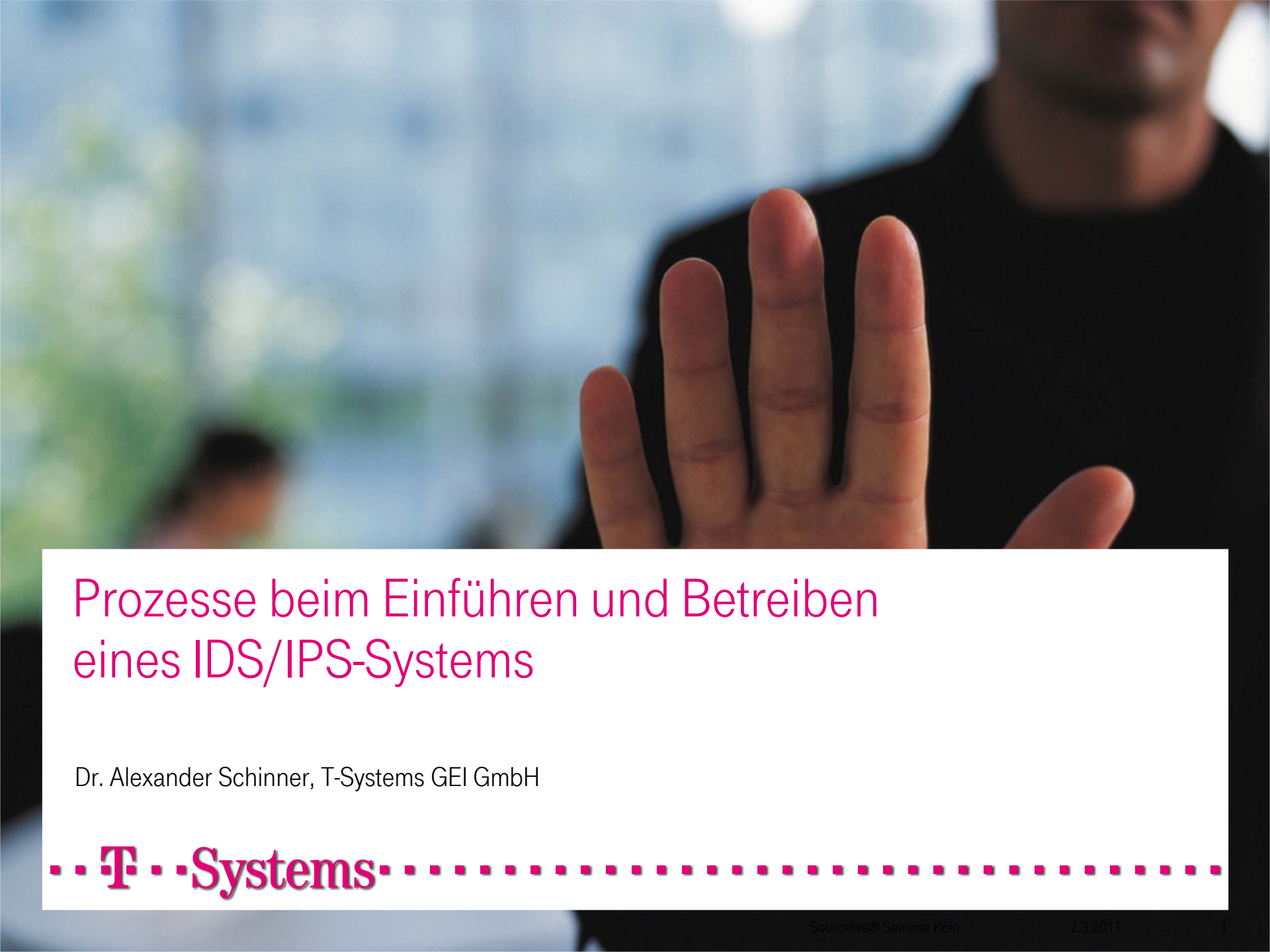


Prozesse beim Einführen und Betreiben eines IDS/IPS-Systems

Dr. Alexander Schinner, T-Systems GEI GmbH

T · · Systems

Vorstellung

Dr. Alexander Schinner

- T-Systems International GmbH
- Security Consulting & Engineering
- Standort München

Arbeitsgebiete

- Intrusion Detection Systeme
- Penetrationstests
- Beratung

T · · Systems

Kurzvorstellung Security Consulting & Engineering

- mehr als 25 Jahre Erfahrungen im Beratungs- und Lösungsgeschäft auf dem Gebiet IT-Sicherheit.
- weltweit führende Prüfstelle: akkreditiert durch
  - Bundesamt für Sicherheit in der Informationstechnik (BSI),
  - VISA International, MasterCard International, PCI und viele andere Organisationen weltweit.
- Mehr als 200 Geschäftskunden und 100.000 Privatkunden.
- Großprojekte und Top-Referenzen.
- ca. 200 Sicherheitsspezialisten.
- Herstellerunabhängig

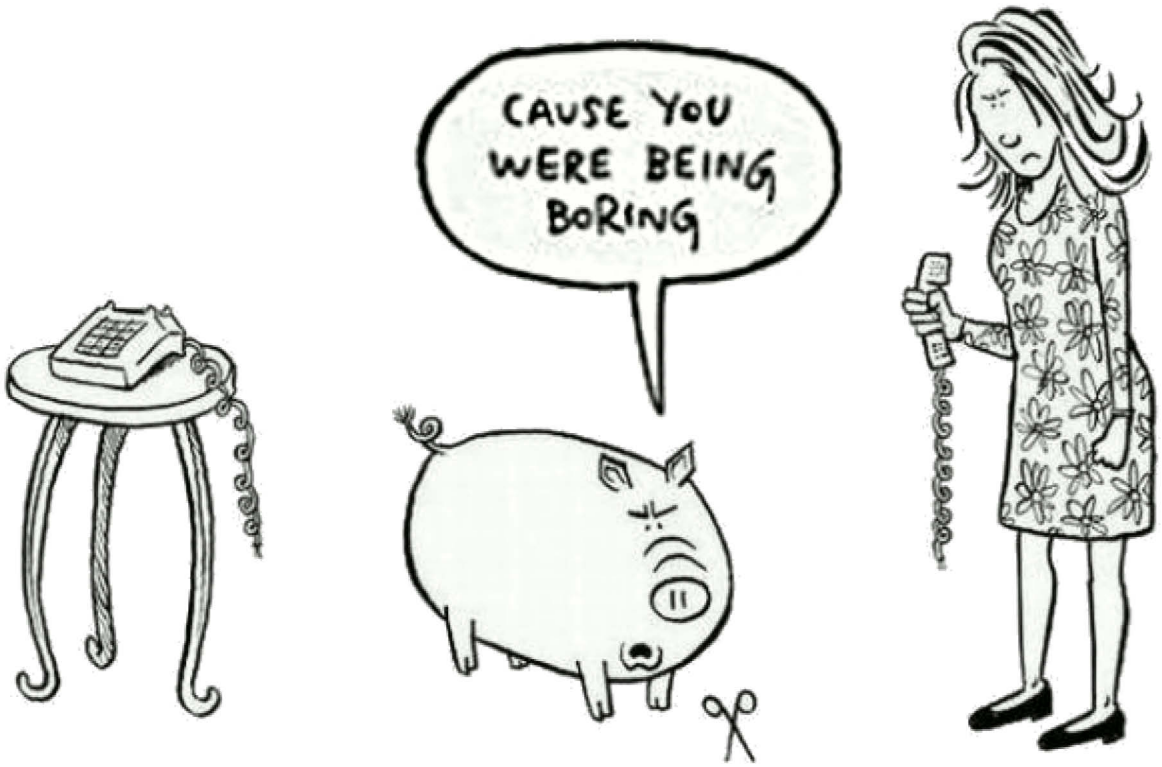
T · · Systems

Agenda

- Einführende Worte, Motivation
- Wie plane ich ein IDS / IPS für mein Unternehmen?
  - Verschiedene Zielsetzungen
  - Verschiedene Architekturen
  - Verschiedene Organisationsformen
- Welche Hilfe kann mir ein IDS geben?
  - RNA
  - RUA
  - Informationen in den Alarmen etc.
- Welche Prozesse sollten um ein IDS etabliert werden?

T · · Systems

Einführende Worte



- http://www.funnyburger.com/schweine-comics

Einführende Worte

- http://www.funnyburger.com/schweine-comics

T · · Systems

Wo ist das Problem?

Ein Schüler Rikyus fragte einst folgendes: „Was genau sind die wichtigsten Dinge, die bei einer Teezeremonie verstanden und beachtet werden müssen?“

„Bereite eine köstliche Schale Tee; lege die Holzkohle so, dass sie das Wasser erhitzt; ordne die Blumen so, wie sie auf dem Feld wachsen; bereite alles rechtzeitig vor; stelle dich auf Regen ein, und schenke denen, mit denen du dich zusammenfindest, dein ganzes Herz.“

Der Schüler war mit dieser Antwort unzufrieden, weil er in ihr nichts von so großem Wert finden konnte, dass es als Geheimnis des Verfahrens hätte bezeichnet werden können. „Das alles weiß ich bereits...“

Rikyu antwortete, „Wenn du also eine Teezeremonie leiten kannst, ohne von einer der Regeln die ich nannte abzuweichen, dann will ich Dein Schüler werden!“

T · · Systems

Das Märchen vom Plug-and-Play IDS-System

„Das ist das Schöne an einem Fehler:
man muss ihn nicht zweimal machen.“
Thomas Alva Edison (1847-1931)

Dr. Alexander Schinner, T-Systems GEI GmbH

T · · Systems

Das Märchen vom Plug-and-Play IDS-System
Agenda

- Motivation für die Beschaffung eines IDS/IPS

  „Ich will alles wissen…“
- Planung eines IDS/IPS

  „Wissen Sie, was ein Fachmann kostet?“
- Betrieb eines IDS/IPS

  „Das haben wir ja schon immer so gemacht…“
- Prozesse für den Betrieb eines IDS/IPS

  „Immer diese Bürokratie…“
- Unterstützung des Betriebs durch das IDS/IPS

  „Lasst mich in Ruhe arbeiten…“
- Abschluss

  „Ach so geht das…“

T · · Systems

Motivation
Warum wollen wir ein IDS/IPS?

- Gründer der Techniker
  - Schutz von Systemen
  - Bedrohungslage (Advanced Persistent Threads)
  - Systemüberwachung

Gefahr: Spielzeug für Techniker

- Gründe des Management
  - Rechtliche Vorgaben
  - Firmenpolicy
  - Verträge (häufig bei Outsourcing)

Gefahr: Pro-forma IDS

- Grenzen für beide
  - Zeit
  - Geld

T · · Systems

Motivation
Was ist Intrusion Detection? Erster Versuch:

- Techniker
  - Ich will wissen, ob wir angegriffen werden!
- Management
  - Besteht Gefahr für unser Geschäftsmodell?
- Die Lösung:

T · · Systems

Motivation
Was ist Intrusion Detection? Zweiter Versuch:

- Attack vs. Intrusion
  - Was ist mit einem ping sweep?
  - Was ist, wenn jemand telnet auf meinen Server macht?
  - Und sich als „root" anzumelden versucht?
  - Und ein Nessus Scan?
  - Und wenn er PHP Skripten auf dem Webserver ausprobiert?
  - Und Erfolg hat und sich einlogged?

Vorteile

- Fallabhängige Entscheidung

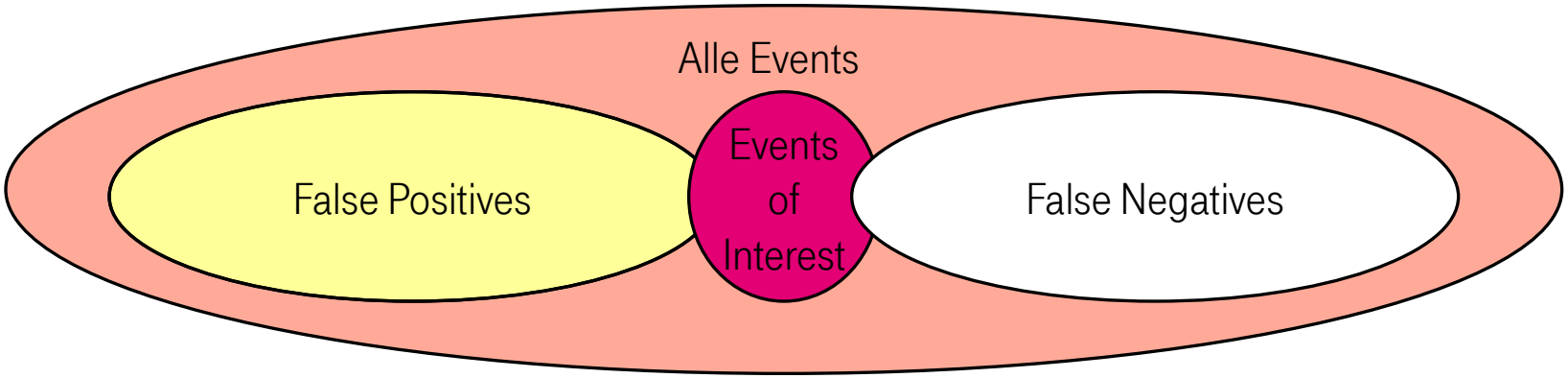
Nachteile

- nicht praktikabel

T · · Systems

Motivation
Was ist Intrusion Detection? Dritter Versuch:

- Alles, was das IDS meldet



Vorteile

- verständlich
- Vorgehensmodell nach SANS

Nachteile

- Ersatz einer Definition durch drei andere

T · · Systems

Motivation
Was ist Intrusion Detection? Letzter Versuch:

- Ein Eindringversuch (Intrusion) ist alles, was der Policy des Systems widerspricht
- Intrusion Detection ist der Prozess, der den Eindringversuch identifiziert

Vorteile

- robuste Definition
- konsensfähige Definition

Nachteile

- Wir brauchen eine Policy
- Wir müssen alle unsere Systeme kennen
- Klären bei der Einführung eines IDS

T · · Systems

Planung eines IDS/IPS
Verdrängungsstrategien

- Management
  - „Wir haben eine Firewall.“
  - „Bei uns gibt es nichts für Hacker zu holen.“
  - „Unsere Leute müssen arbeiten können.“

- Techniker
  - „Wir haben zwei Firewalls.“
  - „Bei uns ist noch nie was passiert.“
  - „Ich weiß, was in meinem Netz los ist.“

Planung eines IDS/IPS
Grundlegende Schritte

- Konkretisierung der Ziele des IDS-Einsatzes
- Architekturen
- Festlegung einer geeigneten Organisation

Planung eines IDS/IPS
Konkretisierung der Ziele des IDS-Einsatzes

- Variante 1
  - billig
  - keine Änderung in der Organisation
  - geringe Folgekosten

Gefahr: Pro-forma IDS

- Variante 2
  - teuer
  - Kompletter Umbau der Technik
  - aufwendiger Betrieb

Gefahr: Spielzeug für Techniker

- Variante 3
  - Passgenaue Lösung

T · · Systems

Planung
Architektur

- Auswahl der Technik
  - IDS,
  - IPS
  - oder doch Firewall, WAF, etc.

- Ist-Aufnahme der technischen Infrastruktur
  - Ziel ist die Sensorplatzierung
  - Netzwerkdiagramm
  - Kommunikationsbeziehungen
  - Kommunikationstechniken

- Betriebsblindheit
  - externe Hilfe

Planung
Einbettung in den Betrieb

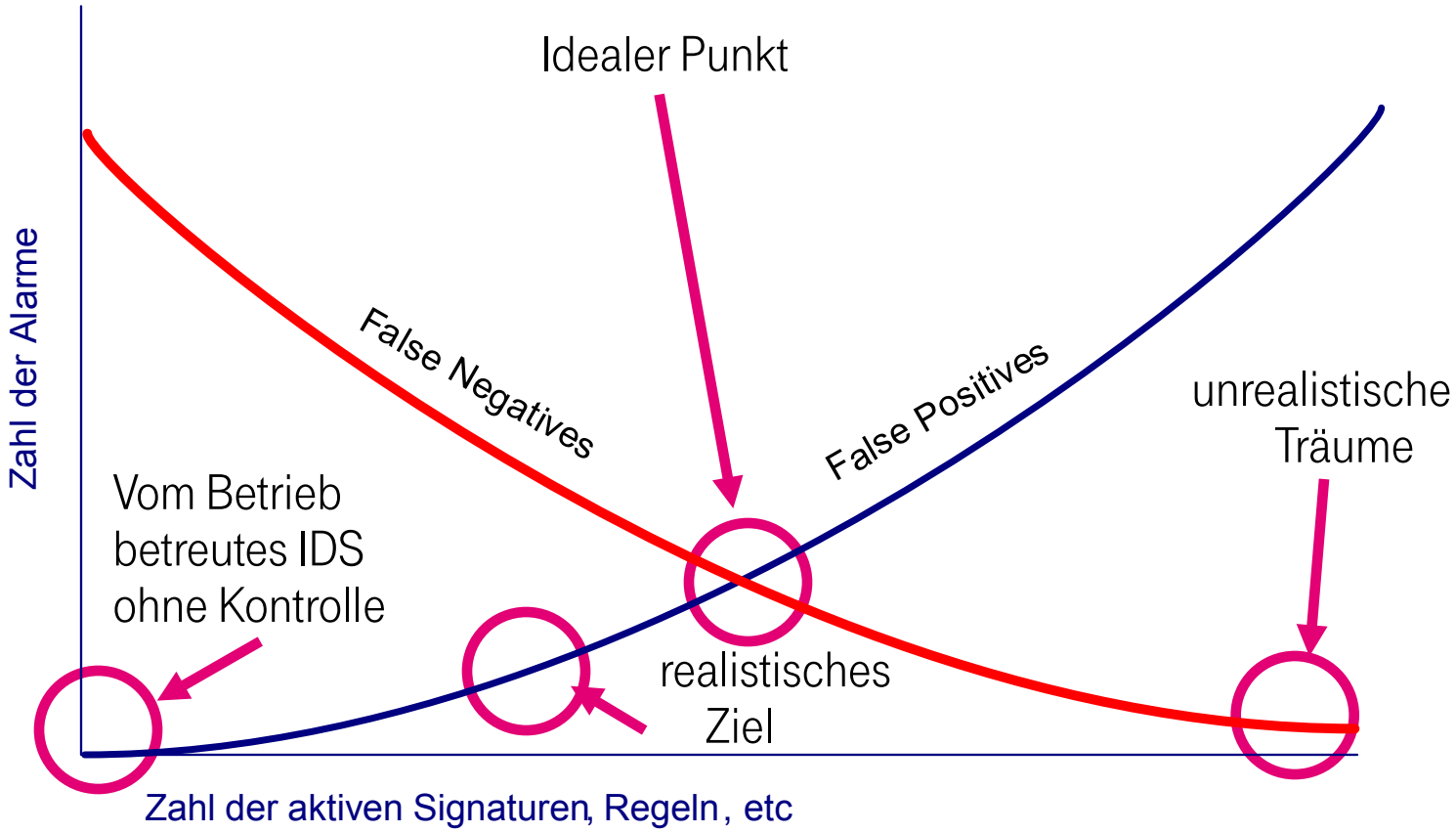
- Ist-Aufnahme der bestehenden Incident-Response-Organisation
  - Wie ist die Vorgehensweise zur Verfolgung von Sicherheitsvorfällen?
  - Gibt es eine zentrale Stelle, bei der Probleme und Alarme auflaufen?
  - Kann das IDS/IPS an vorhanden Strukturen andocken?

- Sensibilisierung der Entscheider
  - Management
  - Systemadministration und –betrieb
  - Revision
  - Datenschutzbeauftragter
  - Personalvertretung

Guter Zeitpunkt, die Gesamtsituation zu überprüfen

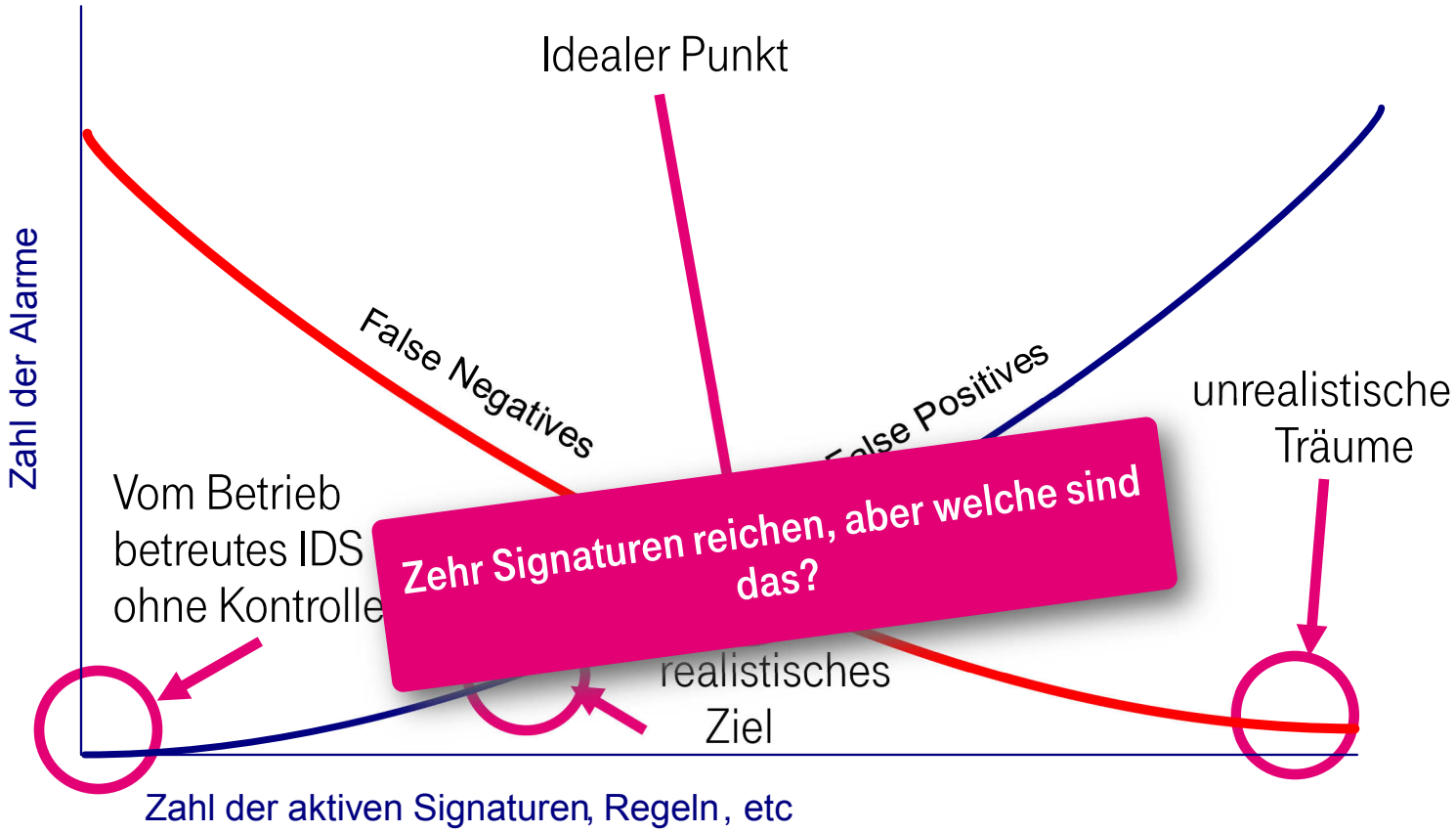
T · · Systems

Betrieb eines IDS/IPS
Warum zehn Signaturen völlig ausreichen



T · · Systems

Betrieb eines IDS/IPS
Warum zehn Signaturen völlig ausreichen



T · · Systems

Betrieb eines IDS/IPS
Wir haben gute Leute, die brauchen keine Schulung...

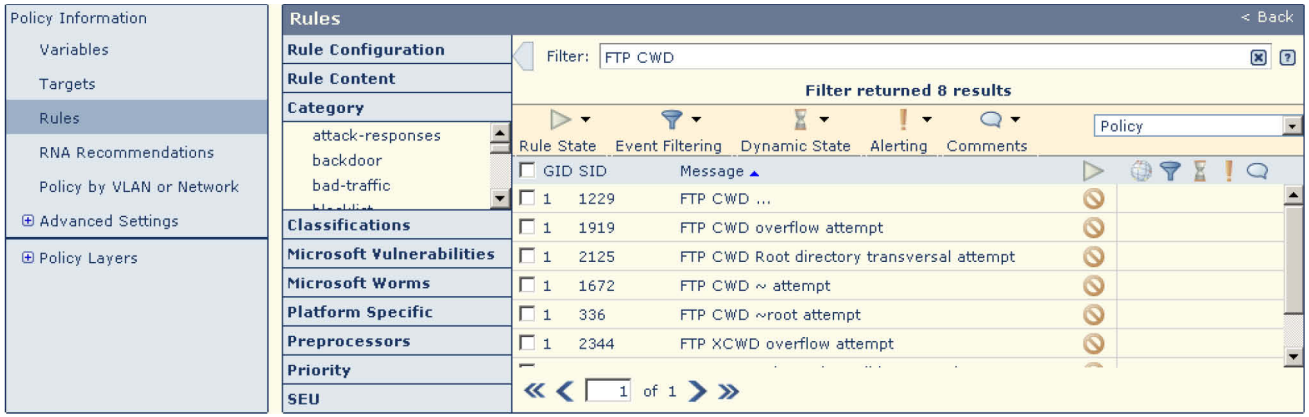
- Schulung beim Hersteller
  - Kennenlernen des Werkzeug
- Allg. Schulung zum Thema IDS (SANS, Black Hat)
  - Kennenlernen des Gegners
- Am Anfang gelegentlich einen Berater des Herstellers/Resellers hinzuziehen
  - Kennenlernen der Arbeitsweise

T · · Systems

Betrieb eines IDS/IPS
Wir haben gute Leute, die brauchen keine Schulung...

- Schulung beim Hersteller
  - Kennenlernen des Werkzeug

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP
CWD overflow attempt"; flow:to_server,established;
content:"CWD"; nocase; isdataat:100,relative;
pcre:"/^CWD\s[^\n]{100}/smi"; sid:1919; rev:19;)
```



Betrieb eines IDS/IPS
Wir haben gute Leute, die brauchen keine Schulung...

- Allg. Schulung zum Thema IDS (SANS, Black Hat)
  - Kennenlernen des Gegners

```
 03:09:06.526507 00:03:e3:d9:26:c0 > 00:00:0c:04:b2:33, ethertype IPv4 (0x0800),
 length 574: IP (tos 0x0, ttl 45, id 55450, offset 0, flags [DF], length: 560,
 bad cksum 9bb8 (->516e)!) 195.232.55.6.1701 > 207.166.87.42.21: P
[bad tcp cksum 7135 (->25e2)!] 2184450005:2184450513(508) ack 1127458918 win
5840 <nop,nop,timestamp 1040178 3948516>

0x0000: 0000 0c04 b233 0003 e3d9 26c0 0800 4500 .....3....&...E.
0x0010: 0230 d89a 4000 2d06 9bb8 c3e8 3706 cfa6 .0..@.-.....7...
0x0020: 572a 06a5 0015 8234 0fd5 4333 a866 8018 W*.....4..C3.f..
0x0030: 16d0 7135 0000 0101 080a 000f df32 003c ..q5.........2.<
0x0040: 3fe4 4357 4420 3030 3030 3030 3030 3030 ?.CWD.0000000000
0x0050: 3030 3030 3030 3030 3030 3030 3030 3030 0000000000000000
[…]
0x0120: 3030 3030 3030 3030 3030 3030 3030 3030 0000000000000000
0x0130: 3030 3030 3030 3030 3030 3030 3030 3030 0000000000000000
0x0140: 3030 3030 3030 f0fc 4031 0708 985f 0808 000000..@1..._..
```

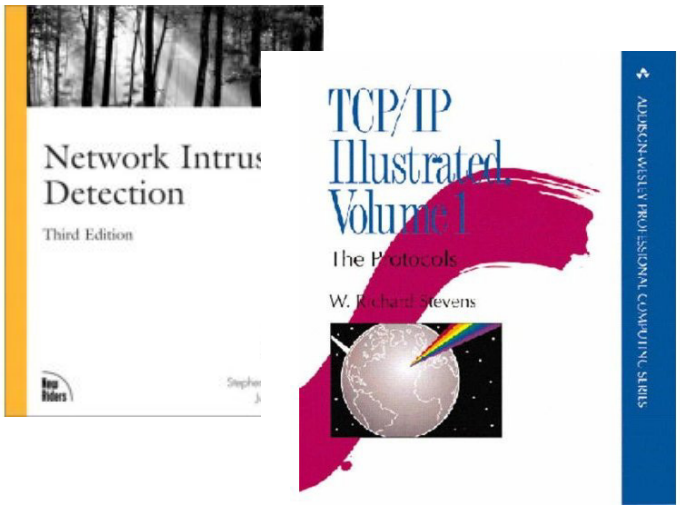
Betrieb eines IDS/IPS
Wir haben gute Leute, die brauchen keine Schulung...

- Am Anfang gelegentlich einen Berater des Herstellers/Resellers hinzuziehen
  - Kennenlernen der Arbeitsweise von Angreifern bei Ihnen

T · · Systems

Betrieb eines IDS/IPS
Wir haben gute Leute, die brauchen keine Schulung...

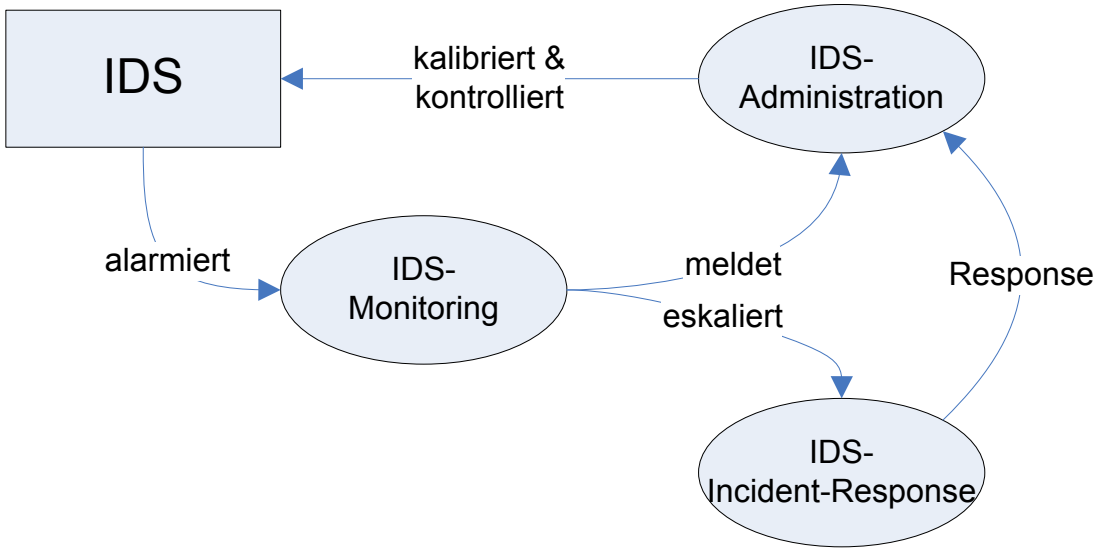
- Zusätzlich:
  - Zugang zu Büchern
  - Zugang zu Informationsquellen
  - Zeit zum lernen



T · · Systems

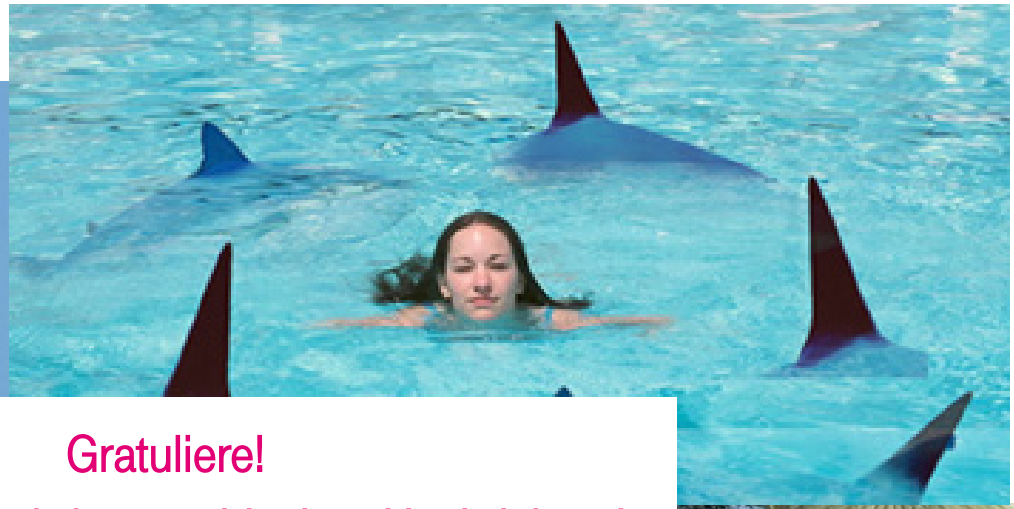
Betrieb eines IDS/IPS
Das kann der Firewalladmin doch gleich mitmachen...

- Festlegung einer geeigneten Organisation
  - IDS-Manager
  - IDS-Administration
  - IDS-Monitoring
  - Incident-Response



T · · Systems

Prozesse



Gratuliere!

Sie sind der Überbringer schlechter Nachrichten!

T · · Systems

Prozesse
Wenn ein Alarm auftritt, wird schon jeder wissen, was er machen muss

Klasse 1

- Sehr wichtige Alarme
- Geringe Fehlalarmrate erwartet
- Erwartete Häufigkeiten <5 pro Jahr
- Schnelle Erstreaktion notwendig (<60 Minuten)
- Erstprüfung um die Eskalation von Fehlalarmen zu vermeiden

Klasse 2

- Wichtige Alarme
- Mittlere Fehlalarmrate erwartet
- Erwartete Häufigkeiten 10-100 pro Woche (genaue Zahlen erst nach Betriebsbeginn)
- Zeitnahe Reaktion empfehlenswert (täglich)
- Erstprüfung um die Eskalation von Fehlalarmen zu vermeiden

Klasse 3

- Alarme zur Beurteilung der Gesamtlage
- Mittlere bis hohe Fehlalarmrate erwartet
- Erwartete Häufigkeiten 100 bis 1000 pro Tag (genaue Zahlen erst nach Betriebsbeginn)
- Regelmäßige Prüfung der kumulierten Alarme

T · · Systems

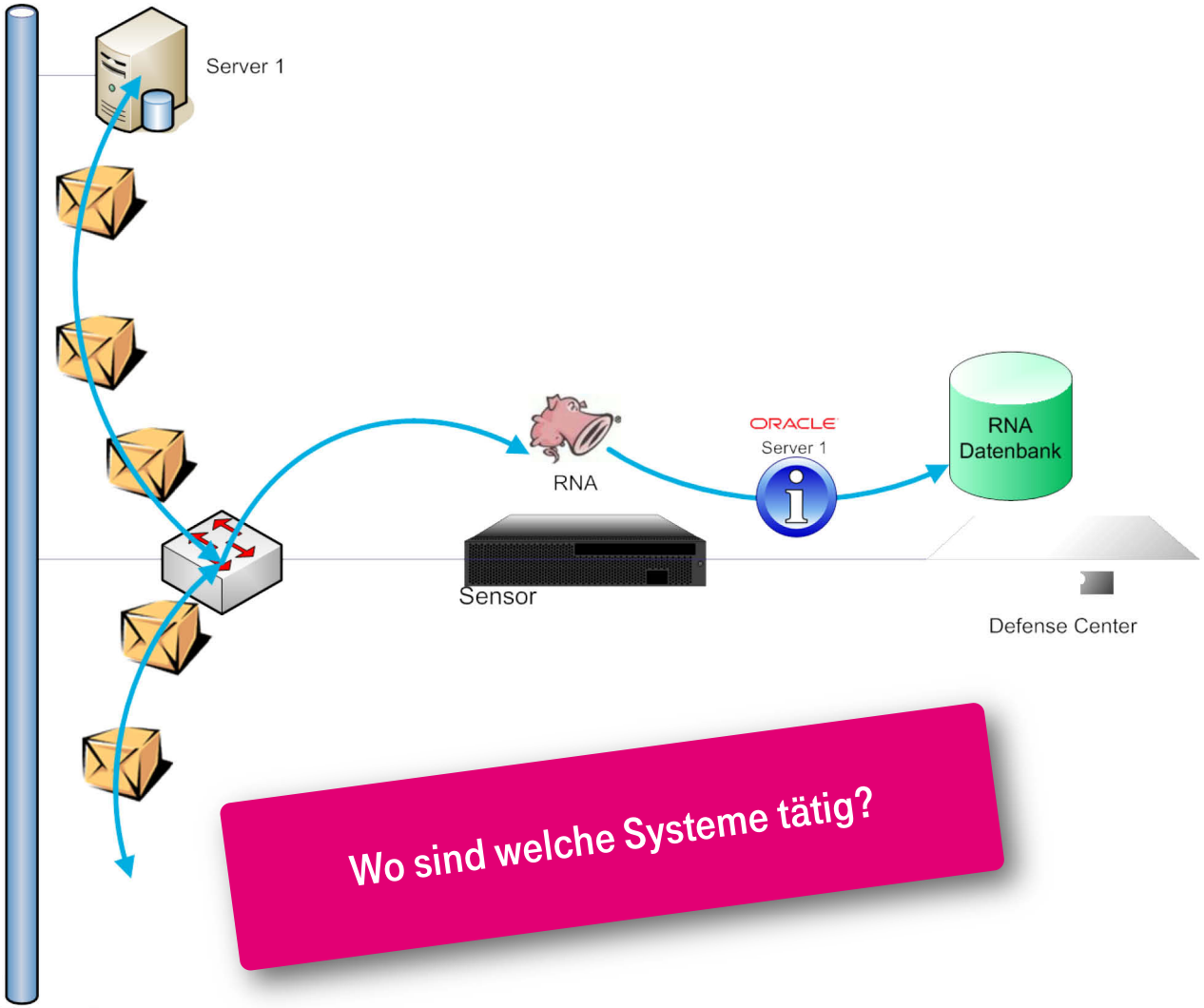
Prozesse
Wenn ein Alarm auftritt, wird schon jeder wissen, was er machen muss

- Anhand der Alarmdaten muss entscheiden werden, welche Prozesse ausgelöst werden
  - Sicherheit und Verantwortung für den Betrieb
- Es muss über die aktuelle Gefährdungslage und Ereignisse informiert werden
  - Transparenz der Arbeit
- Vermeidung von Spezialprozessen
  - Nutzung des gelebten Incident Management Prozesses

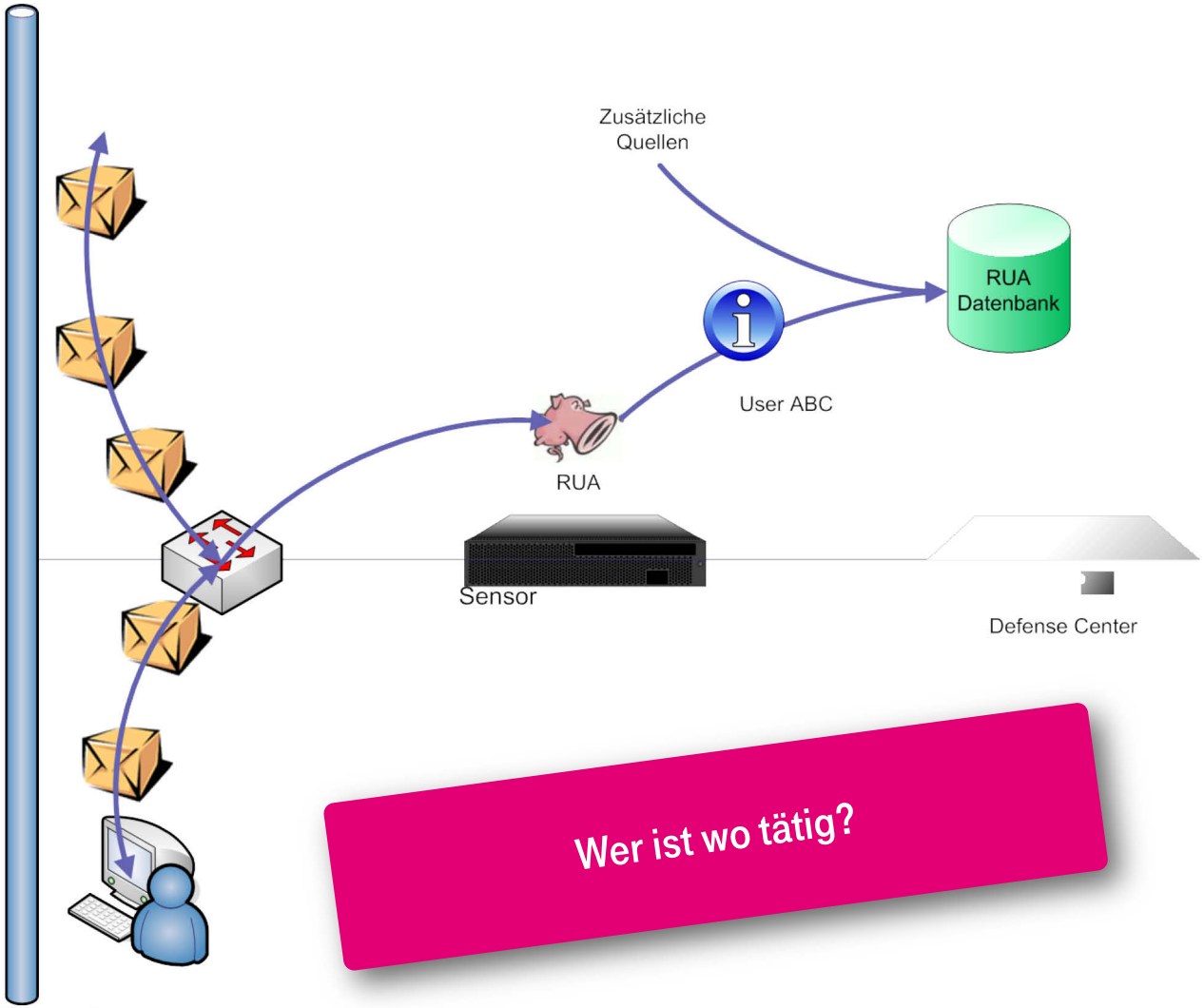
So viel wie nötig, sowenig wie möglich

T · · Systems

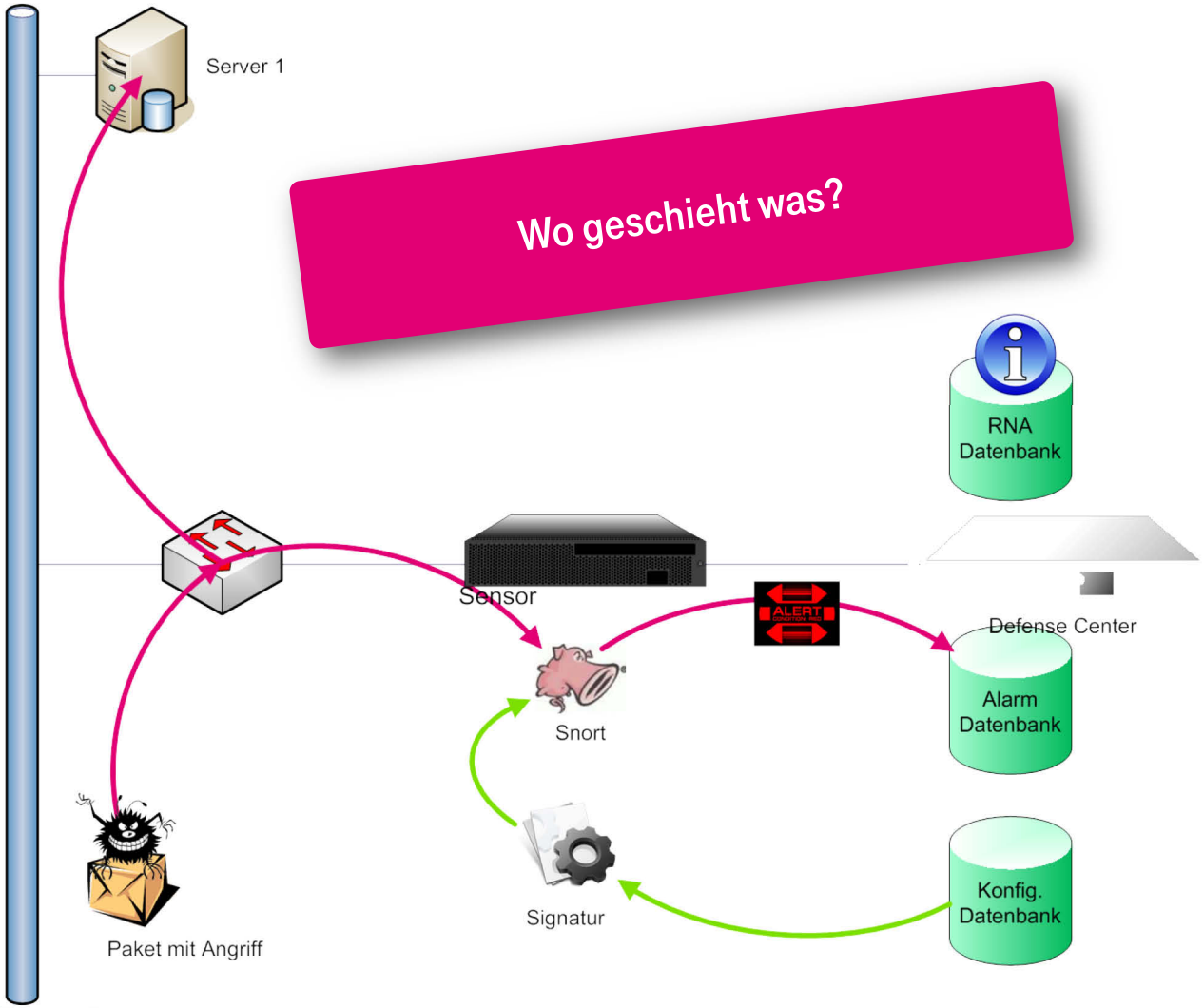
Das IDS will mir helfen, was muss ich alles ignorieren?
RNA



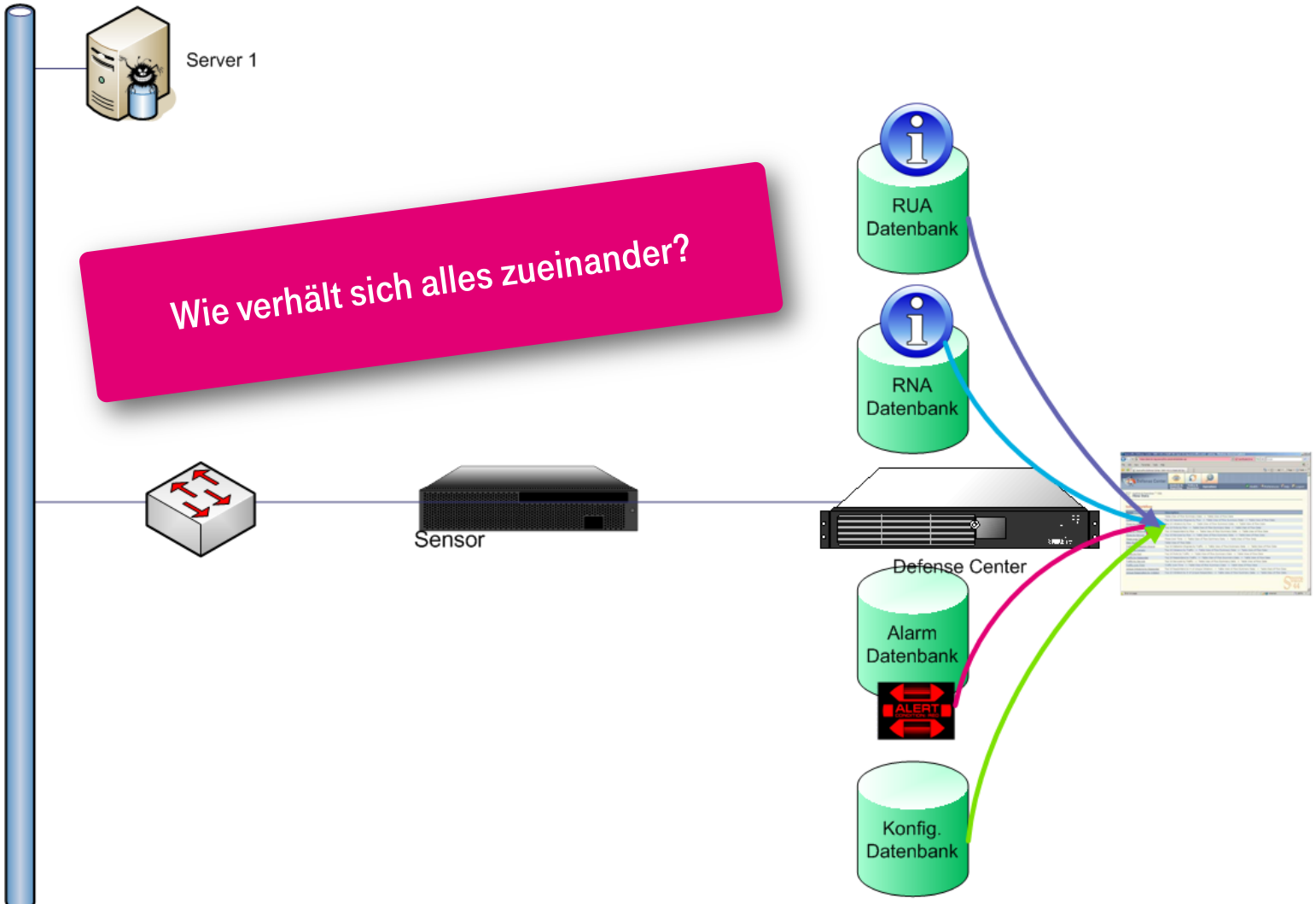
Das IDS will mir helfen, was muss ich alles ignorieren?
RUA



Das IDS will mir helfen, was muss ich alles ignorieren?
Events



Das IDS will mir helfen, was muss ich alles ignorieren?
Korrelation



T · · Systems

Das IDS will mir helfen, was muss ich alles ignorieren? Wie verhält sich alles zueinander?

- Das Defense Center zeigt als Ergebnis die folgenden Daten
  - Zielsystem: Server1
  - Angriff: SQL sp_password password change
  - Priorität: High
  - Impact: Vulnerable
  - User: ABC
  - Nachzulesen: CVE 12345, Bugtraq 9876

T · · Systems

Das IDS will mir helfen, was muss ich alles ignorieren? Reports

- Bericht, Plural: Be·rich·te

Text, der einen Sachverhalt oder eine Handlung objektiv schildert

- Ergebnisse der Untersuchung eines oder mehrere Vorfälle
- Erstellung regelmäßig oder bei Bedarf
- Manuelle Erstellung
- Freitext

Ziel: Wissensübermittlung

- Report, Plural: Re·por·te

ausführliche Beschreibung eines Geschehens oder Sachverhalts; Bericht mit vielen Einzelheiten

- Darstellung
- Statistiken
- Erstellung regelmäßig
- Automatisierte Erstellung
- Festes Format

Ziel: Informationsübermittlung

T · · Systems

Das IDS will mir helfen, was muss ich alles ignorieren? Reports

- Zielstellung:
  - Informationsquelle zur sicherheitstechnischen Lage
  - Grundlage für strategische Planung
  - Planungskontrolle
  - Dokumentation von langfristigen Entwicklungen

- Zu klärende Fragen:
  - Wie oft sollen die Reports erstellt werden?
  - Welche Informationen sollen die Reports bereitstellen?
  - Wie detailliert sollen die Reports erstellt werden?
  - Wie sollen die Reports übermittelt werden?

Das IDS will mir helfen, was muss ich alles ignorieren?
Reports

- Zielstellung:
  - Informationsquelle zur sicherheitstechnischen Lage
  - Grundlage für strategische Planung
  - Planungskontrolle
  - Dokumentation von langfristigen Entwicklungen
- Zu klärende Frage
  - Wie oft sollen
  - Welche Informationen sollen die Reports bereitstellen?
  - Wie detailliert sollen die Reports erstellt werden?
  - Wie sollen die Reports übermittelt werden?

Achtung!
Mit einem Report wird man nie einen Hacker fangen!

T · · Systems

Das IDS will mir helfen, was muss ich alles ignorieren?
Reports

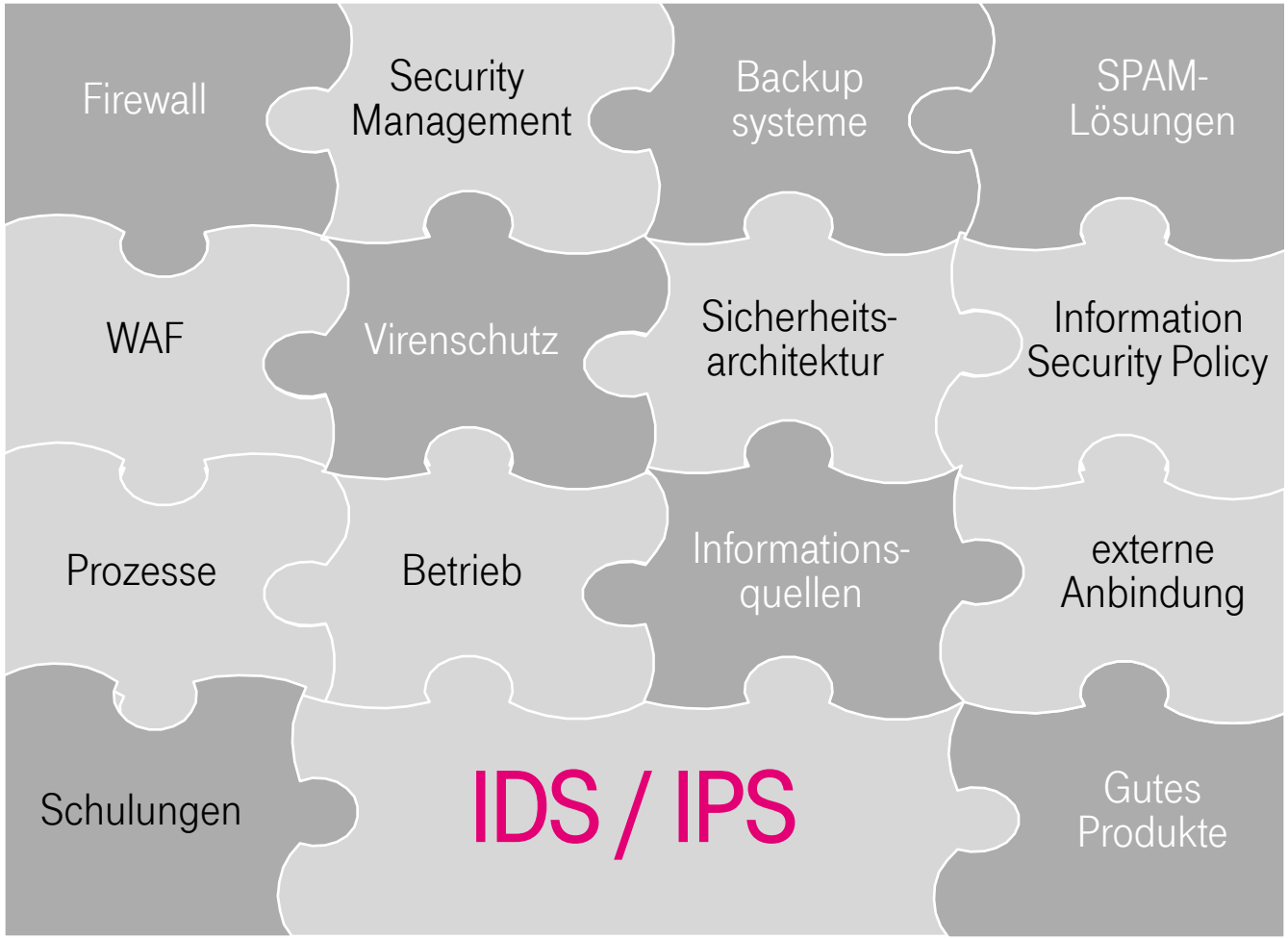
- Zielstellung:
  - Informationsquelle zur sicherheitstechnischen Lage
  - Grundlage für strategische Planung
  - Planungskontrolle
  - Dokumentation von langfristigen Entwicklungen

- Zu klärende Frage
  - Wie oft sollen
  - Welche Informationen sollen die Reports bereitstellen?
  - Wie detailliert sollen die Reports erstellt werden?
  - Wie sollen die Reports übermittelt werden?

...aber man kann Transparenz schaffen!

T · · Systems

Zusammenfasssung
Das große Ganze



T · · Systems

Zusammenfasssung
Was ist ein IDS nicht?

- Low-maintenance
- Ein Ersatz für
  - Netzwerk Monitoring
  - Logging
  - Firewalls
- IPS ist keine Verteidigung gegen alle unbekannten Angriffe
- So was ähnliches wie ein Virenscanner
- Einmal installiert und läuft dann ewig
- Wartungsarm

T · · Systems

Zusammenfassung
Was ist ein gutes IDS

- Ein IDS kann eine sehr gute Ergänzung der bestehenden Sicherheitsinfrastruktur darstellen
- Ein IDS ist komplexer im Management und Betrieb als eine Firewall
- Ein IPS braucht relativ lange, bis man es wirklich produktiv nehmen sollte
- Ein gut gepflegtes IDS in den Händen von gut geschultem und erfahrenem Personal kann überragende Ergebnisse bringen

T · · Systems

Vielen Dank für Ihre Aufmerksamkeit.

T · · Systems