Entwicklung eines Intrusion-Detection-Verfahrens zur Erkennung von VoIP-initiierten DoS-Attacken auf Rettungsleitstellen

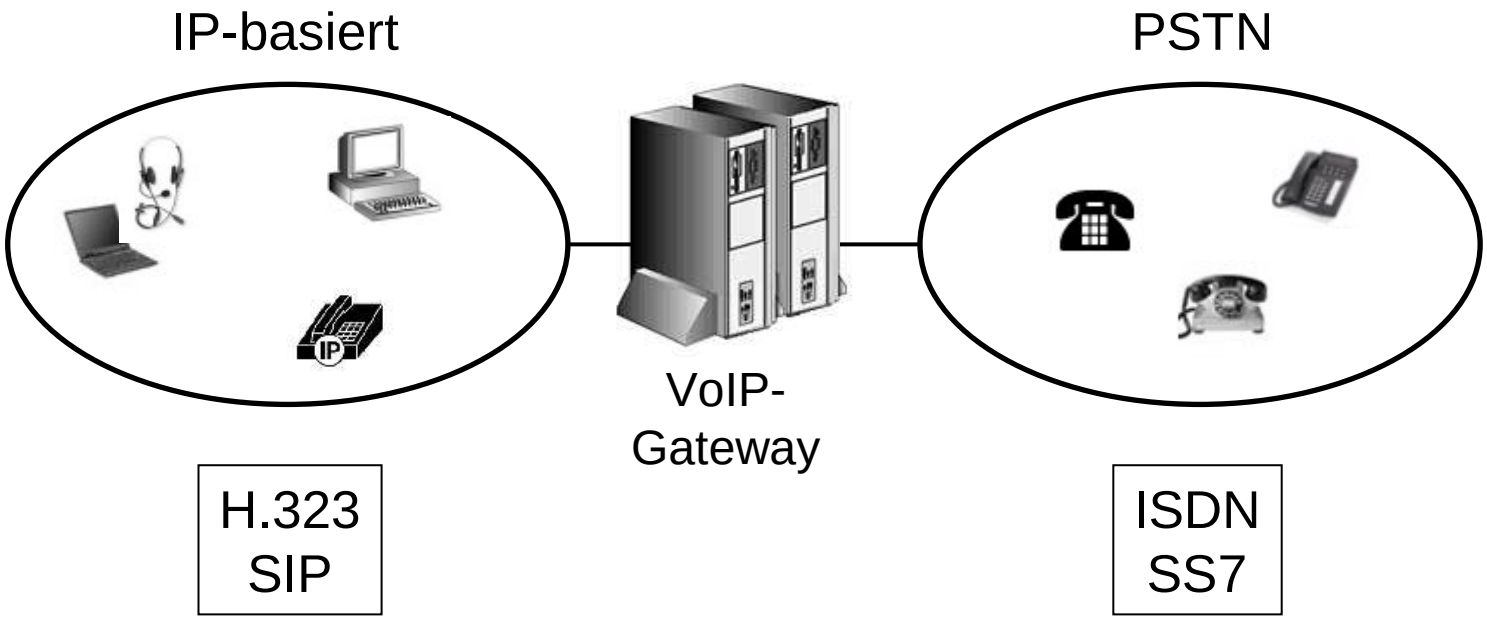
Christoph Fuchs
Universtität Bonn

12.07.2006

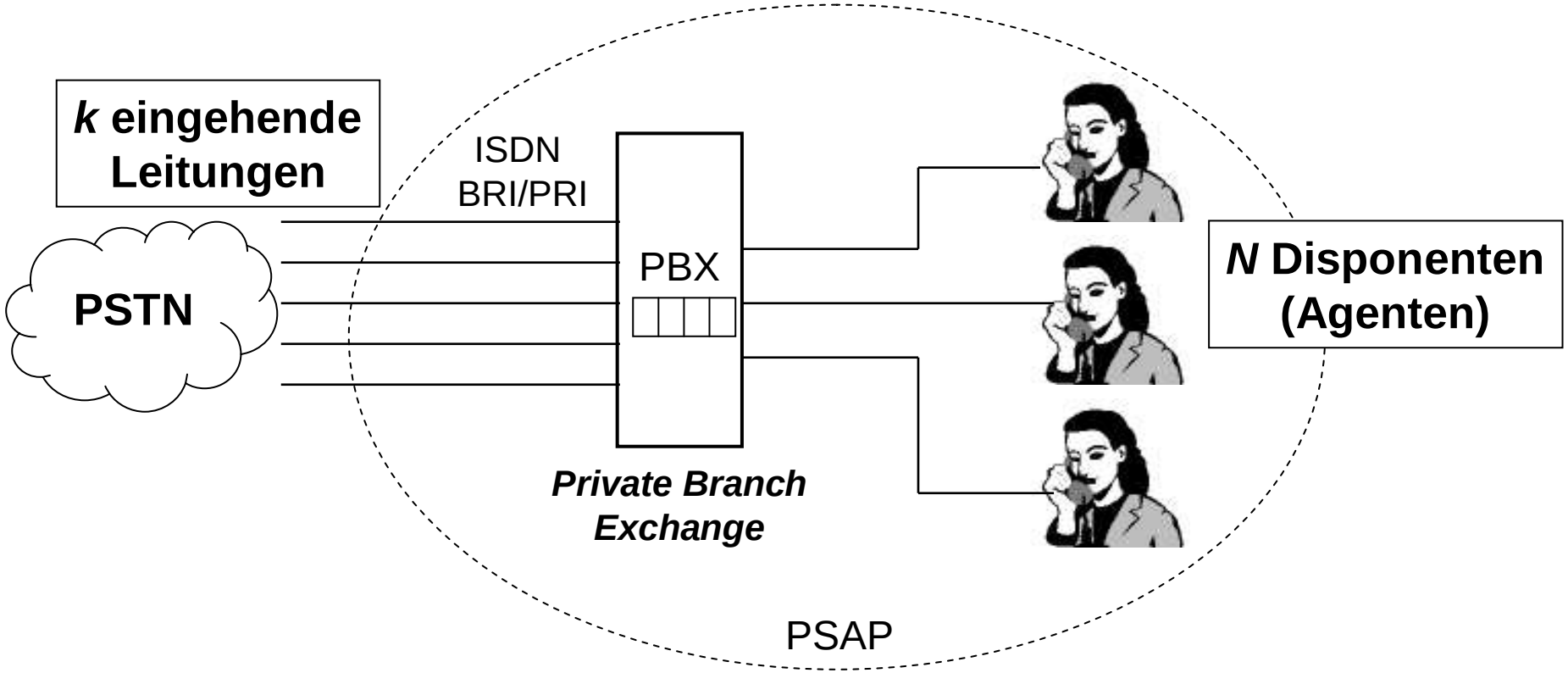
1. Problemstellung

Welche Sicherheitsrisiken entstehen durch die Integration von VoIP für den Notrufdienst (112) ?

Momentane VoIP-Architektur:

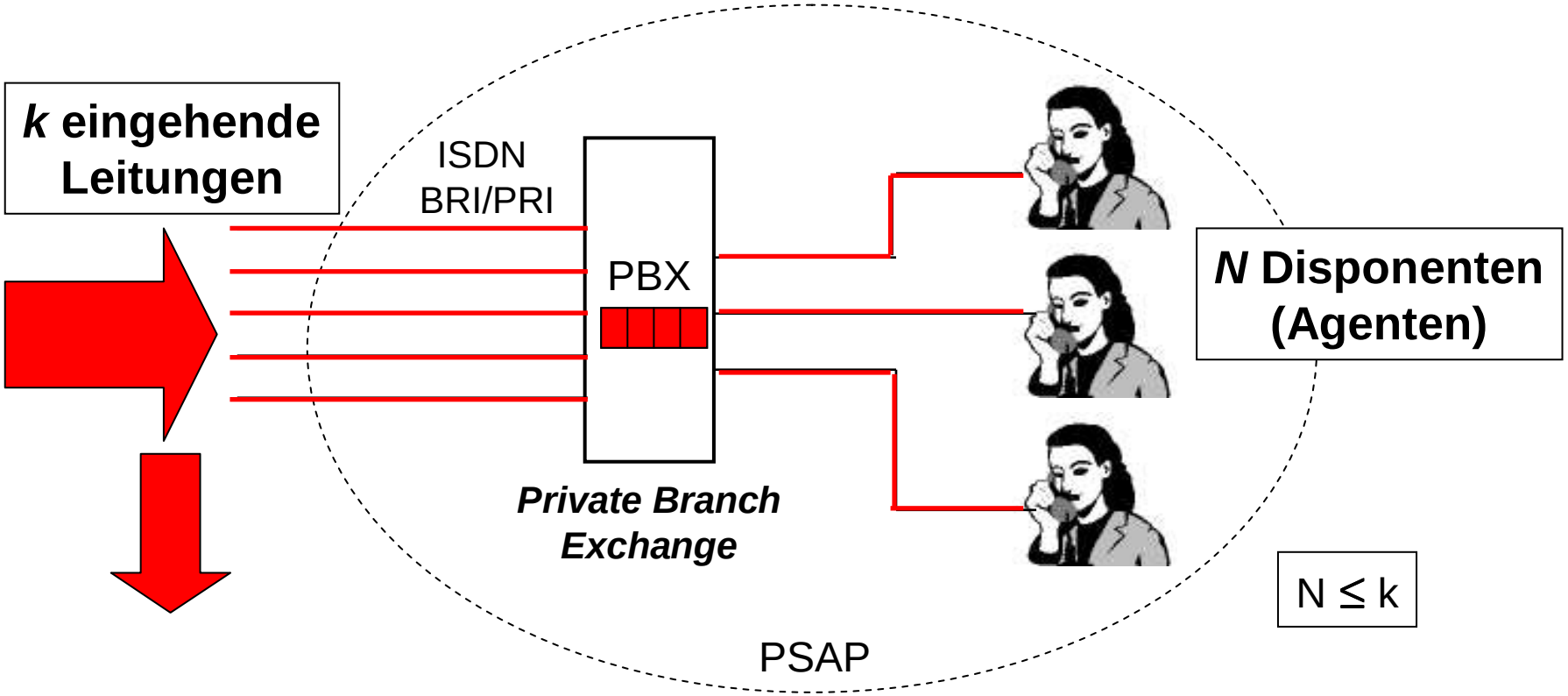


Architektur im PSAP (Leitstelle)



⇨ **Begrenzte Ressourcen**

Überlastung des PSAP



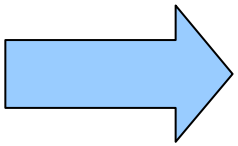
Gefahr von Denial-Of-Service-Angriffen !

2. Lösungsweg - Gegenmaßnahmen zu DoS-Attacken

- **Präventive Maßnahmen, die die Verfügbarkeit einschränken wie z.B. Authorisierung, sind für den öffentlichen Notrufdienst ungeeignet.**

Daher:
Allenfalls reaktive Maßnahmen bei Vorliegen einer DoS-Attacke möglich.

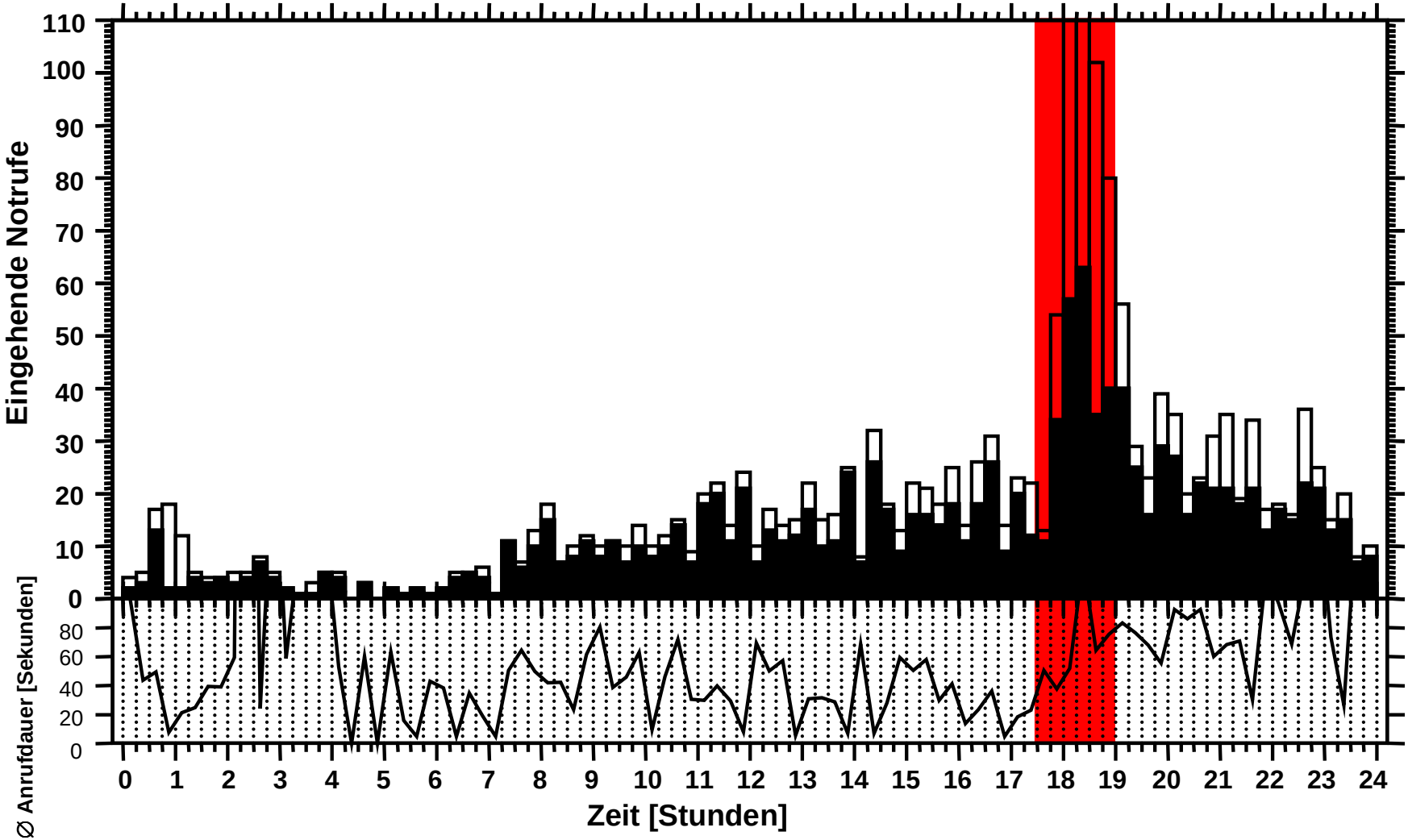
Wichtig für die Effektivität:
Möglichst frühzeitige Erkennung eines Angriffs.



Intrusion Detection

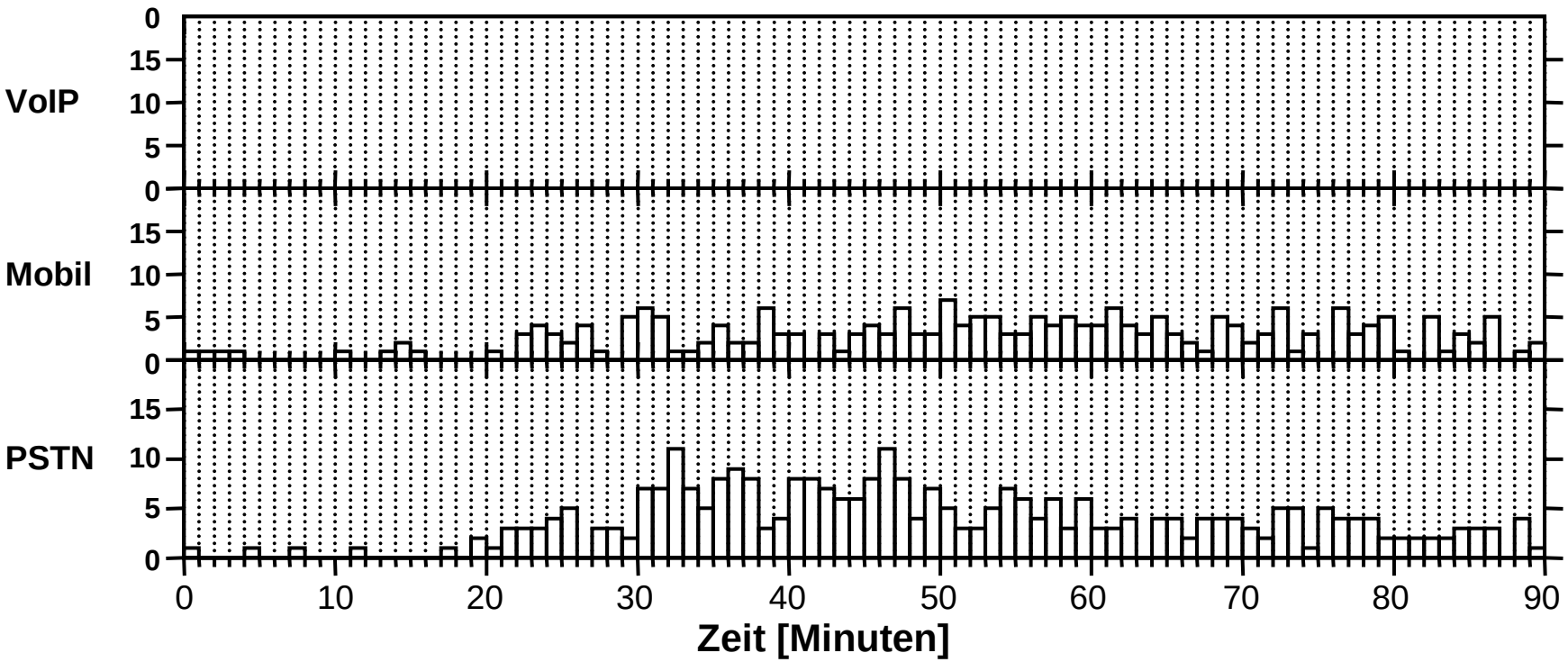
Problem:
Unterscheidung von Angriffs- und Katastrophenfall.

Unterscheidung zwischen Angriff und Katastrophenfall



Unwetterlage am 27.07.2005, PSAP Köln

Notrufprofile klassifiziert nach Ursprungsnetz

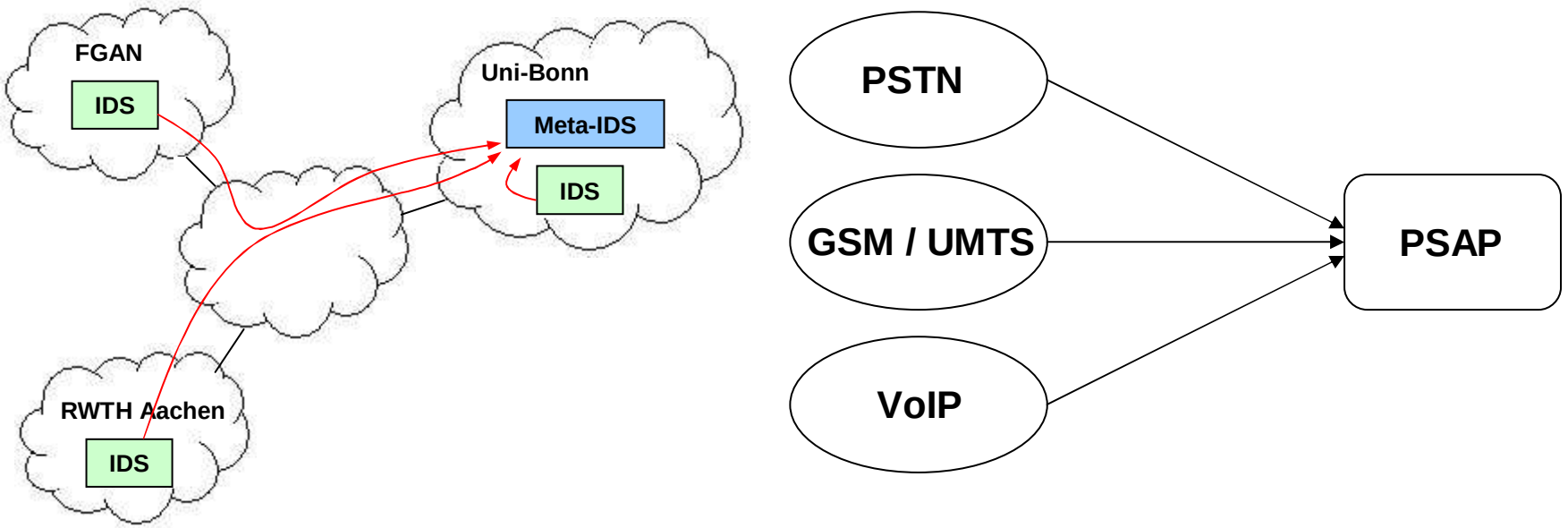


⇨ **Bei Katastrophen ähnliche Entwicklung der Notruflast aus verschiedenen Ursprungsnetzen**

Kooperative Intrusion-Detection

Kooperative Intrusion-Detection-Systeme:

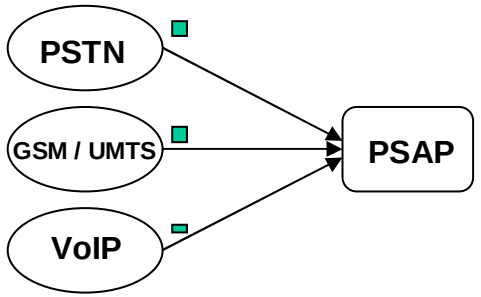
- ID-Systeme verschiedener Domänen senden ihre Daten an ein Meta-IDS
- bessere Erkennungsleistung bestimmter Angriffe (z.B. Würmer)



Betriebsszenarien im PSAP

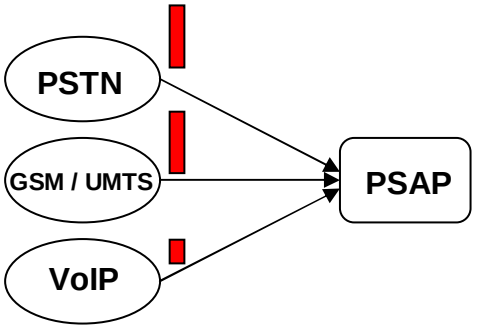
Normalbetrieb

- niedrige und relativ gleichmäßig verteilte „Last“



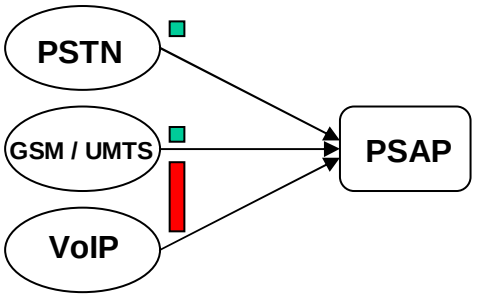
Katastrophenfall

- hohes Lastaufkommen aus allen Domänen zu erwarten

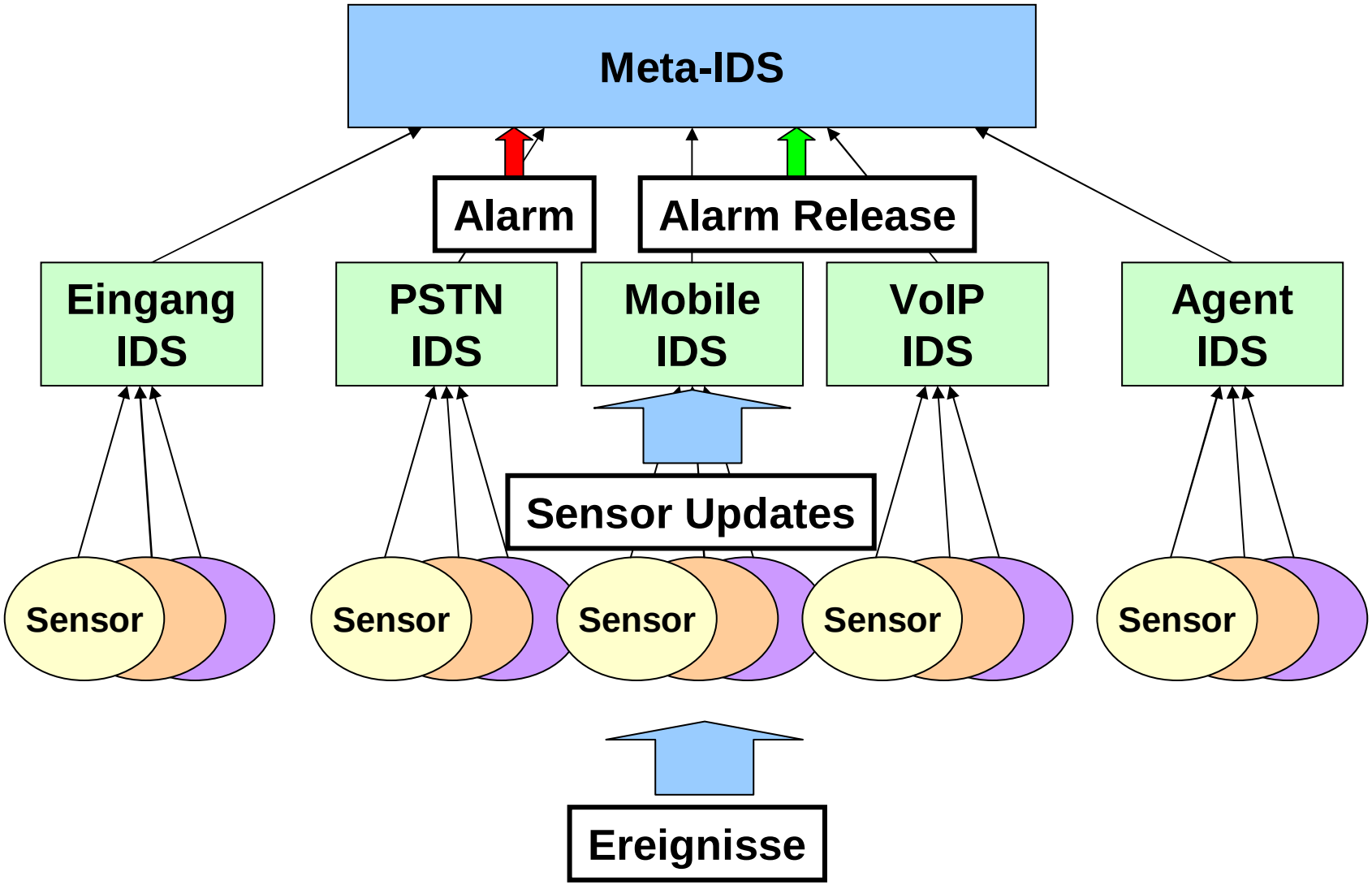


DoS-Angriff

- extrem hohe Last aus VoIP-Bereich
- unauffällige Last aus PSTN- und GSM/UMTS-Domänen

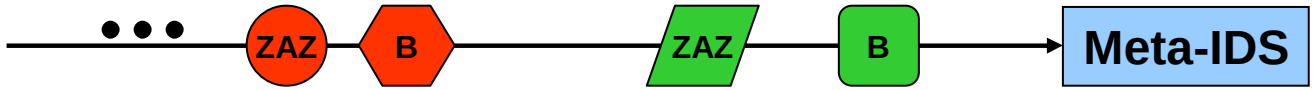


Architektur des ID-Systems und Ereignisreduktion



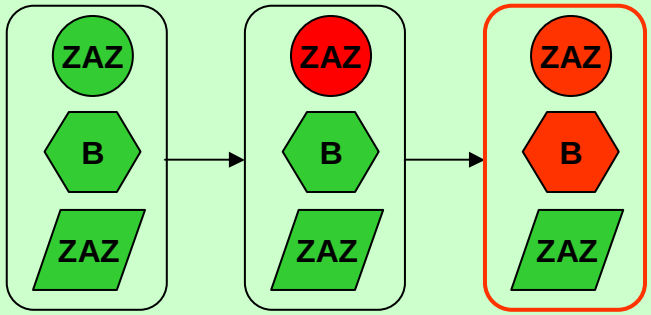
Angriffserkennung im Meta-IDS

Alarmmeldungen führen zu Ereignisstrom im Meta-IDS



Zustandsbasierte Angriffserkennung

Identifizierung von Systemzuständen, die einen Angriff kennzeichnen



Zweistufiges Alarmkriterium

1. Stufe: Liegt kritische Ressourcenauslastung vor?

2. Stufe: Vergleich der Alarmzustände von PSTN, Mobilnetzen und VoIP

⇨ Angriffsalarm bei Erfüllung beider Kriterien

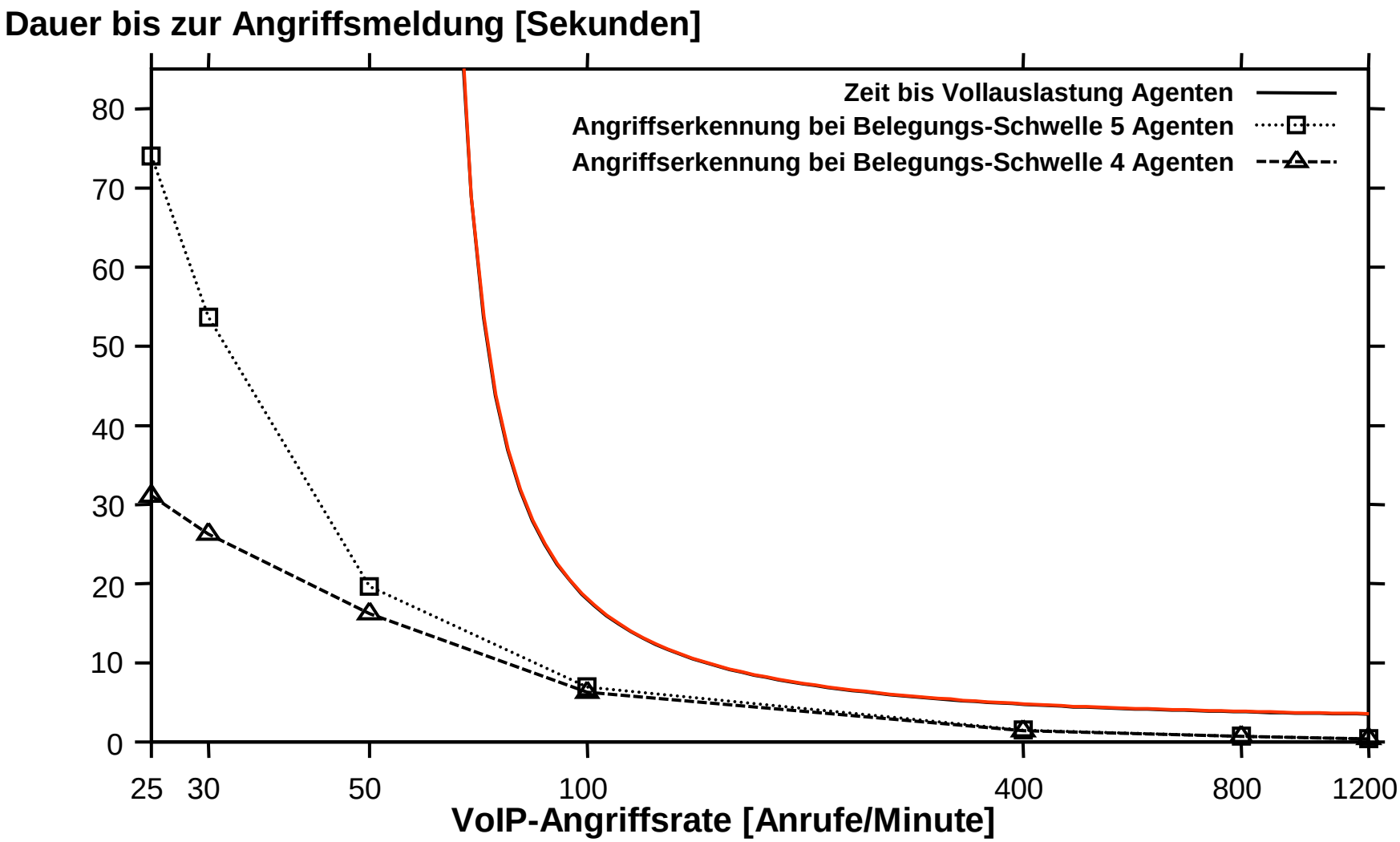
3. Ergebnisse - Evaluation

Bewertung der erzielten Erkennungsleistung

- **Reaktionszeit der Angriffserkennung**
  - vor Vollauslastung
  - vor „manueller“ Erkennung
- **Zuverlässigkeit der Angriffserkennung**

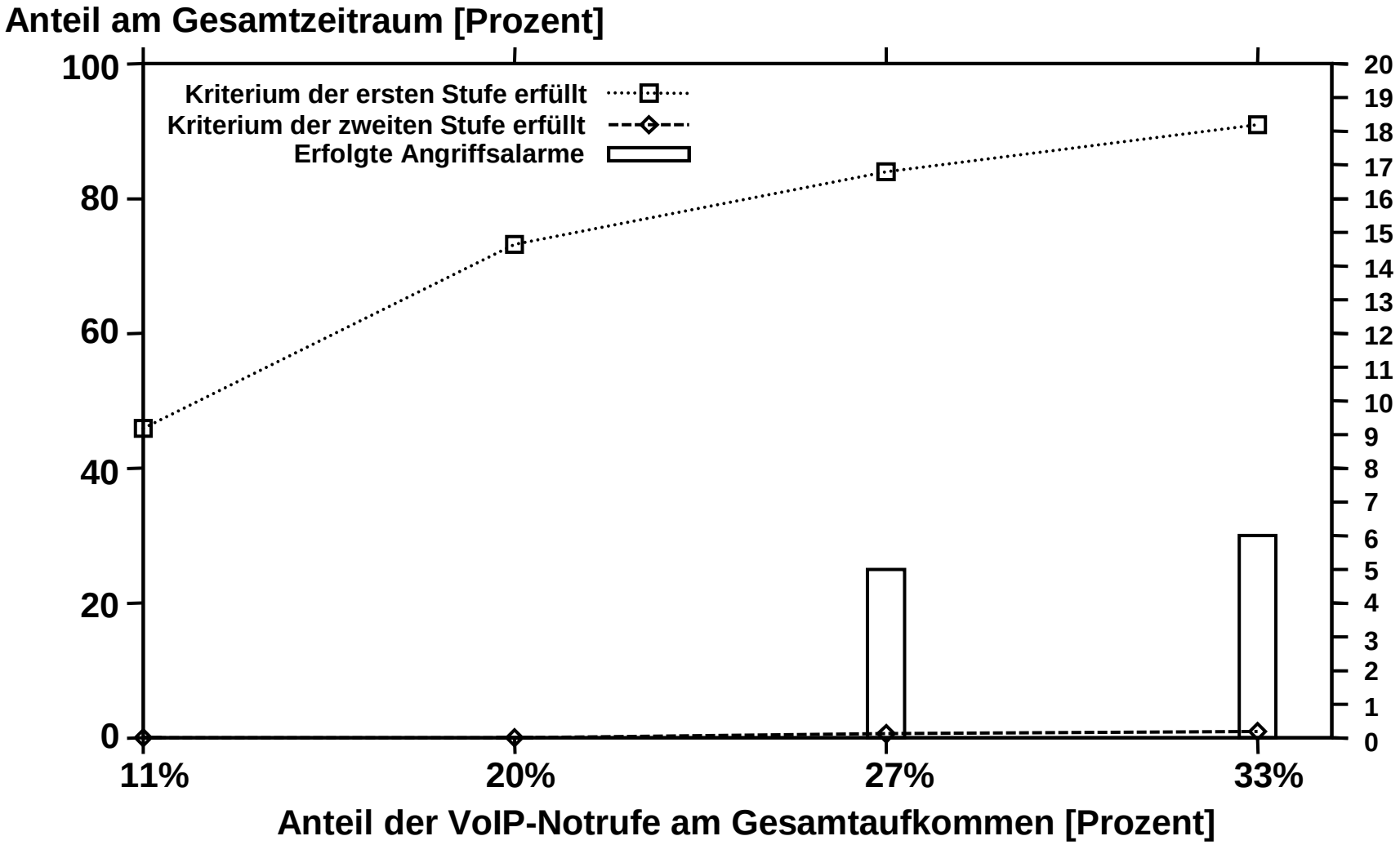
  ⇨ Unterscheidung von Angriff und Katastrophenfall

Reaktionszeit der Angriffserkennung



⇨ **Angriffserkennung deutlich vor Erreichen der Vollauslastung**

Zuverlässigkeit der Angriffserkennung



⇨ **Zuverlässige Erkennung bis zu einem VoIP-Anteil von ca. 20%**

Ausblick

- Auswirkungen der PSAP-Größe auf die Angriffserkennung
- Anomalieerkennung statt Missbrauchserkennung
- Erfassung zusätzlicher Eigenschaften oder Verschärfung der Angriffskriterien bei zunehmender VoIP-Verbreitung

Intrusion-Response ?

Ende

Fragen?

Möglichkeiten der Intrusion-Response

Beschränkung der durch VoIP-Notrufe belegbaren PSAP-Ressourcen

- **VoIP-Notrufe werden nur von fester Anzahl Agenten bedient**
- **Priorisierung der Warteschlangen von PSTN und Mobilnetzen**
- **Beschränkung der durch VoIP-Notrufe belegbaren Leitungen**