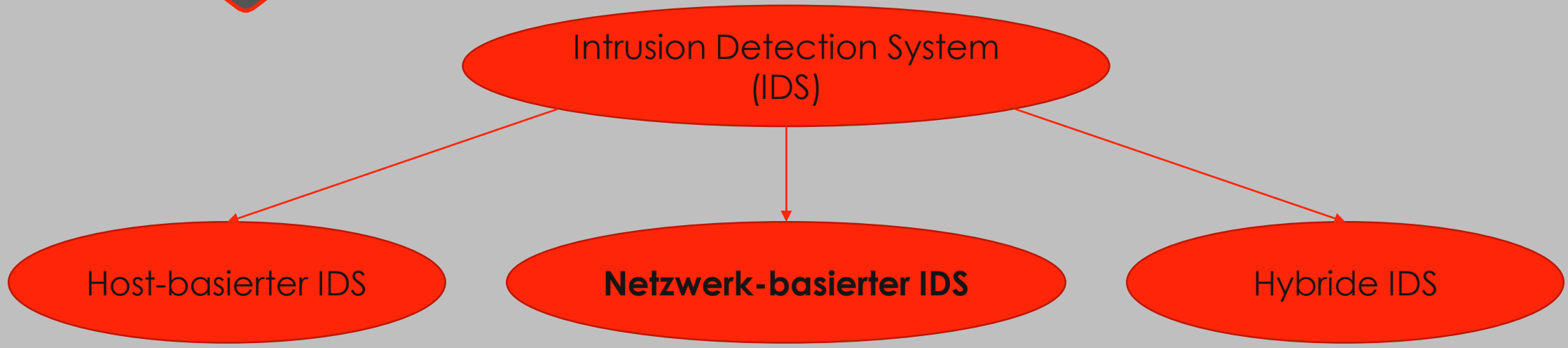
HAW HAMBURG

NADS
Network based **A**nomaly **D**etection **S**ystems

Einblick in ein Angriffserkennungssystem

Angriffserkennungssysteme: Architekturen

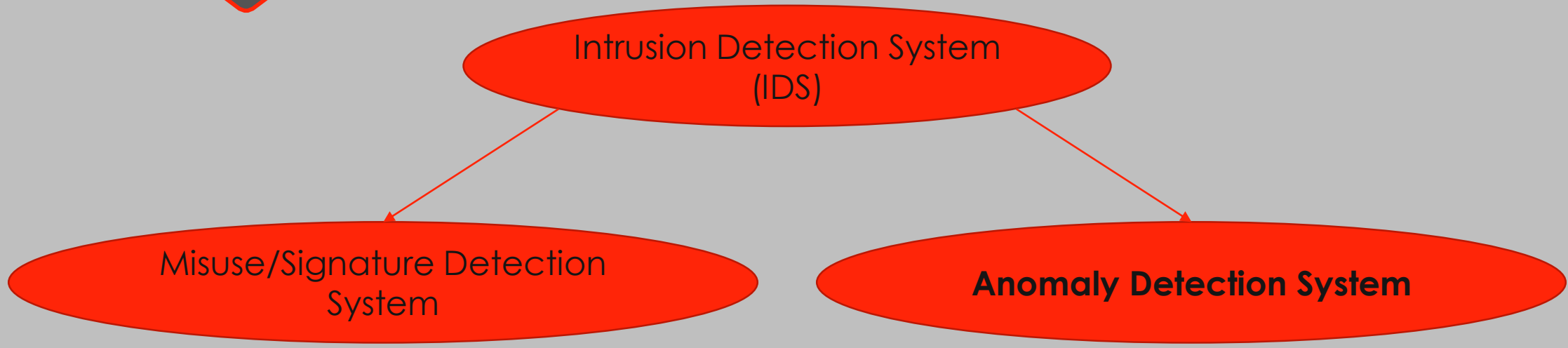


- Überwacht einen Host
- Informationen aus Systemdateien:
  - Logs
  - Registry
  - …

- Überwacht Netzwerk
- Informationen aus Netzwerkverkehr:
  - Ethernet
  - IP
  - TCP/UDP
  - …

- Verbindet beide Ansätze
- Besteht aus Host- und Netzbasierten Seonsoren

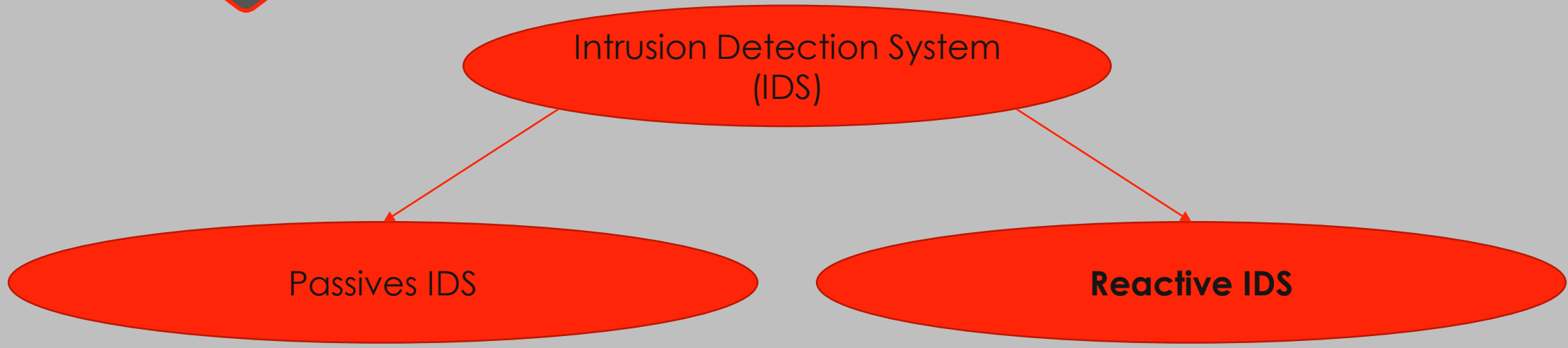
Angriffserkennungssysteme: Umsetzungen



- Angriffszustand wird definiert
- Nicht definierte Angriffe können auch nicht erkannt werden
- Beispiel: Antivirus

- Normalzustand wird definiert
- Leichte Abweichungen vom Normalverhalten können fälschlicherweise als Angriff interpretiert werden (false positive)

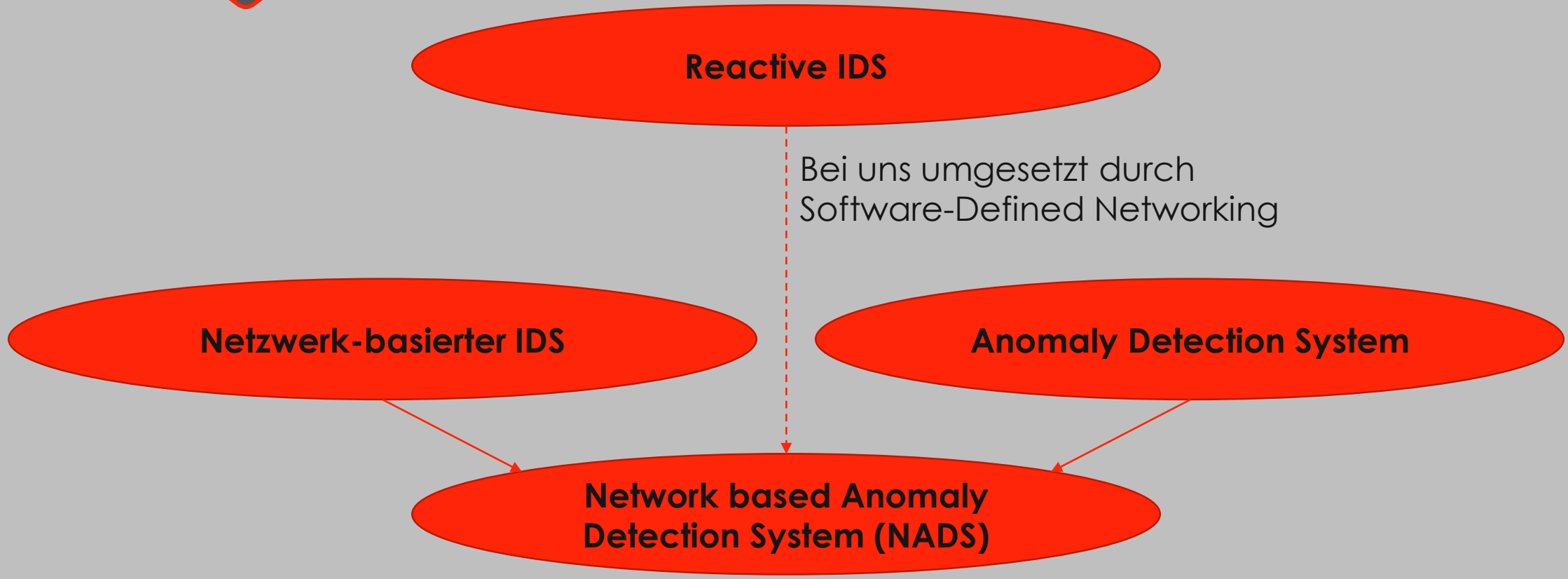
Angriffserkennungssysteme: Reaktionen



- Meldet Angriffe an höhere Instanz/Log

- Meldet Angriffe an höhere Instanz/Log
- Initiiert eine Reaktion auf den Angriff

NADS
Network based **A**nomaly **D**etection **S**ystem



NADS
Datengrundlage

- Alles was das Netzwerkkabel hergibt:
  - Ethernet Header
  - IP Header
  - TCP/UDP Header
  - Metadaten:
    - Bandbreite
    - Paketgrößen
    - Paketabstände

NADS
Algorithmen

- Statistical
- Classification (supervised)
- Clustering (unsupervised)
- Knowledge Based
- Hybrid

NADS
Herausforderungen

- Welche Anomalien möchte man erkennen?
- Welche Technologie einsetzen?
- Wie bekomme ich die Informationen zur Laufzeit?
- Wie ist eine Anomalie definiert?
- Wie beeinflusst die False Positive Rate das Gesamtsystem?
- Welche Reaktion folgt auf eine Anomalie?

NADS
Network based **A**nomaly **D**etection **S**ystems