deutsches forschungsnetz

Security Operations im DFN

71. DFN-Betriebstagung | 24.09.2019

Ralf Gröper

Was sind SecOps?

- Security Operations umfassen
  - **operative Aspekte**: Erkennung, Information und Abwehr konkreter **aktueller Bedrohungen** bzw. Angriffe **in Echtzeit**
  - **strategische Aspekte**: **Langfristige** Voraberkennung und Information über potentielle **zukünftige Bedrohungen** bzw. Angriffe

- Die hierfür notwendigen Prozesse werden von einer dedizierten Organisationseinheit durchgeführt, dem **Security Operations Center** (SOC)

SecOps für wen? 1. für DFN-Infrastruktur

- Aspekt „SecOps für DFN-Dienste“:
  - Welche **Verfügbarkeit** benötigen DFN-(Zusatz-)Dienste?
  - Mit welchen Reaktionszeiten müssen **Vertraulichkeit** und **Integrität** gesichert werden?
  - DFN-Dienste mit „Best Effort, 8/5“:
    - DFN-AAI, eduroam, DoS-Basisschutz, DFN-CERT, DFNconf, DFNTerminplaner, DFN-Listserv
    - Mehr haben das X-WiN, DFN-MailSupport und der Erweiterte DoS-Schutz

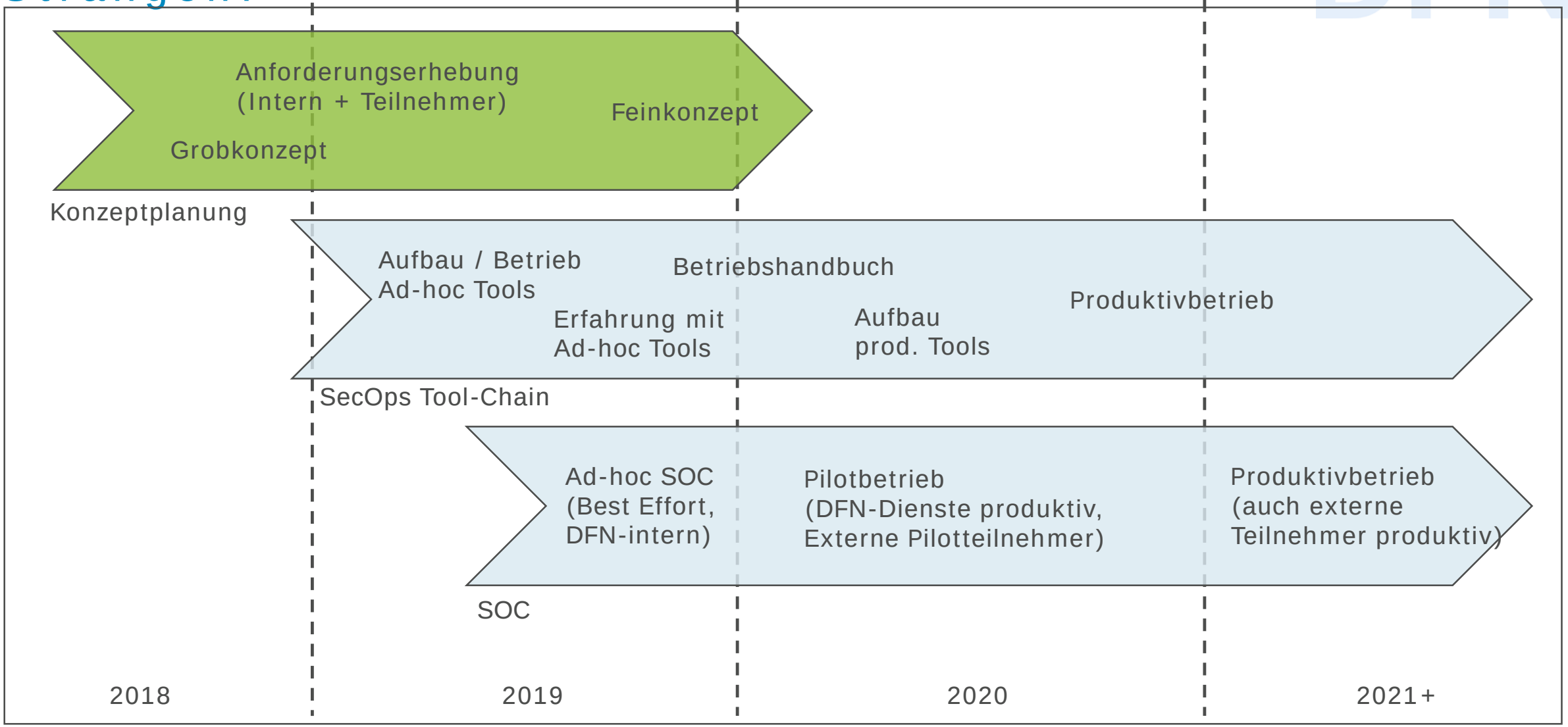
- Wenn wir erweiterte Bereitschaftszeiten brauchen (24/7, 8/7, 12/5, 12/7) müssen Voraussetzungen geschaffen werden

SecOps für wen? 2. für Teilnehmer

- Sehr heterogene Teilnehmer haben Interesse an DFN-SecOps:
  - Sehr große Einrichtungen
    - Anforderungen: 24/7, Full Service
    - Eher wenige (einstellig)
  - Die breite Mehrheit, hauptsächlich HS-/Uni Rechenzentren
    - Anforderungen: weniger als 24/7, aber ggf. mehr als 8/5, ausgewählte wichtige Use Cases
    - Sehr viele Einrichtungen (potentiell dreistellig)

- Welche Zielgruppe soll bei DFN SecOps priorisiert behandelt werden?
  - Vorgehen: Mit der breiten Mehrheit anfangen
  - Paradigma „Start small, grow smart“

Das Projekt „SecOps im DFN“: Vorgehen in drei Strängen:

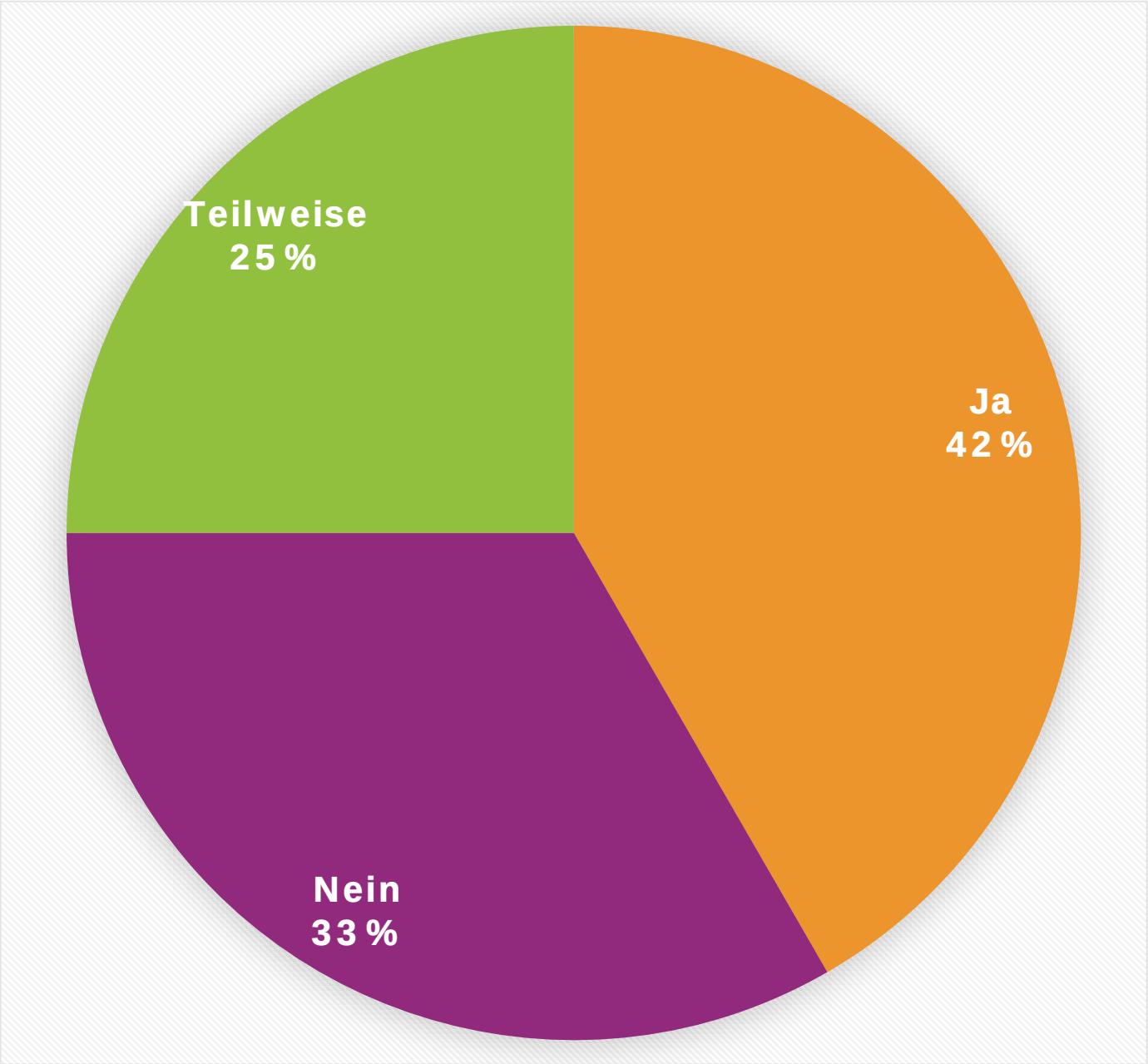


Die 5 Fragen vom letzten Mal

- Bisher 12 Antworten
- Vielen Dank für das Feedback!
- Zusammenfassung der Antworten im Folgenden

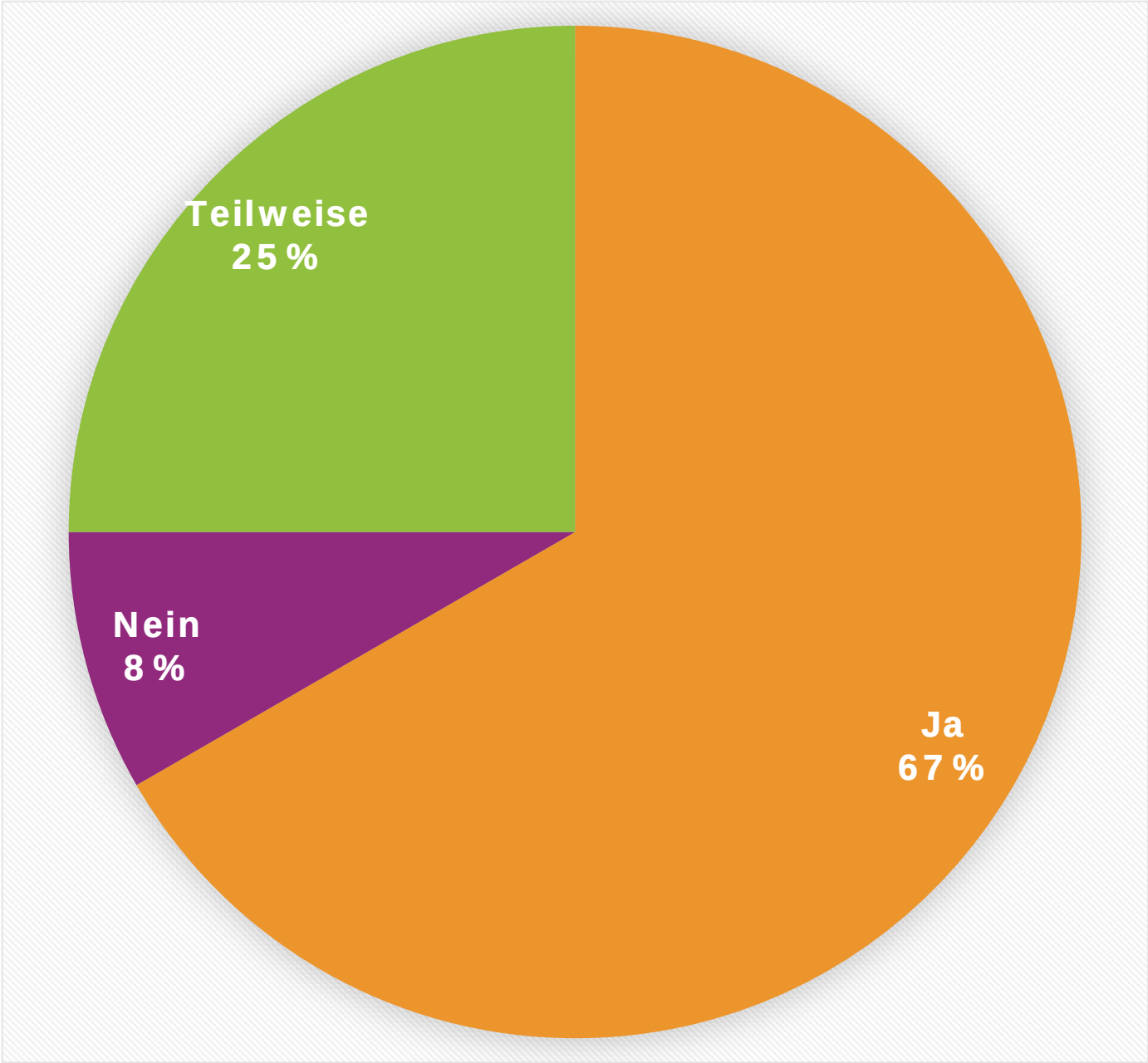
1. Frage

- Haben Sie ein SOC oder haben Sie darüber nachgedacht, eines einzurichten oder einzukaufen?



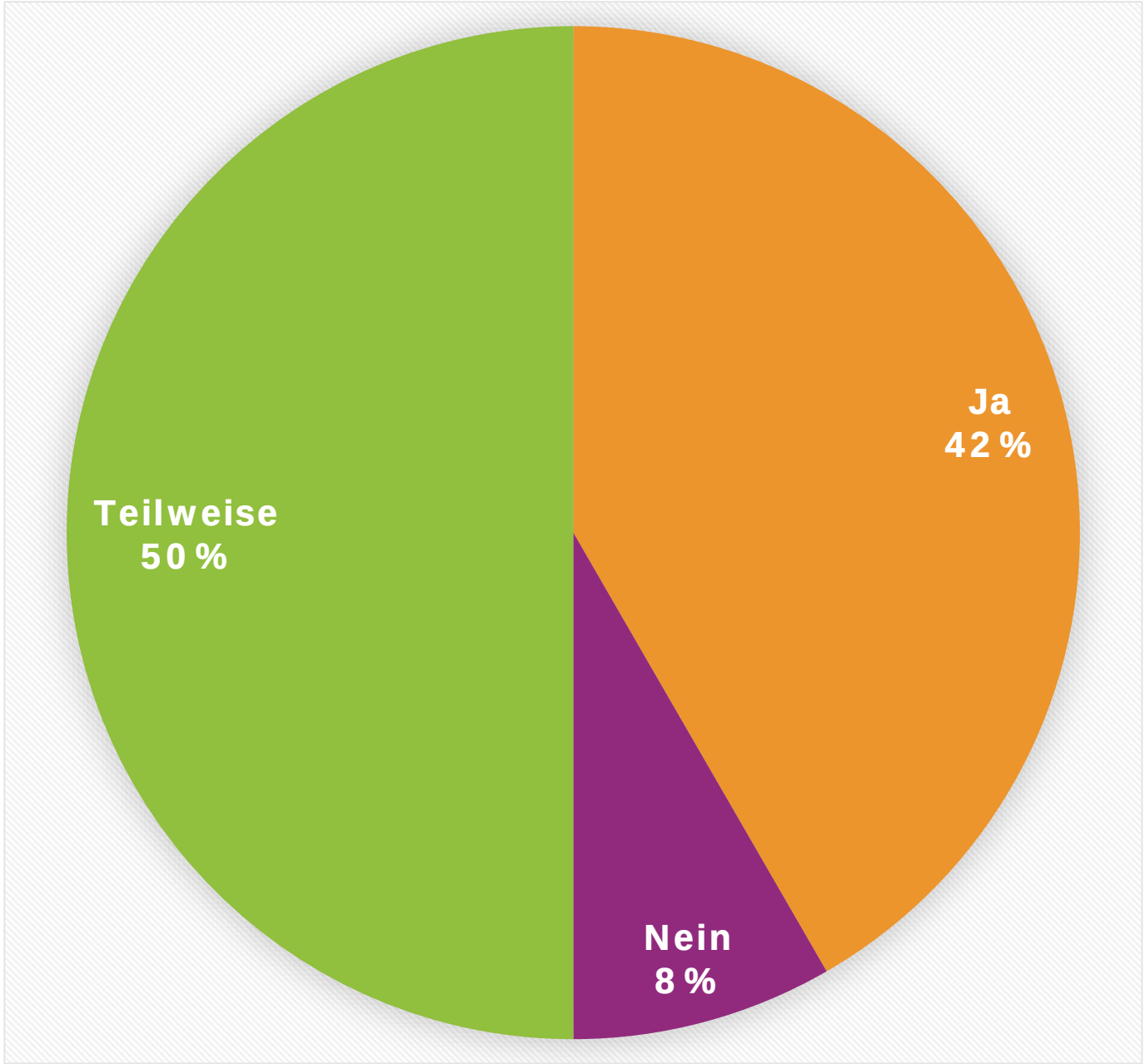
2. Frage

- Können Sie sich grundsätzlich vorstellen, dem DFN-CERT Zugriff zu Log-Daten zur Angriffserkennung und -aufklärung zu gewähren?



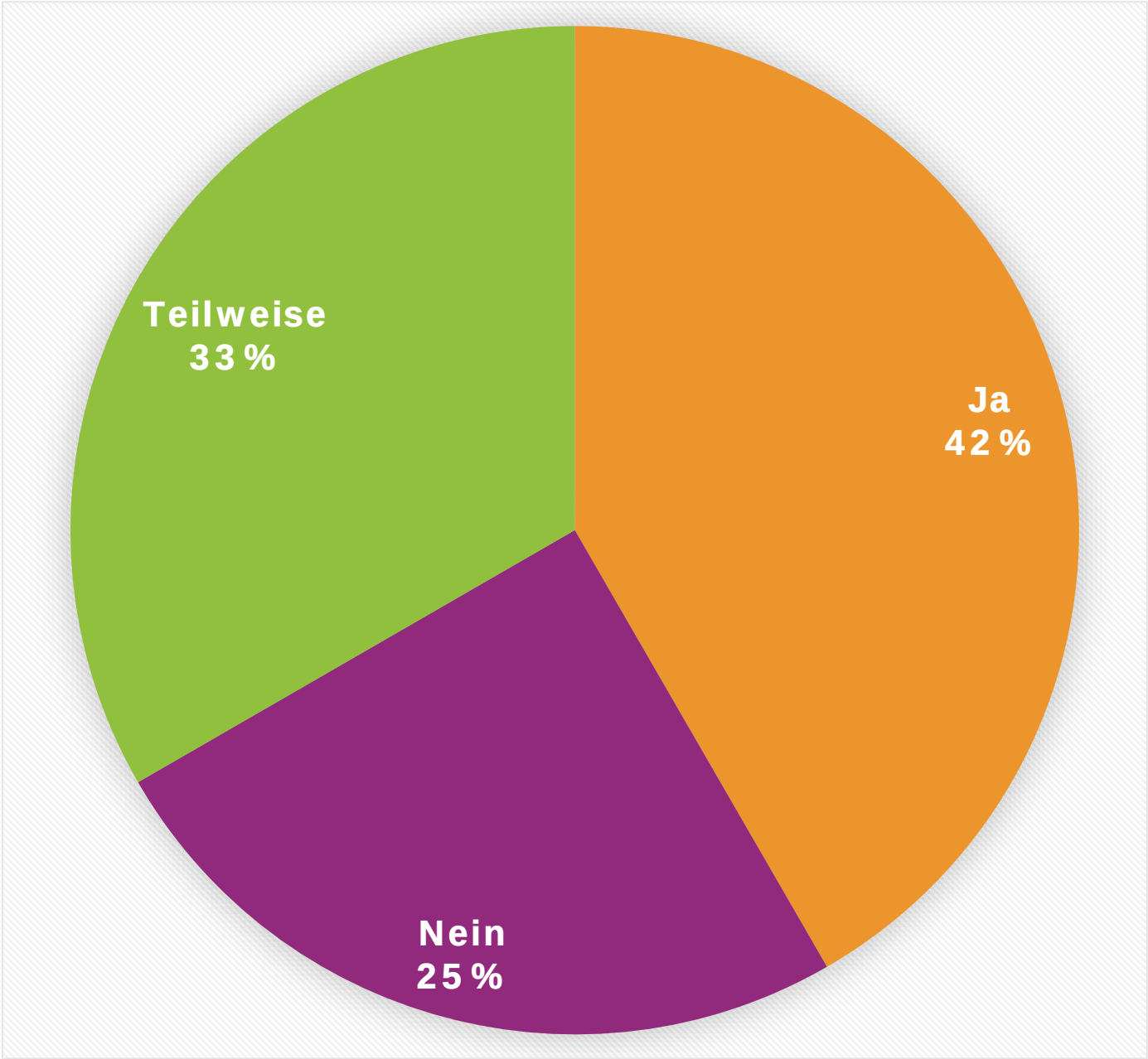
3. Frage

- Dürfte der DFN bzw. das DFN-CERT Dritte (z.B. kommerzielle Anbieter) als Unterauftragnehmer mit einbeziehen? Falls ja: Nur Deutsche/Europäische Anbieter?
- Anbieter aus Drittstaaten? → Ziemlich klares „Nein“



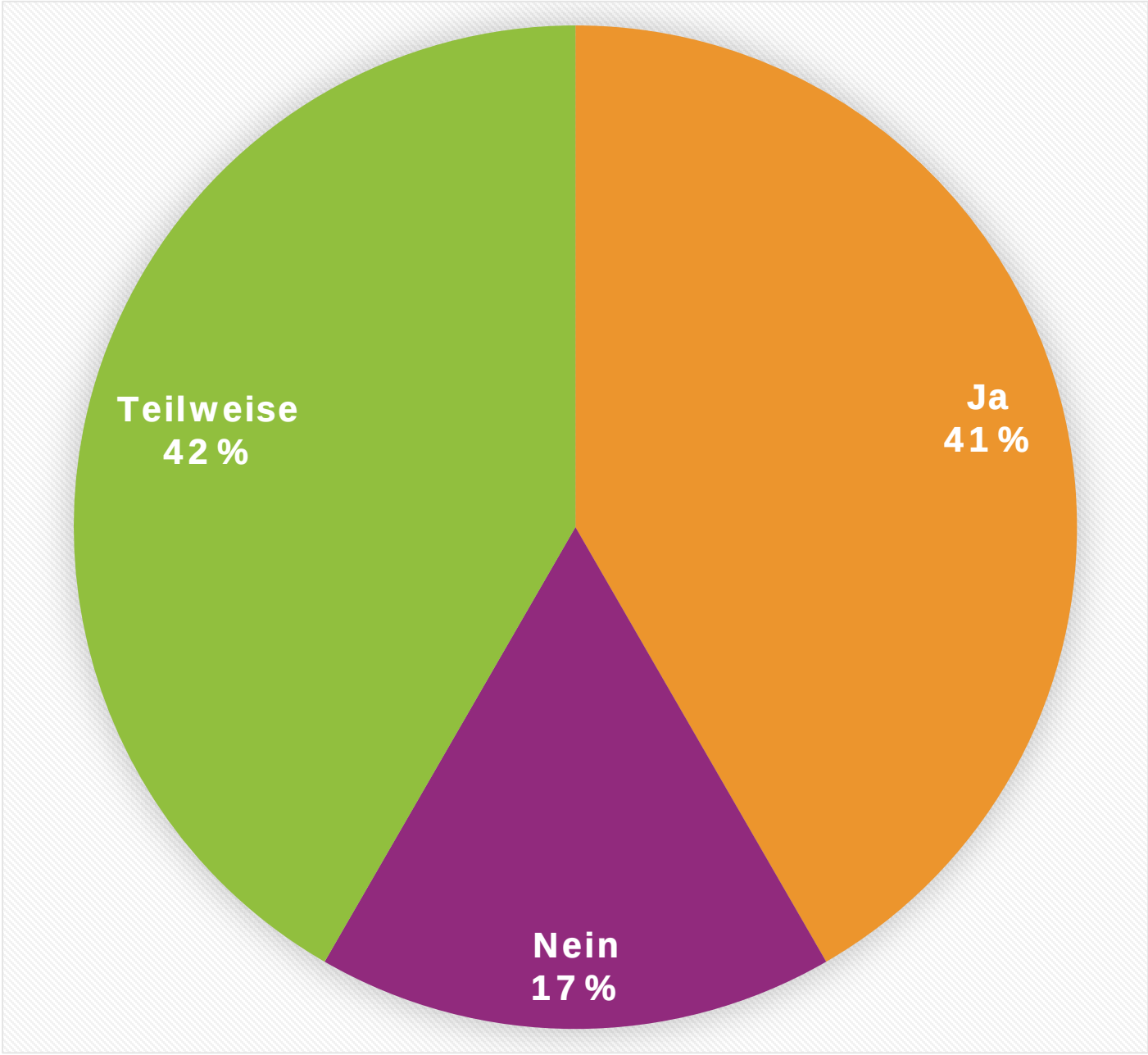
4. Frage

- Wünschen Sie einen erweiterten Dienst (z.B. 24/7 Erreichbarkeit, manuelle Voranalyse der Alarme durch ein gemeinsames DFN-SOC) gegen zusätzliches regelmäßiges Entgelt?



5. Frage

- Wünschen Sie einen Basisdienst, bei dem nur ein kleineres regelmäßiges Entgelt anfällt für die notwendige lokale Sensorik in Ihrem Netz, aber keine manuelle Auswertung/Reaktion erfolgt?



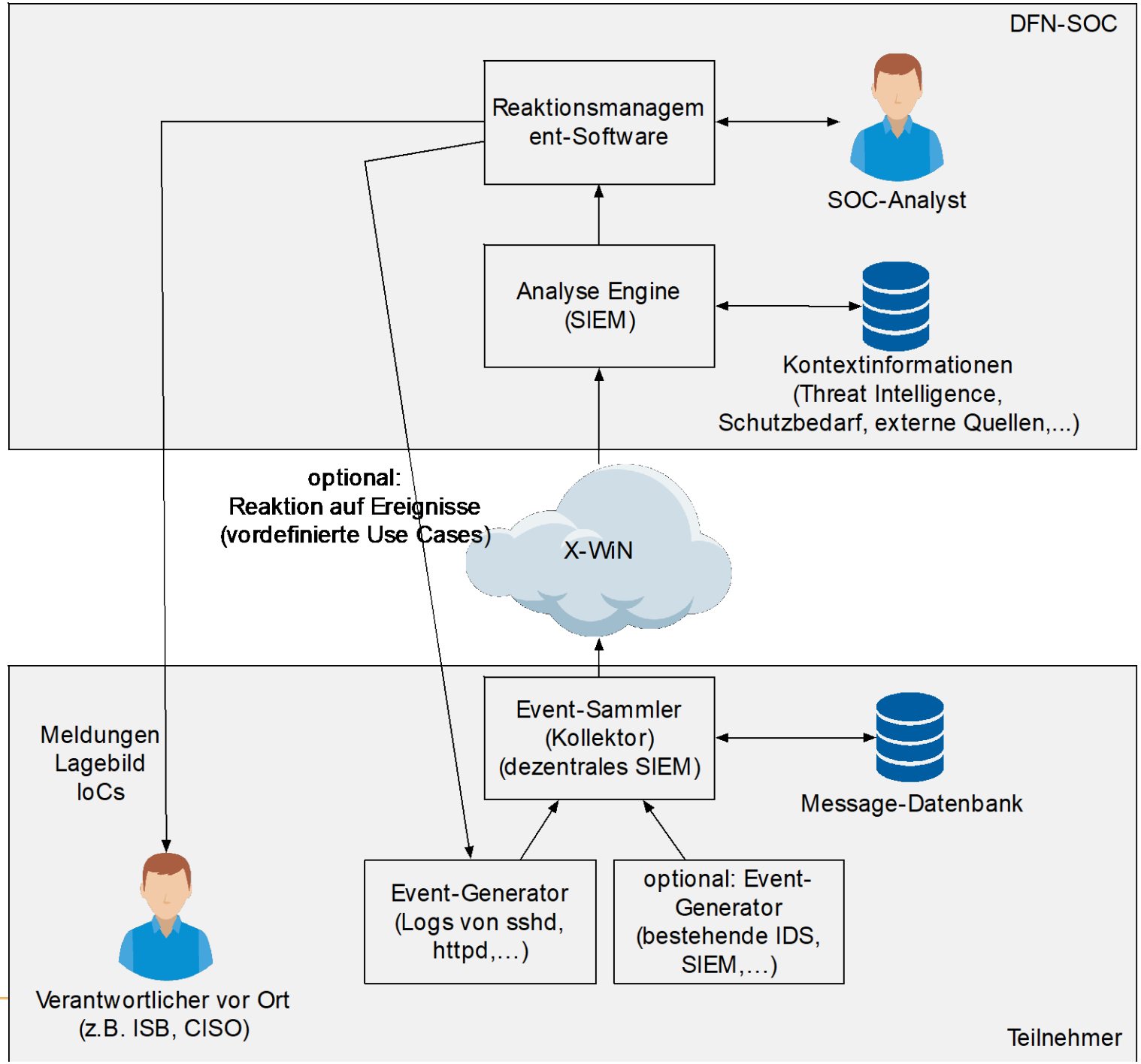
Technische Umsetzung: SecOps-Toolchain

- SecOps-Tools bestehen in der Regel aus fünf verschiedenen Modulen:

1. Event-Generatoren
2. Event-Sammlern
3. Message-Datenbank (Message = aggregierte Events)
4. Analyse-Engines
5. Reaktionsmanagement-Software

Zielarchitektur

- Herausforderungen:
  - Dezentrales SIEM
  - „Rückkanäle“



Ad-Hoc SOC (DFN-Intern)

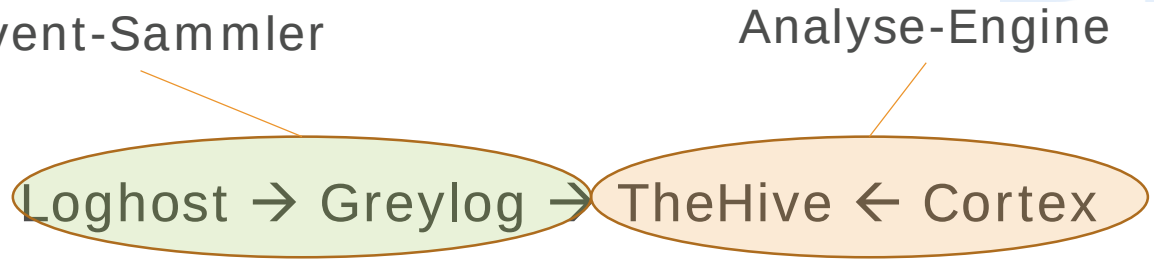
Primäres Ziel:

Erfahrungen sammeln

(noch kein produktives „Mehr an Sicherheit“)

- Das heißt: Validierung von organisatorischen Prozessen und technischen Werkzeugen
- DFN-eigene Serverinfrastruktur wird bereits überwacht…
  - …naja – Teile davon
  - Warum nur Teile? → EU-DSGVO - wir arbeiten dran :o)

Ad-Hoc SOC (DFN-Intern)



- Ad-Hoc-Tool-Chain:
  - Log-Daten der Einzelsysteme → Loghost → Greylog → TheHive ← Cortex
  - Mit Anbindung an viele Analyse-Tools mit Open Source Intelligence
    - Kommerziell, nicht kommerziell, extern, intern,... → Viele Möglichkeiten
    - Virus Total, etc.

- Reaktion bzw. Kommunikation derzeit noch manuell
  - Später: IoC geeignet bereitstellen (Blacklists, Signaturen, Pattern, MISP)
  - Evtl. genau definierte Use Cases mit reaktiven Maßnahmen durch SOC

Überlegungen zum Dienst („SOC“) für Teilnehmer

- Drei abgrenzbare Dienstklassen:
  1. **Basisdienst ohne Sensorik beim Teilnehmer**
  2. **Basisdienst mit Sensorik beim Teilnehmer**
  3. **Erweiterter Dienst**

- Diese Dienstklassen werden derzeit mit der Realität abgeglichen

1. Basisdienst ohne Sensorik beim Teilnehmer

- entspricht bestehendem (fortentwickelten) CERT-Dienst

- Diesen Dienst gibt es bereits und wird es auch weiterhin geben

2. Basisdienst mit Sensorik beim Teilnehmer

- Paradigmen hierfür: Self-Service, 8x5, passive Maßnahmen im Teilnehmernetz (Sensorik), vergleichsweise kleines zusätzliches Entgelt

- Einige „leichtgewichtige“ Use Cases mit automatisierten reaktiven Maßnahmen
  - z.B. über DFN-MailSupport oder per Bereitstellung von IoCs per Blacklist, Pattern etc.

- Zusätzliches Entgelt voraussichtlich notwendig für
  - Support für lokale Sensorik-Appliance
  - SOC-Analysten

- Den Basisdienst mit Sensorik werden wir nach derzeitigem Stand in den kommenden Monaten/Jahren einführen und anbieten

3. Erweiterter Dienst

- Paradigmen: Full Service durch DFN(-CERT), evtl. 24x7 (12x5?)
  - Ebenfalls mit Sensorik beim Teilnehmer
- Erweiterte (ggf. auch reaktive) Maßnahmen im Teilnehmernetz
- Vergleichsweise höheres zusätzliches Entgelt
  - Support für lokale Sensorik-Appliance
  - SOC-Analysten mit erweiterter Verfügbarkeit
  - Support für manuelle reaktive Maßnahmen
- Den erweiterten Dienst werden wir perspektivisch bei Vorliegen entsprechender Anforderungen der Teilnehmer umsetzen

Der (erste) geplante „High-Level Use-Case“

- Mail bzw. Anti Phishing
  - Wir wollen Phishing- und Malware-Kampagnen gegen DFN-Teilnehmer zuverlässiger und schneller erkennen als generische Black-List-Anbieter
  - Threat-Intelligence kann sehr schnell über die RZ gesammelt werden
    - Teilnehmer A ist zuerst betroffen und gibt die Info sofort an das DFN-SOC
    - Teilnehmer B-Z sind schnellstmöglich geschützt (z.B. durch SpamAssassin-Regeln mit konkreten IoC dieses Angriffs
  - Auswertung durch geeignete Tools (z.B. Sandbox)

- Dieser Use Case eignet sich auch hervorragend für‘s Marketing in Richtung nicht technikaffiner Entscheidungsträger ;-)

Fazit

- Thema Security Operations / SOC wird vom DFN mit dem DFN-CERT aktiv vorangetrieben
- Interesse und Bedarf in vielen Einrichtungen ist vorhanden bzw. wächst
  - Diverse Aktivitäten im nationalen und internationalen Umfeld
- Falls Ihre Einrichtung auch an entsprechenden Themen alleine oder im Verbund mit anderen arbeitet, sind wir sehr an einer Zusammenarbeit bzw. Abstimmung interessiert
- Weiterhin alle Arten von Feedback willkommen

Kontakt & Fragen

Dr. Ralf Gröper

DFN-Verein
Alexanderplatz 1
10178 Berlin

E-Mail: groeper@dfn.de
Telefon: +49 30 884299-337