Integrated Security Incident Management

Concepts & Real world experiences

Stefan Metzger, Dr. Wolfgang Hommel, Dr. Helmut Reiser

6th International Conference on
IT Security Incident Management & IT Forensics

Stuttgart, 10. - 12. Mai 2011

Leibniz-Rechenzentrum

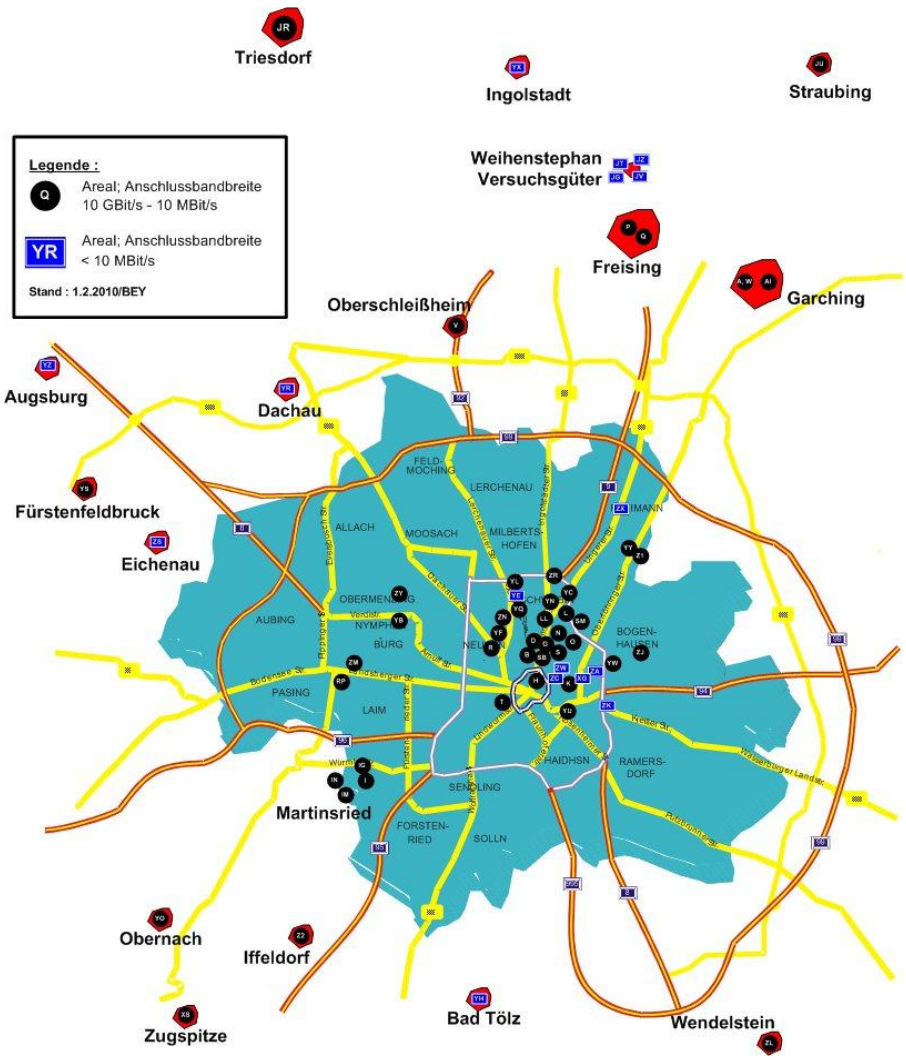
Who we are?

- DC for Munich‘s HEIs
- Operation of Munich scientific network (MWN)

Foto: Ernst A. Graf

Munich scientific network (MWN)
Facts

- 120.000 users
- ~ 80.000 devices
- Decentral administration and responsibility



Attacker‘s motivation to attack HEIs

- Stealing data
  - Personal data of students and employees
  - E-Mail-Adresses
  - Personnel numbers
  - Research results, …
- High bandwidth internet link (spam-sending, (D)DoS)

DoS activity outgoing

Timestamp (1 hour): 04:13:16 15.04.2011

129.xxx.xx.xxx: In : 303995 Bytes, Out : 688564204 Bytes

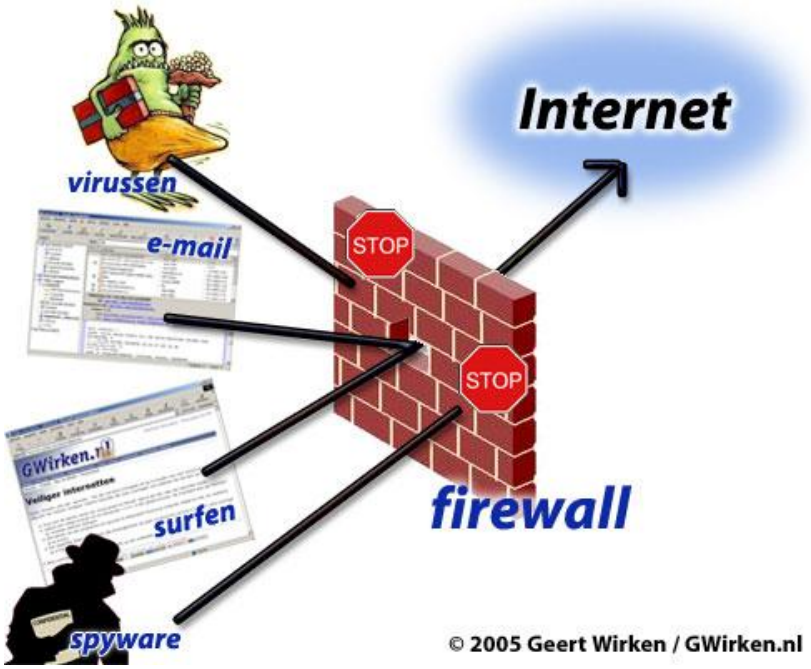
Our definition of a security incident

- Definition ISO/IEC 27001:
  A *Security incident* is an event, which has a negative effect on security, especially on confidentiality, data integrity and availability of information.

- Security monitoring at LRZ:
  - External → Internal (attacks against internal systems)
  - Internal → External (compromised internal systems)

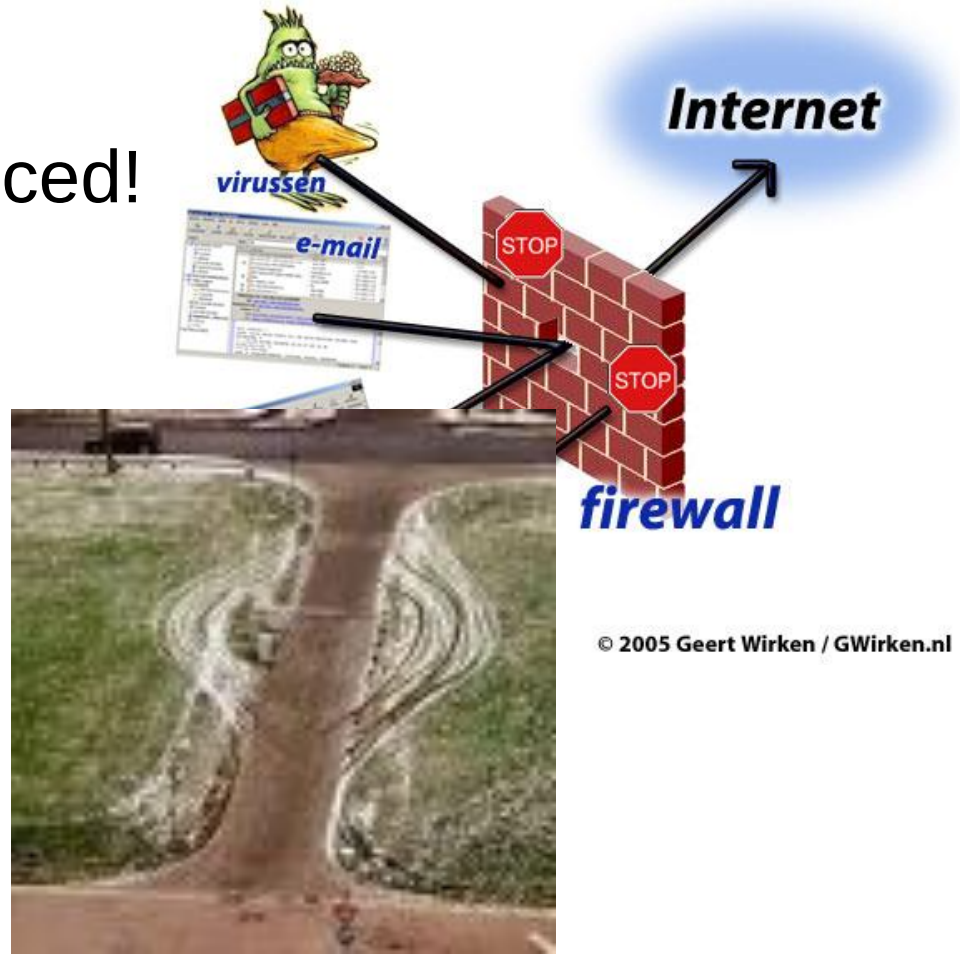
Common countermeasures

- Installation of security patches couldn‘t be forced! (infection rate: 1 - 5%)
- Firewalls
- Intrusion Detection / Prevention systems



Common countermeasures

- Installation of security patches couldn‘t be forced! (infection rate: 1 - 5%)
- Firewalls
- Intrusion Detection / Prevention systems



Common countermeasures

- Installation of security patches couldn‘t be forced!

Only preventive security controls are insufficient and couldn‘t be forced!

- Firewalls

- Intrusion Detection / Prevention systems

Integrated and reactive response

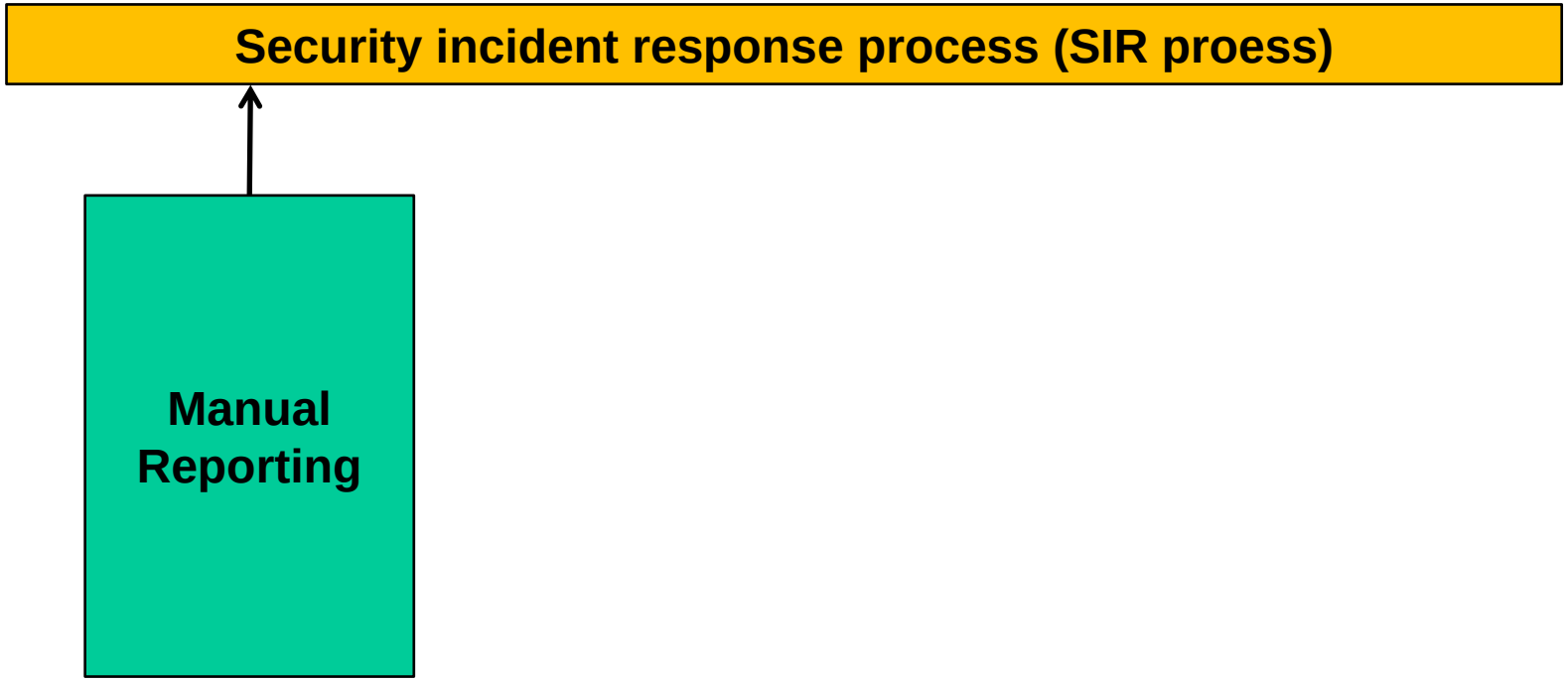
Our goals:

- Structured, coordinated workflow!
- Defined responsibilities and tasks
- automated response capabilities

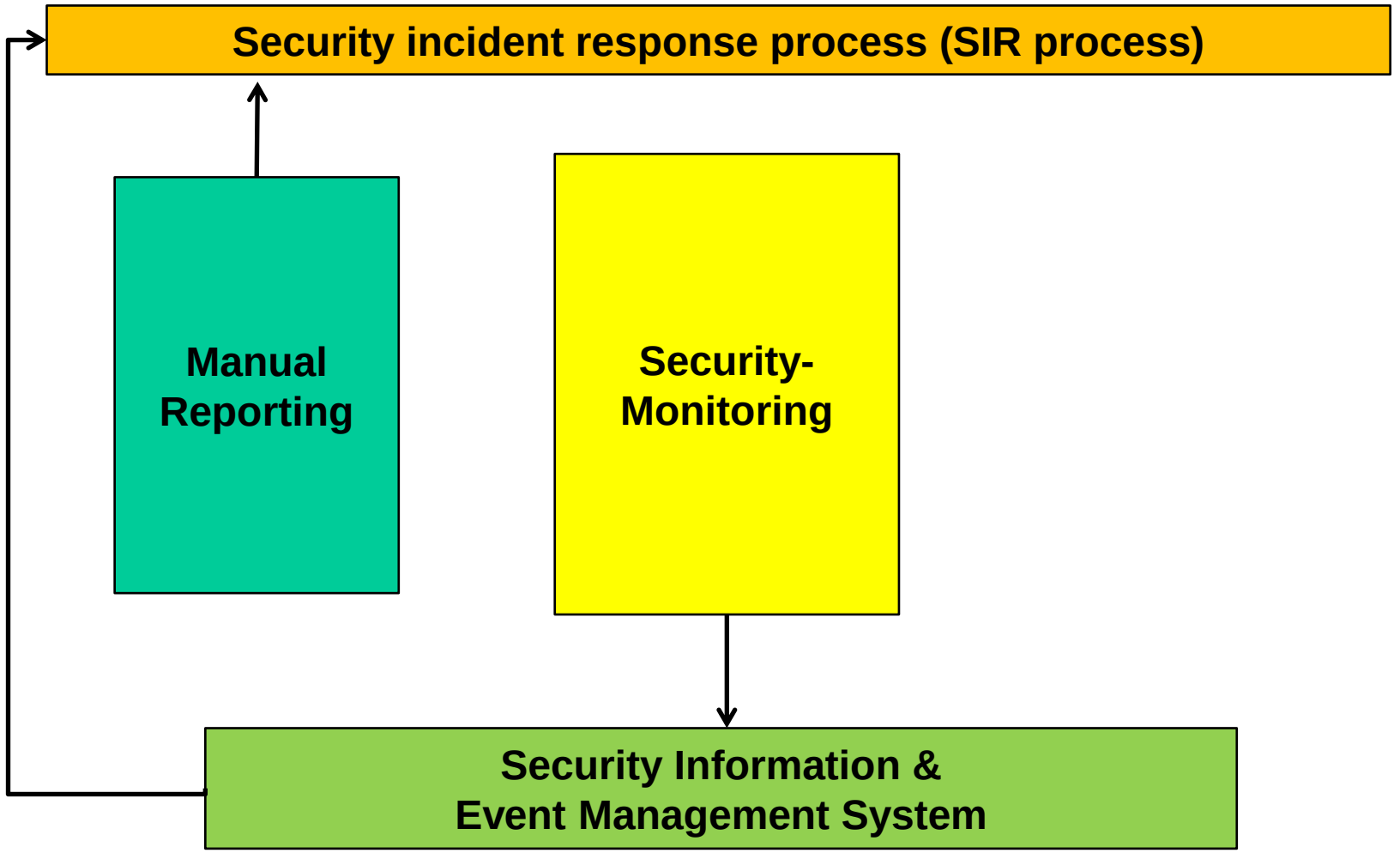
Integrated and reactive response

Security incident response process (SIR process)

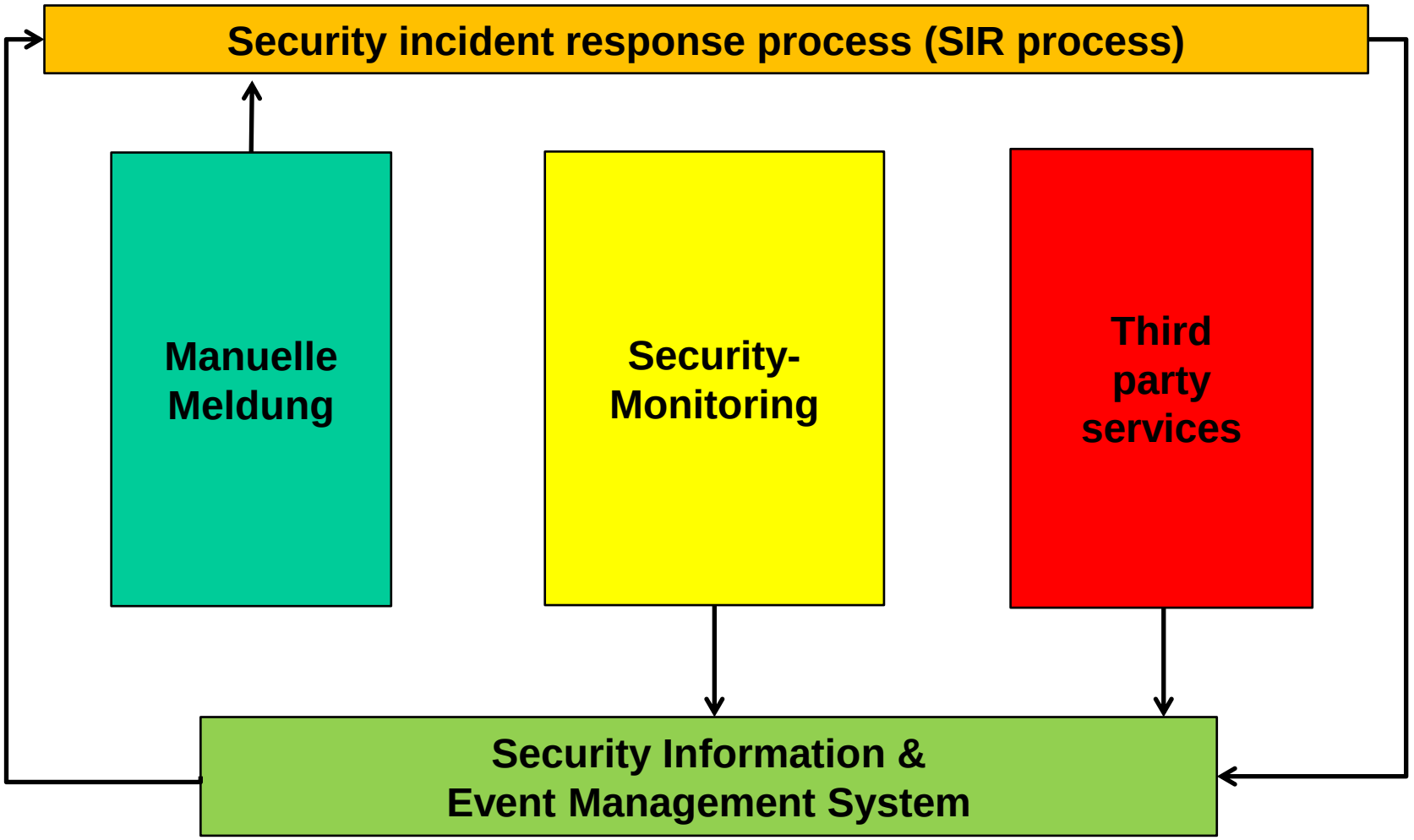
Integrated and reactive response



Integrated and reactive response

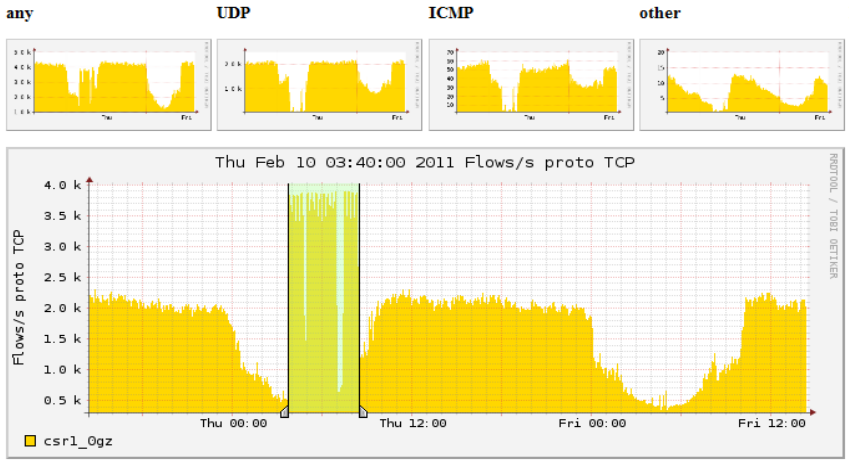


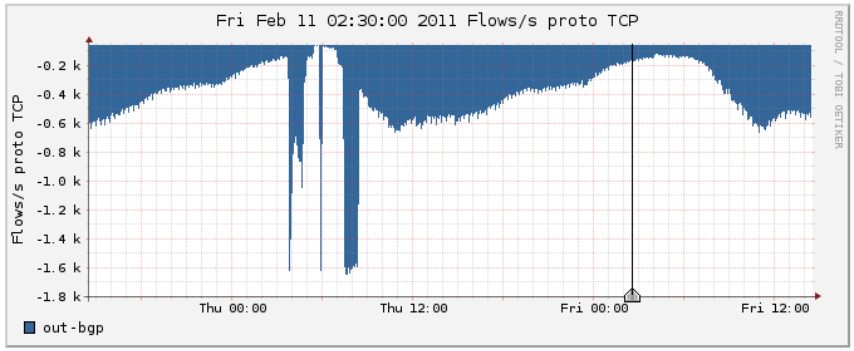
Integrated and reactive response



Tool based security monitoring

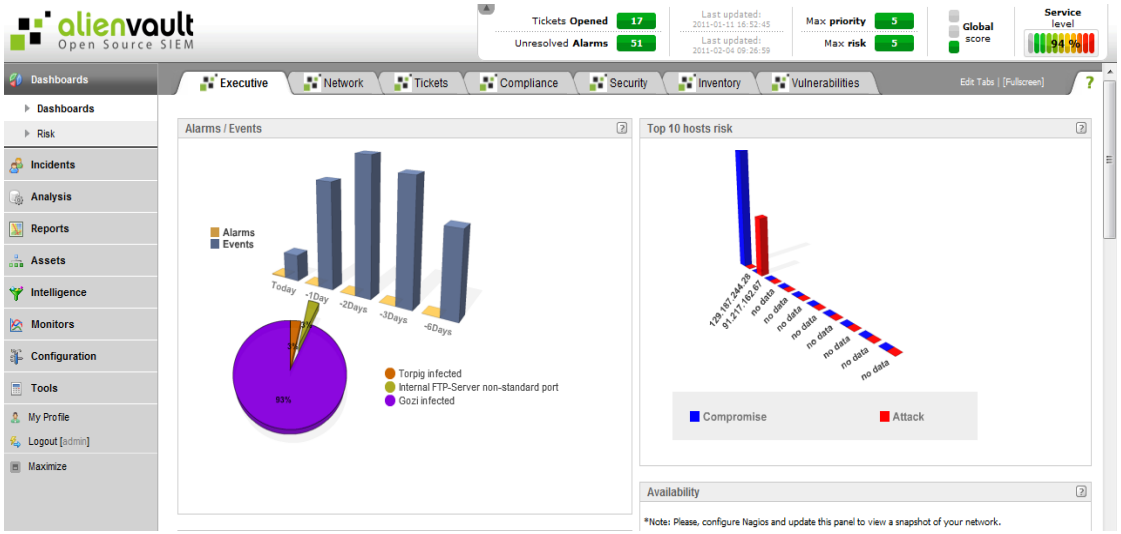
- SNORT IDS
- NfSEN (Netflow)
- Accounting
  (SPAM senders, DoS)
- NAT-o-MAT / Secomat





Security Information & Event Management (SIEM)

Open Source SIM (OSSIM)



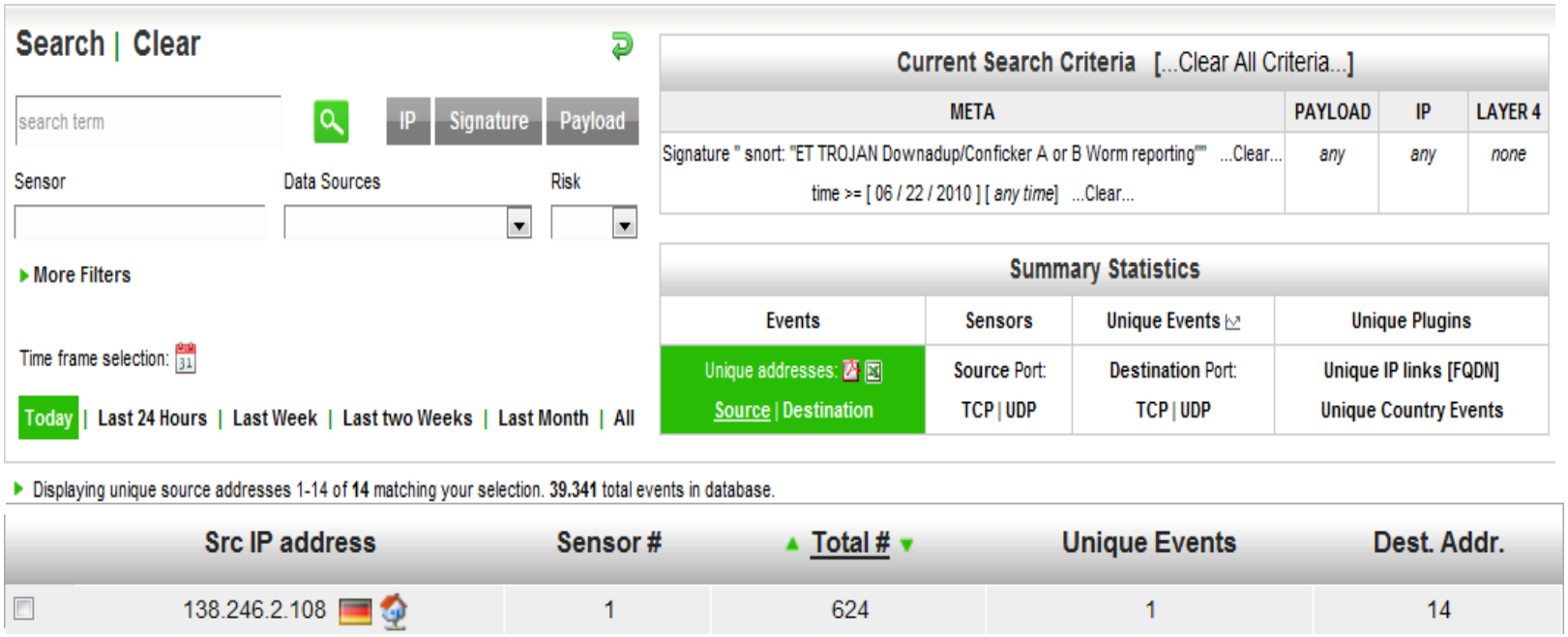
- Dashboards
- Reporting
- Event correlation
- Automated responses

Security Information & Event Management (SIEM)

Open Source SIM (OSSIM)

Integrated sorting and filtering functions

- unique events
- source- / destination (ip or port)
- time window



DFN CSIRT services
Automated security warnings

- Sensors at DFN CSIRT
- Suspicious ip addresses are reported to DFN facilities

Message:

IP	Message typ	last seen
129.xxx.xxx.xxx	Bot	2011-02-12 14:06:03 GMT+0100

DFN CSIRT services
Automated security warnings

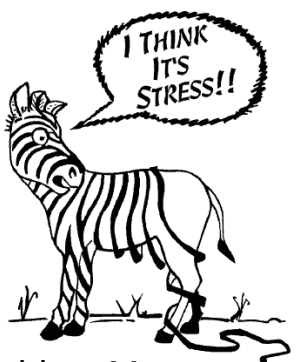
- Sensors at DFN CSIRT
- Suspicious ip addresses are reported to DFN facilities

Details:

System: 129.xxx.xxx.xxx
Message typ: Bot
Timestamp: 2011-02-12 14:06:03 GMT+0100 >

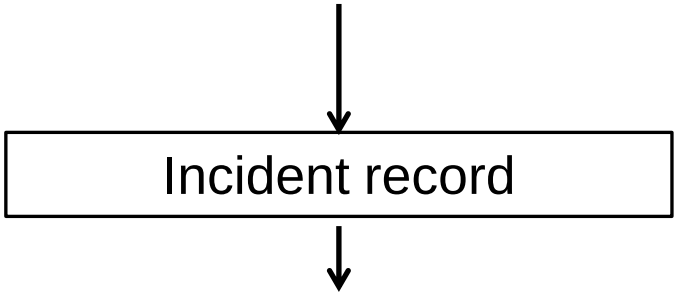
Protocol	Src port	Dst port	malware typ	Timestamp(GMT+0000)
unbekannt		6667	unbekannt	2011-02-12 11:06:03
unbekannt		6667	unbekannt	2011-02-12 13:06:03

After a security incident has occured …



Security incident response process
Incident record

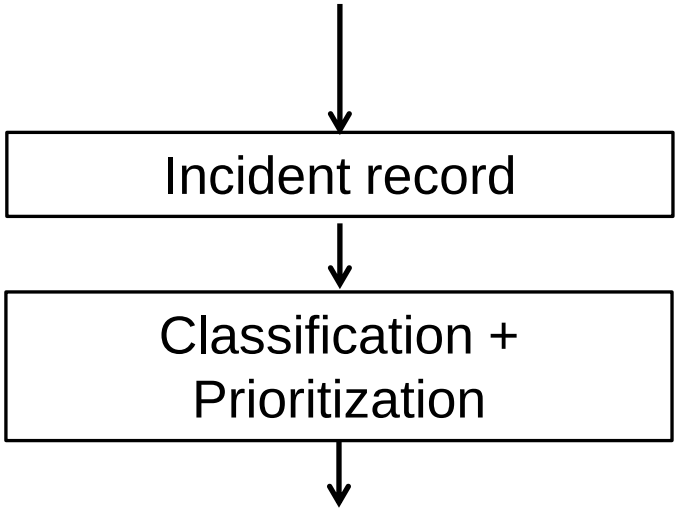
- **What happened**?
- **On which system?**
- **Who is responsible for this system**?
- **When**?



Security incident response process
Classification + Prioritization

- Which type of attack?

- **Prioritization**
  - Attacker‘s location?
  - Victim‘s location?
  - How many systems are affected?
  - Which services are affected?

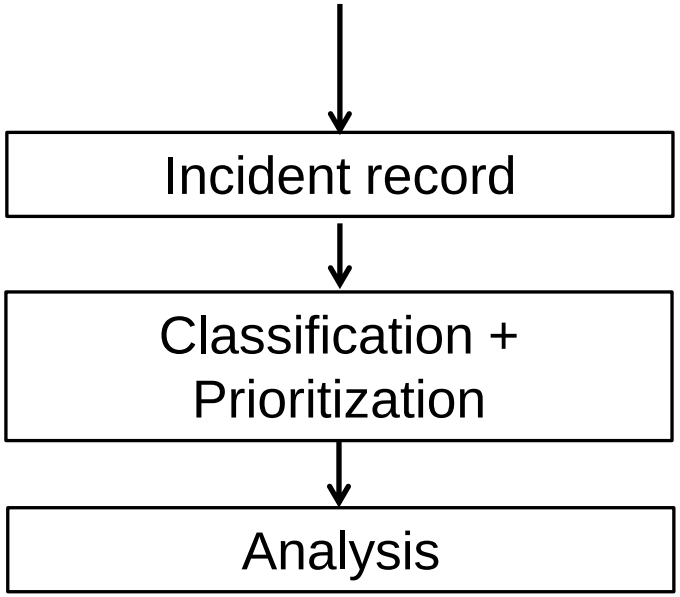


Security incident response process
Classification + Prioritization

Impact/ Criteria	Low	Medium	High
Victim	external (1)	MWN or Grid (2)	LRZ internal (3)
Services, Data	not concerned (1)	MWN or Grid (2)	Important services (3)
# involved systems	1 (1)	2-3 (2)	> 3 (3)
Attacker	external (1)	MWN or Grid (2)	LRZ internal (3)

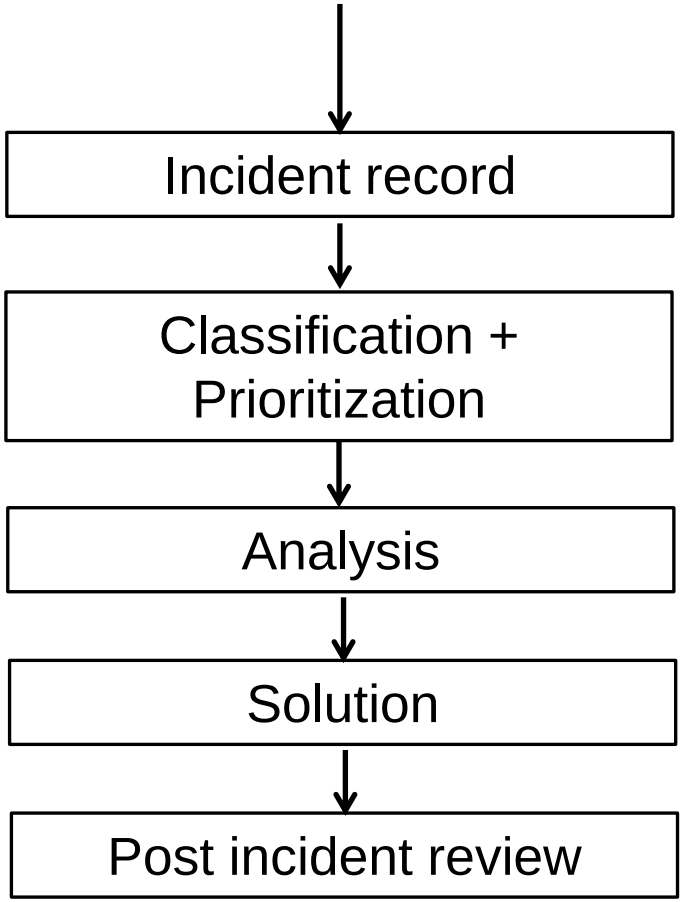
Security incident response process
Incident handling

- Standard security incident?
  → defined procedure
- First measures
- Analysis & Diagnose of compromised systems



Security incident response process
Solution

- Goal: fastest possible service recovery
- Further suspicious activities?
- Post incident review meeting



Security incident response at LRZ
Example

- SNORT IDS detects events (bot c&c server traffic)
- Forwarding to central SIEM

snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 13:05:14	129	194. :6667
snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 12:04:52	129.	195. :6667
snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 11:04:40	129.	194. :6667
snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 10:02:50	129.	194. :6667
snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 09:02:08	129.	194. .6667

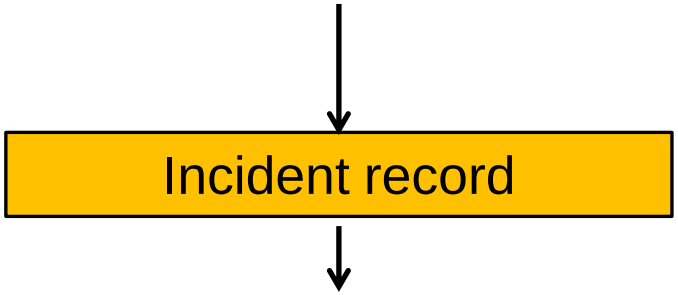
- Event correlation (> 5 events / 8 hours) → alerting!

Security incident response at LRZ
Example

After the alert →

- Create security incident ticket

- Inform system administrators plus LRZ-CSIRT



Security incident response at LRZ
Example

Event: **snort: "ET DROP KNOWN BOT C&C Server Traffic TCP"**

IP address: 129.xxx.xxx.xxx
FQDN: <HOSTNAME>

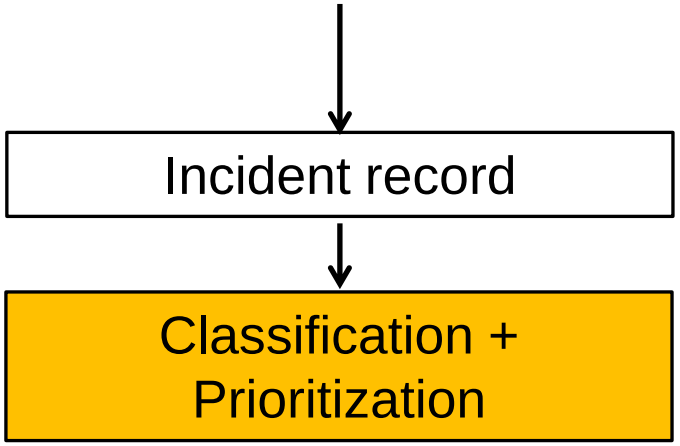
Location: <building, institution, address)>
Switch port:
<SWITCH-PORT DETECTION>

Source port: xxxxx
Destination ip address: 194.xxx.xxx.xxx
Destination port: 6667

Timestamp: Sat Feb 12 13:05:14 2011

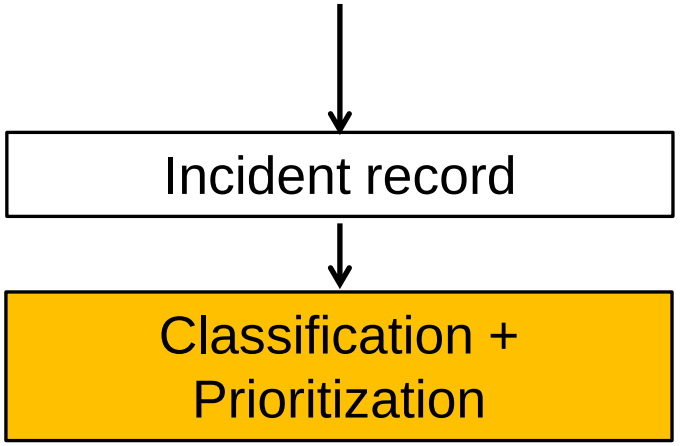
Security incident response at LRZ
Example

- **Classification**:
  - Botnet C&C-Server
  - Internal to external
- Setting priority:



Security incident response at LRZ
Example

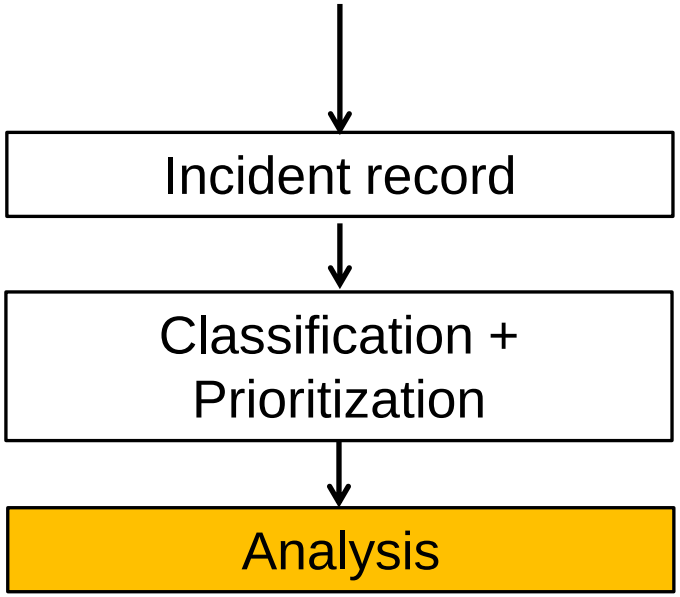
- **Classification**:
  - Botnet C&C server
  - Internal to external



- Setting priority:

Victim	External (1)	Grid, MWN	Internal
Services	Not concerned (1)	Grid, MWN	Important services
# systems	1 (1)	2,3	> 3
Attacker	External	Grid, MWN	Internal (3)

Security incident response at LRZ
Example



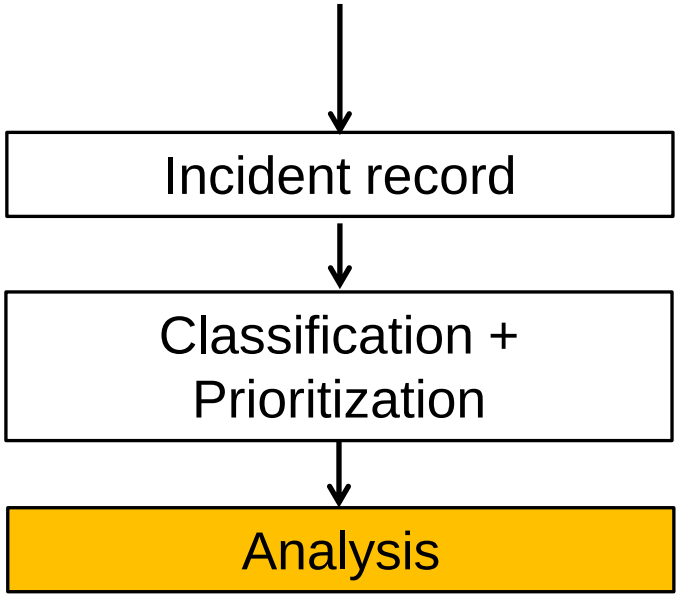
DFN AW Service message:
Confirmation internal monitoring

Message:

IP	Type	Last seen
129.xxx.xxx.xxx	Bot	2011-02-12 14:06:03 GMT+0100

Security incident response at LRZ
Example

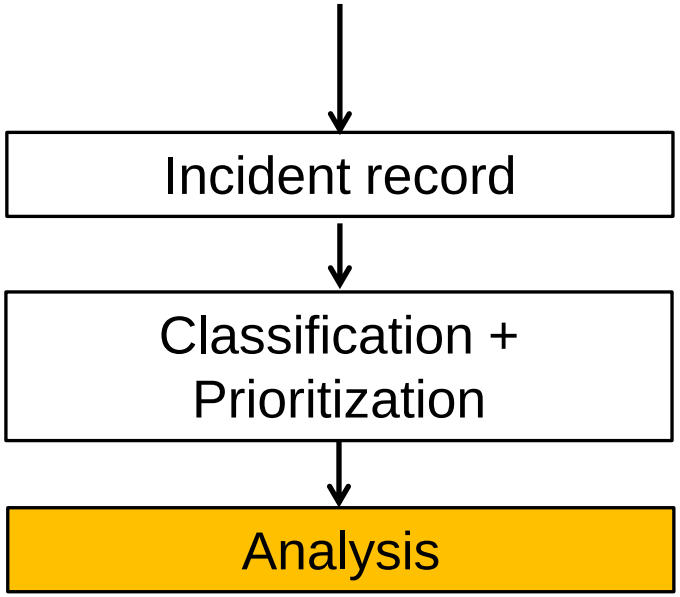
- **First measures: Disconnecting system from network**
- **Analysis & Diagnose:**
  - Analyzing SIEM events
  - Analyzing logfile entries



Security incident response at LRZ
Example

- **Analyzing SIEM events**

  „External SSH-Attacker“
  Destination 129.xxx.xxx.xxx



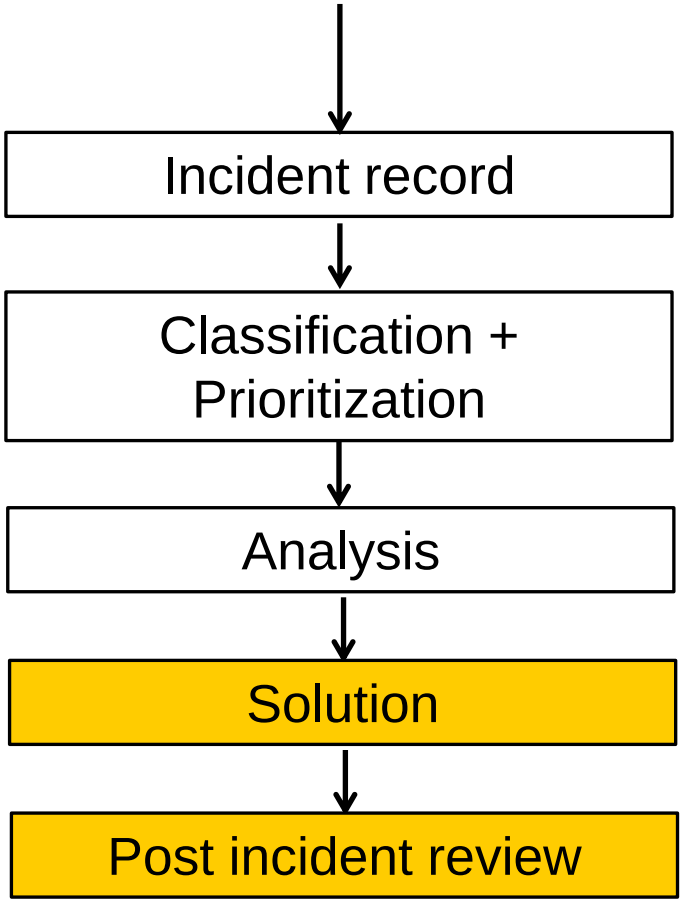
- **Analyzing logfiles**
  - SSH login from external ip address
  - Account „test“ weak password („test123!“)
  - Root exploiting
  - Installation bot software package

Security incident response at LRZ
Example

- **Solution:**
  Re-installation including all security patches

- **Post Incident Review:**

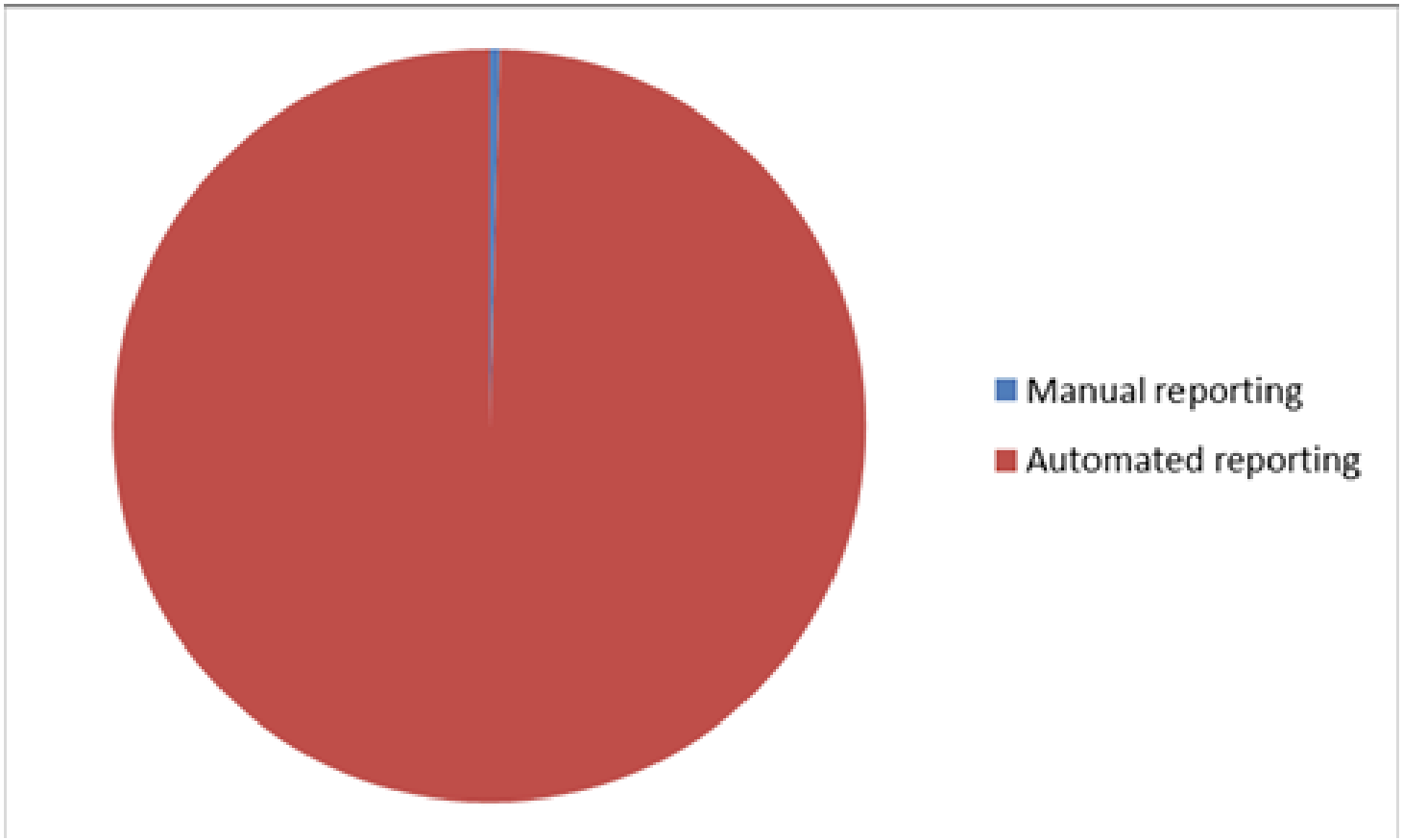
  Automated Blocking



Practical experiences

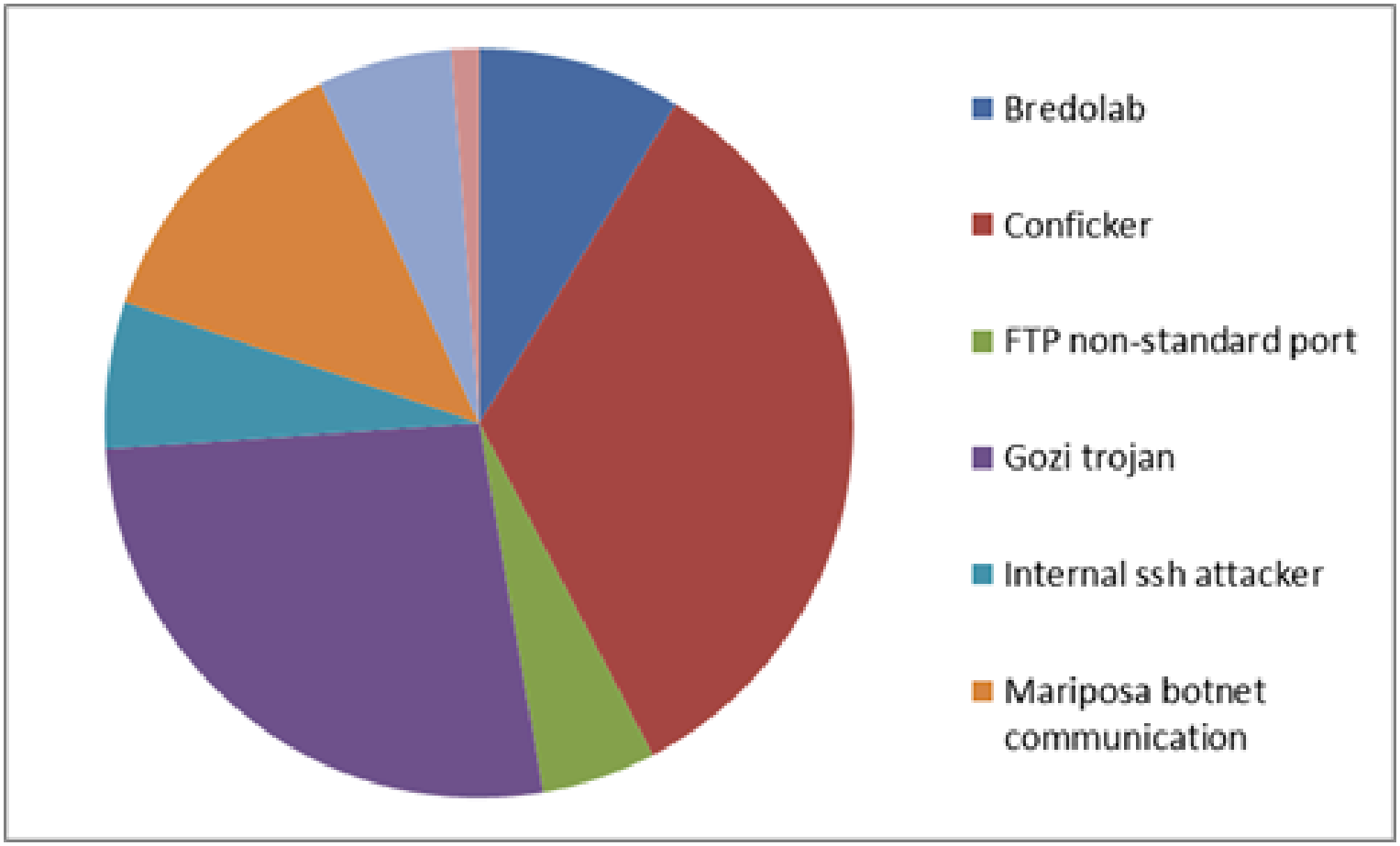
2010:

935 incidents: 99,6 % automated reporting & response!



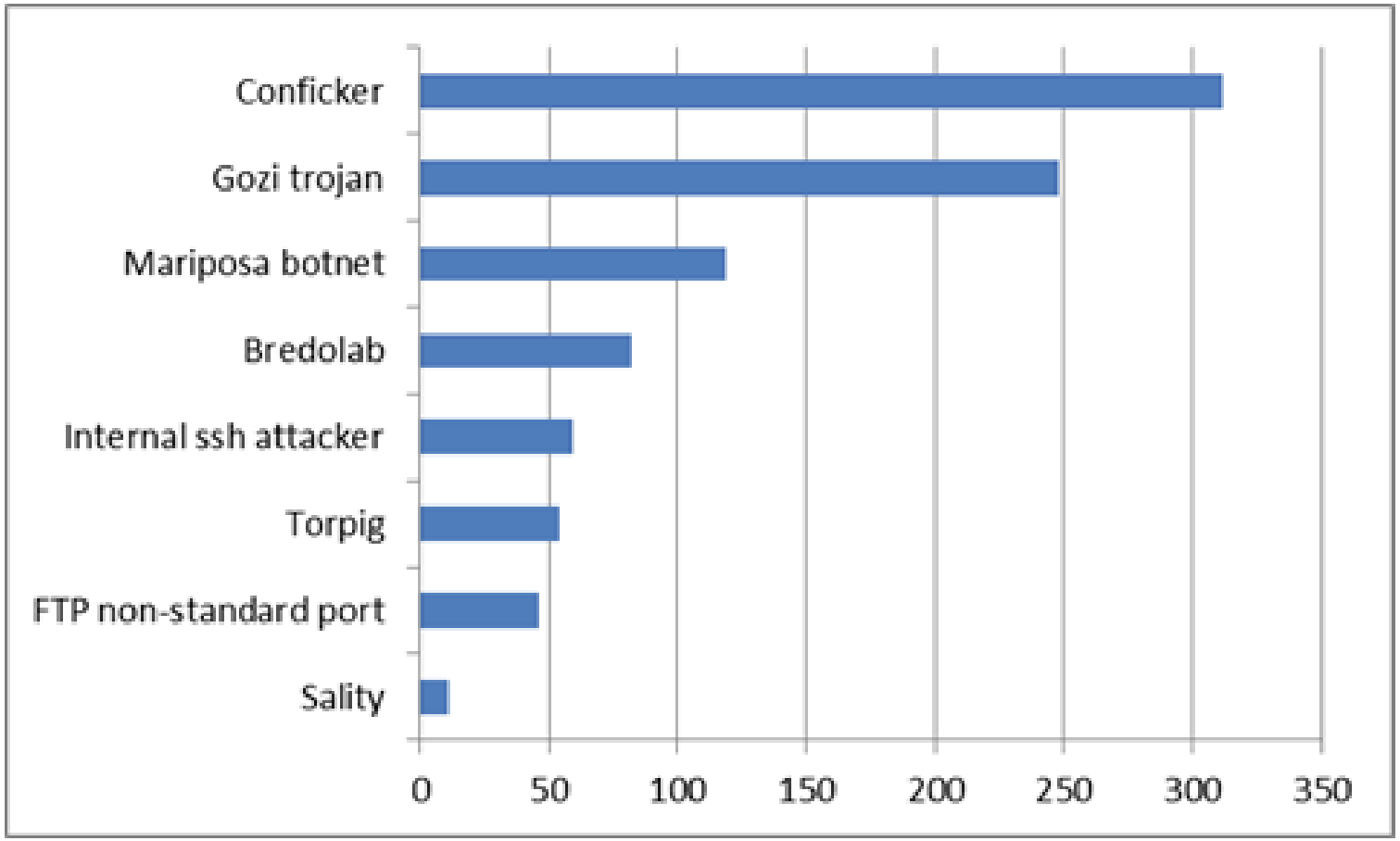
Practical experiences

2010: Compromised internal systems



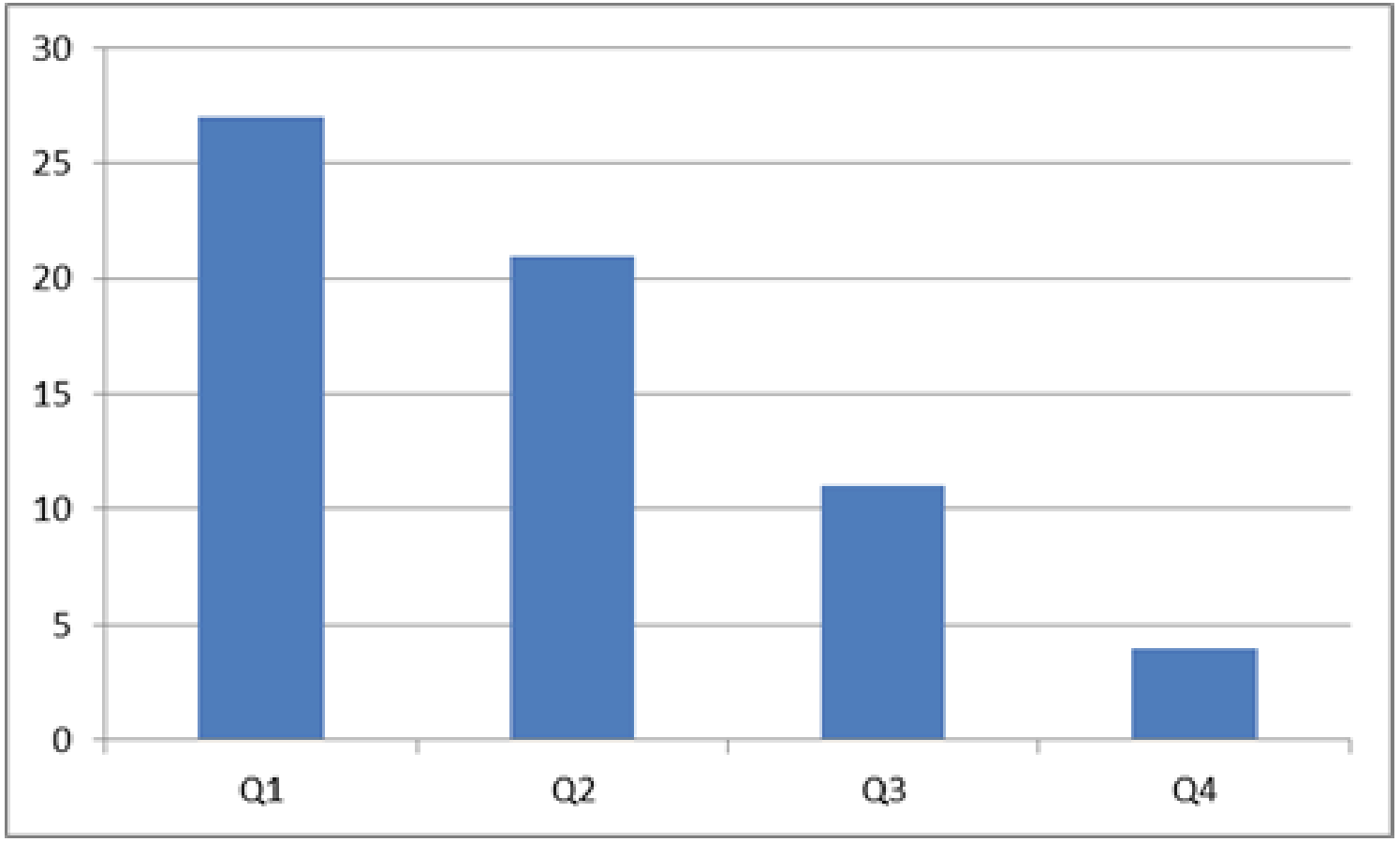
Practical experiences

2010: Compromised internal systems



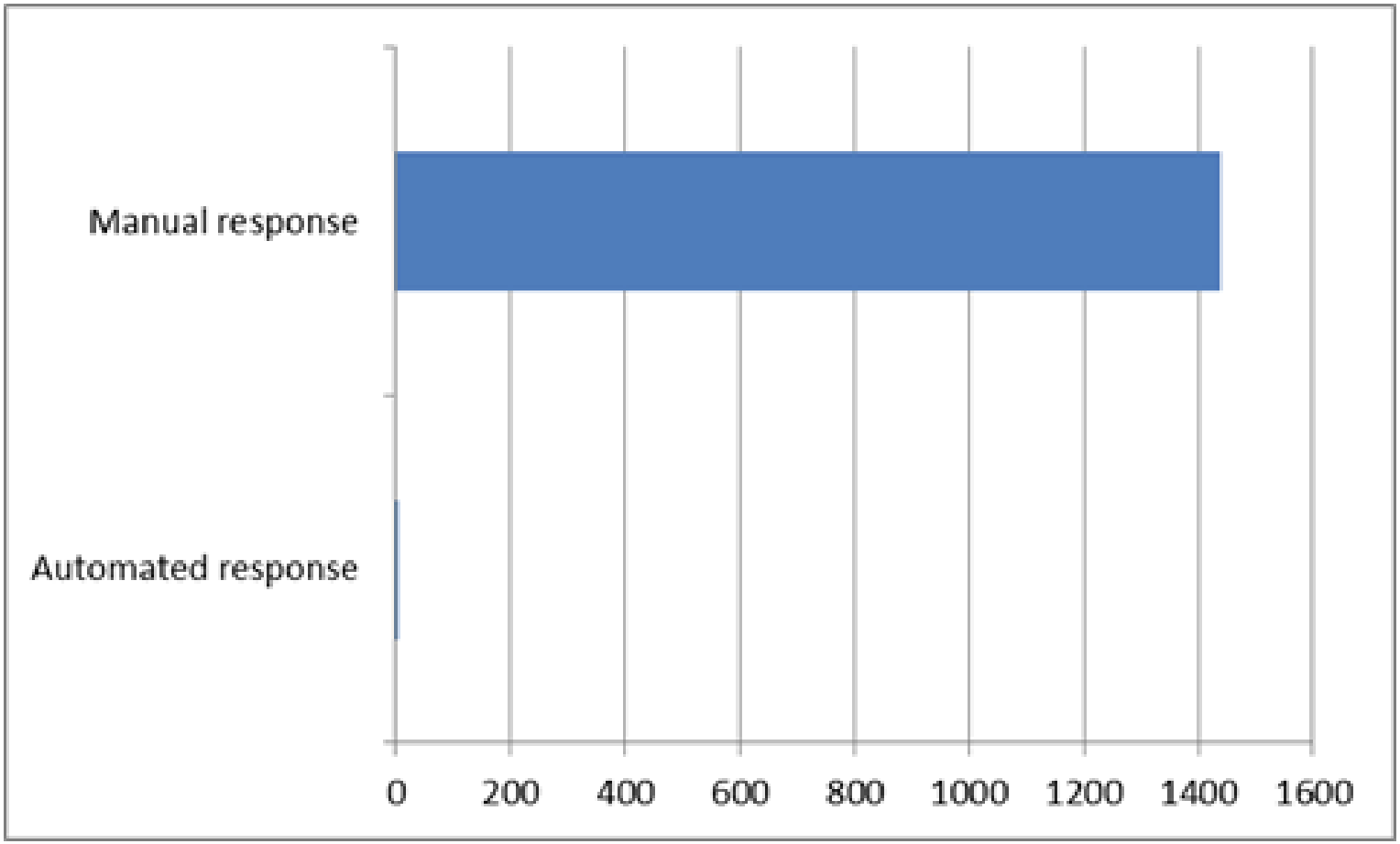
Practical experiences

Average # of ip addresses in DFN CSIRT warnings



Practical experiences

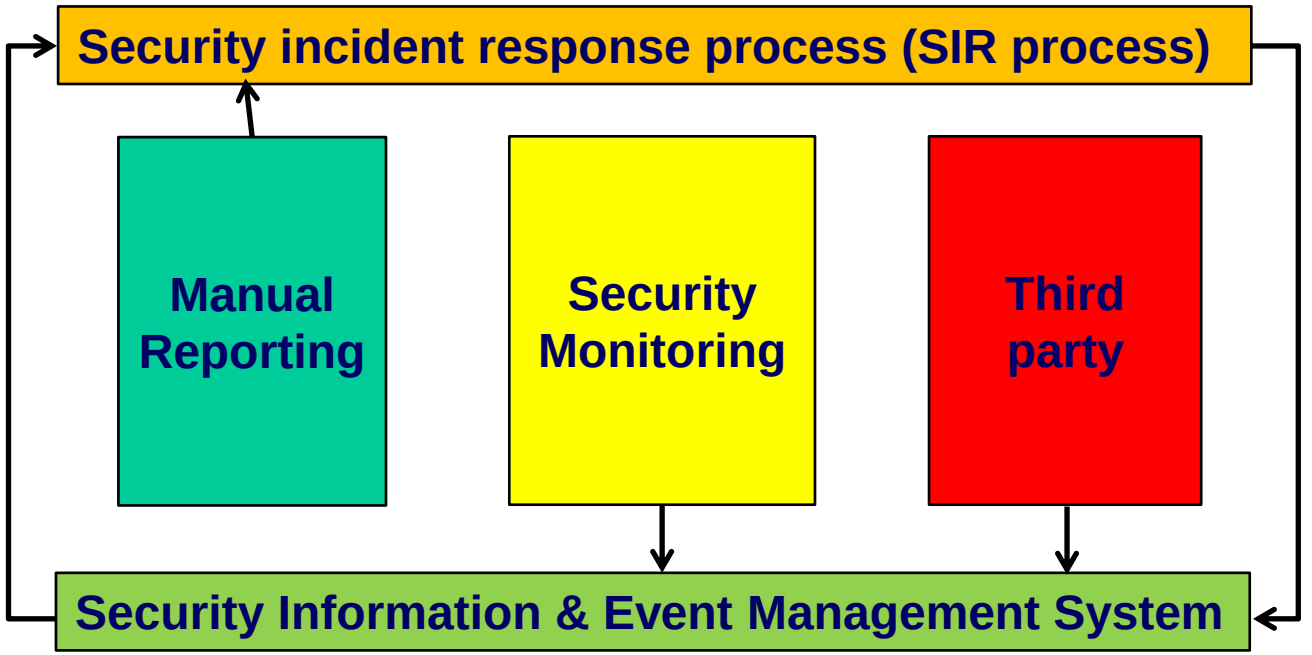
Average response time (in mins)



Recommended proceedings

- Define a security incident response process, including roles, responsibilities and tasks for
  - Administrators
  - PR department, management, law enforcement, …
  - System‘s user
  - Security incident coordinator (!)
- Use monitoring tools plus central SIEM
- Correlate security events and trigger automated responses

Questions?


Security incident response process (SIR process)
Manual Reporting
Security Monitoring
Third party
Security Information & Event Management System