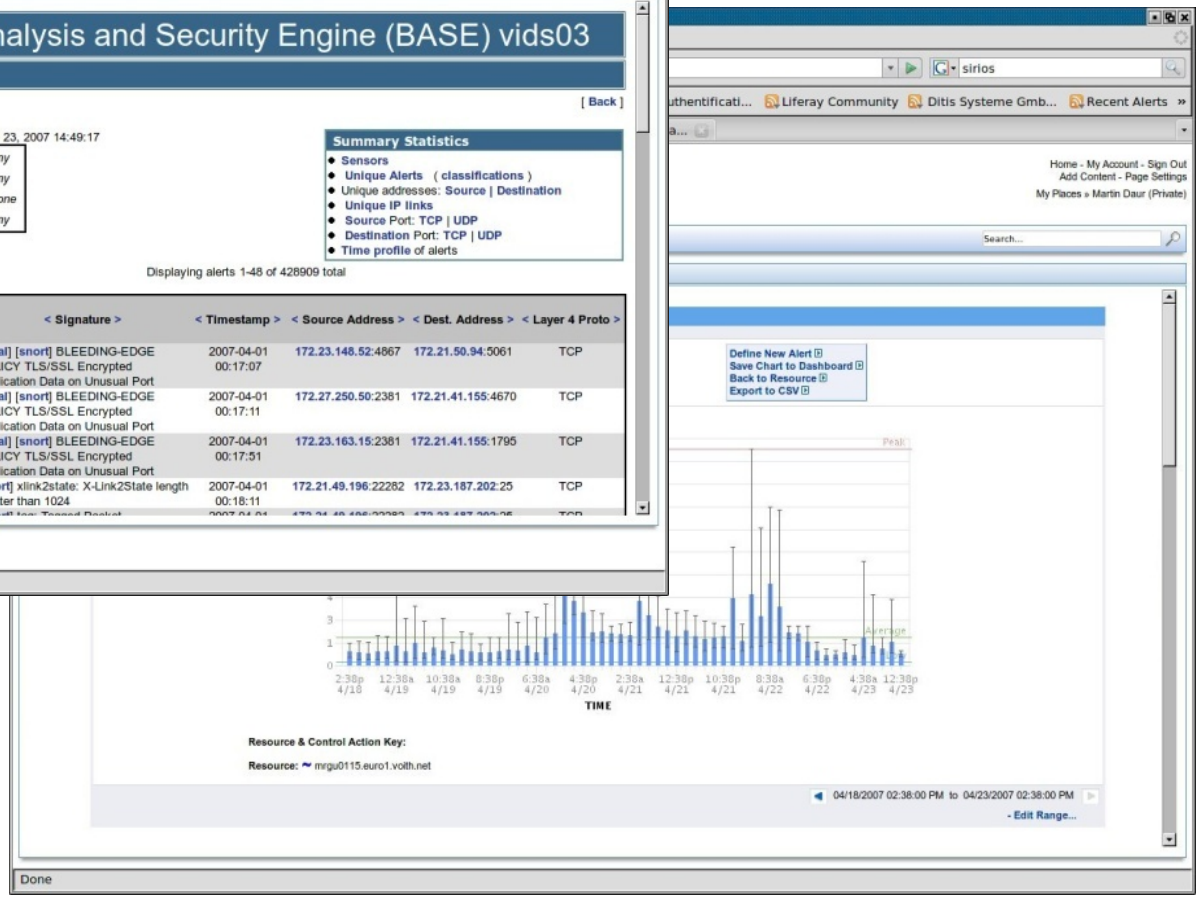
Voith Monitoring Tool



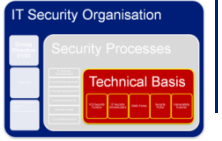
Voith IT Solutions

Monitoring Team



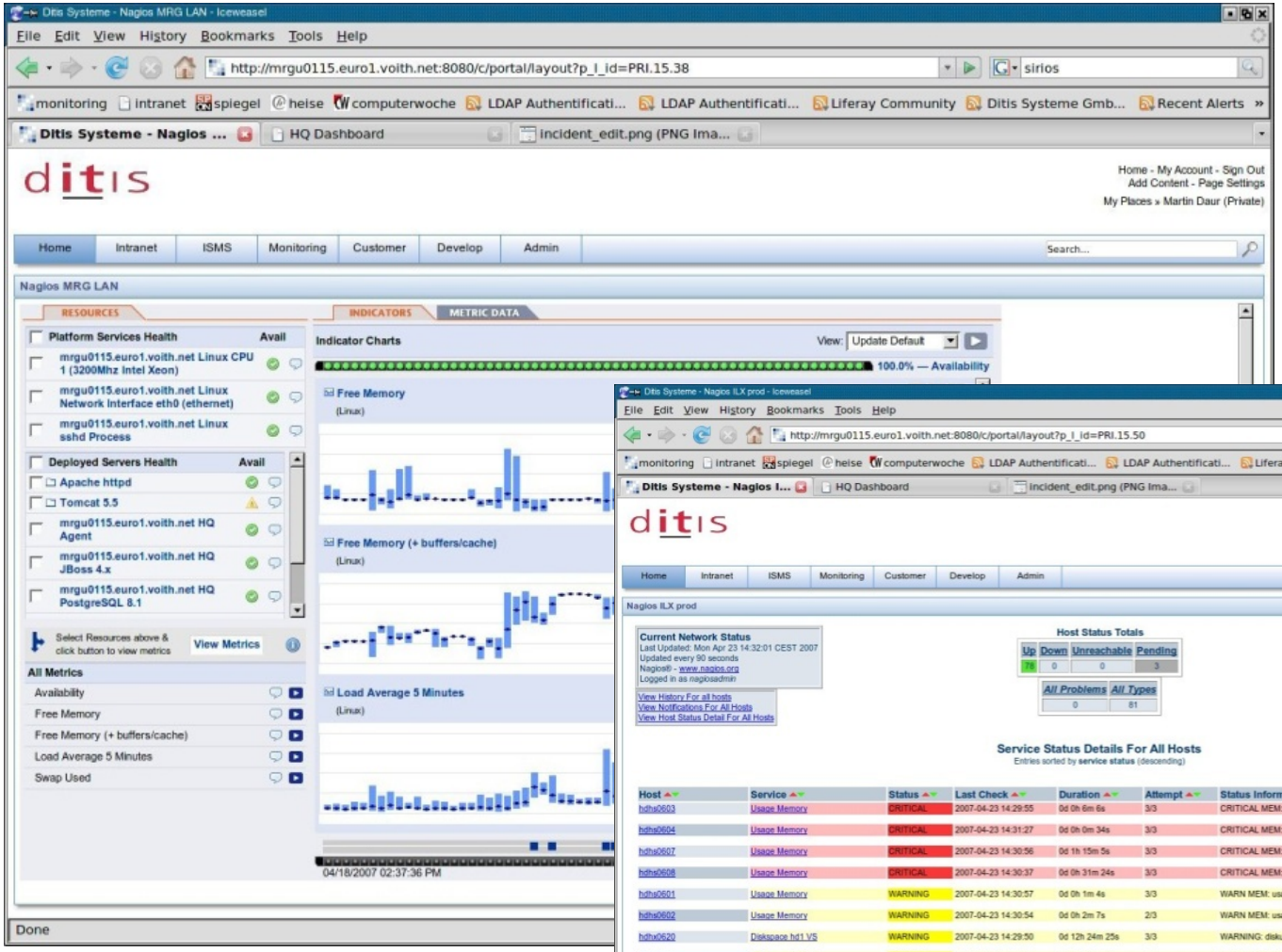


Voith Monitoring Tool



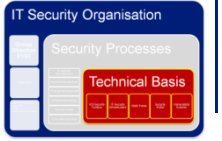
Voith IT Solutions

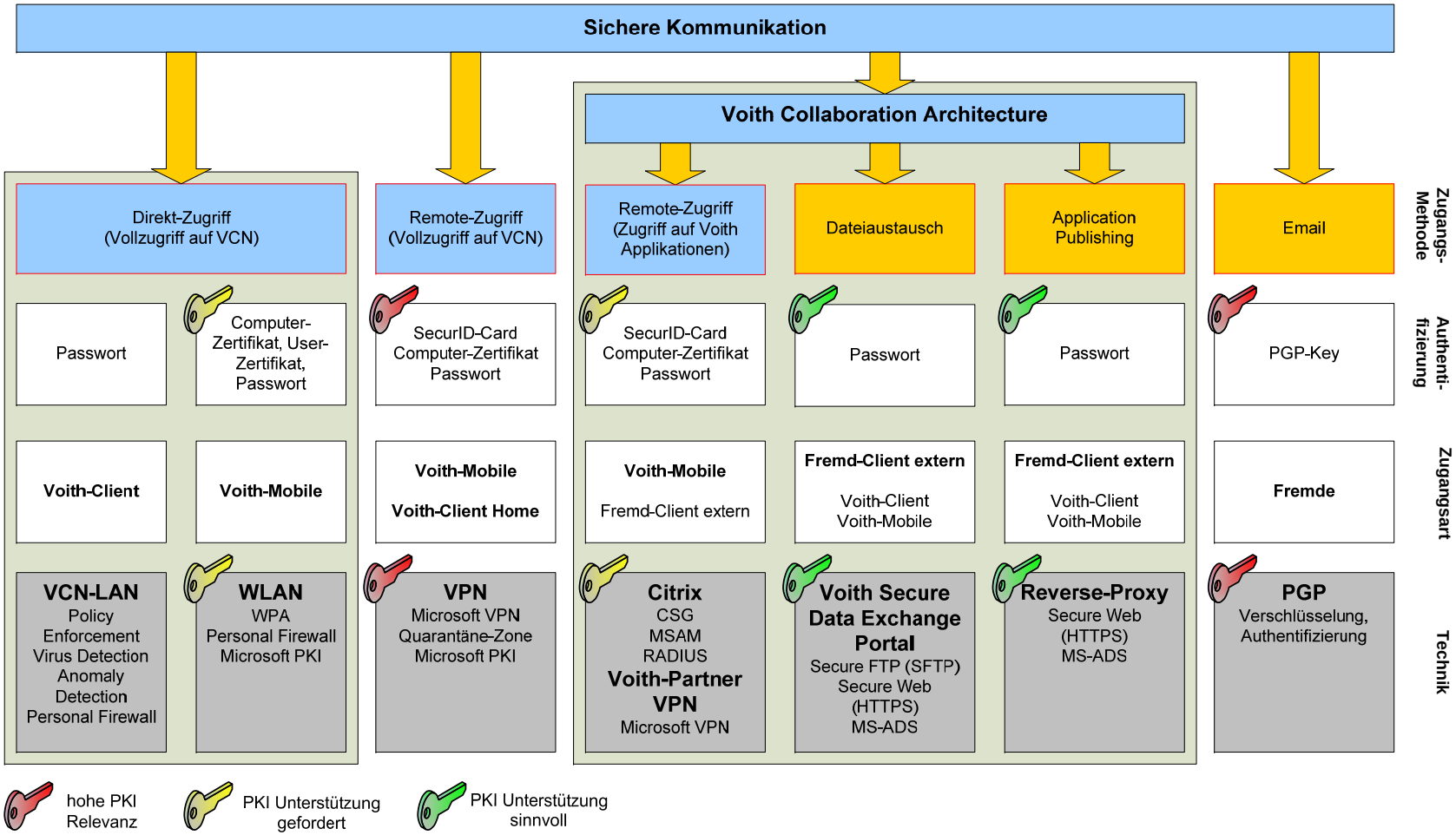
Monitoring Team



Secure Communication

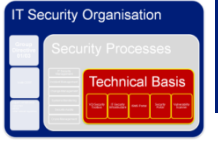
Access Management



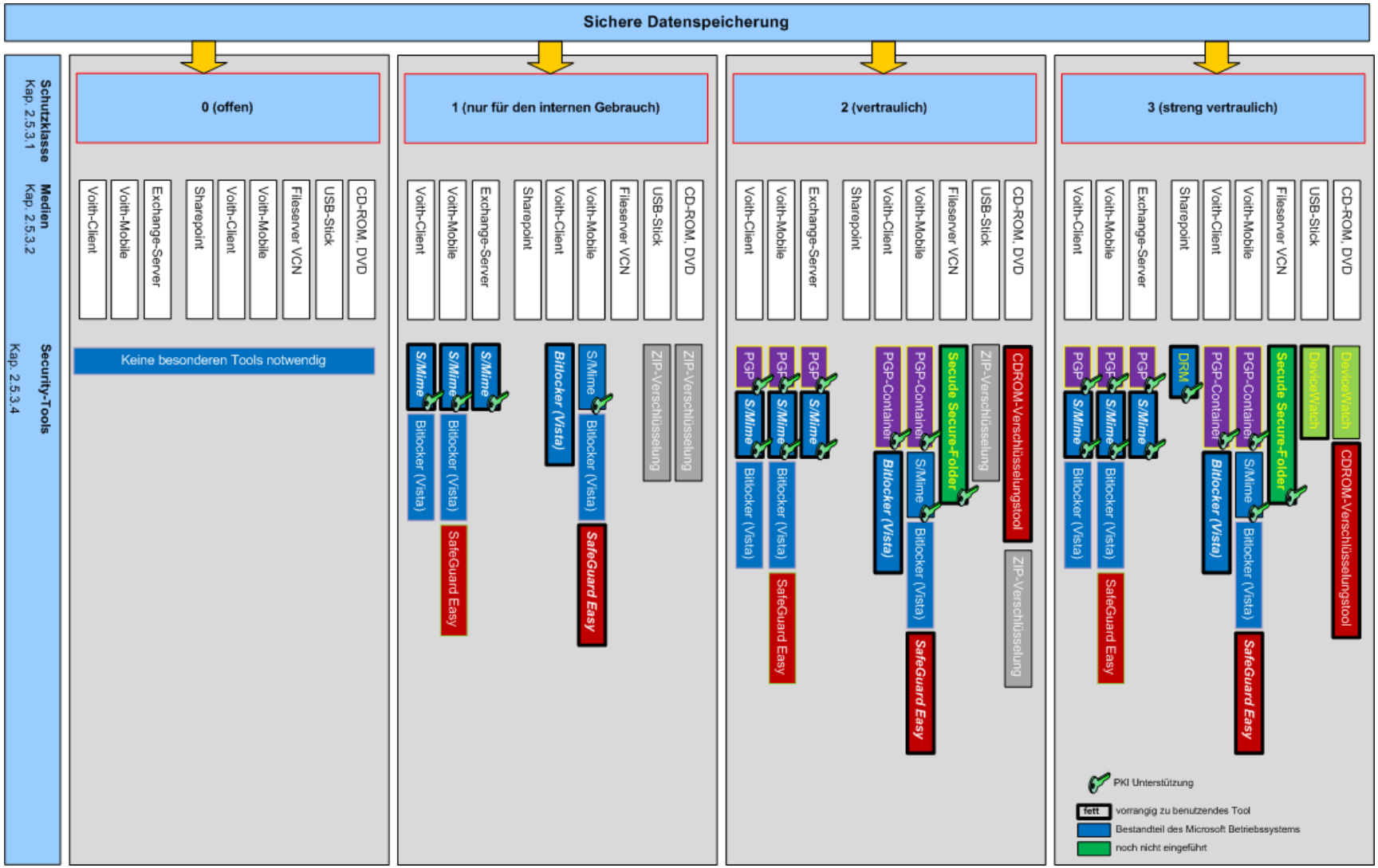


Secure Data Storage

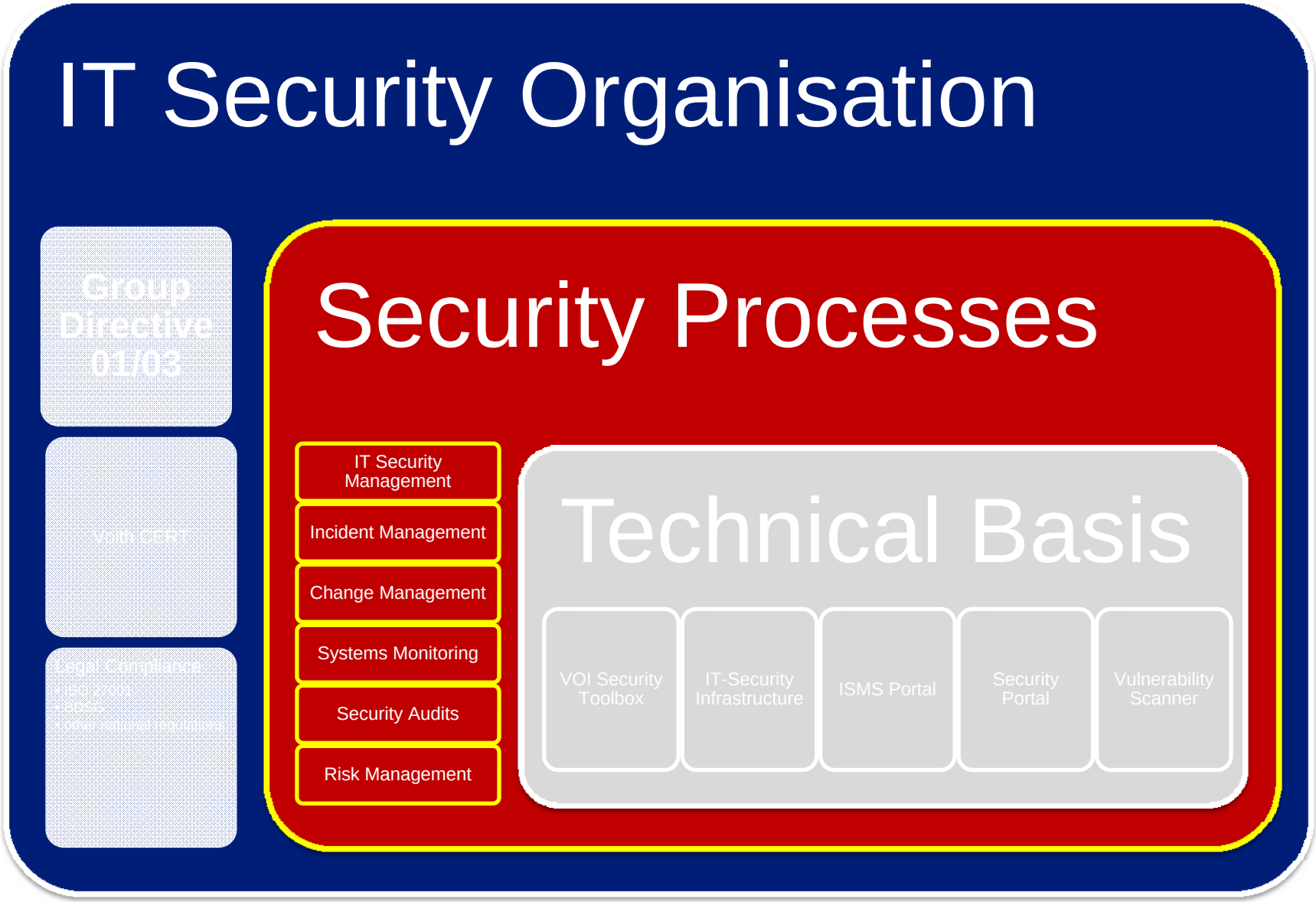
Data Leakage Prevention



Voith IT Solutions



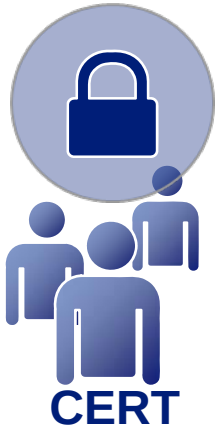
Security Processes



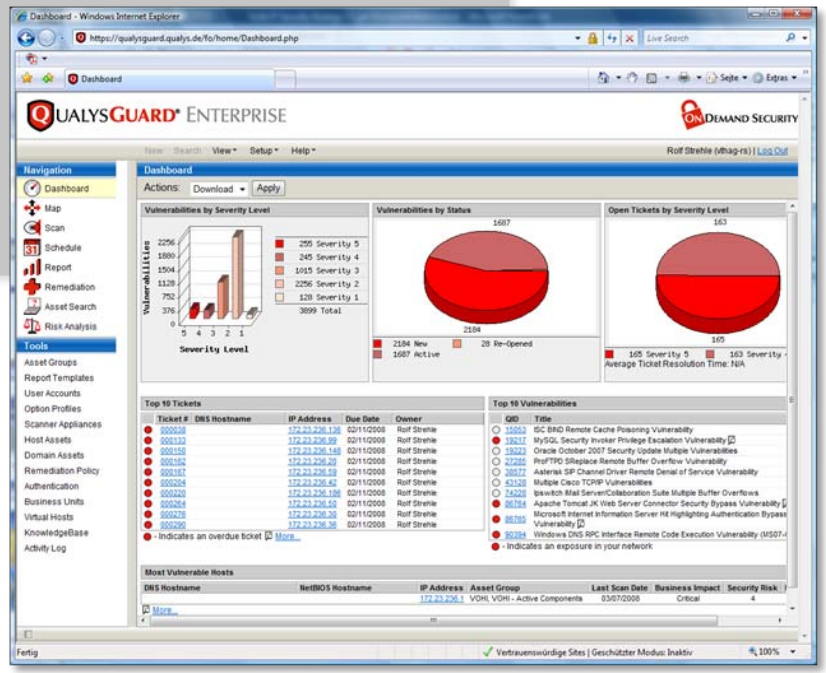
Vulnerability Management

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

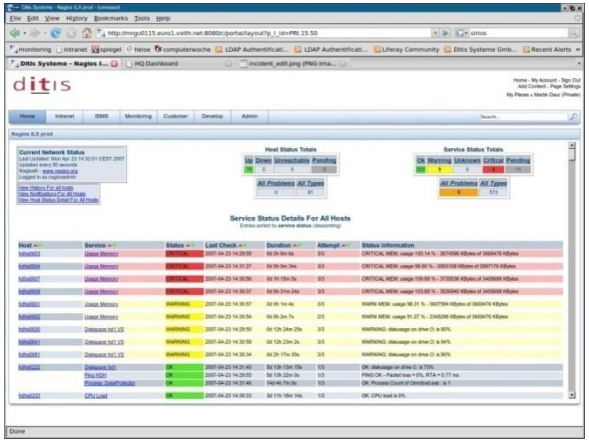


Technology: Qualys, Nessus

Global Monitoring

Voith IT Solutions

Global Support



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

Awareness Campaign

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!