Universität Rostock

Traditio et Innovatio

Service- and Security Monitoring

Auswertung, Konsolidierung, Korrelierung und Visualisierung IT-Sicherheitskritischer Ereignisse

Martin Steinbach
Universität Rostock, Institut für Informatik

Seminar Sommersemester 2018
Auswertung und Visualisierung komplexer Daten

Struktur

Struktur

Struktur

Einführung

- Warum Überwachung?
- Überwachungsformen

Aktives Monitoring

- Was kann überwacht werden
- Fallbeispiel: DDoS

Passives Monitoring

- Logkorrelation in Cloud-Umgebungen

Warum Überwachung?

Servicemonitoring = Securitymonitoring?

Ziele der Informationssicherheit

- Vertraulichkeit
- **Verbindlichkeit**
- **Integrität**
- **Verfügbarkeit**

Betrachtungen

- Zeitliche Perspektive
- Schweregrad (severity)
- Quelle
- Ereigniskorrelation

Ziele der Informationssicherheit

- Vertraulichkeit
- **Verbindlichkeit**
- **Integrität**
- **Verfügbarkeit**

Betrachtungen

- Zeitliche Perspektive
- Schweregrad (severity)
- Quelle
- Ereigniskorrelation

Warum Überwachung?

Servicemonitoring = Securitymonitoring?

Ziele der Informationssicherheit

- Vertraulichkeit
- **Verbindlichkeit**
- **Integrität**
- **Verfügbarkeit**

Betrachtungen

- Zeitliche Perspektive
- Schweregrad (severity)
- Quelle
- Ereigniskorrelation

Servicemonitoring = Securitymonitoring?

Ja!?

Nur ein unmanipulierter Dienst, der erwiesenermaßen seine Aufgaben erfüllt, hält die Ziele der IT-Sicherheit ein.

Beweis durch Überwachung

- Unerwartetes Verhalten
- Erreichbarkeit
- Angriffserkennung
- Nachvollziebarkeit

Servicemonitoring = Securitymonitoring?

Ja!?

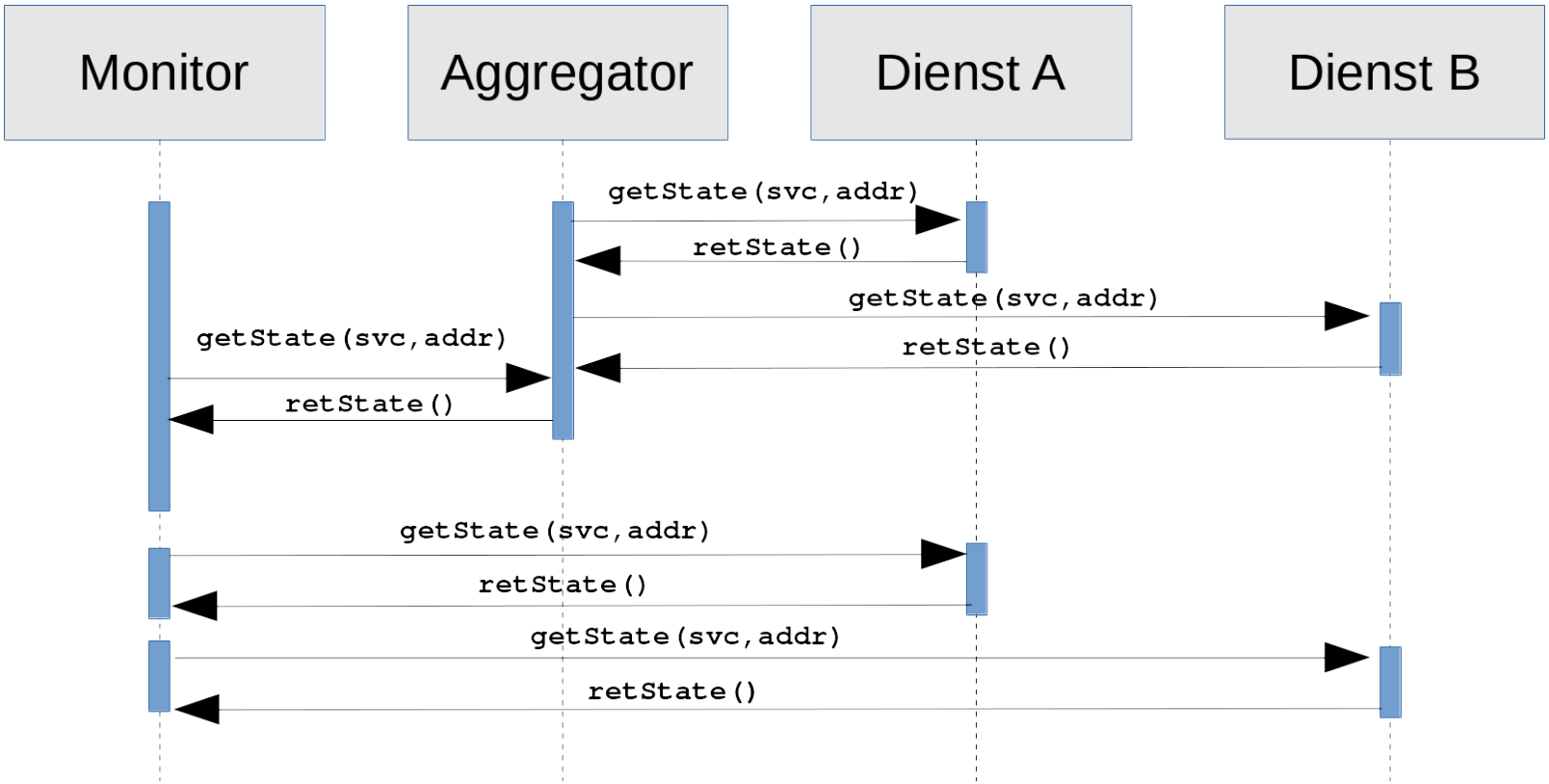
Nur ein unmanipulierter Dienst, der erwiesenermaßen seine Aufgaben erfüllt, hält die Ziele der IT-Sicherheit ein.

Beweis durch Überwachung

- Unerwartetes Verhalten
- Erreichbarkeit
- Angriffserkennung
- Nachvollziebarkeit

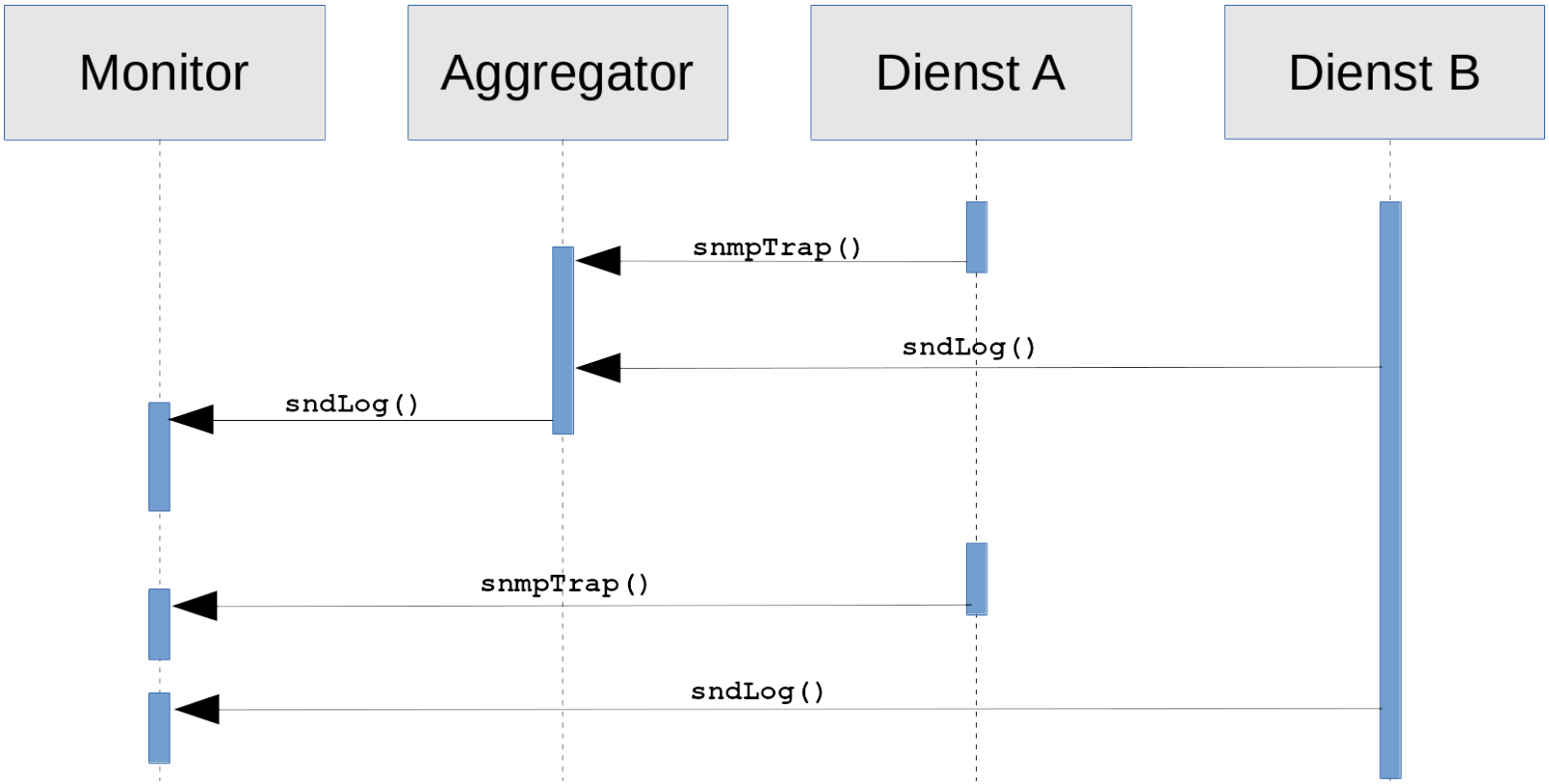
Aktive Überwachung

Beispiel Sequenzdiagramm



Passive Überwachung

Beispiel Sequenzdiagramm



Aktive Überwachung

Was kann überwacht werden?

Jede Entität, deren Status deutlich zueinander abgrenzbar sind.

- Betriebsystemabhängig
  - Betriebsystemparameter
    - Auslastung
    - Speicher
    - Prozesse
  - Updates
  - Sicherheitsauditierung
- Betriebsystemunabhängig
  - Netzwerkdienste
    - L3: ICMP{4,6}
    - L4: TCP, UDP - basierend
    - L4+: SNMP
  - Sensoren
  - Aktive Netzwerkkomponenten

There Is No Largest Prime Number

There Is No Largest Prime Number