



# Nets Information Security

Risikoanalyse og testing: med perspektiv fra frontlinjen

Stig Torsbakken – Nets SIRT

# Agenda

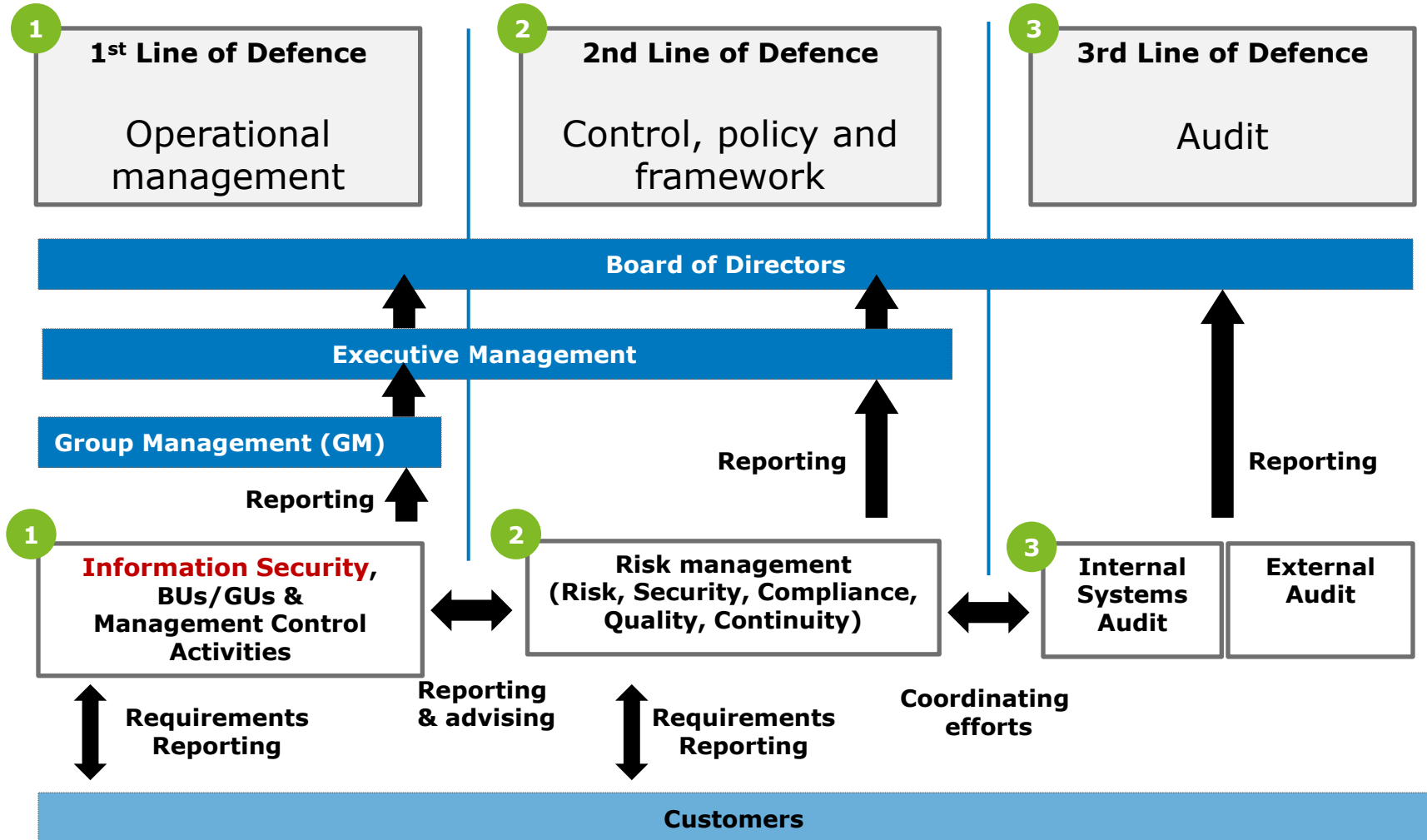
- › Nets
- › Nets threat landscape
- › Nets security testing
- › Security testing and security incidents

# Nets



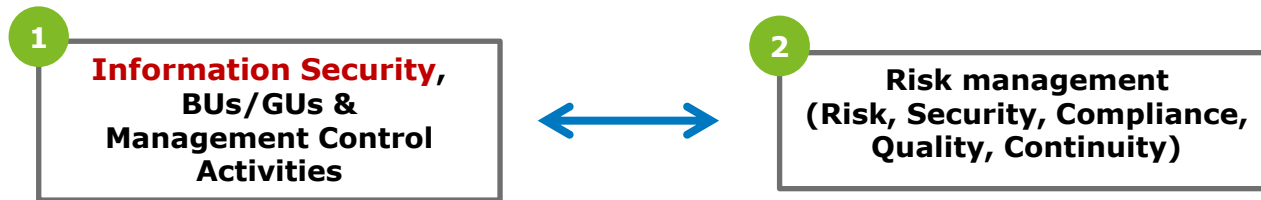
# Three lines of defence

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



# Nets security

*Simplified*



> Orientation

- > Threat
- > Technical
- > Operational

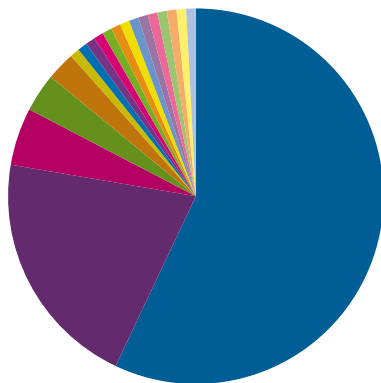
> Orientation

- > Compliance
- > Business
- > Risk

# Nets SIRT security incidents 2013

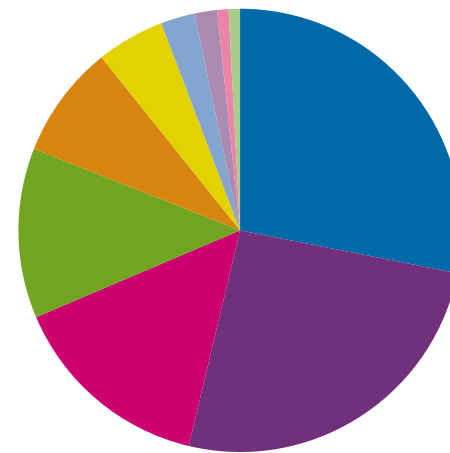
Critical	<b>2</b>
High	<b>11</b>
Medium	<b>81</b>
Low	<b>27</b>
	<b>121</b>

## Service



- Client
- Perimeter
- User
- NemID
- Guest network

## Category



- Malicious code infection
- Exposed to malicious code
- Vulnerability
- Reconnaissance
- DDoS
- Suspicious user activity
- Policy violation
- Exercise or network defense testing
- Access
- Phishing

# Nets SIRT security incidents 2013

**Fra:** [Nets.Service@kortet](mailto: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 muliggjøre 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

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

VERSION 2

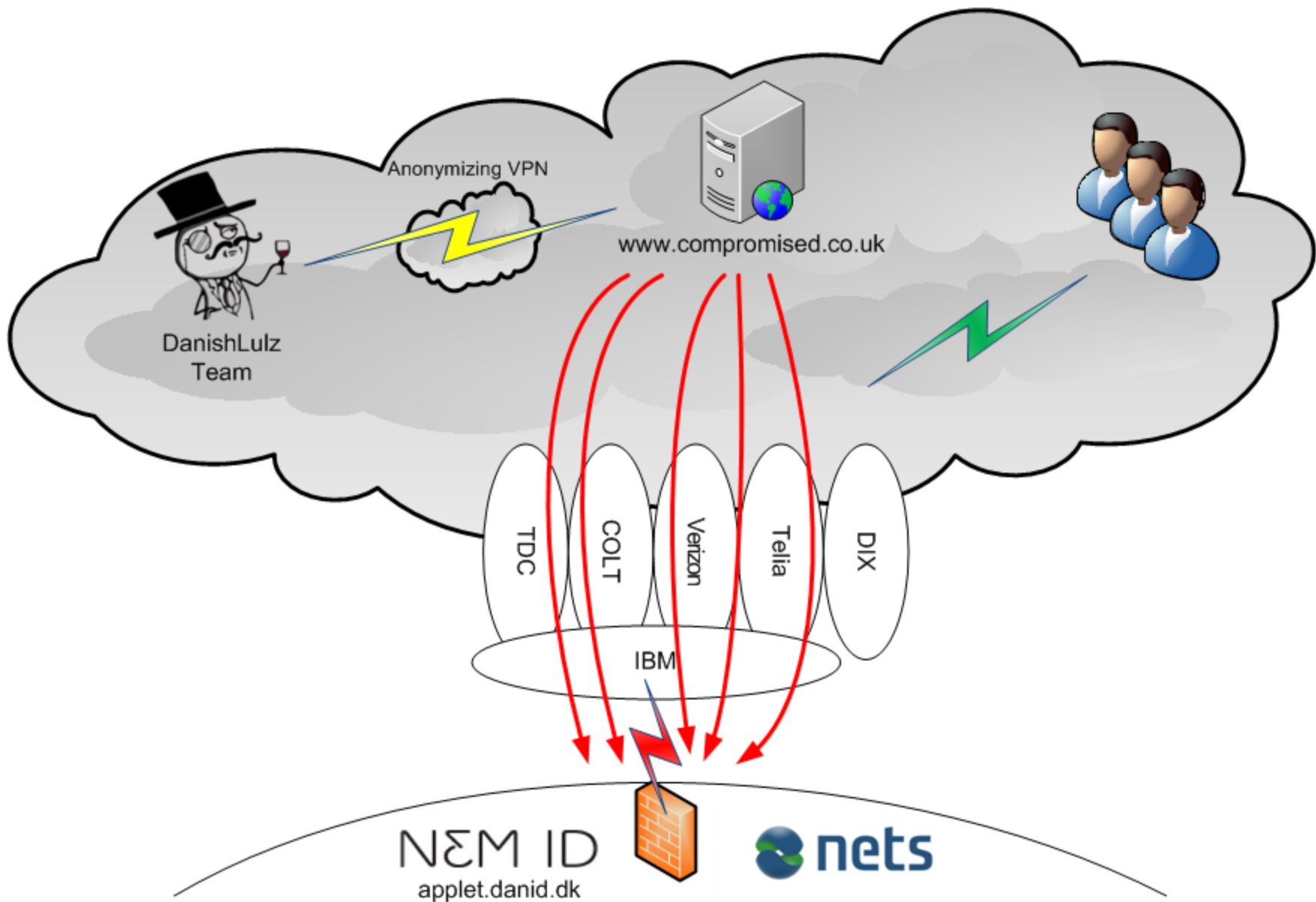
 **Danish LulzTeam** @DanishLulzTeam apr 10  
Nu kan hele danmark se, hvor svagt internet sikkerheden i danmark virkelig er. #nemid  
Mer

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

*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.*

```
Terminal - stitor@ip-10-39-25-202: ~
File Edit View Terminal Go Help
12:57 -!- Channel #DanishLulzTeam created Thu Apr 11 12:40:10 2013
12:57 -!- Irssi: Join to #DanishLulzTeam was synced in 1 secs
12:57 <@s0x> okay, NU bliver jeg i tvivl...
12:57 <@s0x> Endnu en lurker, eller den ægte vare?
12:57 <pik> lol
12:57 <Version2> hey - hvem er det?
12:58 <@s0x> Nååå, lad os bare fortsætte
12:58 <Version2> vi kan jo lave en tilsvarende twitterbesked-autentificerings-ting, hvis I synes
12:58 <@s0x> Nejnej, skidt med det
12:58 <@s0x> Grunden til angrebet er vel simpelt nok, at vise danmark hvor lidt der skal til...
12:58 -!- pik is now known as champ1
12:59 <@s0x> Hvor nemt det egentlig er at hive selv store sider ned, som f.eks. nemid
12:59 -!- LULU [len@VoxAnon-ege.gdl.dvbkje.IP] has joined #DanishLulzTeam
12:59 <Version2> altså "bare" et statement?
12:59 <@s0x> Vi ville bare give Nets et lille prik på skulderen om at hey, det her skal i sku gøre noget ved
12:59 <ANB> Et voldsomt hint
```





# Security testing in Nets

*In numbers – Nets Norway*

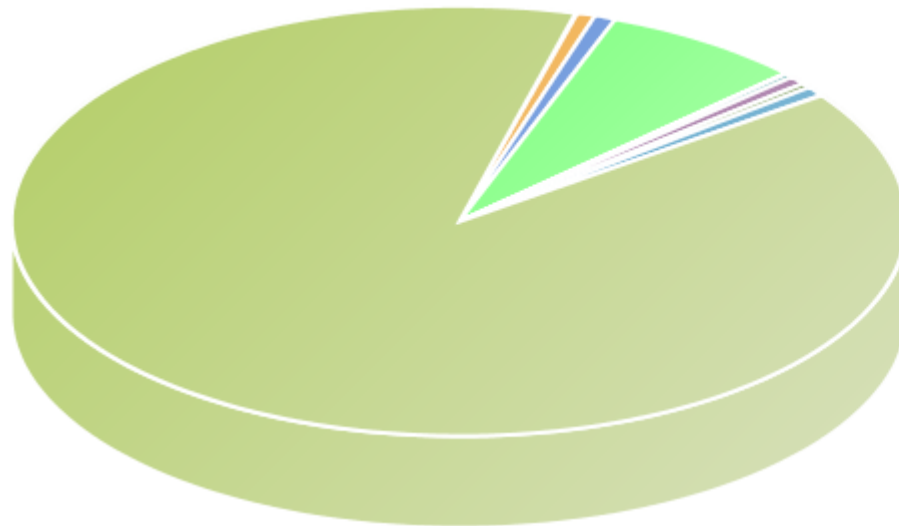
- › Vulnerability scanning
  - › External: 4
  - › Internal: 4+
  - › Scanningless scanning: 365
- › Pentesting
  - › New applications/systems: approx. 1 every week(!)
  - › Yearly pentests: 20
- › Risk analysis
  - › Yearly risk analysis of all infrastructure
  - › Risk analysis of new services
  
-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

Top 10 Solutions



- Workaround-Microsoft IIS = 1
- Workaround-HTTP = 6
- Workaround-ICMP = 7
- Workaround-ICMP = 67
- Workaround-SSL = 1
- Reconfigure-HTTP = 2
- Workaround-Web Application Scanning = 6
- Workaround-an FTP server = 3
- Workaround-SSL = 7
- Workaround-SSL = 819

# 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

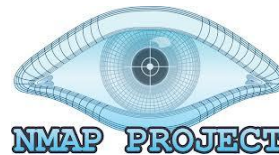
# Security testing in Nets

## *Pentesting*

How to narrow scope?

### > Tool-support

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



**OWASP ZAP**

Version 2.1.0



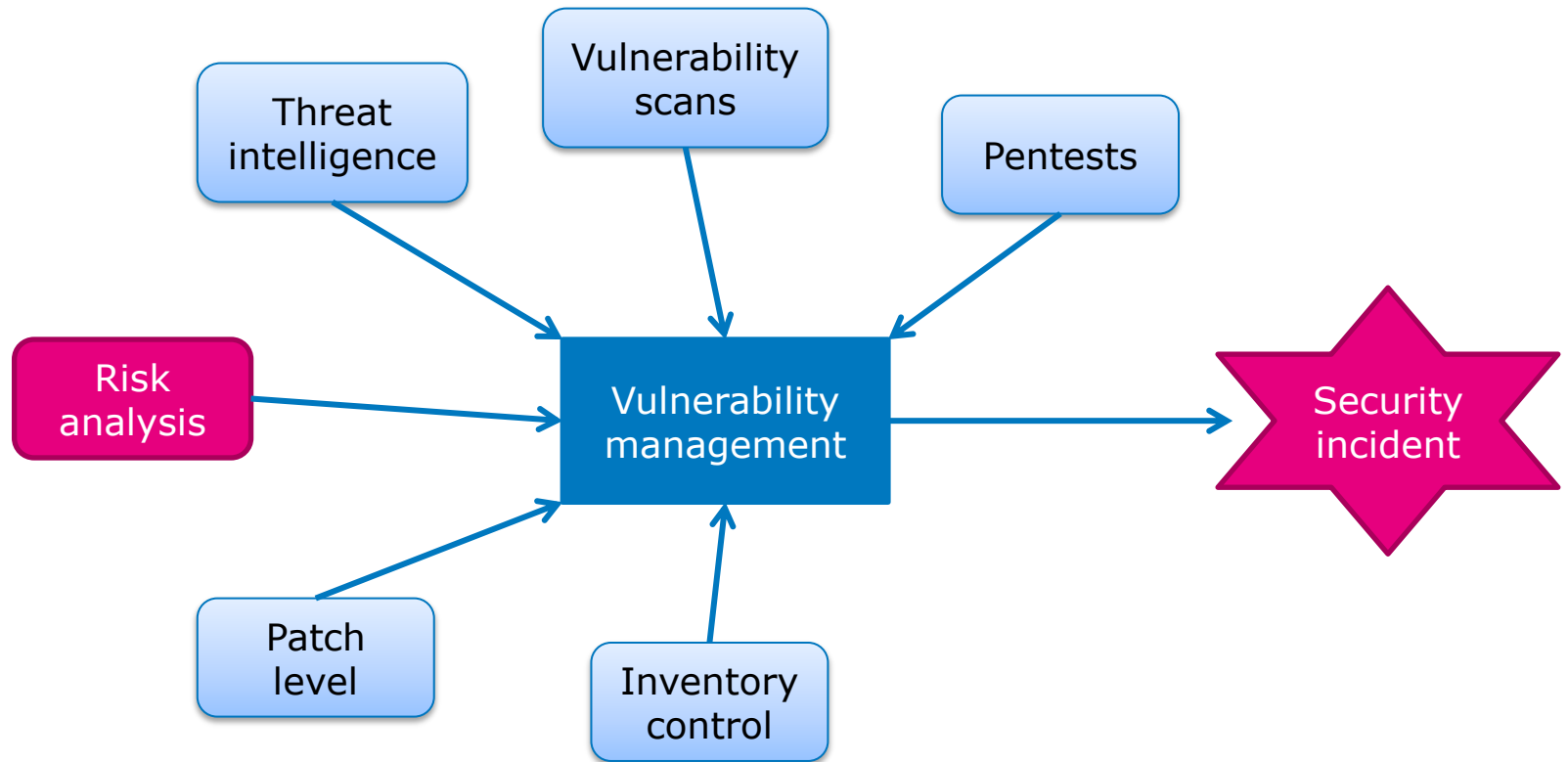
# Security testing in Nets

## *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 architecture design

# Security testing and security incidents



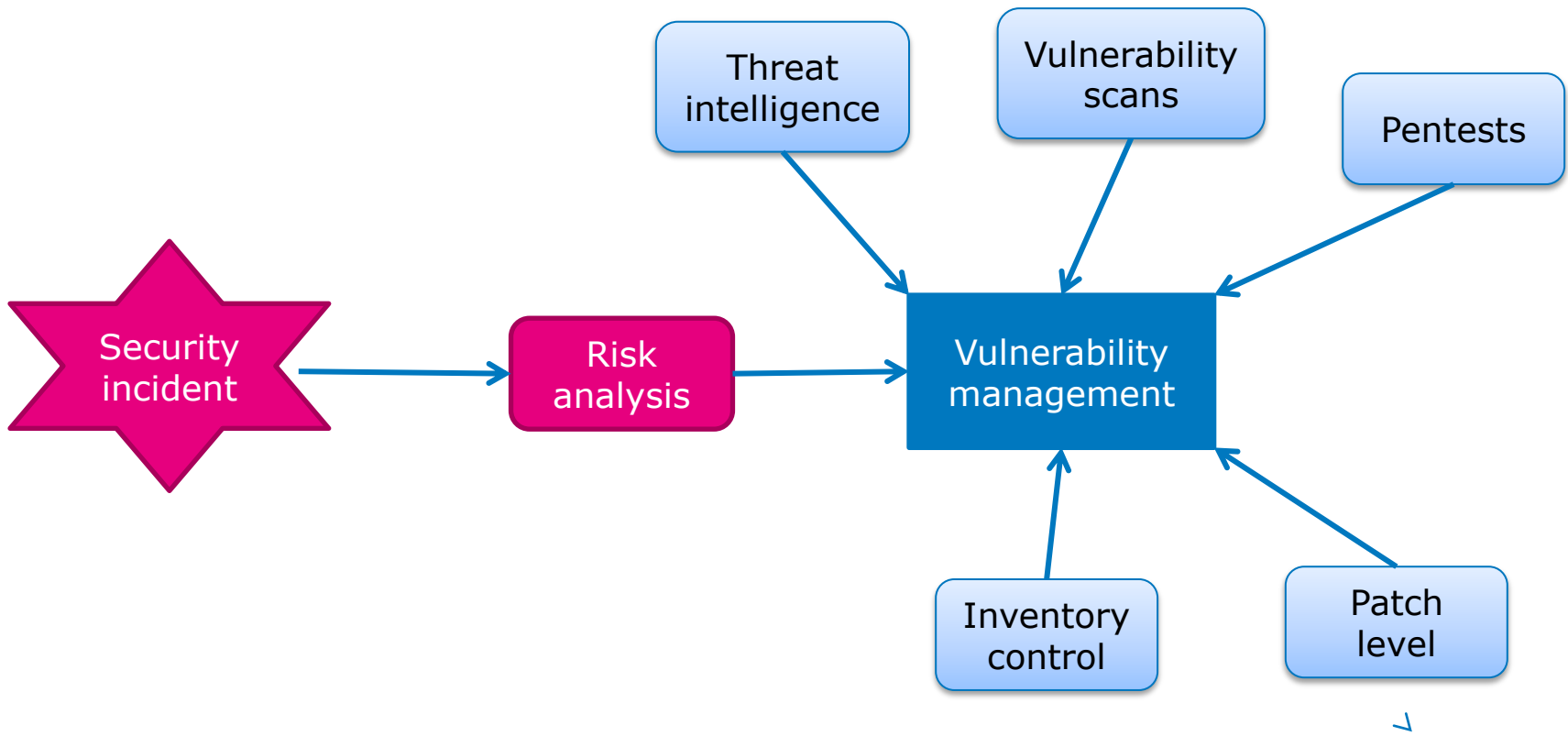
# Security testing and security incidents

*Nets SIRT vulnerability management procedure*

Nets pentest/vulnerability scan findings	Priority:
<ul style="list-style-type: none"><li>• affect production systems</li><li>• remote exploitable</li><li>• <b>would cause a Major 1 or 2 incident if exploited</b></li></ul>	<b>Major 1&amp;2</b>
<ul style="list-style-type: none"><li>• do not affect production systems</li><li>• not remotely exploitable (only internally)</li><li>• would cause a Major 1 or 2 incident if exploited after system is released</li></ul>	3
<ul style="list-style-type: none"><li>• do not require immediate actions</li></ul>	4



# Security testing and security incidents



# Fully implemented DDoS protection

Project «DDoS Shield»

