GI SIDAR IMF 2006

# Automated resolving of security incidents as a key mechanism to fight massive infections of malicious software

Jochen Kaiser, Alexander Vitzthum, Peter Holleczek,
Regionales Rechenzentrum
Falko Dressler
Department of Computer Science 7
Communication Systems
Universität Erlangen-Nürnberg

# Overview

- PRISM is a tool which allows incident management.

- Introduction of PRISM
  - Architecture
  - Sensors
  - Workflow and Escalationmodel
  - Use-Cases
  - Screenshots

# Motivation/ Problems of Computer Security Teams

- An increase of computer security incidents means an increase of administrative work for CSIRT Teams
- Massive infections with malicious software increase the noise level in a network resulting in more IDS events
- Extrusion Detection becomes more difficult
- More reports from external CSIRTs about malicious activity in the local network

## Consequences

→ Reduce the noise level in the computer security incidents

→ Try to **differentiate between qualified and unqualified** computer security events

# Using conventional Helpdesksystems for CSIRT tasks

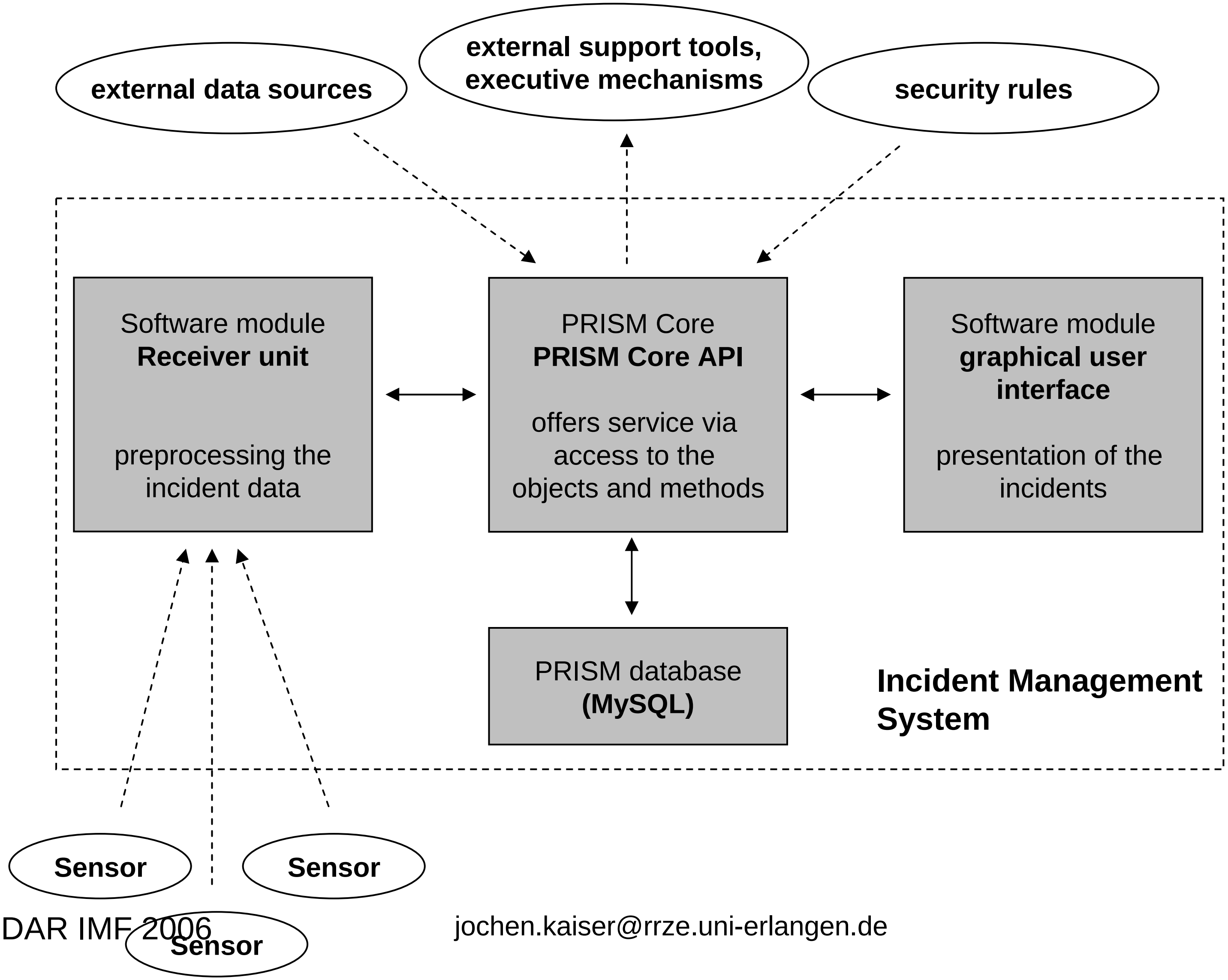
- Very often, CSIRTs use a modified Helpdesksystem for handling the computer security incidents.
- Components:
  - Mail2TT-Gateway
  - Queues for priorities to
  - maybe: Self service terminal tells status of own TT
  - maybe: Solution database
- missing:
  - self service terminal with advanced functions
  - automated assignment between incidents and solutions
  - delegation of computer security incidents

→ Development of the incident management tool PRISM:
(Portal for Reporting Incidents and Solution Management)

# PRISM architecture

- Modular System with well defined interfaces
- open source components:
  FreeBSD, Apache, MySQL, PERL
- IDMEF is used for the
- Terminal for Administrators
- Self service terminal for end users
- Escalation paths
- Role model differentiates in users, admins and CSIRTs
- Support for solution finding

# Modular Architecture



external data sources

external support tools, executive mechanisms

security rules

Software module
**Receiver unit**

preprocessing the incident data

PRISM Core
**PRISM Core API**

offers service via access to the objects and methods

Software module
**graphical user interface**

presentation of the incidents

PRISM database
**(MySQL)**

**Incident Management System**

**Sensor**

**Sensor**

**Sensor**

# Prerequisites which have to be fullfilled before an incident management can operate

- **Update Networks**
  resources for updating the end user systems in a network

- **Tool for blocking hosts**
  a tool is needed implements disconnection of a host upon required:
  block <IP>
  unblock <IP>
  *(the update resources must be reachable though!)*

- **Tool for information about the institutions organizational structure**
  a tool to deliver information about the responsible computer administrators and the head of departments of a given IP address

- **Optional: a tool to by-pass WWW queries to the incident management**
  the WWW-queries of an affected host shall be by-passed to the incident management so that the user gains knowledge of the problems.

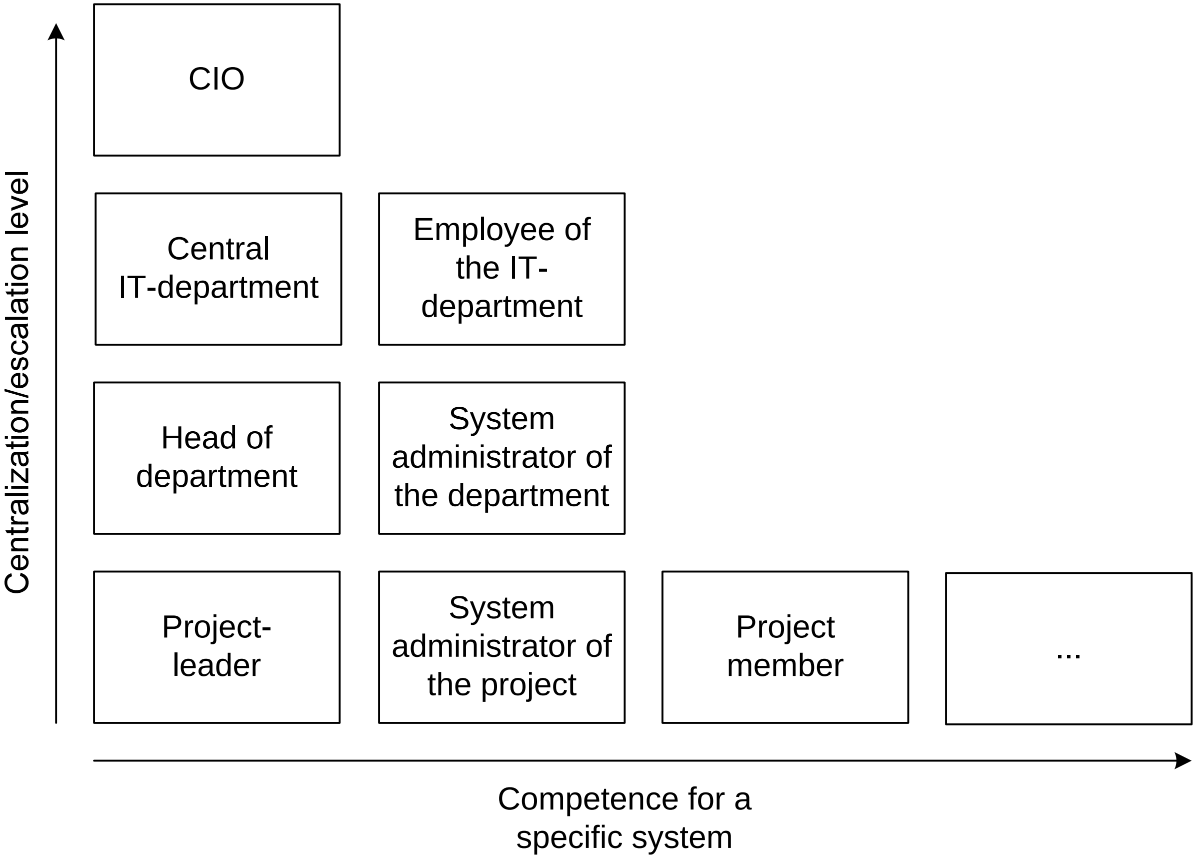
# PRISM sensors

- An incident report  IDMEF sensor
  (Intrusion Detection Message Exchange Format)
- several sensors are available:
  - sophos virus detection mail gateway
  - Intrusion Detection System Snort
    - IDMEF-Aggregator für Snort
  - manual input of incidents via a WWW interface
  - DNS policies (if a host has no entry in the DNS db)

# Role- and escalation model

- **Different Roles:**
  - end user in the role as a main user of a system
  - computer/network administrator of the sub network
  - CSIRT-Administrators
- **Escalation Models**
  - **Class 1 - Level 1** this describes security incidents which have a low risk to the organization.
  - **Class 1 - Level 2** An escalation to level 2 means that the end user was not able to solve the problem himself and that now the computer administrator which is responsible for the organization has to clear the problem.
  - **Class 1 - Level 3** In case the computer administrator cannot fix the problem in level 2, it is possible to increase the level to level 3 and to have a CSIRT administrator supervising the incident.
  - **Class 2 – all Levels** incidents are those which have a significant impact on the organization. These ones should not be solved from users or network administrators but from the CIRT team. A security incident of this class will never be in the scope of an end user.

# Example for a hierarchy of responsibility



CIO

Central IT-department

Employee of the IT-department

Head of department

System administrator of the department

Project-leader

System administrator of the project

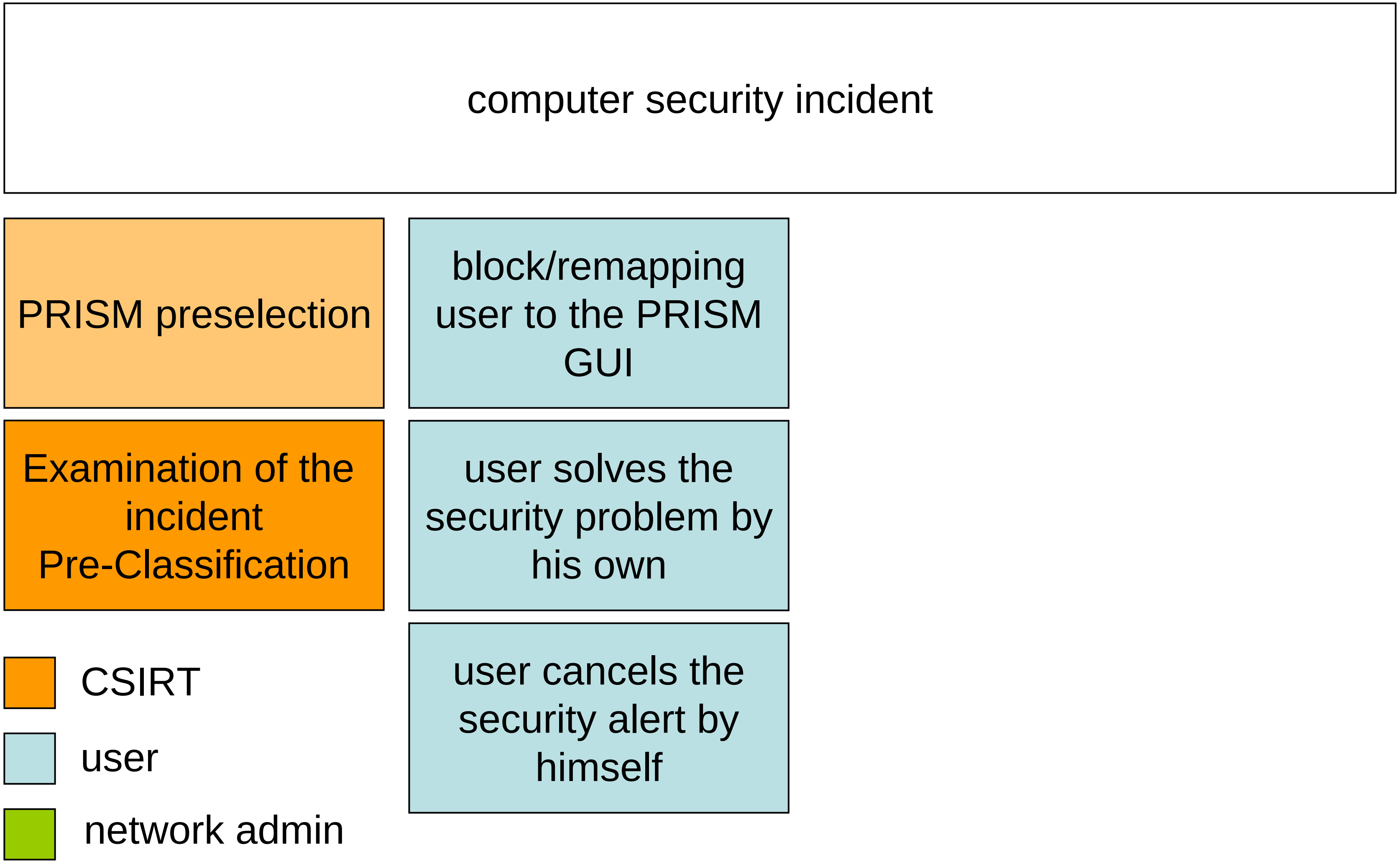
Project member

...

Centralization/escalation level

Competence for a specific system

# Workflow (no escalation)



computer security incident

PRISM preselection

block/remapping user to the PRISM GUI

Examination of the incident Pre-Classification

user solves the security problem by his own

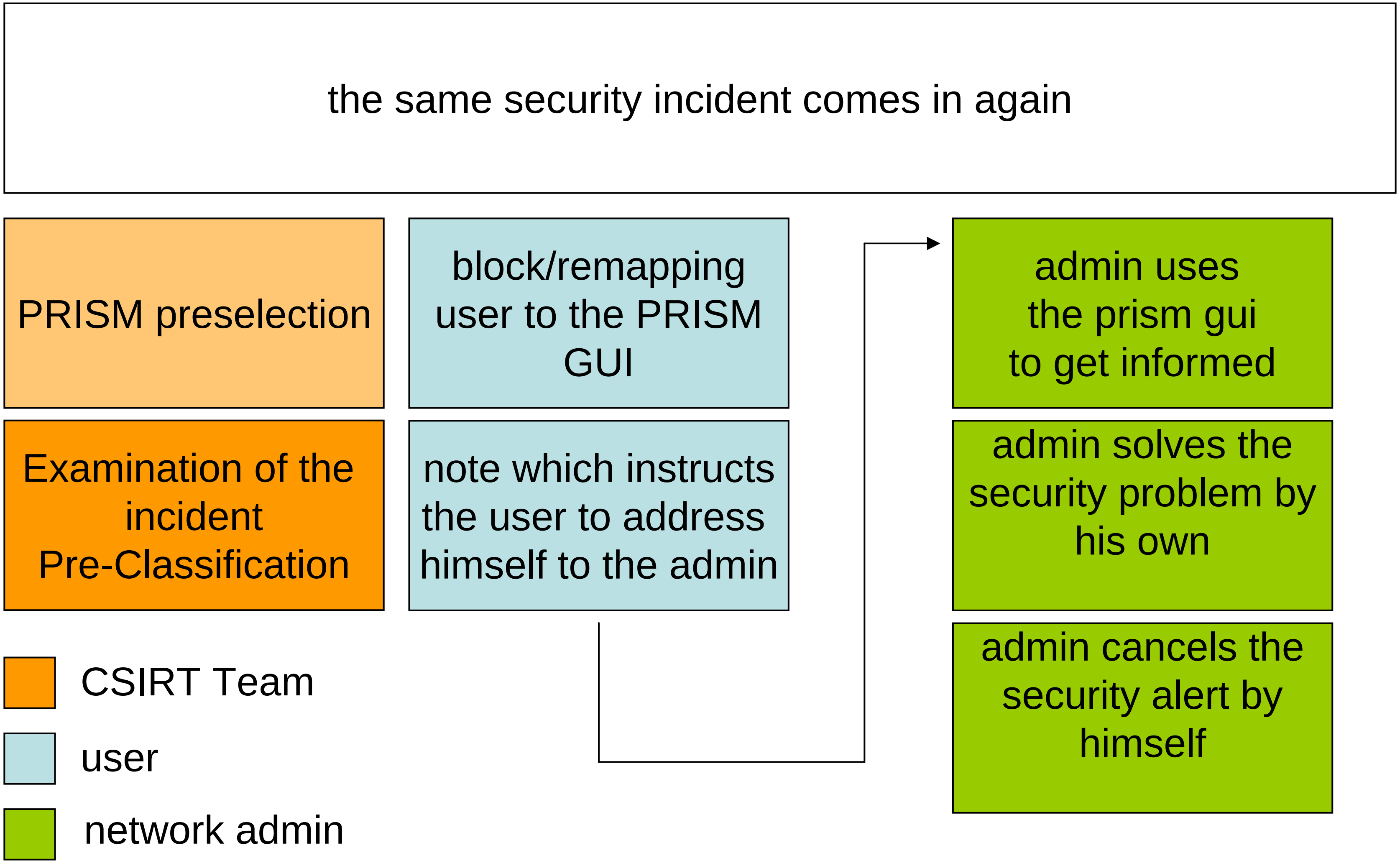
user cancels the security alert by himself

🟧 CSIRT

🟦 user

🟩 network admin

# Workflow (Escalation level 1)



the same security incident comes in again

PRISM preselection

block/remapping user to the PRISM GUI

admin uses the prism gui to get informed

Examination of the incident Pre-Classification

note which instructs the user to address himself to the admin

admin solves the security problem by his own

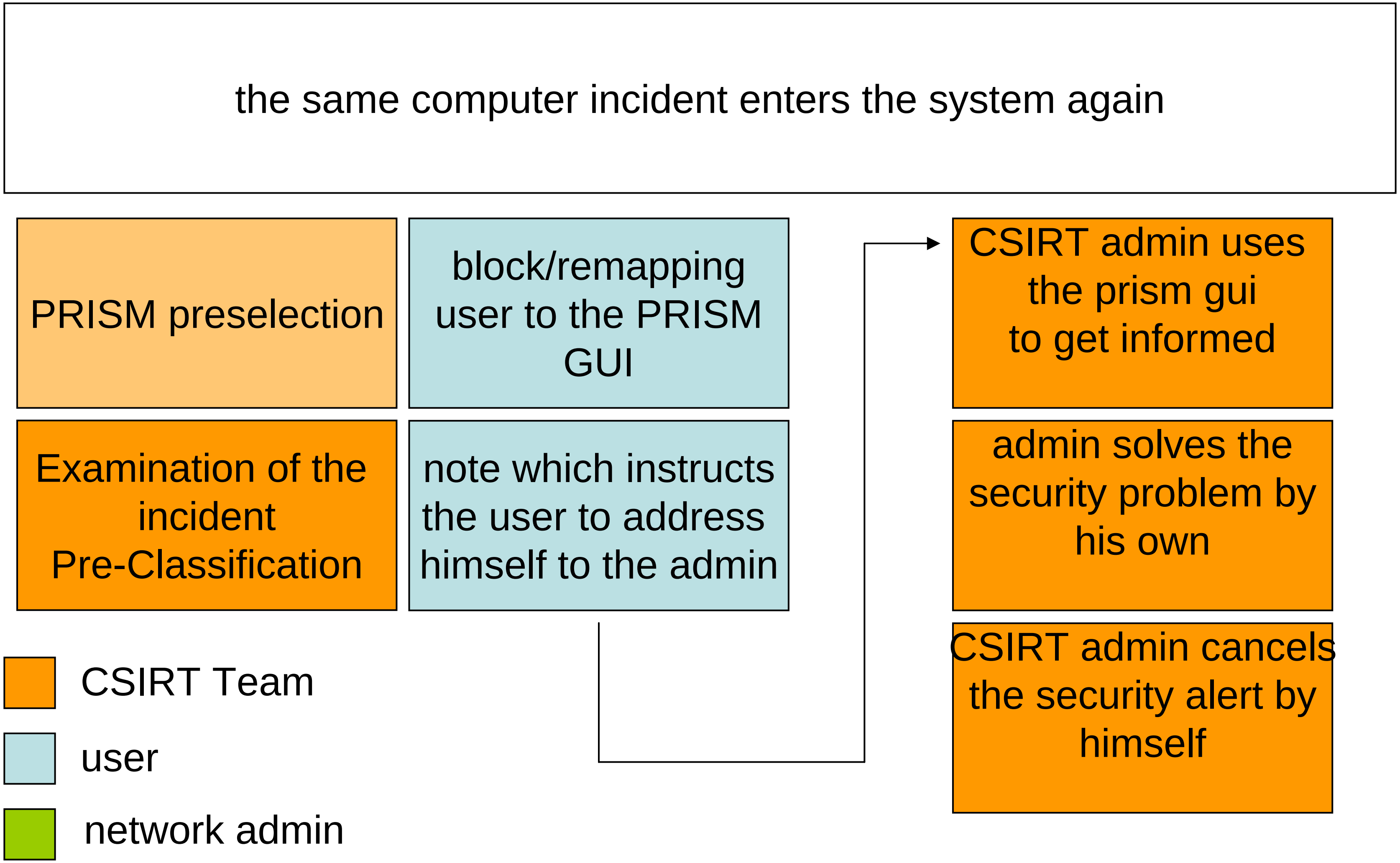
admin cancels the security alert by himself

🟧 CSIRT Team

🟦 user

🟩 network admin

# Workflow (Escalation level 2)



the same computer incident enters the system again

PRISM preselection

block/remapping user to the PRISM GUI

Examination of the incident Pre-Classification

note which instructs the user to address himself to the admin

CSIRT admin uses the prism gui to get informed

admin solves the security problem by his own

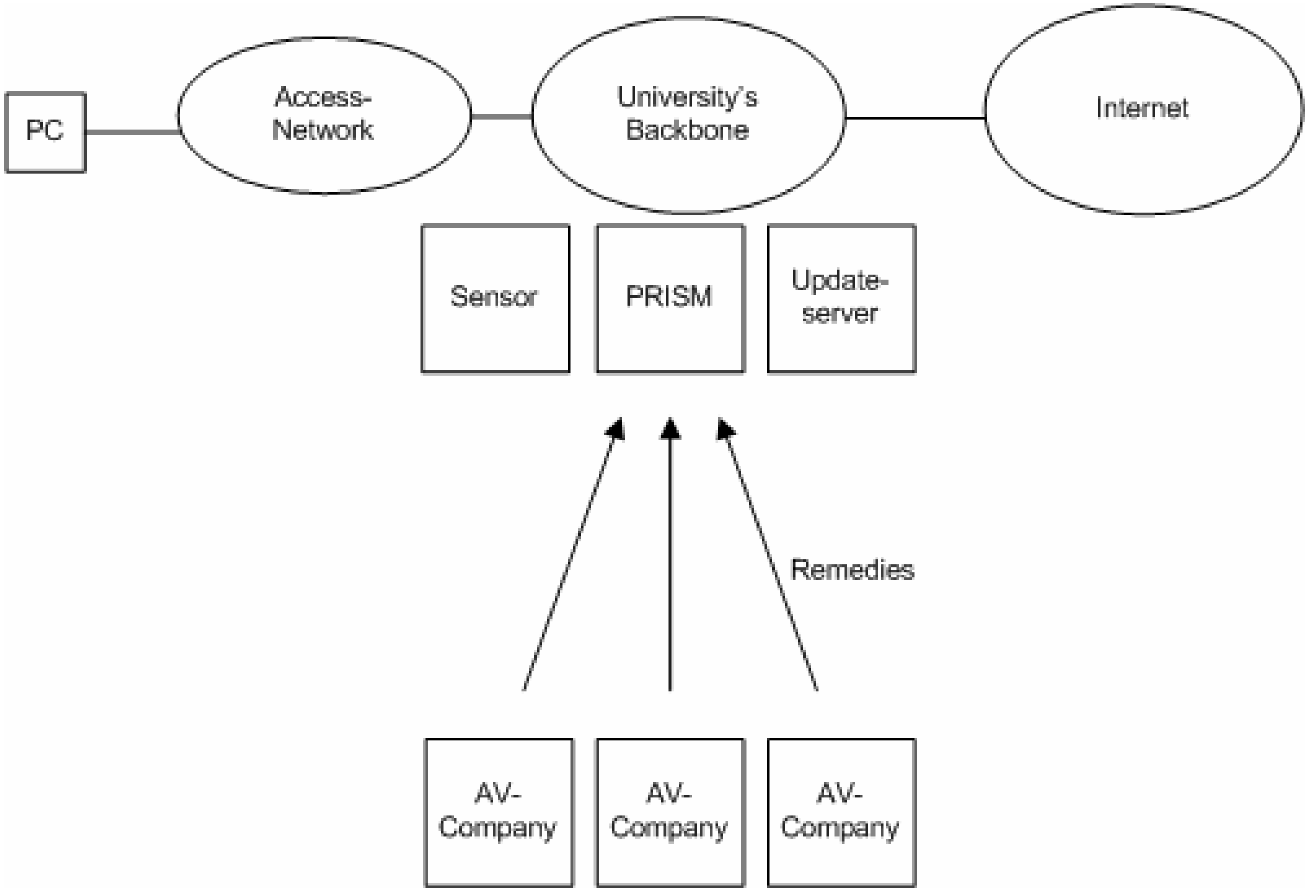
CSIRT admin cancels the security alert by himself

🟧 CSIRT Team

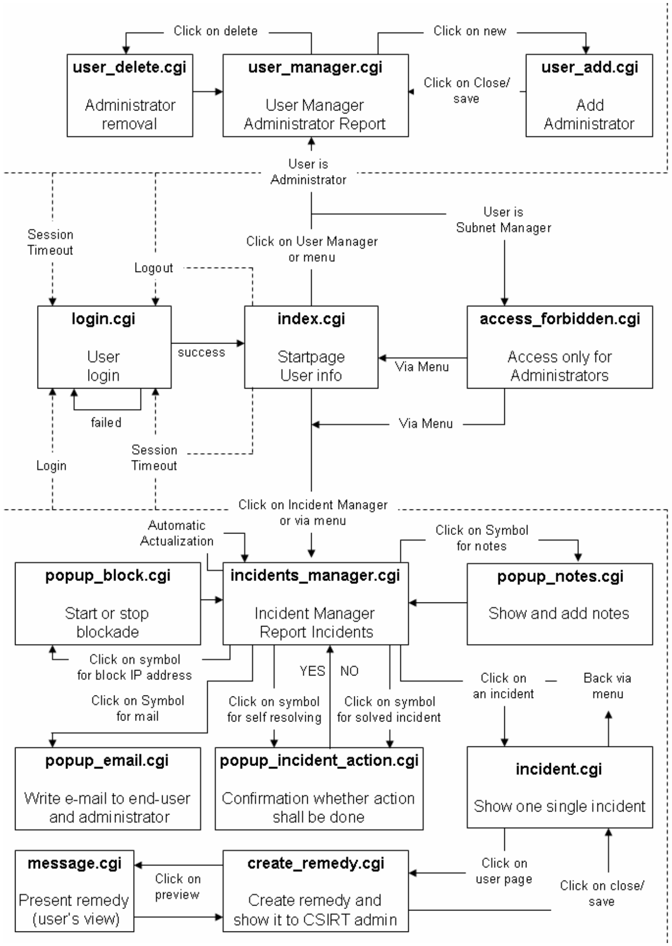
🟦 user

🟩 network admin

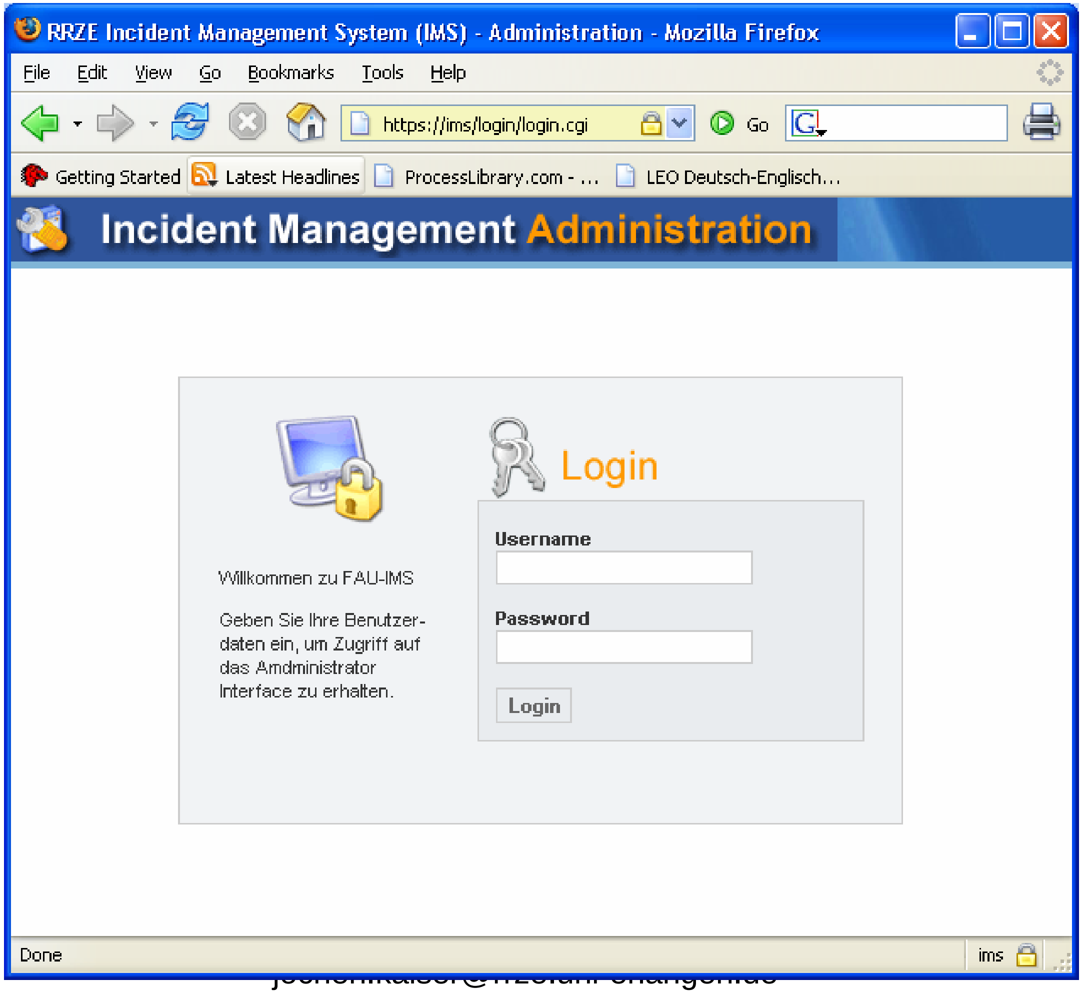
# usage scenario: university



# Overview of the implementation



# Example Session (1) - Login


RRZE Incident Management System (IMS) - Administration - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ims/login/login.cgi
Go
Getting Started
Latest Headlines
ProcessLibrary.com - ...
LEO Deutsch-Englisch...
Incident Management Administration
Done
ims

Willkommen zu FAU-IMS

Geben Sie Ihre Benutzerdaten ein, um Zugriff auf das Amdministrator Interface zu erhalten.

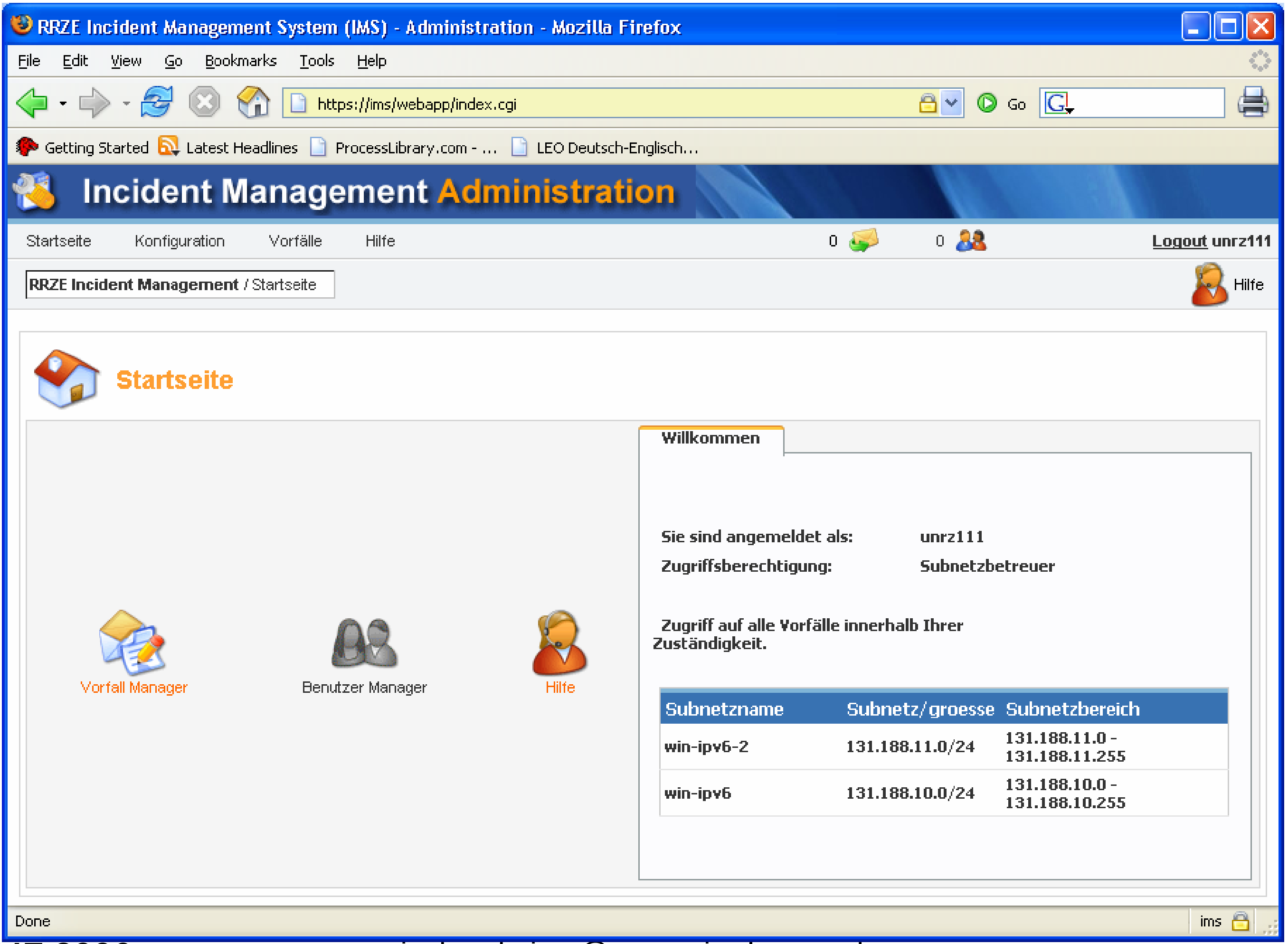
Login

Username

Password

Login

# Example Session (2) – main page



RRZE Incident Management System (IMS) - Administration - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ims/webapp/index.cgi
Go
Getting Started Latest Headlines ProcessLibrary.com - ... LEO Deutsch-Englisch...
Incident Management Administration
Startseite Konfiguration Vorfälle Hilfe
0
0
Logout unrz111
RRZE Incident Management / Startseite
Hilfe
Startseite
Vorfall Manager
Benutzer Manager
Hilfe
Willkommen
Done
ims

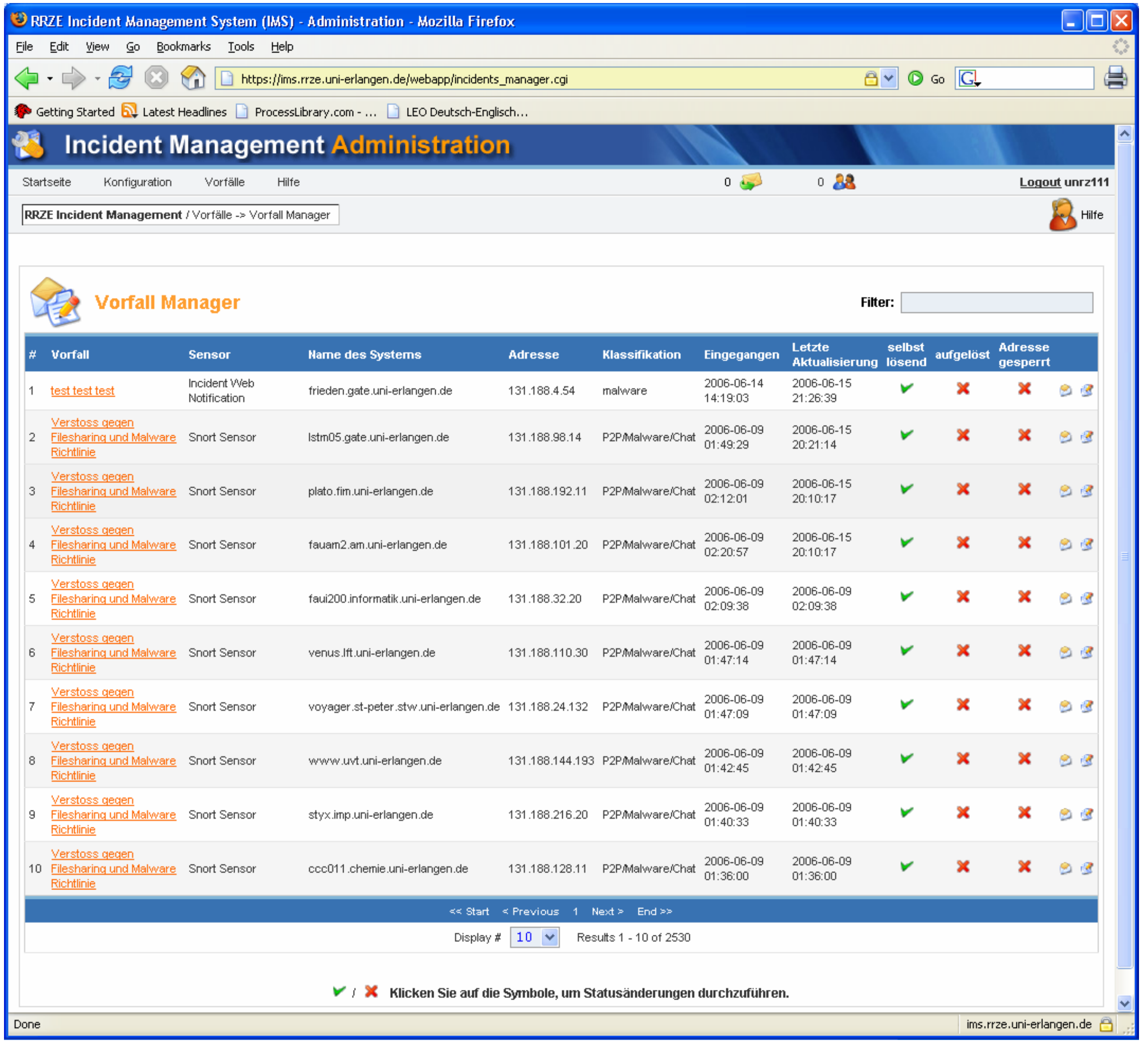
Sie sind angemeldet als: unrz111

Zugriffsberechtigung: Subnetzbetreuer

Zugriff auf alle Vorfälle innerhalb Ihrer Zuständigkeit.

| Subnetzname | Subnetz/groesse | Subnetzbereich |
|---|---|---|
| win-ipv6-2 | 131.188.11.0/24 | 131.188.11.0 -<br>131.188.11.255 |
| win-ipv6 | 131.188.10.0/24 | 131.188.10.0 -<br>131.188.10.255 |

# Example Session (3) – incident manager


RRZE Incident Management System (IMS) - Administration - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ims.rrze.uni-erlangen.de/webapp/incidents_manager.cgi
Go
Getting Started
Latest Headlines
ProcessLibrary.com - ...
LEO Deutsch-Englisch...
Done
ims.rrze.uni-erlangen.de

Incident Management Administration

Startseite Konfiguration Vorfälle Hilfe 0 0 Logout unrz111

RRZE Incident Management / Vorfälle -> Vorfall Manager Hilfe

Vorfall Manager

Filter:

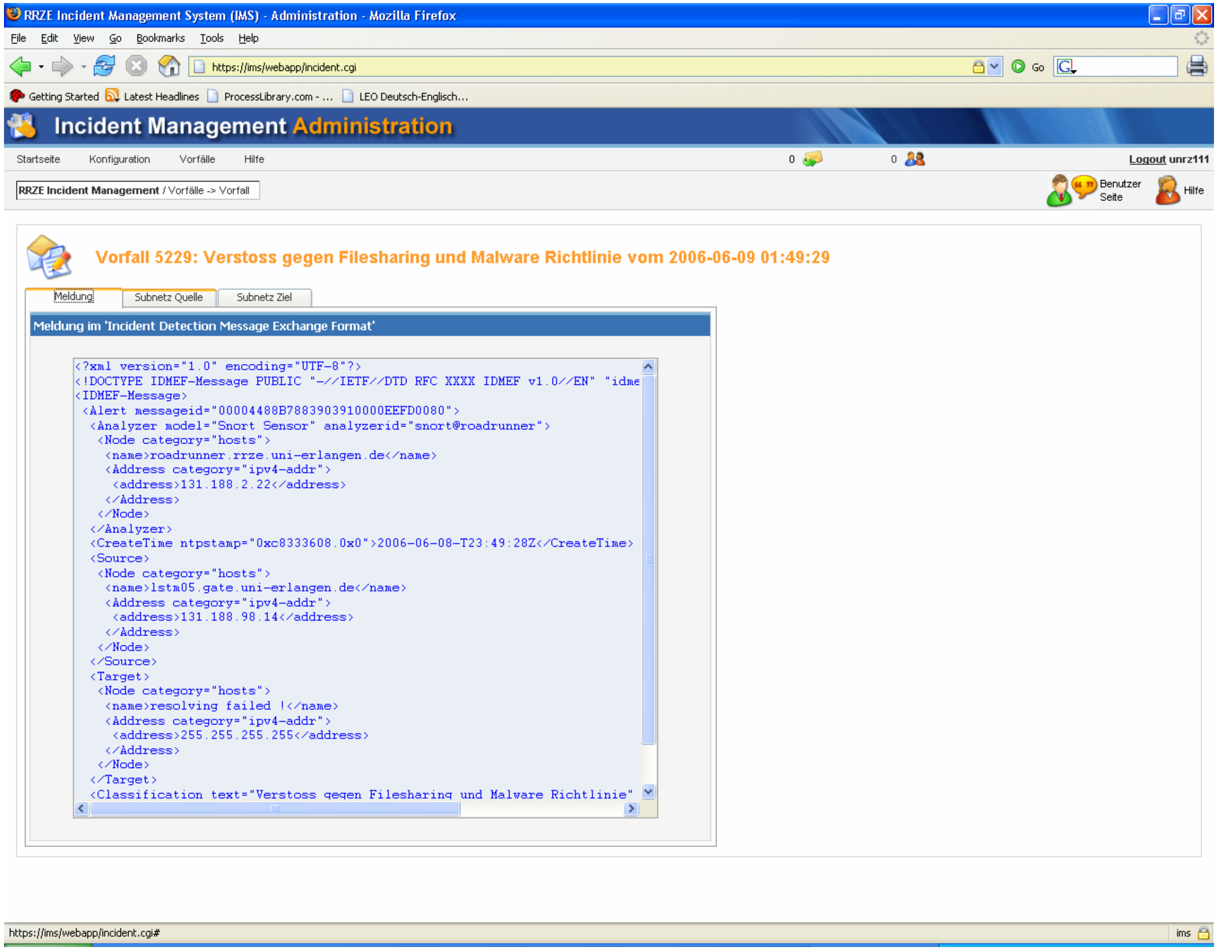
| # | Vorfall | Sensor | Name des Systems | Adresse | Klassifikation | Eingegangen | Letzte Aktualisierung | selbst lösend | aufgelöst | Adresse gesperrt |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | test test test | Incident Web Notification | frieden.gate.uni-erlangen.de | 131.188.4.54 | malware | 2006-06-14 14:19:03 | 2006-06-15 21:26:39 | ✓ | ✗ | ✗ |
| 2 | Verstoss gegen Filesharing und Malware Richtlinie | Snort Sensor | lstm05.gate.uni-erlangen.de | 131.188.98.14 | P2P/Malware/Chat | 2006-06-09 01:49:29 | 2006-06-15 20:21:14 | ✓ | ✗ | ✗ |
| 3 | Verstoss gegen Filesharing und Malware Richtlinie | Snort Sensor | plato.fim.uni-erlangen.de | 131.188.192.11 | P2P/Malware/Chat | 2006-06-09 02:12:01 | 2006-06-15 20:10:17 | ✓ | ✗ | ✗ |
| 4 | Verstoss gegen Filesharing und Malware Richtlinie | Snort Sensor | fauam2.am.uni-erlangen.de | 131.188.101.20 | P2P/Malware/Chat | 2006-06-09 02:20:57 | 2006-06-15 20:10:17 | ✓ | ✗ | ✗ |
| 5 | Verstoss gegen Filesharing und Malware Richtlinie | Snort Sensor | faui200.informatik.uni-erlangen.de | 131.188.32.20 | P2P/Malware/Chat | 2006-06-09 02:09:38 | 2006-06-09 02:09:38 | ✓ | ✗ | ✗ |
| 6 | Verstoss gegen Filesharing und Malware Richtlinie | Snort Sensor | venus.lft.uni-erlangen.de | 131.188.110.30 | P2P/Malware/Chat | 2006-06-09 01:47:14 | 2006-06-09 01:47:14 | ✓ | ✗ | ✗ |
| 7 | Verstoss gegen Filesharing und Malware Richtlinie | Snort Sensor | voyager.st-peter.stw.uni-erlangen.de | 131.188.24.132 | P2P/Malware/Chat | 2006-06-09 01:47:09 | 2006-06-09 01:47:09 | ✓ | ✗ | ✗ |
| 8 | Verstoss gegen Filesharing und Malware Richtlinie | Snort Sensor | www.uvt.uni-erlangen.de | 131.188.144.193 | P2P/Malware/Chat | 2006-06-09 01:42:45 | 2006-06-09 01:42:45 | ✓ | ✗ | ✗ |
| 9 | Verstoss gegen Filesharing und Malware Richtlinie | Snort Sensor | styx.imp.uni-erlangen.de | 131.188.216.20 | P2P/Malware/Chat | 2006-06-09 01:40:33 | 2006-06-09 01:40:33 | ✓ | ✗ | ✗ |
| 10 | Verstoss gegen Filesharing und Malware Richtlinie | Snort Sensor | ccc011.chemie.uni-erlangen.de | 131.188.128.11 | P2P/Malware/Chat | 2006-06-09 01:36:00 | 2006-06-09 01:36:00 | ✓ | ✗ | ✗ |

<< Start < Previous 1 Next > End >>

Display # 10 Results 1 - 10 of 2530

✓ / ✗ Klicken Sie auf die Symbole, um Statusänderungen durchzuführen.

# Example Session (4) – IDMEF raw

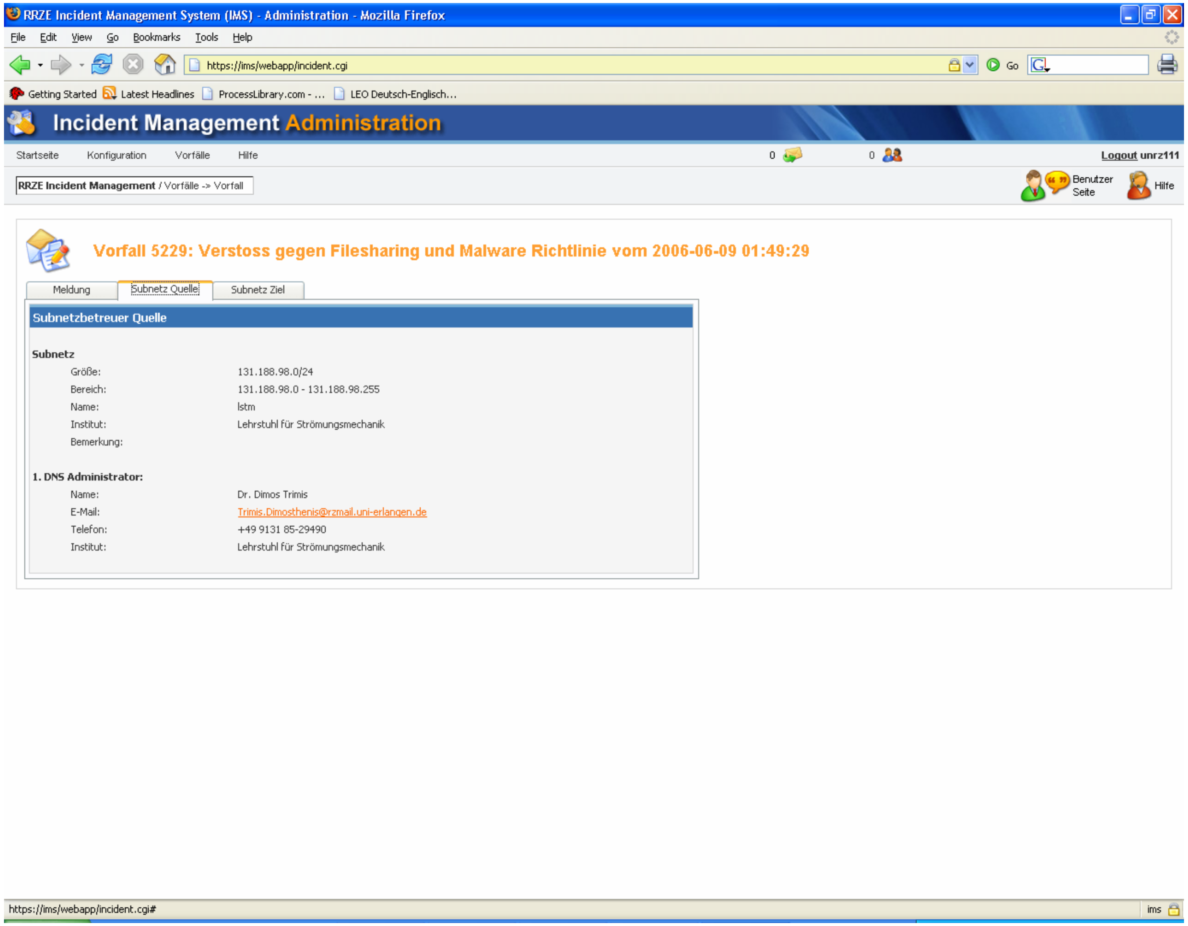

RRZE Incident Management System (IMS) - Administration - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ims/webapp/incident.cgi
Go
Getting Started Latest Headlines ProcessLibrary.com - ... LEO Deutsch-Englisch...
Incident Management Administration
Startseite Konfiguration Vorfälle Hilfe
0
0
Logout unrz111
RRZE Incident Management / Vorfälle -> Vorfall
Benutzer Seite
Hilfe
Meldung
Subnetz Quelle
Subnetz Ziel
https://ims/webapp/incident.cgi#
ims

Vorfall 5229: Verstoss gegen Filesharing und Malware Richtlinie vom 2006-06-09 01:49:29

Meldung im 'Incident Detection Message Exchange Format'

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IDMEF-Message PUBLIC "-//IETF//DTD RFC XXXX IDMEF v1.0//EN" "idme
<IDMEF-Message>
 <Alert messageid="00004488B7883903910000EEFD0080">
  <Analyzer model="Snort Sensor" analyzerid="snort@roadrunner">
   <Node category="hosts">
    <name>roadrunner.rrze.uni-erlangen.de</name>
    <Address category="ipv4-addr">
     <address>131.188.2.22</address>
    </Address>
   </Node>
  </Analyzer>
  <CreateTime ntpstamp="0xc8333608.0x0">2006-06-08-T23:49:28Z</CreateTime>
  <Source>
   <Node category="hosts">
    <name>lstm05.gate.uni-erlangen.de</name>
    <Address category="ipv4-addr">
     <address>131.188.98.14</address>
    </Address>
   </Node>
  </Source>
  <Target>
   <Node category="hosts">
    <name>resolving failed !</name>
    <Address category="ipv4-addr">
     <address>255.255.255.255</address>
    </Address>
   </Node>
  </Target>
  <Classification text="Verstoss gegen Filesharing und Malware Richtlinie"
```

# Example Session (5) – Contact Persons



RRZE Incident Management System (IMS) - Administration - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ims/webapp/incident.cgi
Go
Getting Started
Latest Headlines
ProcessLibrary.com - ...
LEO Deutsch-Englisch...
Incident Management Administration
Startseite
Konfiguration
Vorfälle
Hilfe
0
0
Logout unrz111
Benutzer Seite
Hilfe
Meldung
Subnetz Quelle
Subnetz Ziel
https://ims/webapp/incident.cgi#
ims

**RRZE Incident Management** / Vorfälle -> Vorfall

Vorfall 5229: Verstoss gegen Filesharing und Malware Richtlinie vom 2006-06-09 01:49:29

Subnetzbetreuer Quelle

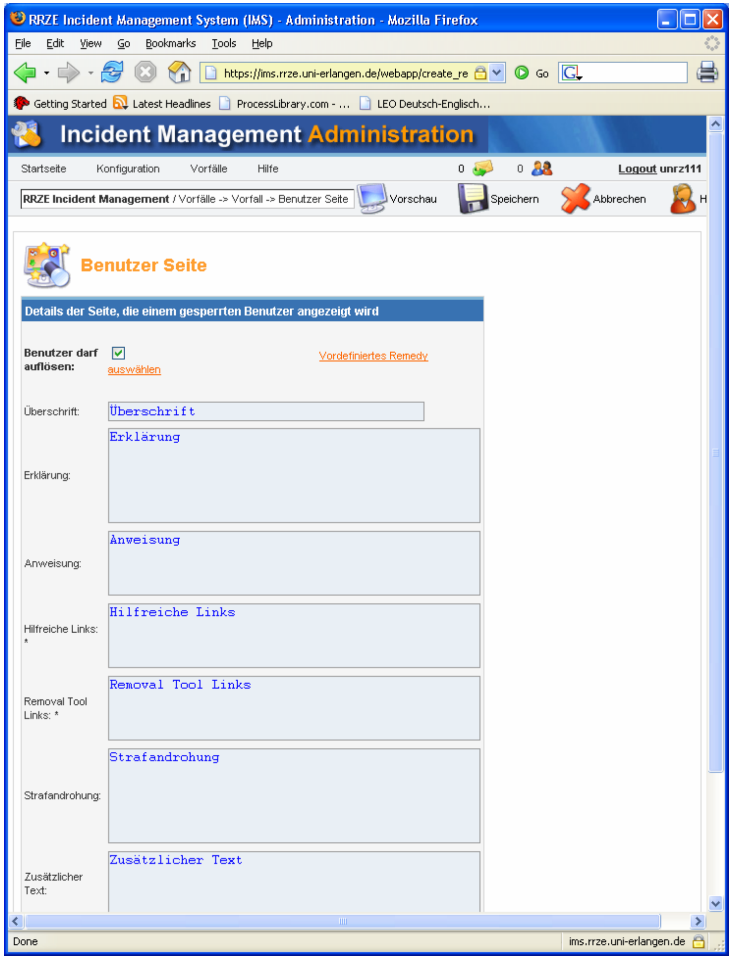
**Subnetz**

| | |
|---|---|
| Größe: | 131.188.98.0/24 |
| Bereich: | 131.188.98.0 - 131.188.98.255 |
| Name: | lstm |
| Institut: | Lehrstuhl für Strömungsmechanik |
| Bemerkung: | |

**1. DNS Administrator:**

| | |
|---|---|
| Name: | Dr. Dimos Trimis |
| E-Mail: | Trimis.Dimosthenis@rzmail.uni-erlangen.de |
| Telefon: | +49 9131 85-29490 |
| Institut: | Lehrstuhl für Strömungsmechanik |

# Example Session (6) – user page


RRZE Incident Management System (IMS) - Administration - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ims.rrze.uni-erlangen.de/webapp/create_re
Go
Getting Started
Latest Headlines
ProcessLibrary.com - ...
LEO Deutsch-Englisch...
Incident Management Administration
Startseite
Konfiguration
Vorfälle
Hilfe
0
0
Logout unrz111
RRZE Incident Management / Vorfälle -> Vorfall -> Benutzer Seite
Vorschau
Speichern
Abbrechen
H
Done
ims.rrze.uni-erlangen.de

**Benutzer Seite**

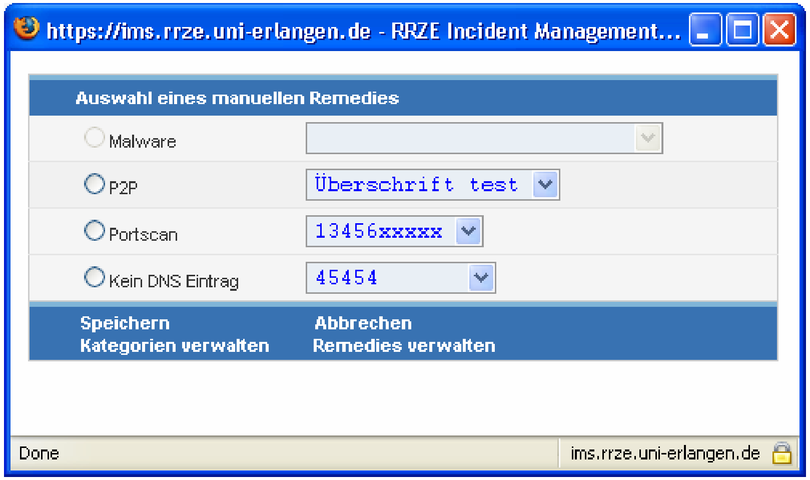
**Details der Seite, die einem gesperrten Benutzer angezeigt wird**

**Benutzer darf auflösen:** ☑ auswählen

Vordefiniertes Remedy

| | |
|---|---|
| Überschrift: | Überschrift |
| Erklärung: | Erklärung |
| Anweisung: | Anweisung |
| Hilfreiche Links: * | Hilfreiche Links |
| Removal Tool Links: * | Removal Tool Links |
| Strafandrohung: | Strafandrohung |
| Zusätzlicher Text: | Zusätzlicher Text |

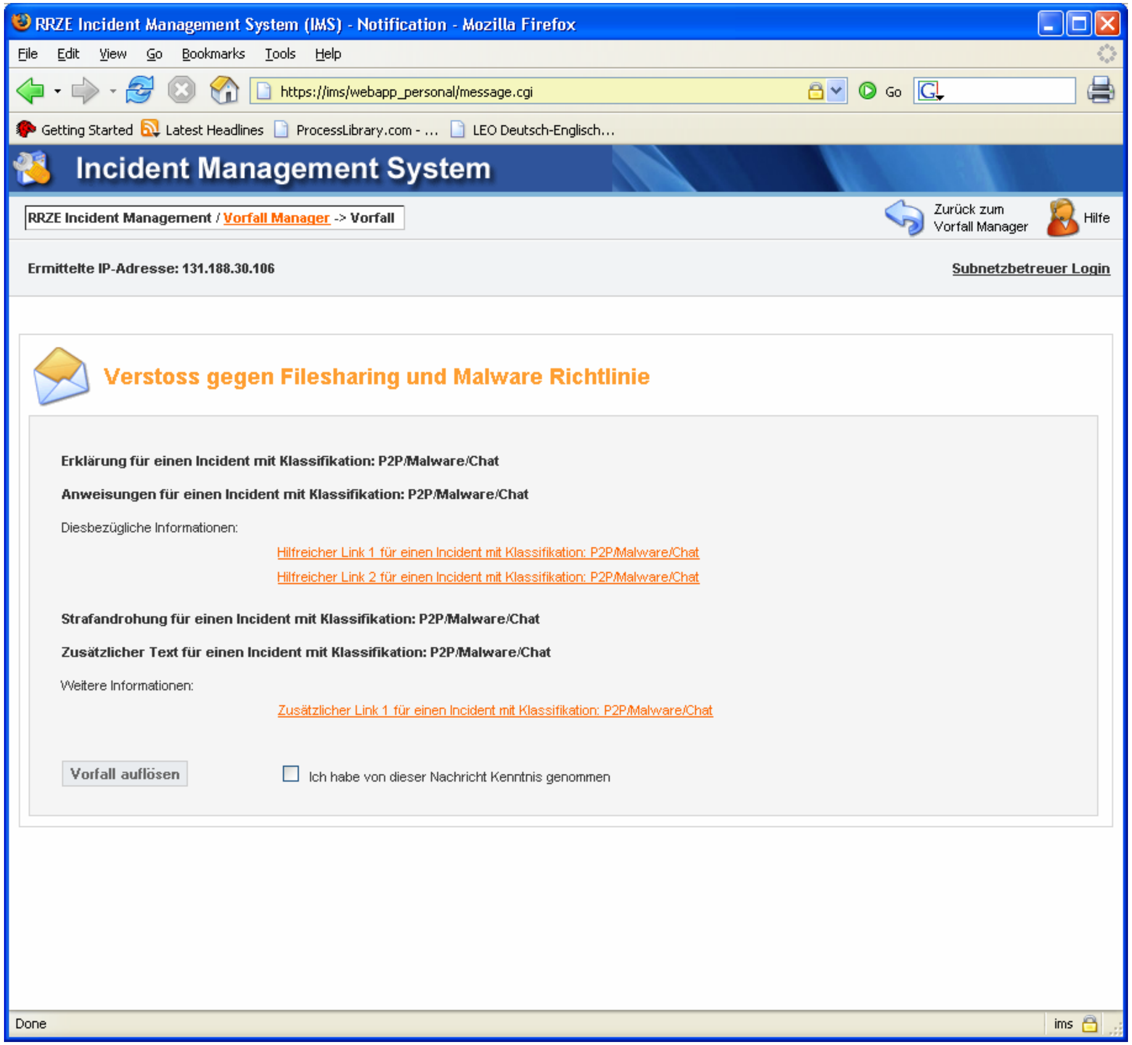
# Example Session (7) – solution selection


https://ims.rrze.uni-erlangen.de - RRZE Incident Management...
Done
ims.rrze.uni-erlangen.de

Auswahl eines manuellen Remedies

| | |
|---|---|
| ○ Malware | |
| ○ P2P | Überschrift test |
| ○ Portscan | 13456xxxxxx |
| ○ Kein DNS Eintrag | 45454 |

# Example Session (8) – WWW user page


RRZE Incident Management System (IMS) - Notification - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ims/webapp_personal/message.cgi
Go
Getting Started
Latest Headlines
ProcessLibrary.com - ...
LEO Deutsch-Englisch...
Incident Management System
RRZE Incident Management / Vorfall Manager -> Vorfall
Zurück zum Vorfall Manager
Hilfe
Subnetzbetreuer Login
Done
ims

Ermittelte IP-Adresse: 131.188.30.106

## Verstoss gegen Filesharing und Malware Richtlinie

**Erklärung für einen Incident mit Klassifikation: P2P/Malware/Chat**

**Anweisungen für einen Incident mit Klassifikation: P2P/Malware/Chat**

Diesbezügliche Informationen:

Hilfreicher Link 1 für einen Incident mit Klassifikation: P2P/Malware/Chat
Hilfreicher Link 2 für einen Incident mit Klassifikation: P2P/Malware/Chat

**Strafandrohung für einen Incident mit Klassifikation: P2P/Malware/Chat**

**Zusätzlicher Text für einen Incident mit Klassifikation: P2P/Malware/Chat**

Weitere Informationen:

Zusätzlicher Link 1 für einen Incident mit Klassifikation: P2P/Malware/Chat

Vorfall auflösen

□ Ich habe von dieser Nachricht Kenntnis genommen

# Conclusion and next steps

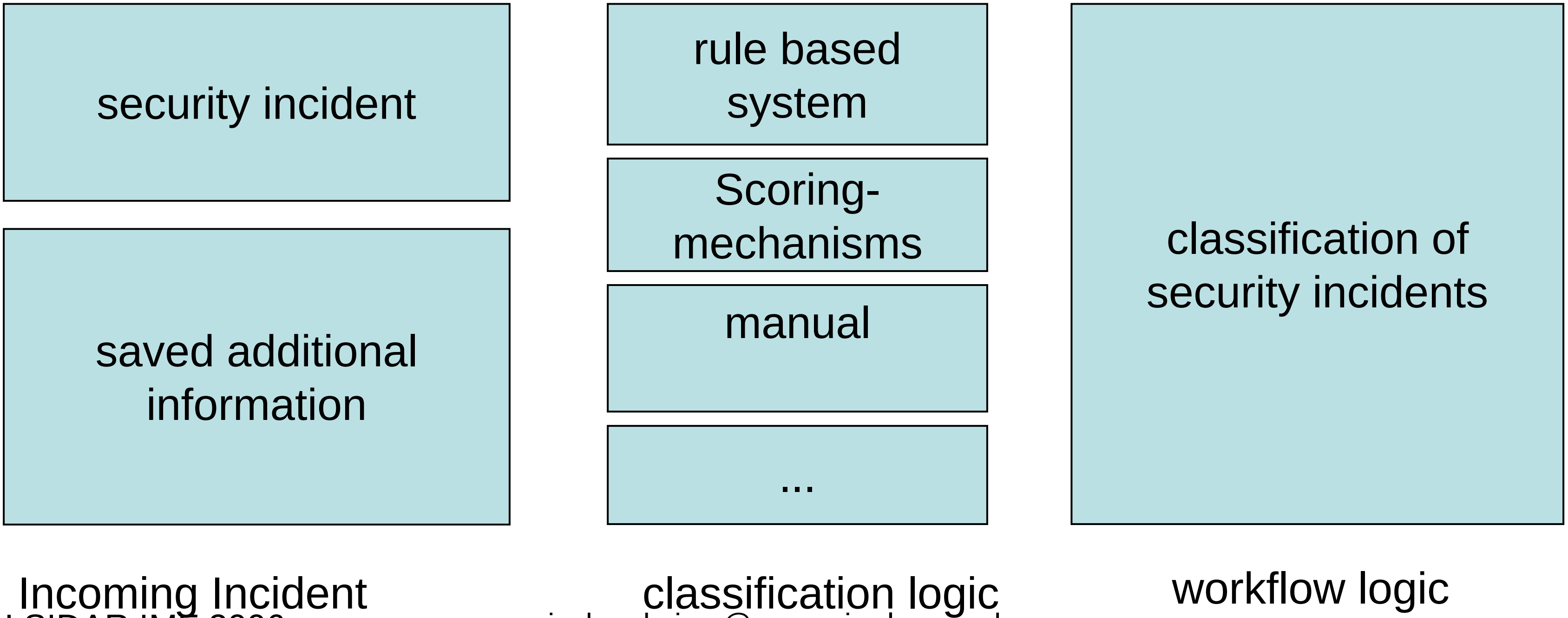
- PRISM is a comfortable tool for administration of security incidents with inclusion of the end user
- PRISM works, but not all prerequisites are fulfilled

Next steps:

- research and implementation of additional incident evaluation methods
- gaining more experience through practical usage
- new research:
  „Strategies for Evaluating computer security incidents“

# Future work:
# Possible classification strategies

- to process a big number of security incidents, automated processing has to be improved
- research has to be done which relevant (meta) information about the security incident is needed


security incident
saved additional information
rule based system
Scoring-mechanisms
manual
...
classification of security incidents
Incoming Incident
classification logic
workflow logic