# Intrusion Detection Parameterization Exchange Format

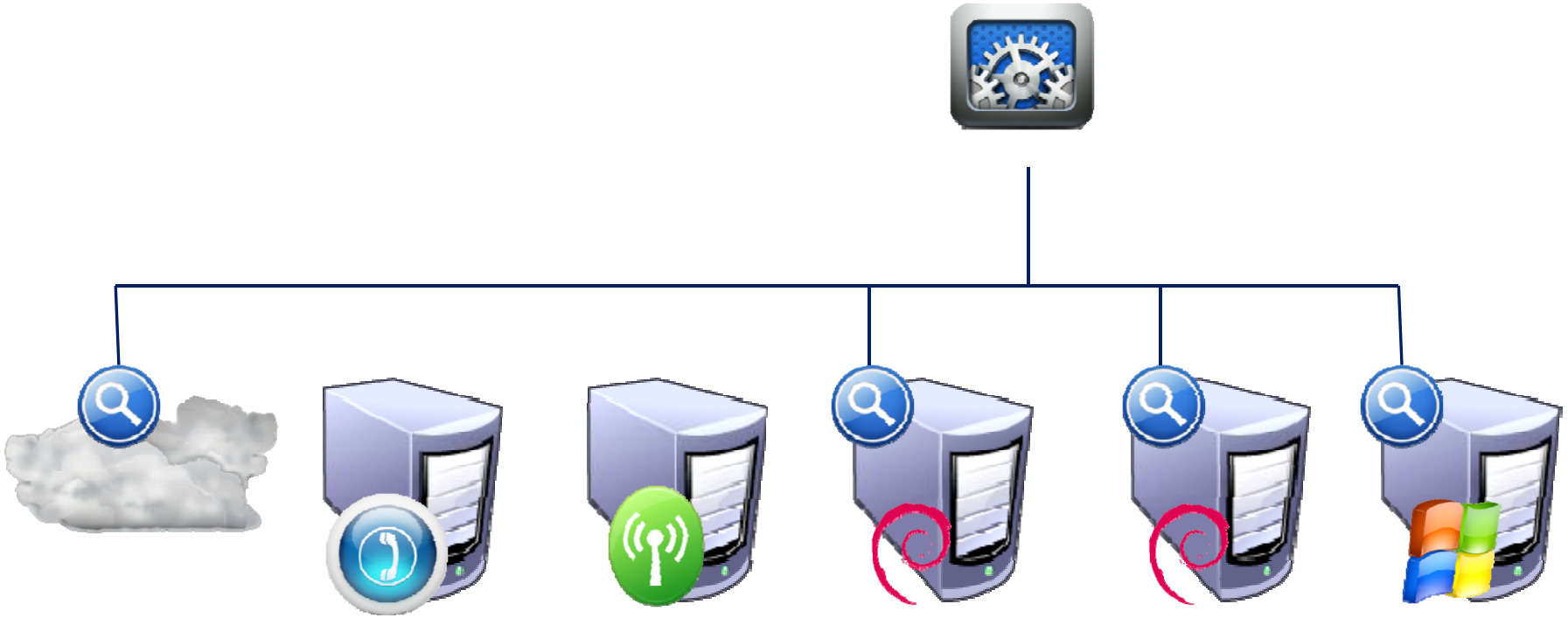
Björn-C. Bösch

# Agenda

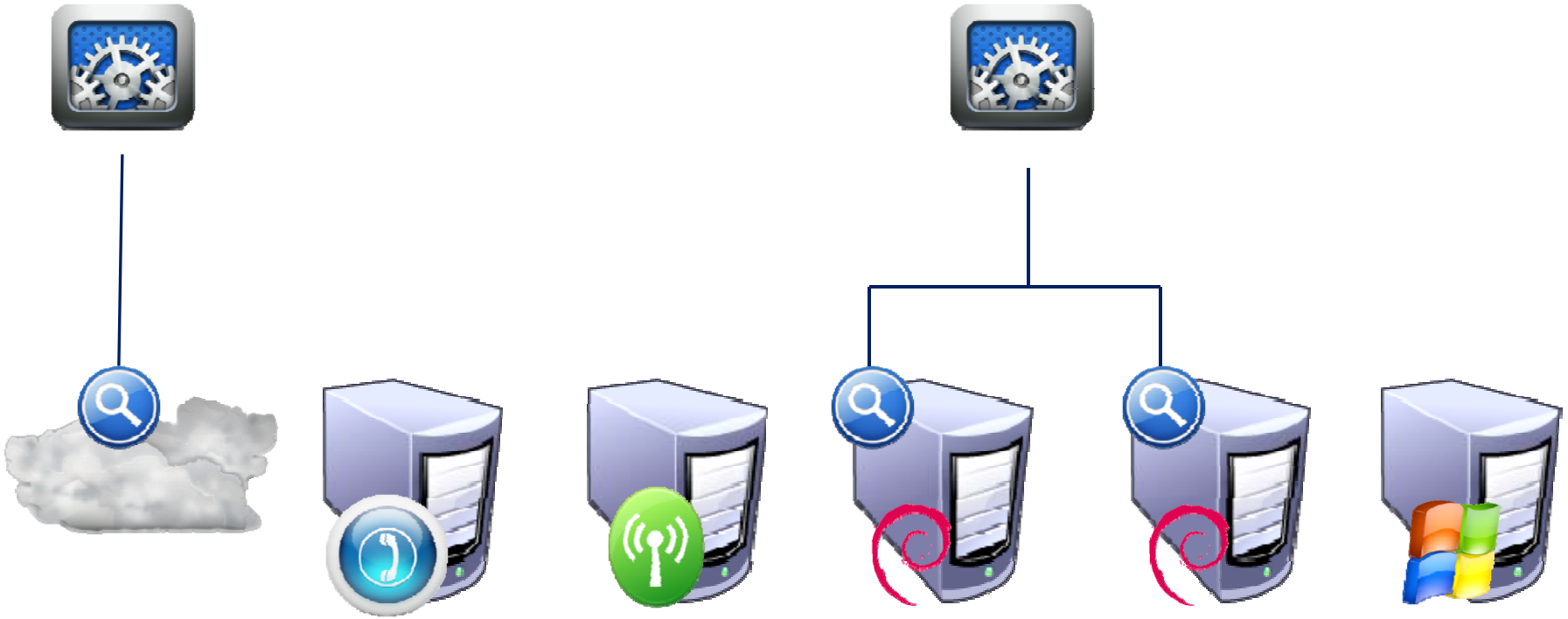
- Aktuelle IDS Integrationsansätze
- SNMPv3
- Derzeitige IDS Model der IETF
- Integrationsmodule
- Struktur von IDPEF an Beispiel einer Snort Regel
- Vorteile standarisierter Parameterisierung
- Zusammenfassung

# IDS Integration

## reduzierte Erkennung



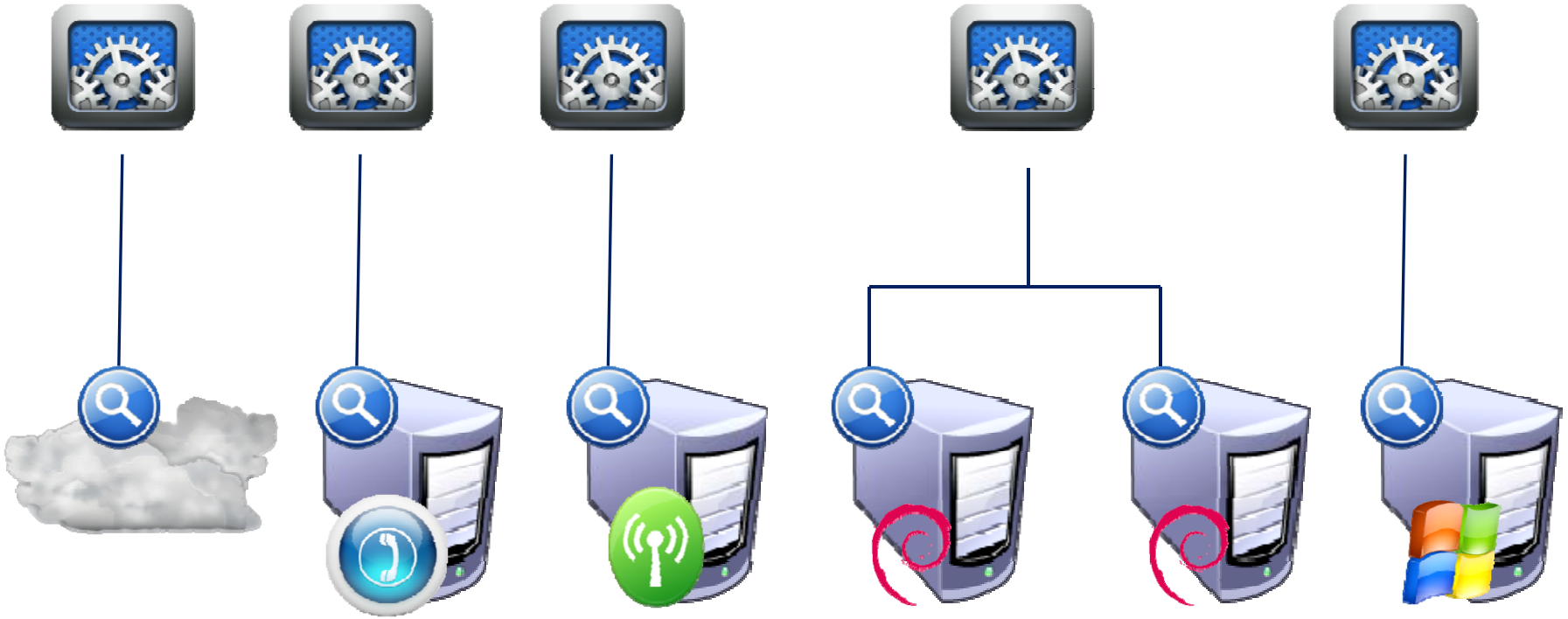
# Reduced Coverage



# IDS Integration

~~Reduzierte~~ Abdeckung

volle



# Einschränkungen aktueller IDS

Einschränkungen heutiger IDS Integrationen:

- 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?**

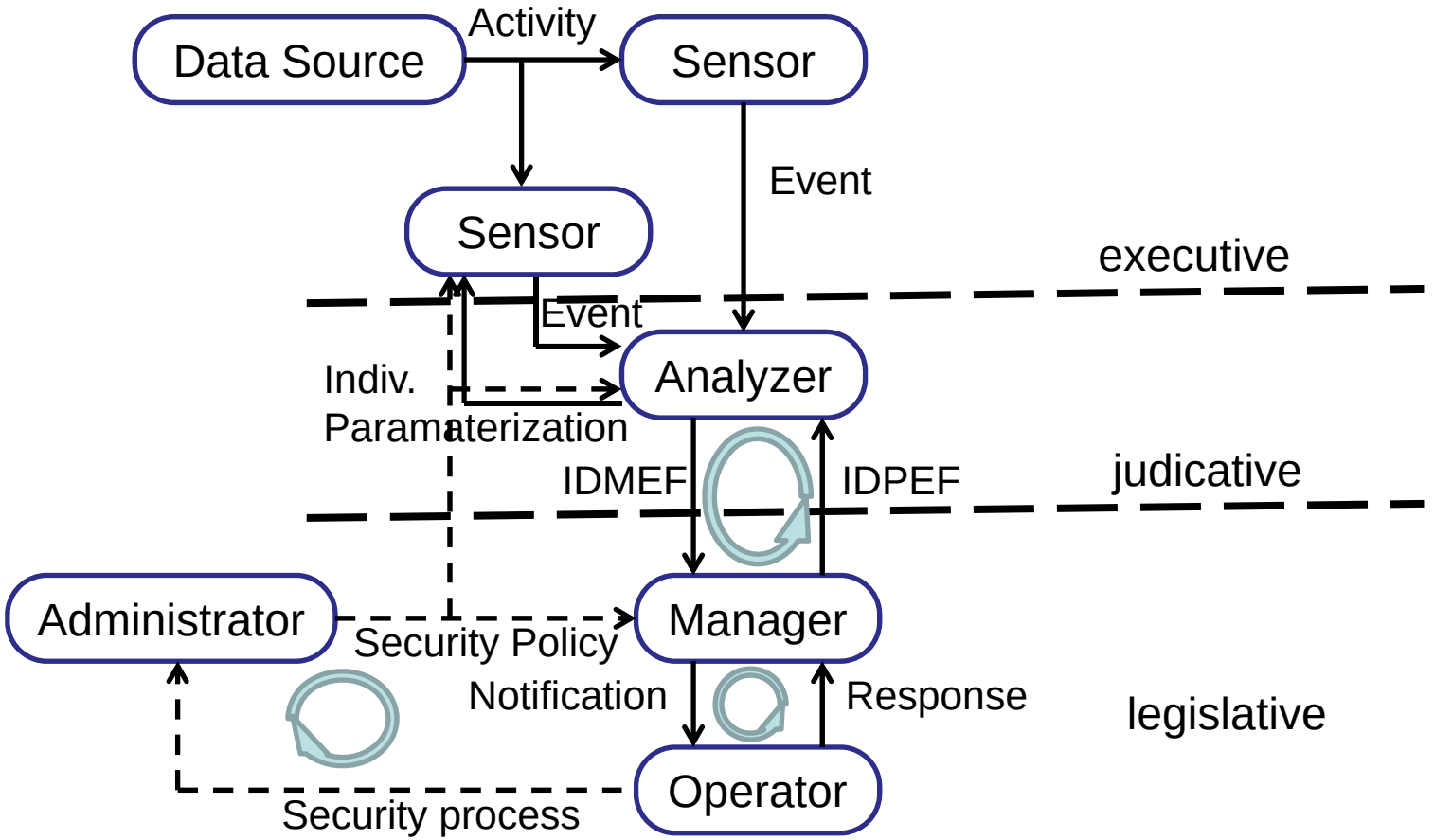
# Aktuelle Management Protokolle

Warum nicht SNMPv3?

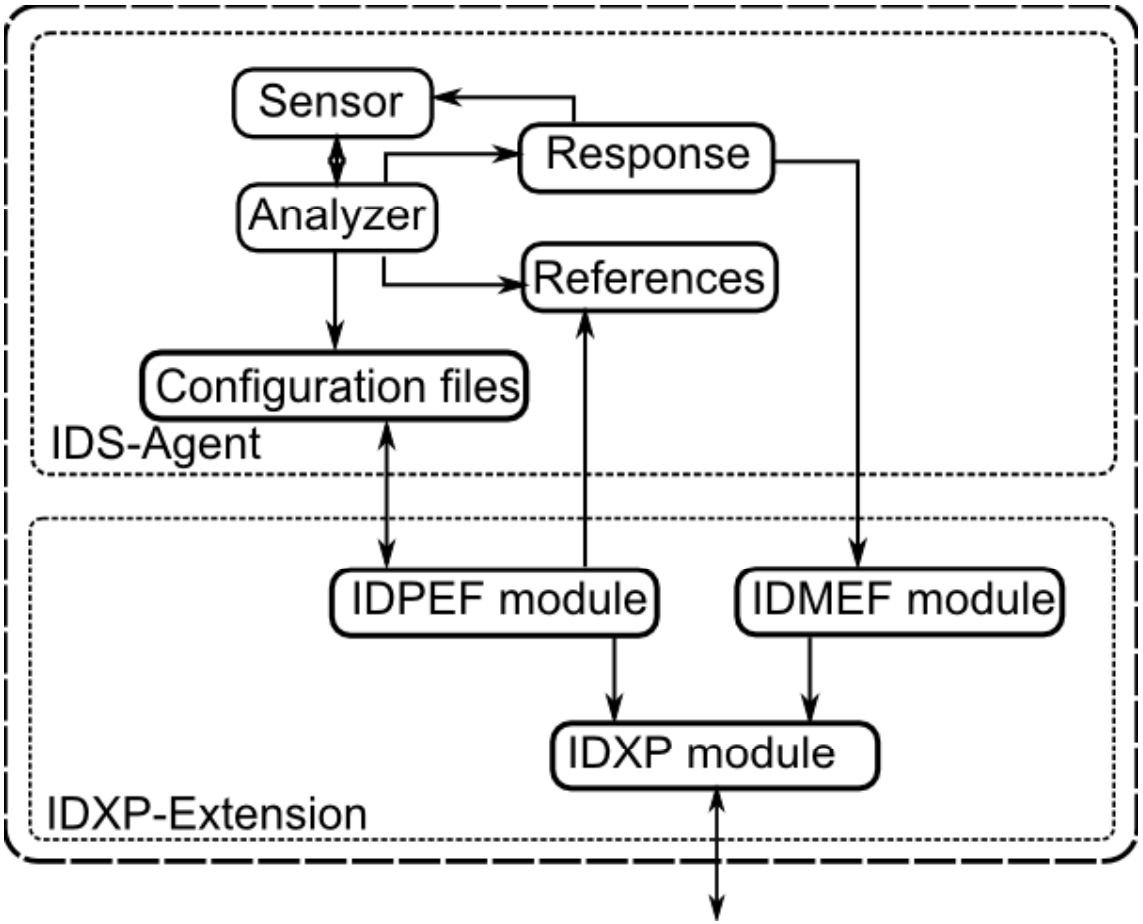
SNMP:

- 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.

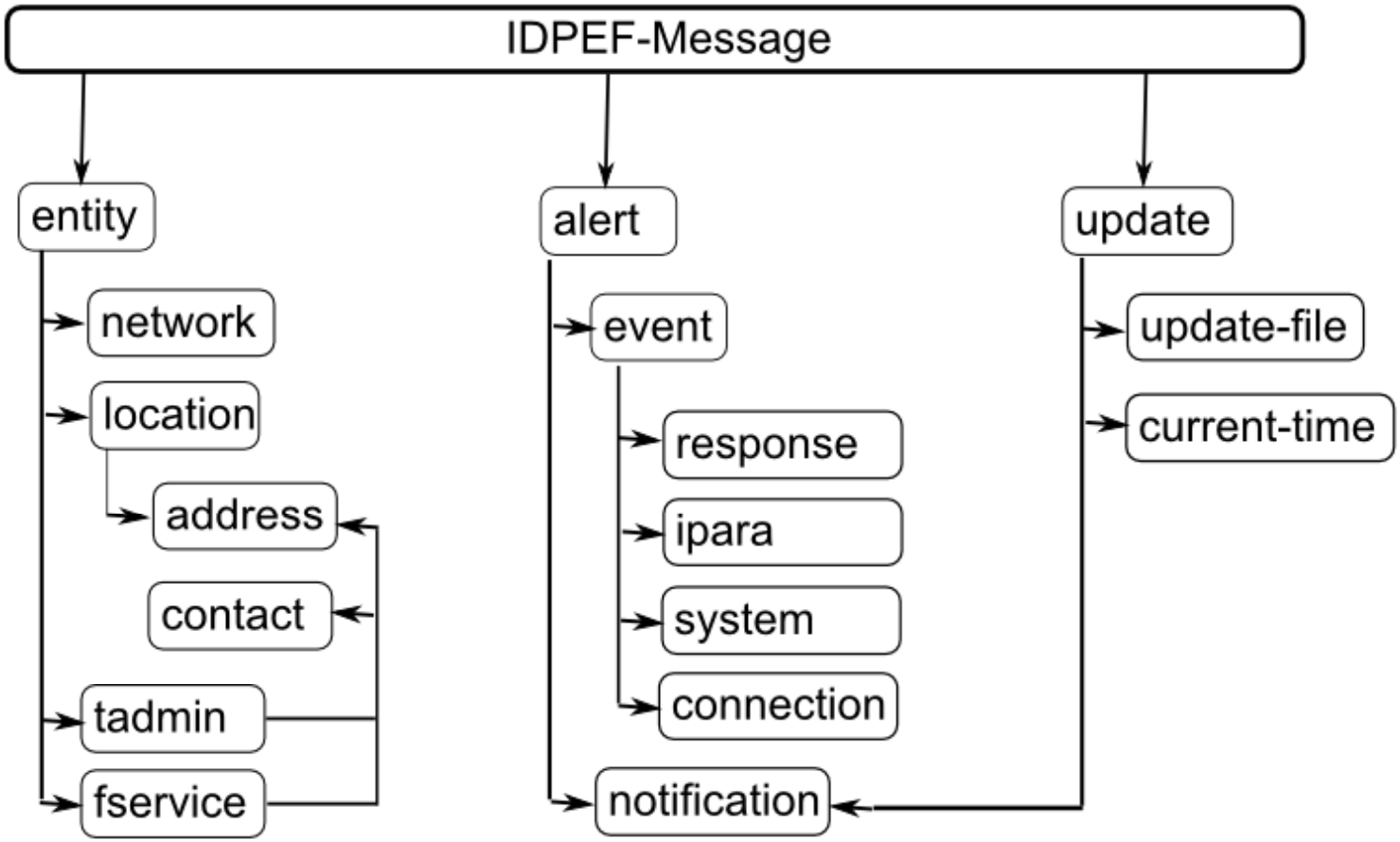
# IETF IDS Model



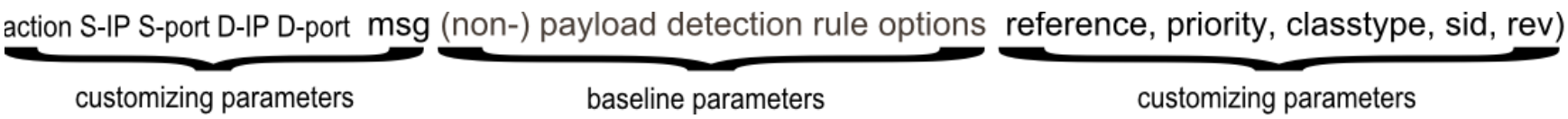
# Integrationsmodul



# Formatstruktur



# Beispiel: Snort Rule

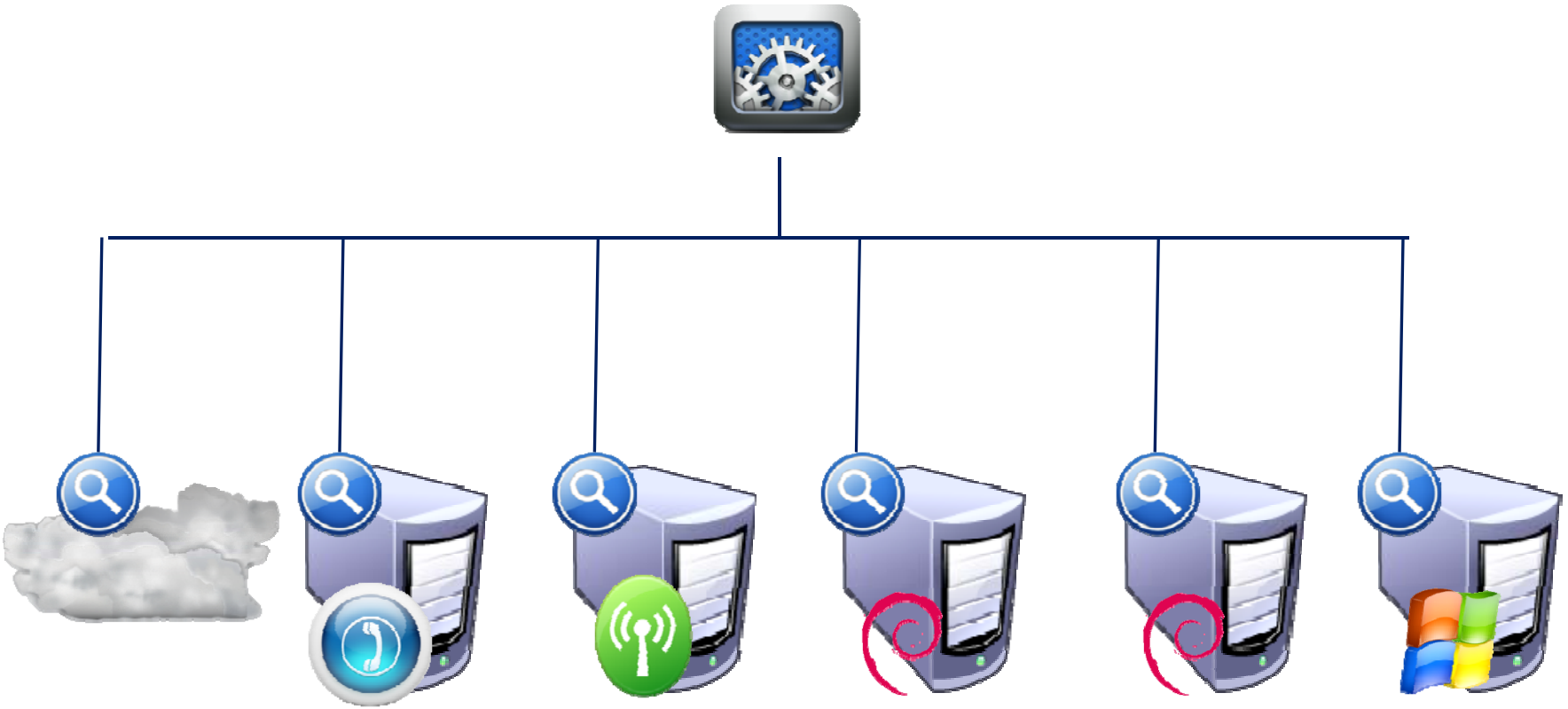



```
alert tcp $EXTERNAL_NET any -> 10.10.10.10 25
(msg:"SMTP expn cybercop attempt";
flow:to_server,established;
content:"expn cybercop";
reference:arachnids,371;
classtype:protocol-command-decode;
sid:632;
rev:5;)
```

# Beispiel: Snort Rule in IDPEF

```
<IDPEF-Message>
  <alert>
    <event enable="yes"
        displayedas="SMTP expn cybercop attempt"
        name="632_5"
        origin="arachnids,371"
        severity="protocol-command-decode"
        impact=“confidentiality” >
      <connection source="any" ruleaction="alert“ direction=“bidirectional"
        destination="10.10.10.10" />
    </event>
 </alert>
</IDPEF-Message>
```

# Künftige IDS Integrationen mit IDPEF



# Vorteile

Im Rahmen der Integrationen wurde festgestellt:

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

# Zusammenfassung

- IDS sind über standardisierte Formate parametrisierbar, Hersteller- und Analyseunabhängig.
- Abgleich von Security Policies einzelner IDS per Logik.
- Unabhängige Entwicklungspfade für Management-System und IDS.

Vielen Dank

für die Aufmerksamkeit!

# Fragen?