CARL VON OSSIETZKY universität OLDENBURG

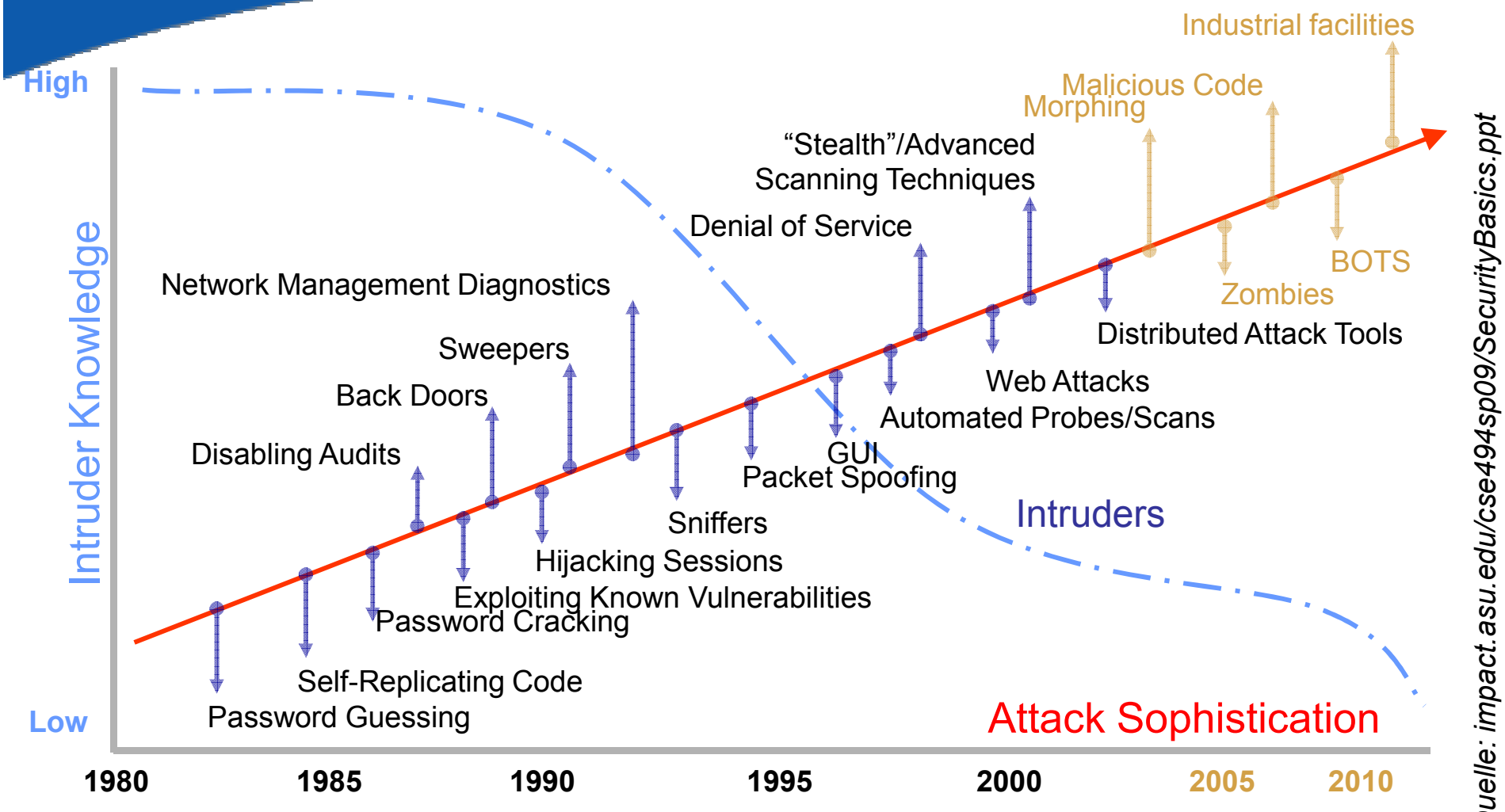
# Ein einheitliches Austauschformat zum Parametrisieren verschiedener IDS

Björn-C. Bösch

# Agenda

- Entwicklung von Angriffskomplexität und Angriffsziele
- Integrationsgrenzen heutiger IDS
- SNMPv3
- IDS Modell der IETF
- Integrationsmodule
- Formatstruktur und Snort Beispiel
- Vorteile und Nutzen standardisierter Parametrisierung
- Fazit & Zusammenfassung

# Angriffskomplexität

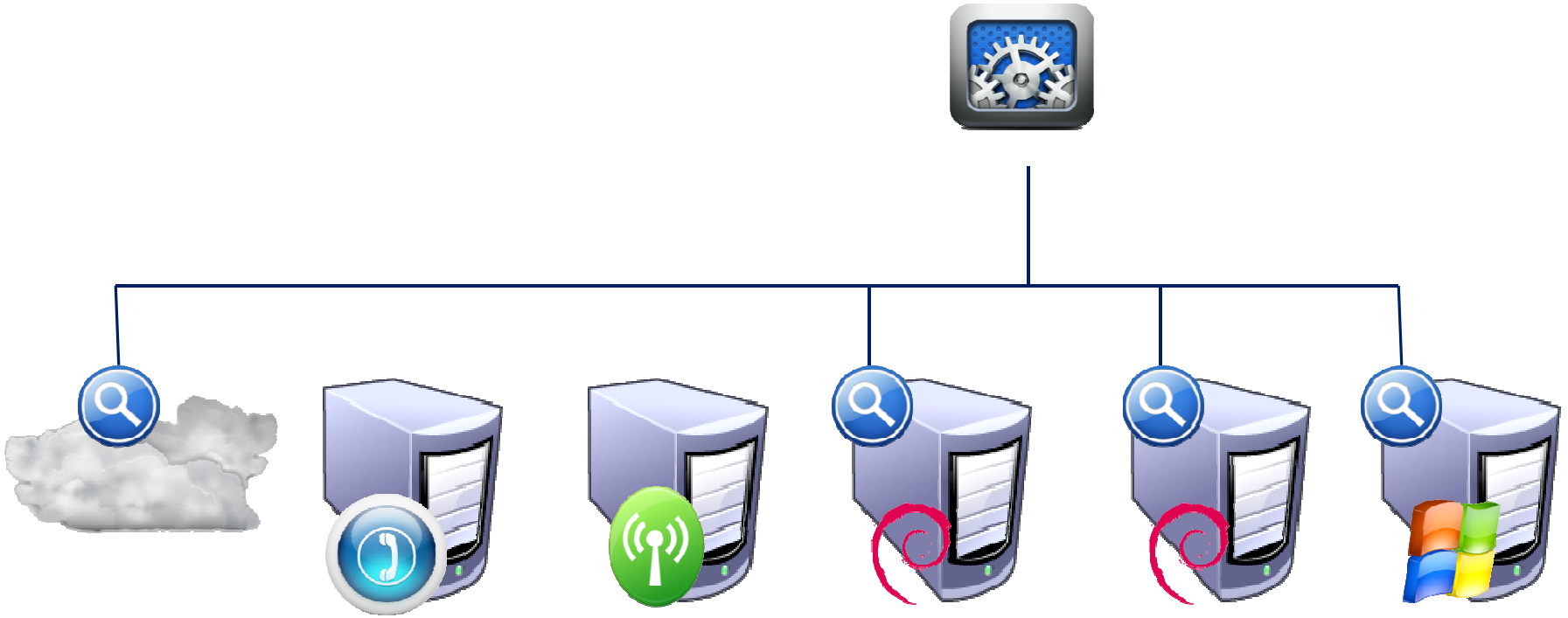



***Sources:*** *Carnegie Mellon University, 2002 and Idaho National Laboratory, 2005*

*Quelle: impact.asu.edu/cse494sp09/SecurityBasics.ppt*

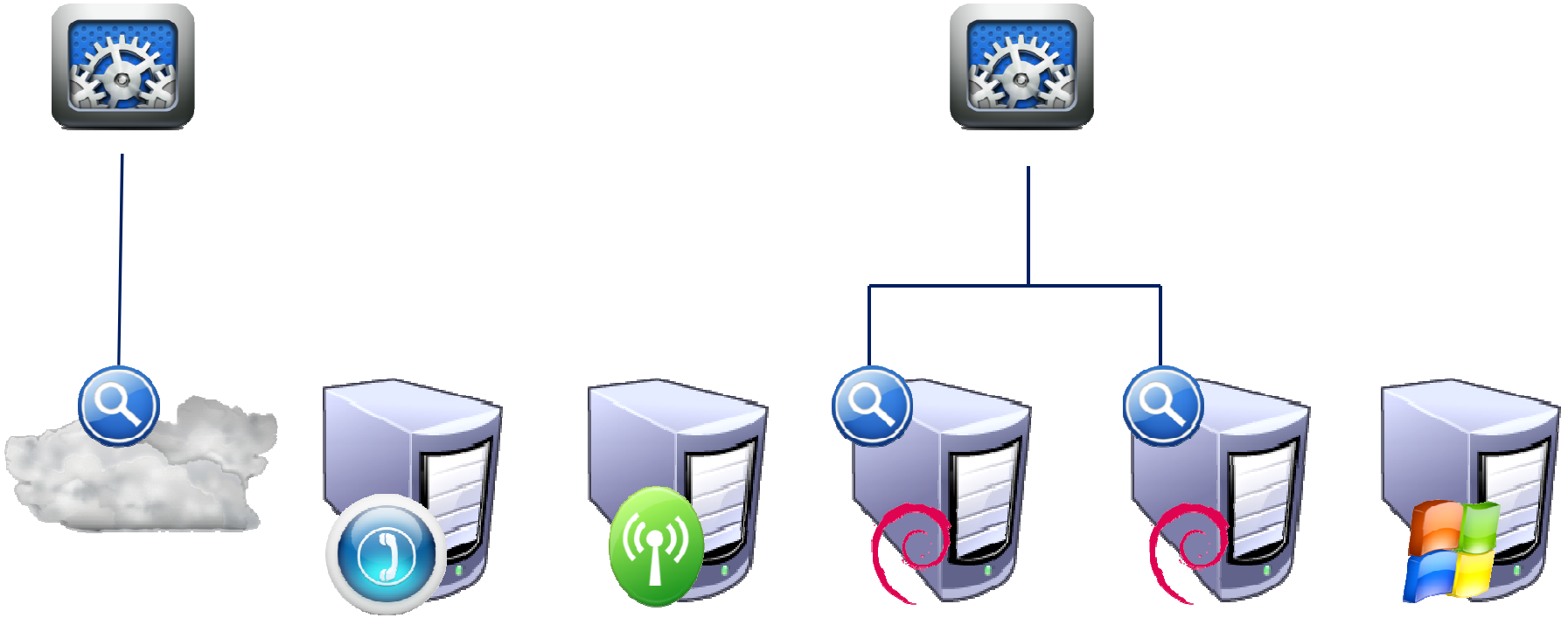
# Aktuelle IDS Integrationen

## reduzierte Erkennung



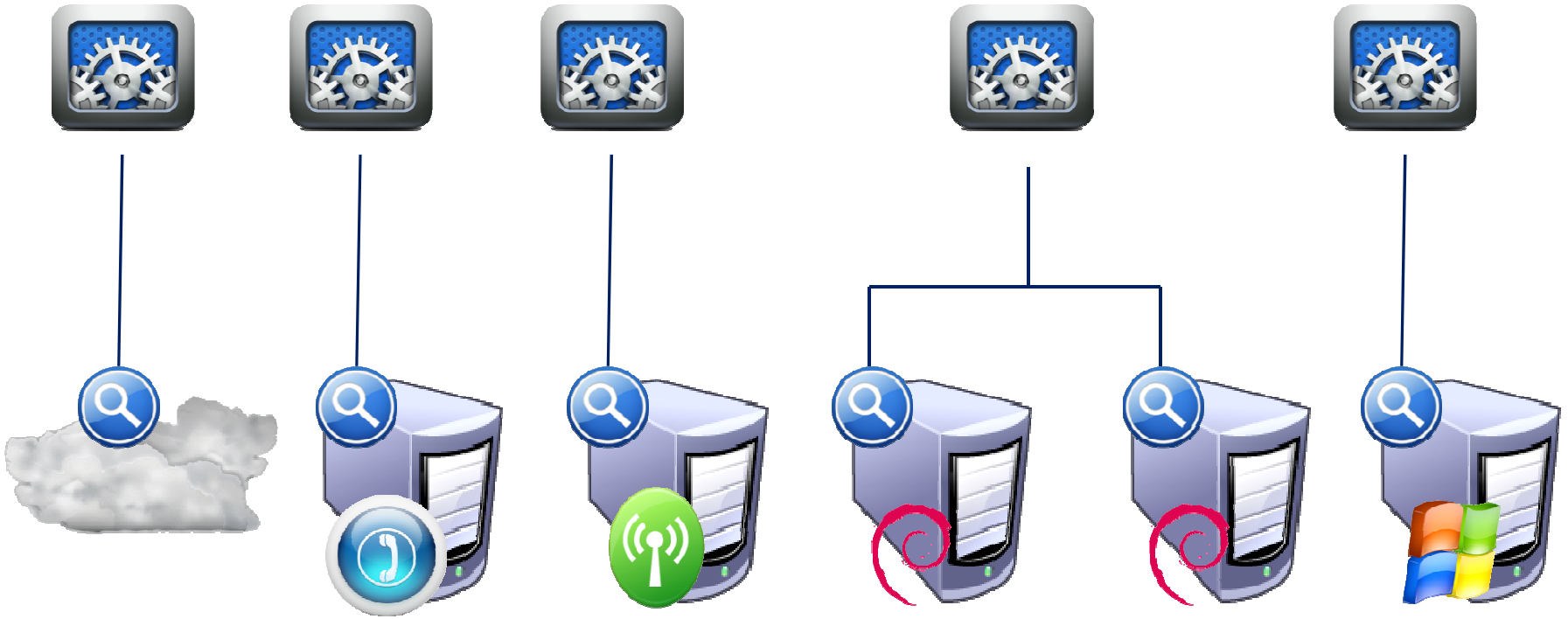
# Aktuelle IDS Integrationen

## reduzierte Abdeckung



# Aktuelle IDS Integrationen

## volle Abdeckung



# Nachteil heutiger IDS

Aktuelle IDS Integration haben folgende Nachteile:

- Oft mehrere spezialisierte IDS im Einsatz
- Ein Management-System pro IDS
- Schulungsaufwand steigt mit jedem IDS
- Individuelle Update-Mechanismen der IDS
- IDS agieren unabhängig nebeneinander
  => kein Informationsaustausch
  => keine durchgängige Security Policy,
- Keine sanfte Migration bei Wechsel eines IDS möglich

# Kernfrage

**Ist es möglich unterschiedliche IDS mit einem zentralen und einheitlichen Management-System zu verwalten?**

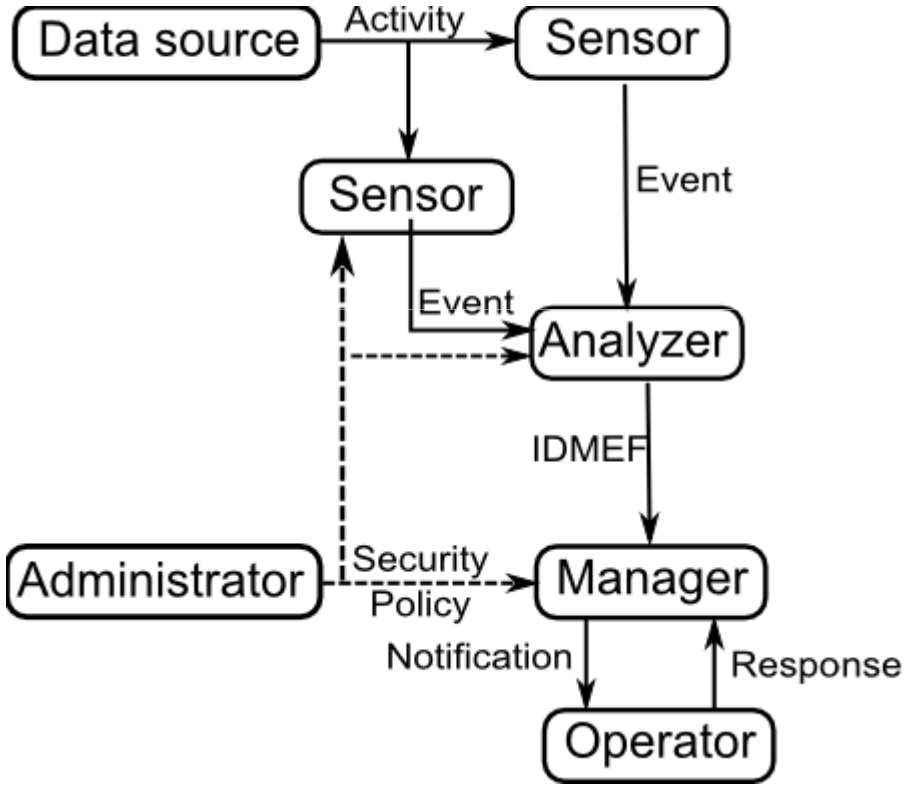
# Aktuelle Management-Protokolle

Warum nicht SNMPv3?

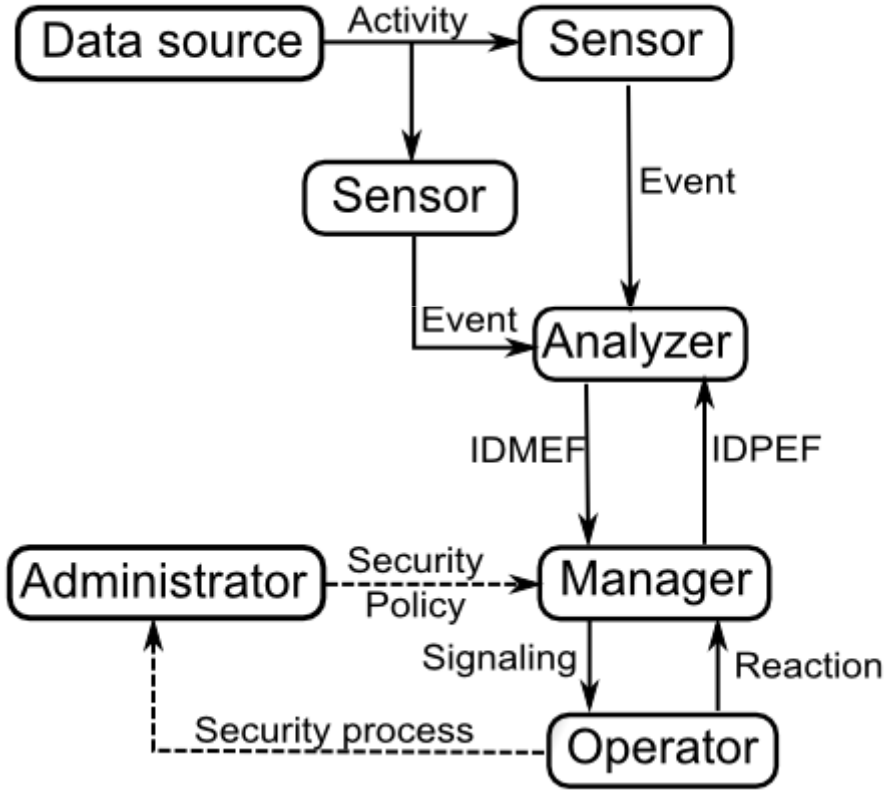
SNMP:

- ist statuslos und schwer kontrollierbar.
- schützt die Integrität und Vertraulichkeit mit 3DES, welches anfällig für kryptoanalytische Methoden ist.
- erfordert auf dem Management-System zusätzliche Informationen zum interpretieren der Daten.
- Ist nicht in der Lage größere Dateien zu übertragen.

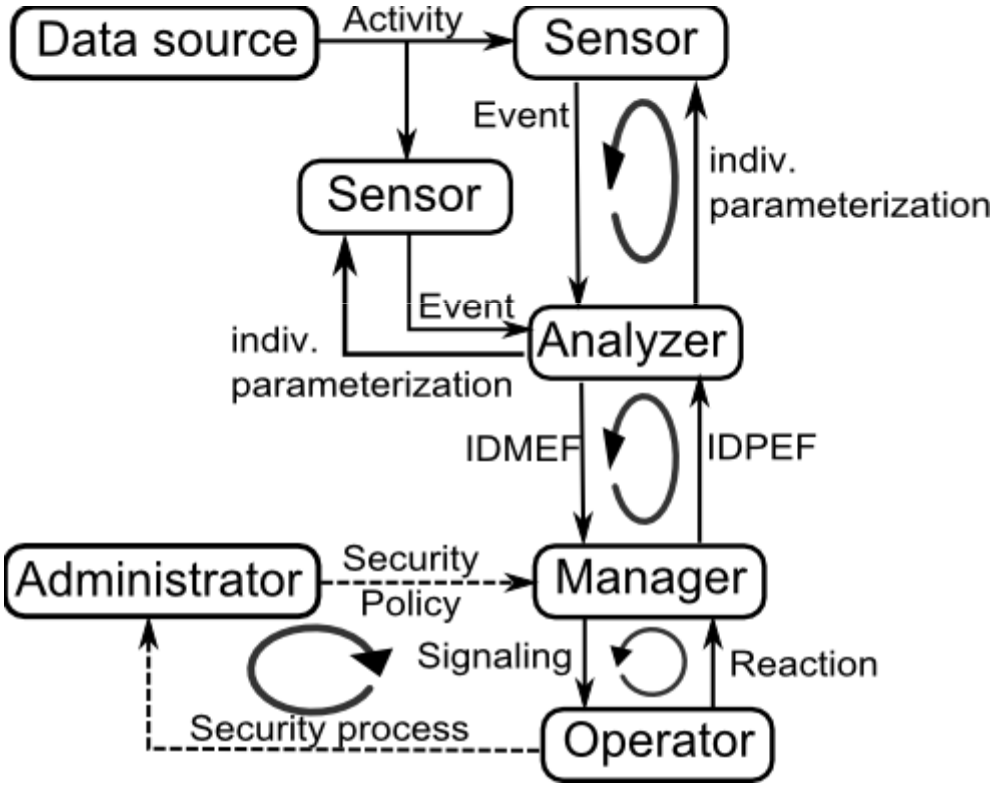
# IETF IDS Modell



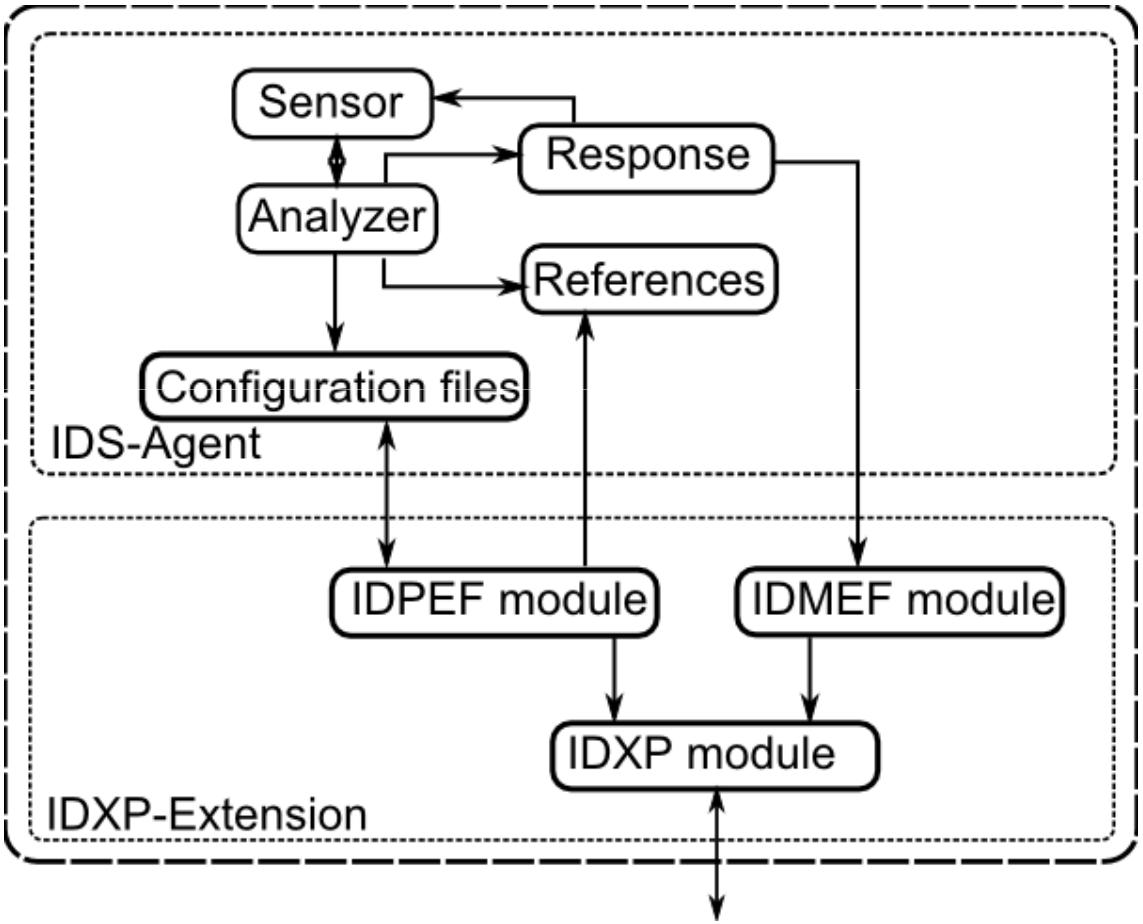
# IETF IDS Modell II



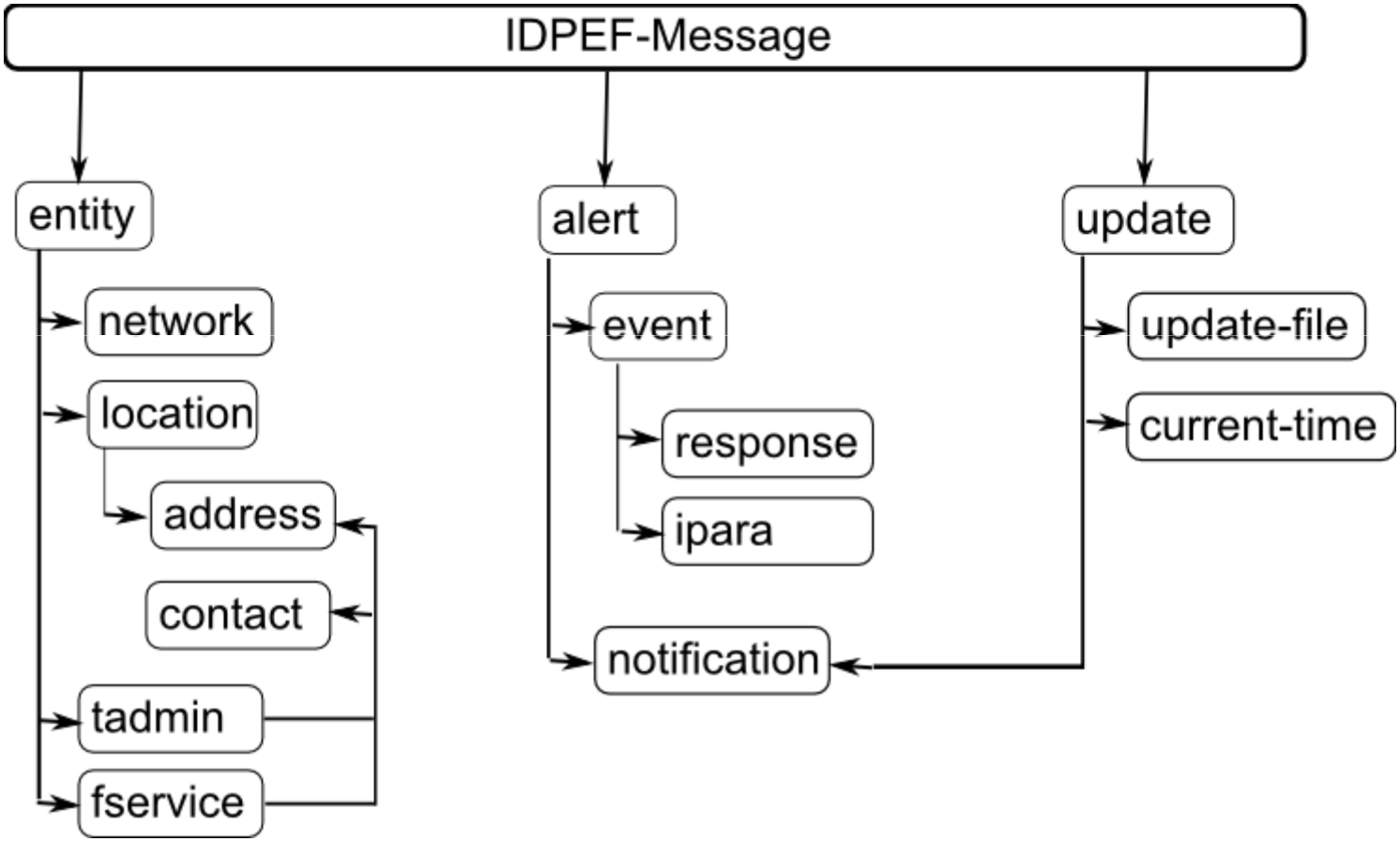
# Regelkreise im IDS Modell



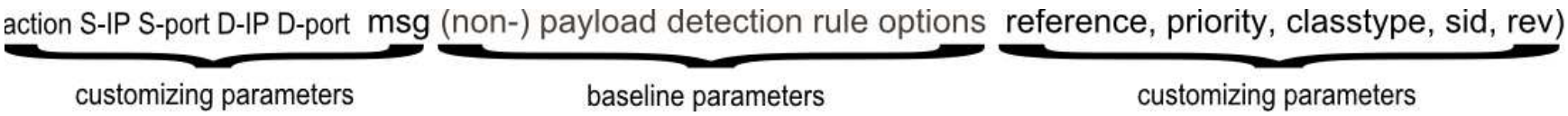
# Integrationsmodule



# Formatstruktur



# Beispiel Snort Regel

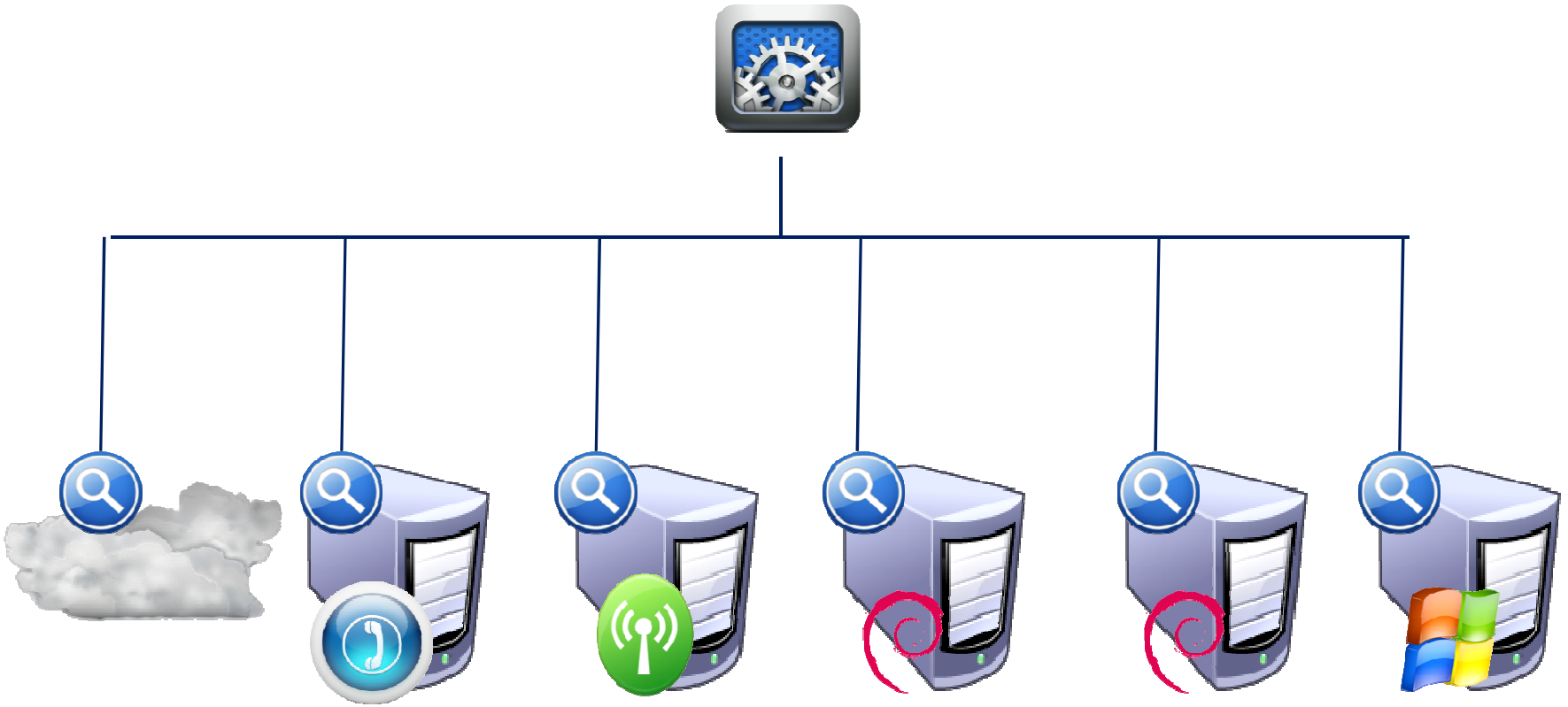



```
alert tcp $EXTERNAL_NET any -> 10.10.10.10 25
(msg:"SMTP expn cybercop attempt";
flow:to_server,established;
content:"expn cybercop";
reference:arachnids,371;
classtype:protocol-command-decode;
sid:632;
rev:5;)
```

# Beispiel Snort Rule in IDPEF

```
<IDPEF-Message>
  <alert>
    <event enable="yes"
        displayedas="SMTP expn cybercop attempt"
        name="632_5"
        origin="arachnids,371"
        serverity="protocol-command-decode" >
          <ipara value="any" name="source" enable="yes"/>
          <ipara value="alert" name="ruleaction" enable="yes"/>
          <ipara value="-&gt;" name="direction" enable="yes"/>
          <ipara value="10.10.10.10" name="destination" enable="yes"/>
    </event>
 </alert>
</IDPEF-Message>
```

# Künftige IDS Integrationen



# Vorteile und Nutzen

Im Rahmen der Integration wurde festgestellt:

- Verwalten aller IDS mit einem Managementsystem.
- Nur eine Hardware und Applikation erforderlich.
- Eine einheitliche Bedienoberfläche für alle IDS.
- Eine zentrale Instanz zum Einspielen und Verteilen von Updates.
- Abgleich von Security Policies einzelner IDS per Logik.

# Zusammenfassung

- IDS sind über standardisierte Formate parametrisierbar.
- IDS Parameter lassen sich auf eine Grundstruktur zurückführen.
- Mit einem zentralen Management-System sind alle IDS zu verwalten.
- Updates werden durch das zentrale Management-System an die Analyzer verteilt.
- Abgleich von Security Policies einzelner IDS per Logik.
- Unabhängige Entwicklungen von Management-System und IDS.

Vielen Dank

für

Ihre Aufmerksamkeit!

# Fragen?