Nets Information Security

Risikoanalyse og testing: med perspektiv fra frontlinjen

Stig Torsbakken – Nets SIRT

Agenda

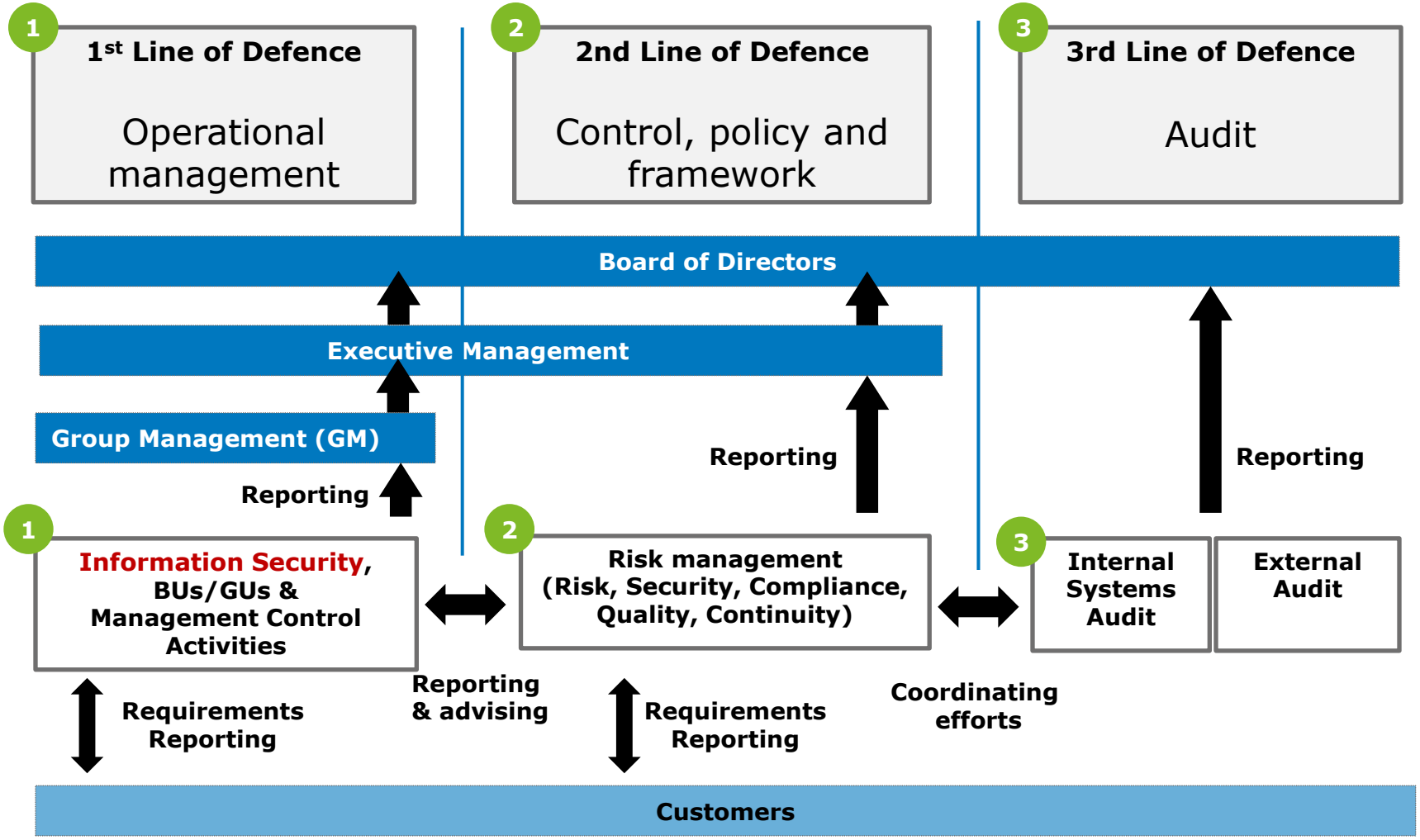
- Nets
- Nets threat landscape
- Nets security testing
- Seurity testing and security incidents

Nets


eFaktura
BETALINGSSERVICE
DK
OUR PRODUCTS - YOUR SERVICE
NEM ID
Avtale Giro
eBoks.dk
e|faktura

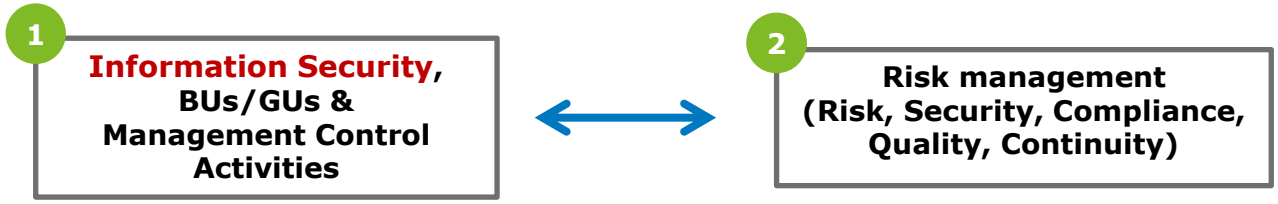
Three lines of defence

Risk management in Nets is organized around the 3 lines of defence model
(Ref. ECIIA & FERMA "Guidance on the 8th EU Company Law Directive")



Nets security

Simplified

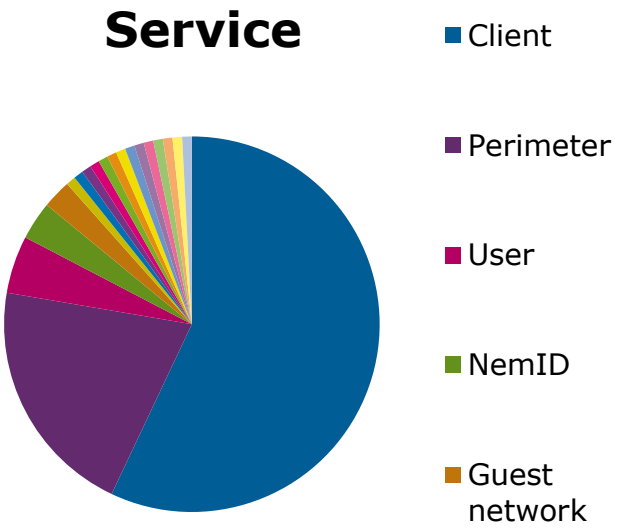


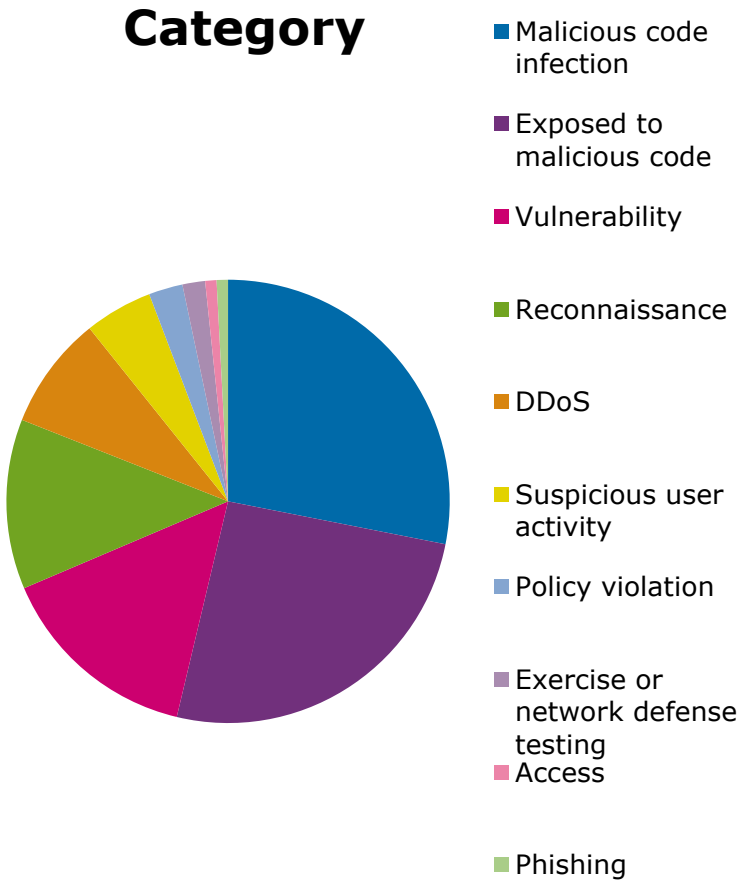
- Orientation
  - Threat
  - Technical
  - Operational

- Orientation
  - Compliance
  - Business
  - Risk

Nets SIRT security incidents 2013

Critical	**2**
High	**11**
Medium	**81**
Low	**27**
	121





Nets SIRT security incidents 2013

Fra: Nets.Service@kortet [mailto:Nets.Service@kortet]
Sendt: 29. mai 2012 03:05
Til:
Emne: Beskyttelse av tjenesten kortet.

Kjære bruker:

Det har blitt brakt til vår oppmerksomhet at VISA / MasterCard må BESKYTTELSE som en del av vår kontinuerlige forpliktelse til å beskytte dine kort og redusere svindel.

Hvis du kunne ta 3-5 minutter av din online opplevelse og muliggre beskyttelse av kortet ditt

Nr du starter å beskytte kortet ditt, vil du ikke oppleve fremtidige problemer med den elektroniske tjenesten.

For å begynne å beskytte ditt kredittkort, klikk på linken nedenfor:

Aktiver beskyttelse

Viktig: Kunne aktivering vil resultere i suspensjon av kortet ditt
Beskyttelse av tjenesten kortet.
internasjonal sikkerhet

DDoS attack April 10

NemID down for 7 hours

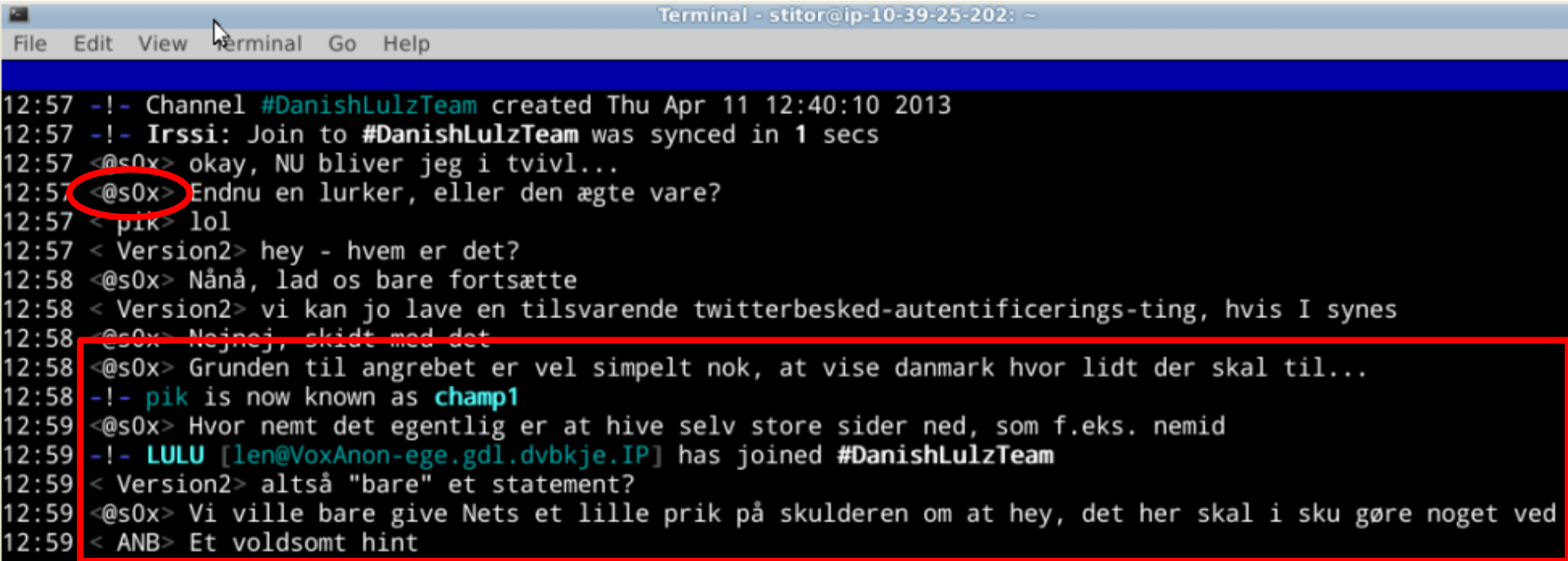
Danish LulzTeam @DanishLulzTeam apr 10
Nu kan hele danmark se, hvor svagt internet sikkerheden i danmark virkelig er. #nemid
Mer

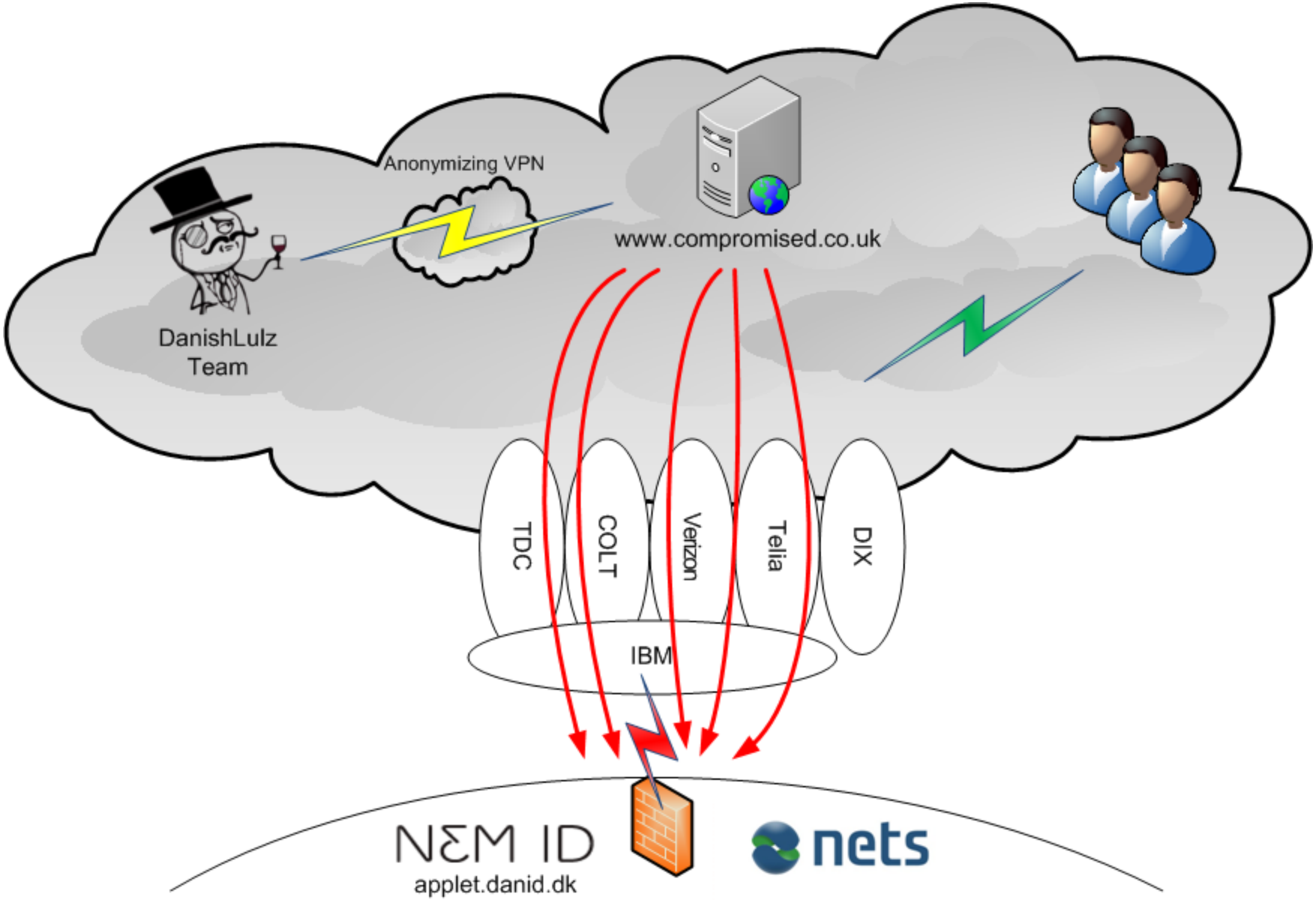
Danish LulzTeam @DanishLulzTeam apr 10
we killed ya, ha-ha #nemid
Mer

Gruppe tager ansvar for NemID-angreb: Vil forsøge at slå til igen

En gruppe, der via Twitter har taget ansvaret for torsdagens angreb mod NemID, siger, at de vil forsøge at få login-tjenesten til at gå ned igen.

version2




Anonymizing VPN
www.compromised.co.uk
DanishLulz
Team
TDC
COLT
Verizon
Telia
DIX
IBM
NEM ID
applet.danid.dk
nets

Security testing in Nets

In numbers – Nets Norway

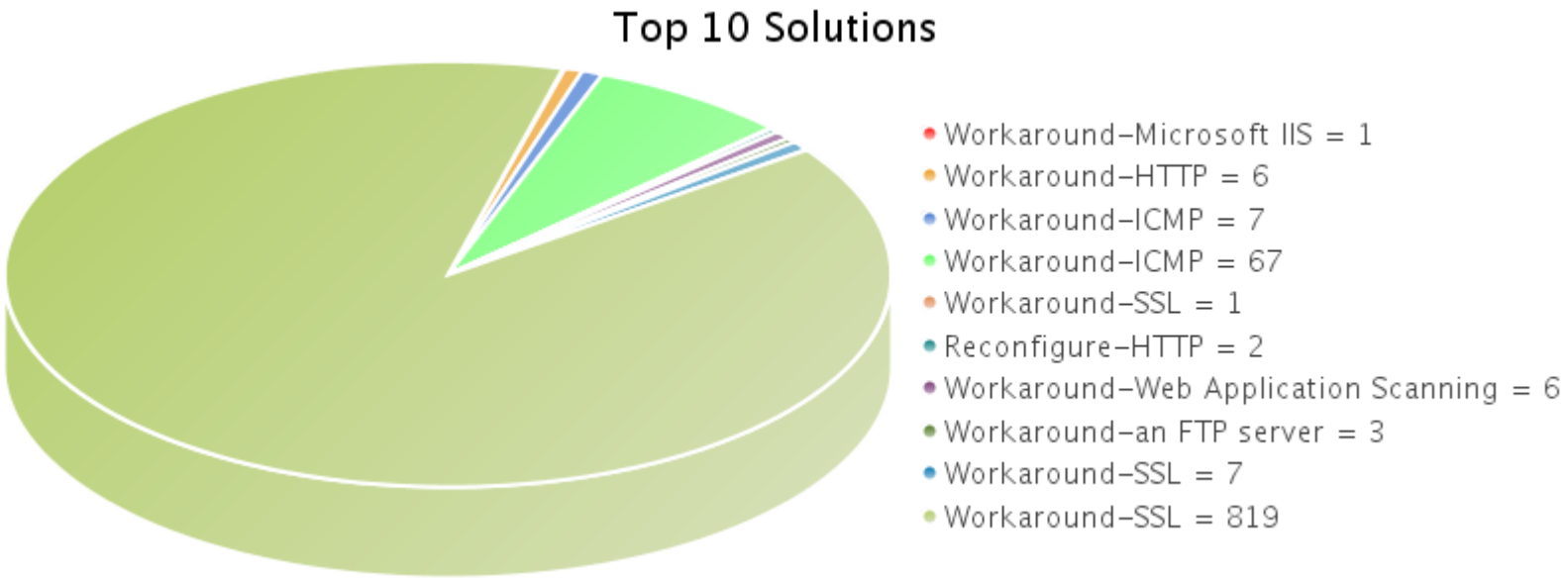
- Vulnerability scanning
  - External: 4
  - Internal: 4+
  - Scanningless scanning: 365
- Pentesting
  - New applications/systems: approx. 1 every week(!)
  - Yearly pentests: 20
- Risk analysis
  - Yearly risk analysis of all infrastructure
  - Risk analysis of new services

- How is this possible?
  - 1 FTE (to be 3-4) dedicated to pentesting
  - 25-30 security officers in Nets in total
  - Heavy use of consultants and 3rd party vendors
  - **Narrowing scope**

Security testing in Nets

Vulnerability scanning

- Quarterly external scan
- Quarterly internal scan
- Scanningless scanning



Security testing in Nets

Pentesting

- Typical findings
  - Input validation
  - Application vulnerabilities
  - Default passwords
  - Vulnerable/unsecure protocols
  - Missing authentication/source verification
  - Design flaws

- 60% of findings through manual tests
  - Narrow scope
  - Narrow scope
  - Narrow scope

Security testing in Nets

Pentesting

How to narrow scope?

- Tool-support
  - Nessus
  - Nmap
  - AppScan
  - Metasploit
  - soapUI
  - Burp Suite
  - ZAP (Zed Attack Proxy)

OWASP ZAP

Version 2.1.0

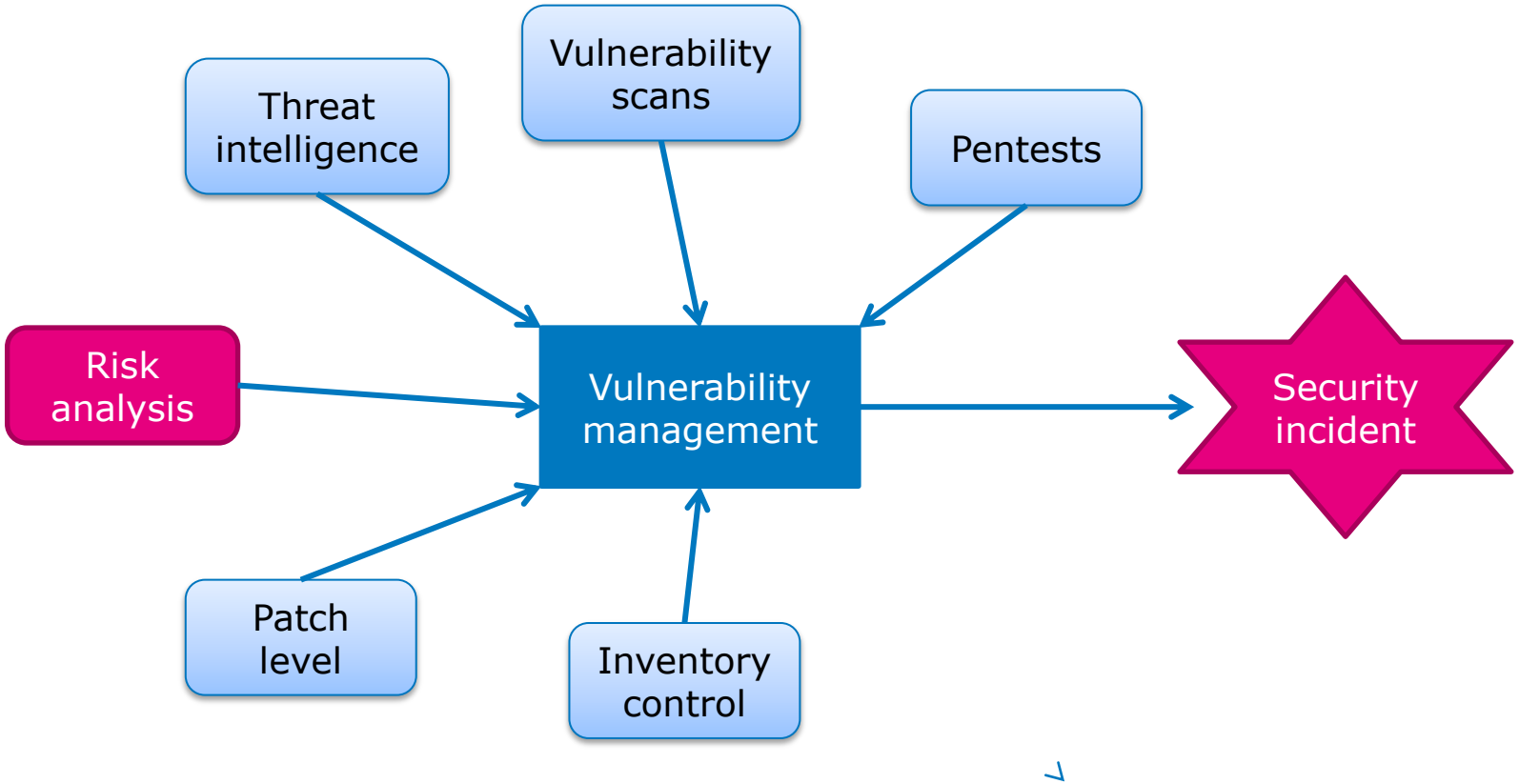
Security testing in Nets

Pentesting

How to narrow scope?

- Risk analysis involving pentest team
  - **Business side priorities**
  - Structured walk-through of functionality
  - Thorough system presentation
- Pentest team involved in software development phase
- Pentest team involved in security arcitechture design

Security testing and security incidents

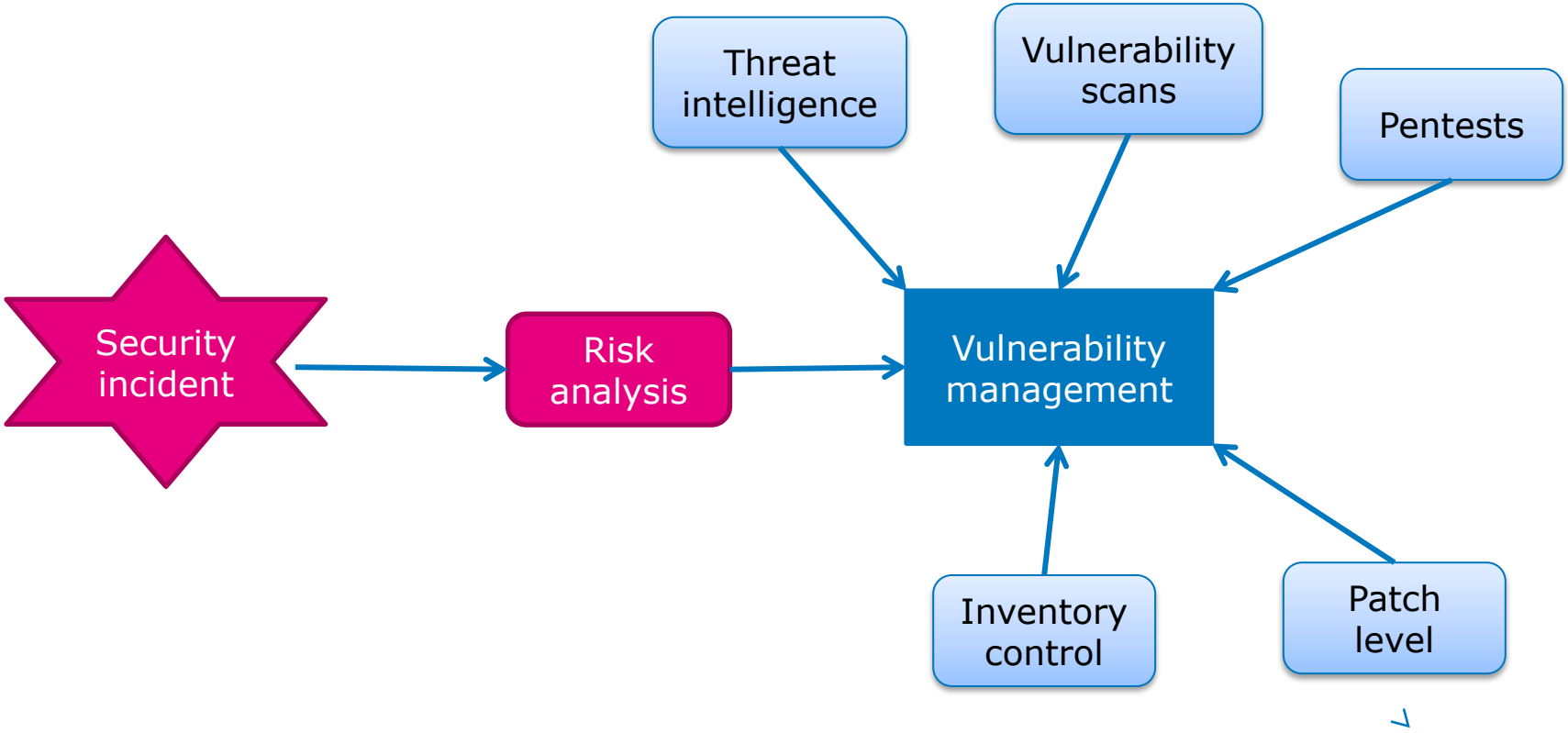


Security testing and security incidents

Nets SIRT vulnerability management procedure

Nets pentest/vulnerability scan findings	**Priority:**
• affect production systems • remote exploitable • **would cause a Major 1 or 2 incident if exploited**	**Major 1&2**
• do not affect production systems • not remotely exploitable (only internally) • would cause a Major 1 or 2 incident if exploited after system is released	3
• do not require immediate actions	4

Security testing and security incidents



Fully implemented DDoS protection

Project «DDoS Shield»