DFN CERT

deutsches forschungsnetz

Neues aus dem DFN-CERT

77. Betriebstagung | 18.10.2022

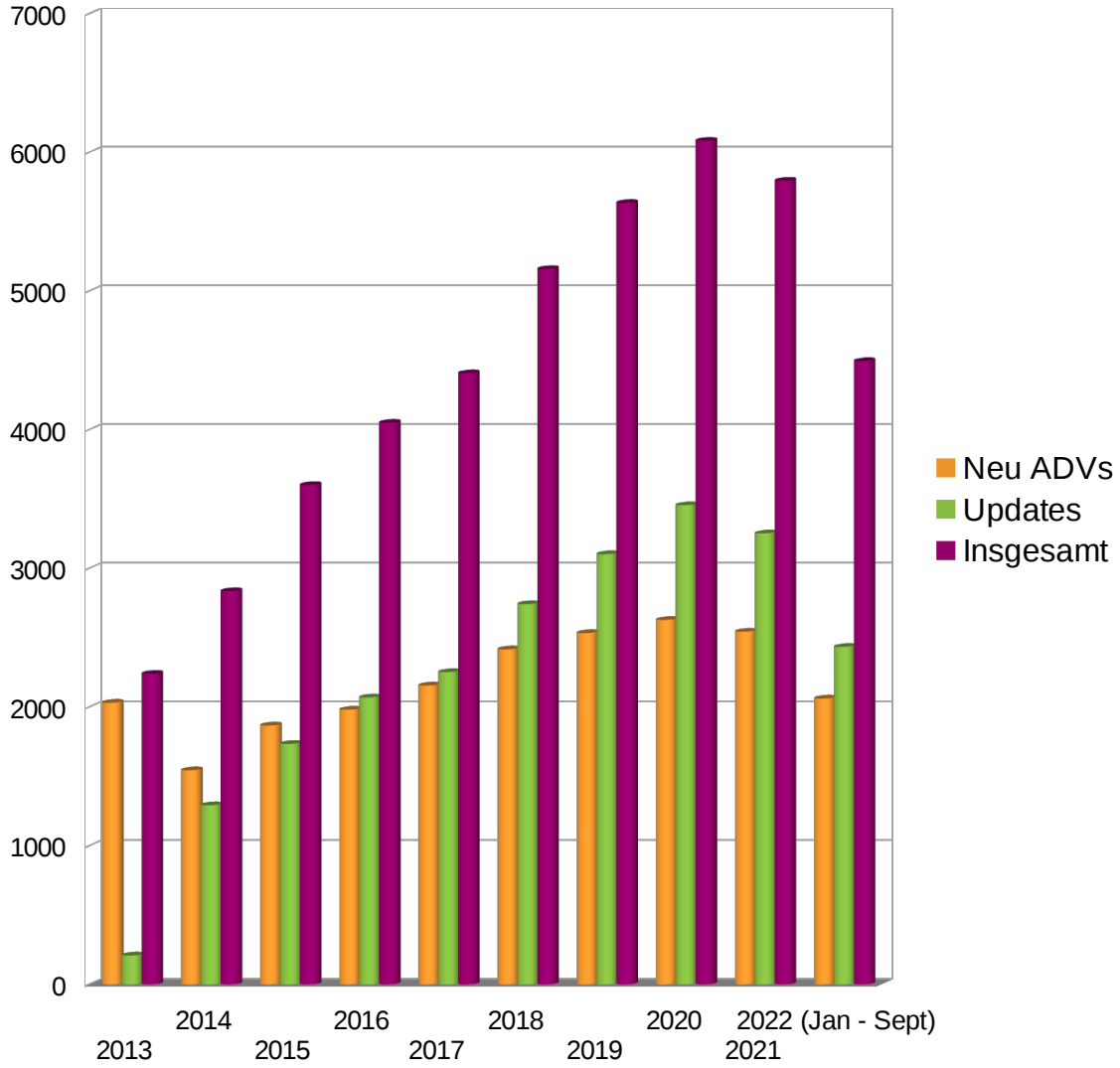
Christine Kahl

Agenda

1. Advisory Statistik und Spring4Shell
2. Automatische Warnmeldungen
3. GÉANT Trainings
4. Erweiterungen für Security Operations

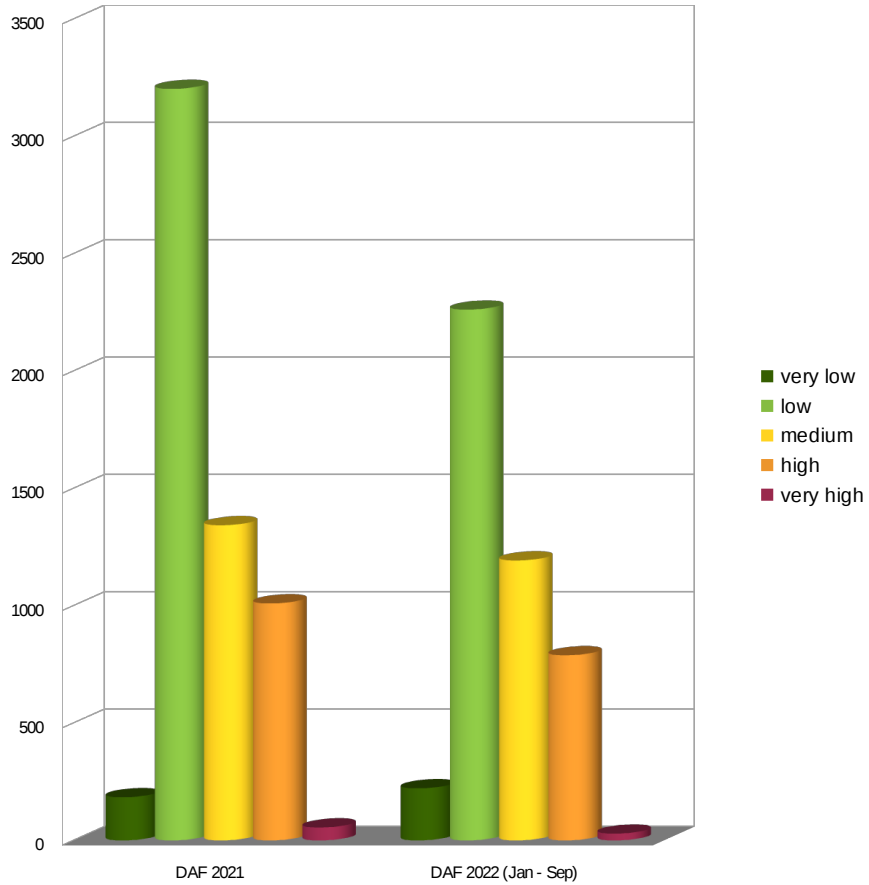
Advisory Statistik und Spring4Shell

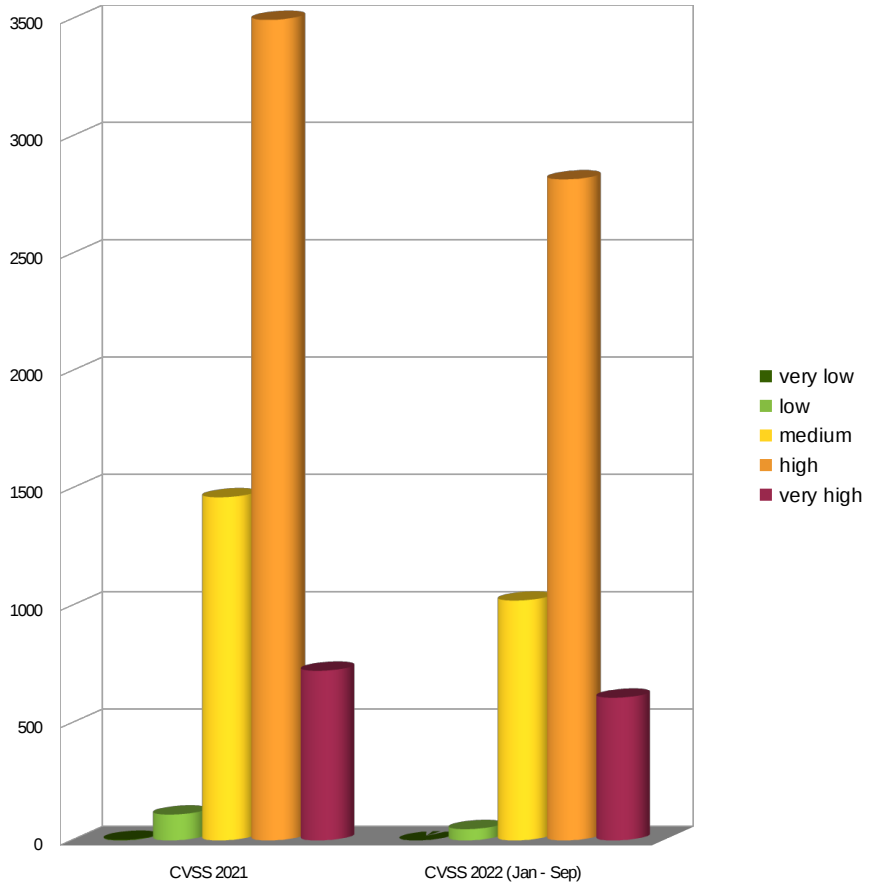
Aktuelle Advisory Zahlen



- Gesamtzahlen
  - 2013: 2240
  - 2020: 6083 (Anstieg um ~8%)
  - 2021: 5795 (Rückgang um ~5%)
- Prognose 2022
  - Zahlen bewegen sich auf die Werte von 2020 zu
  - Also doch wieder ein leichter Anstieg im Vergleich zum Vorjahr
  - Ob erneut die 6000er Marke geknackt wird, bleibt spannend

ADVs nach Schweregrad – DAF – CVSS





DAF und CVSS in 2021 und 2022

- Jeweils keine nennenswerten Änderungen zum Vorjahr, auch keine Änderung bzgl. der Unterschiede

Spring4Shell – CVE-2022-22965

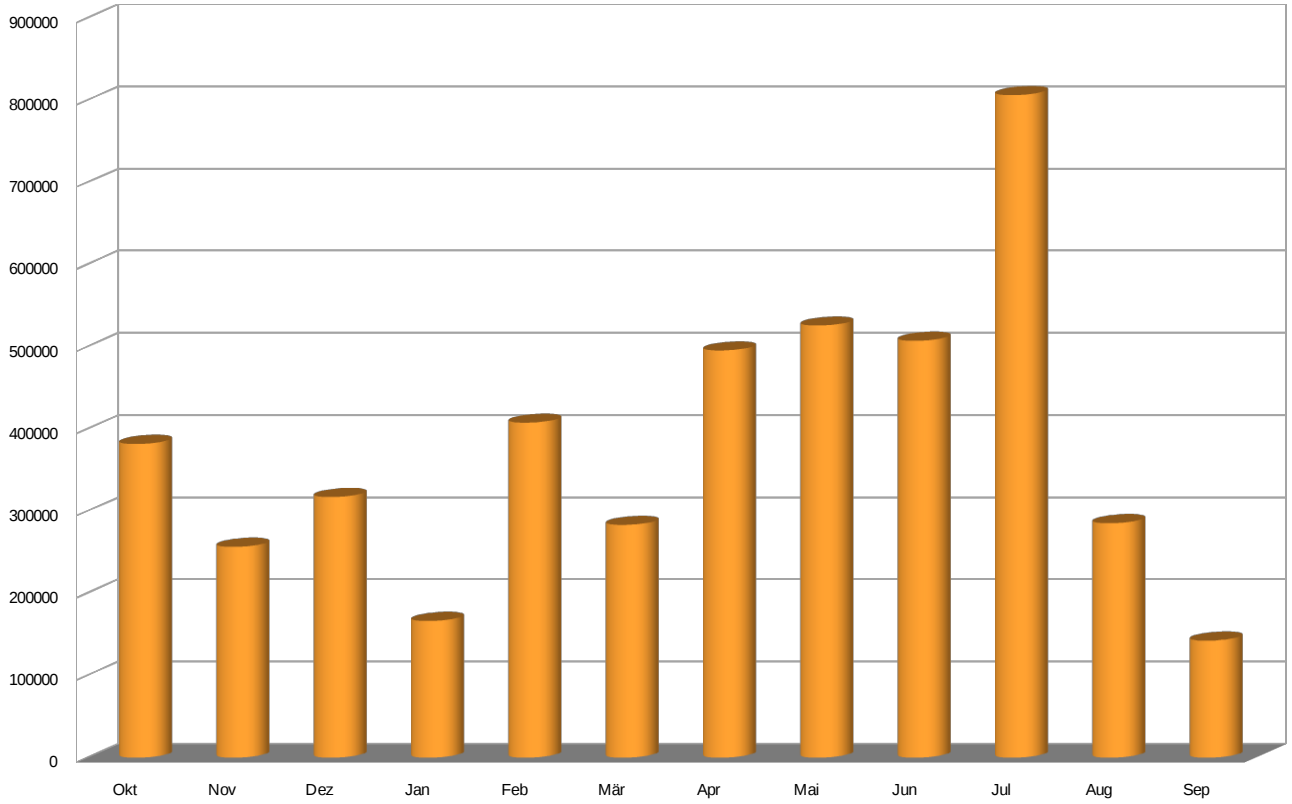
- Ende März tauchten Informationen zu einer 0Day-Schwachstelle im Spring Framework auf
  - Spring ist ein weit verbreitetes Framework zur Entwicklung von Java-Anwendungen
  - Aufgrund der verbreiteten Nutzung des Frameworks, den ersten Informationen zur Auswirkung der Schwachstelle und den sehr präsenten Nachwirkungen der Log4Shell-Schwachstelle wurde die Schwachstelle Spring4Shell getauft
  - Zum Zeitpunkt der ersten Warnungen standen jedoch keine detaillierten Analysen bereit
- Mit der Veröffentlichung von VMware, die Spring seit 2009 entwickeln, legte sich die erste Aufregung
  - Die Ausnutzung der Schwachstelle ist „nur" unter bestimmten Bedingungen möglich
  - Scans und Exploitversuche starteten aber kurz nach Bekanntwerden der Schwachstelle
  - Hersteller patchten proaktiv auch ohne Belege für die Ausnutzbarkeit im eigenen Produkt

Spring4Shell – Sturm im Wasserglas?

- Klare Antwort: Jaein
  - Bei derart verbreiteten Komponenten ist bei Bekanntwerden einer Verwundbarkeit die Zeit innerhalb derer gehandelt wird ein extrem wichtiger Faktor
  - Bevor der Hersteller offizielle Informationen bereitstellte, wurden bereits Scans und Exploitversuche beobachtet
  - Zumeist sind die ersten Informationen unvollständig
- In Fällen wie diesen empfiehlt sich ein aktives Monitoring der Situation
  - Wo eine Schwachstelle ist, fördern detaillierte Analysen meist auch noch weitere Sicherheitslücken zu Tage
  - Bei neuen Erkenntnissen, Ausnutzungsmöglichkeiten und Patches ist eine Reaktion in der Regel nicht innerhalb von Tagen, sondern von Stunden notwendig

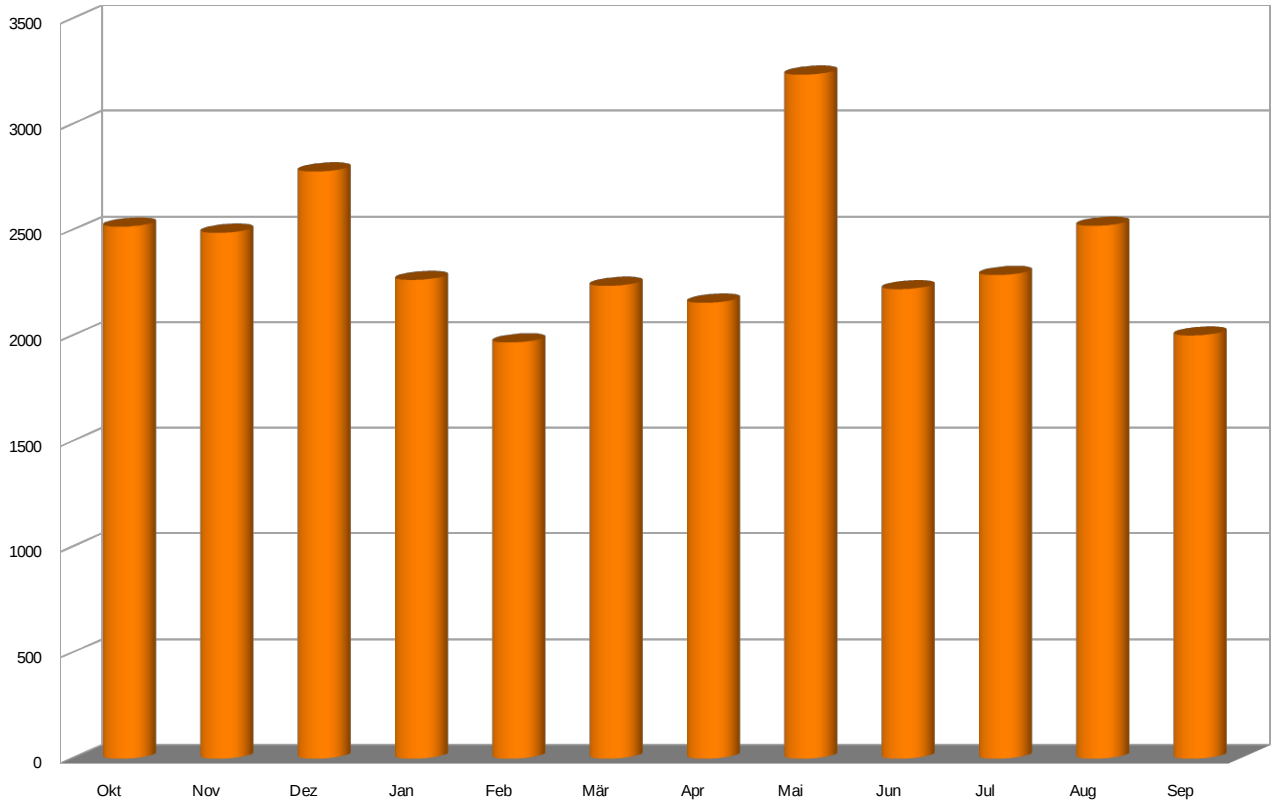
AW-Meldungen

Automatische Warnmeldungen - Events



- Im März Rückgang der Scans (Auswirkung der Semesterferien?) und starker Anstieg der ‚Unrestricted Access'-Fälle bei insgesamt niedrigen Fallzahlen
  - Offene ‚Intelligent Plattform Management Interface' (IPMI) Ports (dienen meist der Systemsteuerung auf HW-Ebene)
  - Insgesamt von 310 (Feb) auf 3700 (Mär) Fälle angestiegen
- Neuer Meldungstyp ‚Vulnerable DDoS Middlebox'
  - Für Anstieg der Fallzahlen im April mit verantwortlich
  - Systeme, die für TCP basierte DDoS-Reflection-Angriffe genutzt werden können
  - Netzwerkkomponenten, die nicht konform zum TCP-Standard arbeiten und auf ‚TCP Packet out of state'-Pakete antworten

Automatische Warnmeldungen - E-Mails



- Anstieg der versendet E-Mails im Mai bedingt durch die erneute kurzzeitige Aktivierung von Warnmeldungen mit hohem ‚false positive'-Anteil aufgrund gewünscht offen erreichbarer Dienste, die aber potentiell problematisch sind
- Seit Juni Zunahme im Bereich von Meldungen durch SecOps, die sich in den absoluten Zahlen aber nicht zeigen
- Juli
  - Deutlicher Anstieg der Events, aufgrund der Aggregierung aber nicht in den E-Mails sichtbar
  - 96% der Vorfälle sind Scans (ca. 300.000 Events mehr als in anderen Spitzenzeiten)
- September
  - Deutlicher Rückgang von Events, der sich nur geringfügig in der Anzahl der E-Mails zeigt
  - Auch hier primär verantwortlich, die Scans (Allzeittief seit kontinuierlicher Erfassung)

DFN

GÉANT Trainings

GÉANT Trainings – Kursmaterial verfügbar

- Im Rahmen des European Union's Horizon 2020 research and innovation Programms wurden insgesamt vier neue Trainingskurse entwickelt
  - Operational Network Security
  - Vulnerability Management
  - IT Forensics for System Administrators I und II
- Aufzeichnungen der Webinare und Schulungsunterlagen mit weiterführenden Informationen verfügbar über https://www.dfn-cert.de/en/Trainings.html
- Aktuell läuft die Detailplanung für das Nachfolgeprojekt GÉANT GN5-1
  - Laufzeit 2 Jahre: 2023 + 2024
  - Auf Basis der erstellten Unterlagen können nach Aktualisierung weitere Kurse – in Person – im Block – ggf. auf Deutsch angeboten werden → Sagen Sie uns, wenn Sie daran Interesse haben!

GÉANT Trainings – Warum?

- Prävention
  - Auf jeden Fall, ohne Frage, klar!

ABER TROTZDEM

- Vorbereitung auf den Ernstfall
  - Theoretische Basis mit IT Forensics for System Administrators I und II gelegt
  - Und nun?

GÉANT Trainingskurs – Ankündigung

- Blue Team Training
  - Was?: Erkennung und Bekämpfung eines Angriffs in einem Team
  - Wann?: Dienstag, 22. November 9:00 – 13:00
  - Wie?: Online Training über Zoom
  - Und sonst so?:
    - Basis Administrationswissen erforderlich
    - Analyse von Logdaten, hier speziell mittels Elasticsearch
    - Erstes Training als erweiterter Test → anschließend brauchen wir Ihr Feedback
    - Sprache im Training und in den Gruppen: Englisch
- Bitte melden Sie sich an über: https://events.geant.org/event/1320/
  - Für die Gruppeneinteilung brauchen wir ein paar Informationen zu den vorhandenen Erfahrungen
  - Außerdem wird die Registrierung bereits am 11. November geschlossen

Erweiterungen für Security Operations

Basisleistungen: 1. Meilenstein erreicht

- Domains im DFN-CERT Portal:
  - Entsprechend der Planung können seit Anfang Juli beliebige einer Einrichtung zugeordnete Domains im DFN-CERT Portal angelegt und validiert werden
  - Stand 13.10.22:
    - 1320 Domains eingetragen
    - 720 verifiziert
  - Es gibt keine einer Einrichtung automatisch zugeordneten Domains, nur eine erleichterte Übernahme von über den DFN-Verein registrierten Domains
  - Das Eintragen von Domains obliegt Handlungsberechtigten Personen und Einrichtungsadministrierenden
    - Sie müssen dafür als berechtigter Benutzer im Portal angelegt sein, ein Zertifikat allein ist für den Zugang nicht ausreichend
  - Validierte Domains werden in den Security Operations für die Weitergabe von Daten berücksichtigt

Basisleistungen: 2 Meilensteine geplant

- Meilenstein 2 – Anfang 2023 – Annahme von Logdaten:
  - Massiver Aufbau von Hardware, um jedem Teilnehmer die Möglichkeit zu geben, Logdaten seiner wichtigsten Systeme einzuliefern
  - Verschiedene Stufen der Aggregation
    - Beginnend mit Kollektoren an Kernnetzknoten
    - Weiter in verschiedenen Stufen am CERT
    - Quasi keine Speicherung der Daten → Fire and Forget
  - Auch wenn wir uns um einen schlanken Prozess bemüht und Automatisierungen angestrebt haben, so gibt es manuelle Aktionen für die Anbindung auch im Basisdienst
- Änderung aufgrund der Erkenntnisse aus dem Pilotbetrieb - SOC-Connector:
  - Anbindung zur Einlieferung der Logdaten eine Hürde
  - Im Netz des Teilnehmers zu installierende Komponente: SOC-Connector
  - Über diesen erfolgt die weitere Übertragung der Daten an die Kollektoren des zuständigen Kernnetzknotens und dann in die internen CERT-Systeme

Basisleistungen: 2 Meilensteine geplant

- Meilenstein 3 – Mitte 2023 – Security-Monitoring:
  - Information über abgelaufene Zertifikate, unbeabsichtigt öffentlich verfügbare Ressourcen und andere, ähnlich gelagerte Sicherheitsmängel
  - Dafür wird die bereits in erster Version existierende Komponente SOC-Probe eingesetzt
  - Nur Prüfung von Systemen, auf die von außerhalb des Teilnehmernetzes zugegriffen werden kann
  - Aktuell aufwändig in der Konfiguration → skaliert nicht für viele Teilnehmer
  - Zeitkritische Events werden direkt (außerhalb der AW-Meldezeitpunkte) weitergegeben
  - Erweiterung des DFN-CERT Portals hinsichtlich der Netzmodellierung und Verwaltung von Hostnamen

Erweiterte Leistungen

- Kurz vor Start des Regelbetriebs
- Bisher gibt es für die Security Operations eine handvoll implementierter Use-Cases
  - Die umgesetzten Use-Cases definieren den Wert des Dienstes
  - Auch im Regelbetrieb muss an den Use-Cases kontinuierlich gearbeitet werden
  - Das können wir nicht alleine, da wir wissen müssen
    - Welches die für den Teilnehmer relevanten Szenarien sind
    - Welche Daten wirklich geliefert werden können
  - Über Workshops werden neue/zusätzliche Use-Cases ermittelt und analysiert
  - Dies erfordert nicht nur bei uns, sondern auch beim Teilnehmer personelle Ressourcen und Know How
- Schutzgegenstände müssen modelliert werden und diese Modellierung muss regelmäßig überprüft und aktualisiert werden
  - Eskalationswege - Kontaktinformationen
  - Schutzgegenstände
- Der erweiterte Dienst kann viel, bedeutet aber eben auch eine Investition über Geldmittel hinaus

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?

- DFN-CERT Hotline
  - cert@dfn-cert.de
  - 040 / 808 077-590
- Weitere Informationen: https://www.cert.dfn.de/