NTS

RELAX,
WE CARE

SECURITY IM FOCUS

NAVIGIEREN DURCH REGULATORISCHE ANFORDERUNGEN MIT NTS-LÖSUNGEN

VORSTELLUNG

NTS

```
FROM FH JOANNEUM
  AS RESEARCHER & COOPERATIONPARTNER NTS

ENV NAME ‚CHRISTOPH PILS‘

ADD BSC.
RESEARCH FIELD EU-ACTS,
               OT DIGITALISATION

EXPOSE CHRISTOPH.PILS@FH-JOANNEUM.AT
```

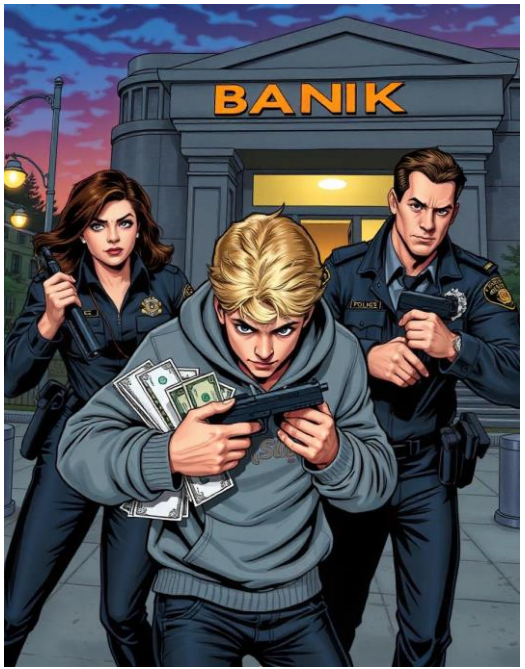
VORSTELLUNG

```
FROM NTS_GRAZ
  AS SALES EXPERT SECURITY

ENV NAME ,KLAUS MITSCHE‘
ENV NTS_SINCE ,2024-06‘
.

EXPOSE KLAUS.MITSCHE@NTS.EU
```

BANKÜBERFALL VS RANSOMWARE



62%

30%(?)

SECURITY CHALLENGES

Generative AI

Ein Mangel an Führungskräften mit ausgeprägten Kenntnissen und Fähigkeiten im Bereich der Cybersicherheit

Lieferketten sind miteinander verknüpft

Ransomware-Angriffe und andere Cyberbedrohungen nehmen zu

Gesetzliche und regulatorische Anforderungen ändern schnell

IT-Betriebsmodelle entwickeln sich weiter

Übernommen von Gartner.

CISCO TALOS IR DATEN

NTS

INCIDENT RESPONSE-DATEN VON 2023

Die Hälfte der Angriffe nutzten als „Initial Access Vector„
- **Exploits in öffentlich zugänglichen Anwendungen** und
- **kompromittierte Anmeldedaten**/gültige Konten

Phishing rundet die Top 3 ab.

Aus verschiedenen Gründen schwer zu bestimmen – zB **fehlenden Loginformationen oder mangelnder Sichtbarkeit in die betroffene Umgebung**

2024 - ZIEL: USER

Im **Q1 2024** zeigen die Zahlen von **Cisco Talos** IR-Einsätzen einen **enormen Anstieg** bei **BEC**-Angriffen (Business Email Compromise).

#1 (29%)

Das häufigste Mittel des initialen Zugriffs betreffen **gestohlene Anmeldedaten.**

46%

der **Einsätze betrafen BEC.**

25%

Benutzer akzeptieren **unautorisierte Push-Benachrichtigungen.**

MFA ist trotz Schwächen immer noch eine der **effektivsten Methoden, um die Identität** eines Benutzers zu überprüfen.

https://blog.talosintelligence.com/talos-ir-quarterly-trends-q1-2024/

THREAT-ACTORS

Cyber-Bedrohungen **sind real und allgegenwärtig.**

Sie werden von unterschiedlichen „Threat-Actors“ durchgeführt

CYBERKRIMINELLE
Finanzielle Motivation

Zugang zu wertvollen Daten

Lösegeld -> Erpressung

NATIONALSTAAT
Gewinnung von Informationen

Nuklear, Finanzen oder Technologie

Strategische Sabotage

Störung der kritischen Infrastruktur

IDEOLOGEN
Verbreitung von Botschaften

Hacker, Terroristen

Antikapitalismus, Antikonzern

Inspiriert von politischen und/oder sozialen Themen

ABENTEURER
Ruhm und Ehre

Experimente, Lernen (nicht darauf aus, Schaden zu verursachen)

Einige werden Trolle – Fehlinformationen

INSIDER
Absichtlich

Verärgerter Mitarbeiter

Unfaire Behandlung

Unterschiedliche "Ziele"

Unabsichtlich

„HOFFNUNG IST KEINE MANAGEMENT METHODE.“

Cyber-Bedrohungen **sind real und allgegenwärtig**

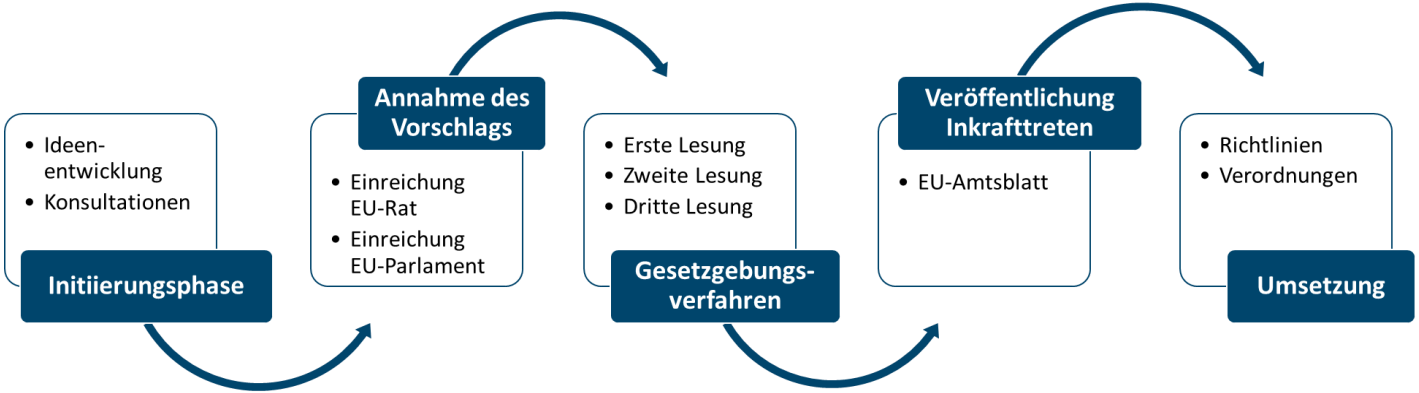
Unzureichende Sicherheitsmaßnahmen
können gravierende Auswirkungen haben.

EU-ACTS

REGULATORIEN

NTS

ENTSTEHUNG EINES EU-ACTS



EU ACTS

NTS

SÄULEN DER EU-CYBERSICHERHEITSPOLITIK

- Verpflichtende Sicherheitsstandards
- Risikomanagement etablieren
- Verbesserung der Reaktionsfähigkeit
- Förderung von Innovation und Technologieentwicklung
- Schutz kritischer Infrastrukturen
- Internationale Zusammenarbeit
- Stärkung der Widerstandsfähigkeit der Lieferkette
- Etablierung klarer Verantwortlichkeiten

ÜBERSICHT EU-ACTS

EU Acts				2022				2023				2024				2025				2026				2027				2028			
Nr.	Bezeichnung	Beschluss	Frist	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	DSA- Digital Service Act	27.10.2022	17.02.2024																												
2	eIDAS- Electronic Identification, Authentication & Trust Service	31.03.2023	30.06.2024																												
3	CSRD- Corporate Sustainability Reporting Directive	28.11.2022	06.07.2024																												
4	RED- Radio Equipment Directive	09.10.2023	31.07.2024																												
5	NIS2- Network and Information Security 2	17.01.2023	17.10.2024																												
6	STEP- Strategic Technologies for Europe Platform	29.02.2024	31.12.2024																												
7	TEN-E- Trans European Networks for Energy	03.06.2022	31.12.2024																												
8	DORA- Digital operational resillience for the financial sector	14.12.2022	17.01.2025																												
9	DATA Act	27.11.2023	12.09.2025																												
10	EED- Richtlinie- Energy Efficiency Directive	10.10.2023	20.10.2025																												
11	Revision of EU electricity market design	31.12.2023	31.12.2025																												
12	AMLA- EU Anti-Money Laundering Authority	01.01.2024	31.12.2025																												
13	CBAM- EU Carbon Border Adjustment Mechanism	13.12.2022	01.01.2026																												
14	AI Act	21.05.2024	31.05.2026																												
15	EBR- EU Battery Regulation	17.08.2023	31.12.2027																												
16	ETS- EU Emission Trading System	01.05.2024	01.06.2029																												
17	Net-zero Industry Act	18.12.2022	31.12.1930																												
18	CRA- Cyber Resillience Act	2024/2025	31.12.2026																												
19	CS3D- Corporate Sustainability Due Diligence Directive	05.24/06.24	05.29/06.29																												
20	PLD- Product Liability Directive	NV																													
21	CRM- European Critical Raw Materials Act	NV																													

Zeitraum für die Umsetzung der Richtlinien in nationales Recht

Abstufungen und Übergangsphasen

NTS

GESETZTE UND REGULATORIEN

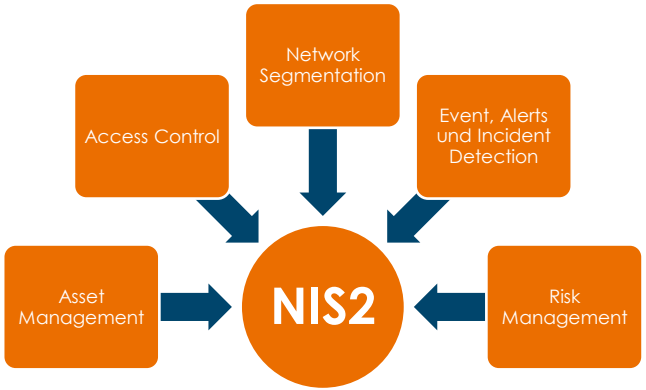
NTS

NIS2 UND DORA

Die **NIS2-Richtlinie** harmonisiert das globale Niveau der Cybersicherheit in der gesamten EU.

Die **DORA-Verordnung** zielt darauf ab, die digitale Betriebsstabilität des Finanzsektors zu stärken.

Ihr **Ziel** ist es ein hohes Maß an digitaler Sicherheit zu erreichen.



NIS2 Main Security Pillars.

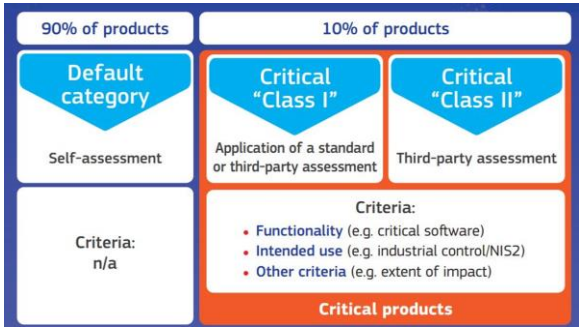
DORA ist „lex specialis“ von NIS2 für den Finanzsektor

GESETZTE UND REGULATORIEN

NTS

CYBER RESILIENCE ACT (CRA)

- CRA legt Cybersicherheitsanforderungen für Hardware & Software in der EU fest **(produziert, vertrieben, eingeführt)**
- **Ziel** Harmonisierung der EU-Cybersicherheitsgesetze zur Reduzierung rechtlicher Unsicherheiten & des Compliance-Aufwands
- Unterscheidung je nach Kategorie, **Risikopotential, Funktionalität & Anwendungsbereich**
- 12. März 2024 durch EU-Parlament genehmigt (wartet auf Zustimmung des Rates) → Inklusive **Übergangsfristen** (21/36 Monate)
- Strafen bis zu 15 Millionen, oder **2,5%** des weltweiten Umsatzes



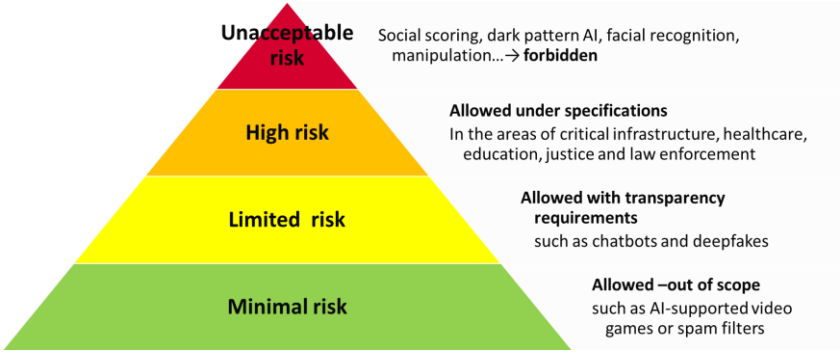
GESETZTE UND REGULATORIEN

NTS

AI-ACT

- **Rechtsrahmen** für KI im europäischen Raum (Ethik & Regulierung)
- → Erwartetes Inkrafttreten zwischen 2027 & 2028
- Rahmen für **Entwicklung, Einführung & Nutzung** von KI
- Bezogen auf maschinelles Lernen, logik- & wissensgestützten Systeme nicht auf klassische Softwaresystem

  → **Überregulierung soll verhindert werden**
- Bewertungssystem „**risk-based approach**“
- **AI Liability Directive**



MEHRWERT

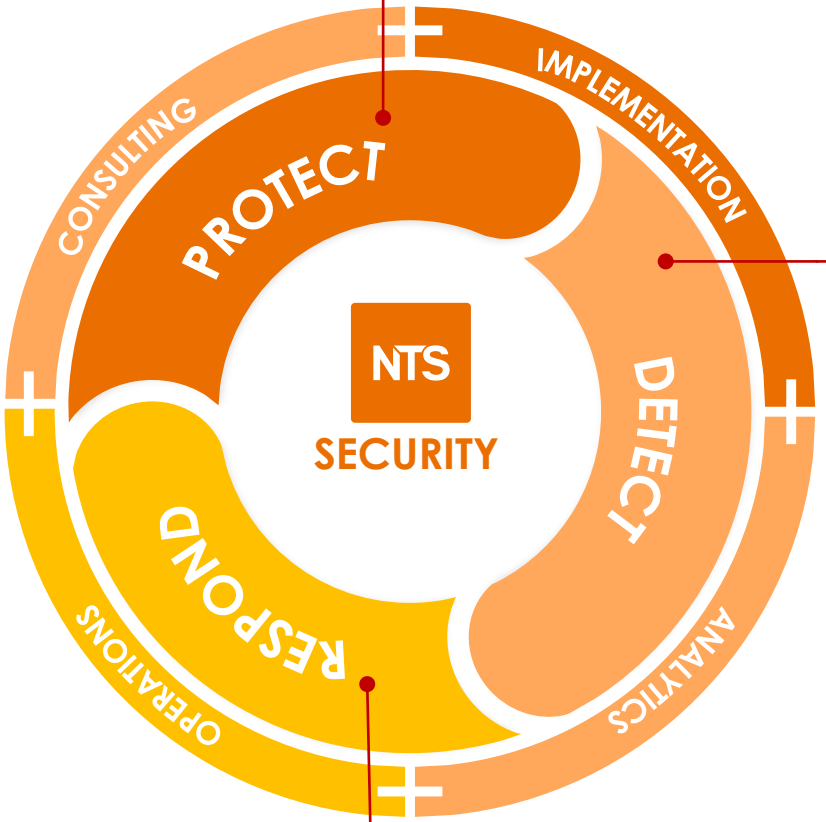
- **Erhöhte Sicherheitsstandards**: Sicherheitsmaßnahmen müssen kontinuierlich überprüfen und verbessert werden, was zu höheren Sicherheitsstandards führt.

- **Struktur**: Die Regulierungen bieten Struktur und Anforderungen, die Unternehmen dabei helfen, ihre Sicherheitsstrategien zu entwickeln und umzusetzen.

- **Wettbewerbsvorteil**: Kunden und Partnern können sicher sein, dass Unternehmen hohe Sicherheitsstandards einhalten.

SECURITY SOLUTION

NTS



Network
Cloud
Application
User & Endpoint
Vulnerability Mgmt.

Thread Detection
SIEM

Network DR
Endpoint DR
eXtendet DR
Managed DR

Incident Response
SOCaaS

NTS

RELAX,
WE CARE

SERVICE TEAMS

DESIGN & IMPLEMENTATION

201
ENGINEERS

24/7
ON SITE | REMOTE

Design
Professional Services
Consulting

OPERATIONS CENTER

213
ENGINEERS

24/7
REMOTE

Break & Fix Support
Managed Service
High Volume Delivery

DEFENSE

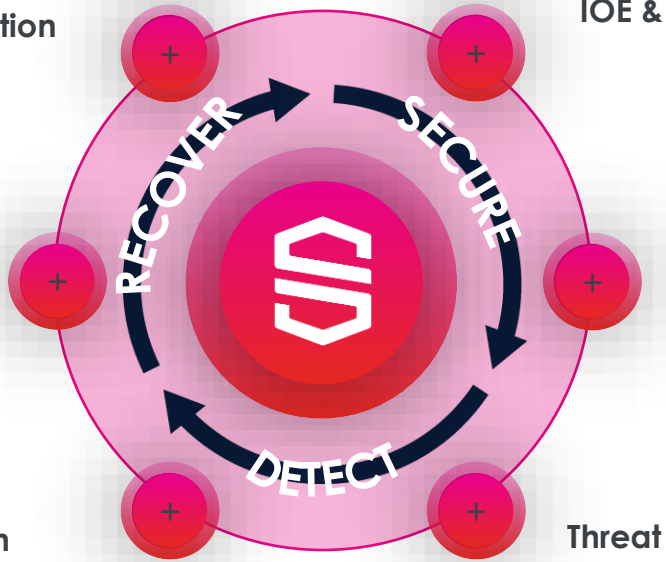
33
ANALYSTS | ENGINEERS

24/7
REMOTE | ON SITE

Vulnerability MGMT
SOCaaS
Incident Response
MDR

IDENTITY SECURITY

POWERED BY SEMPERIS

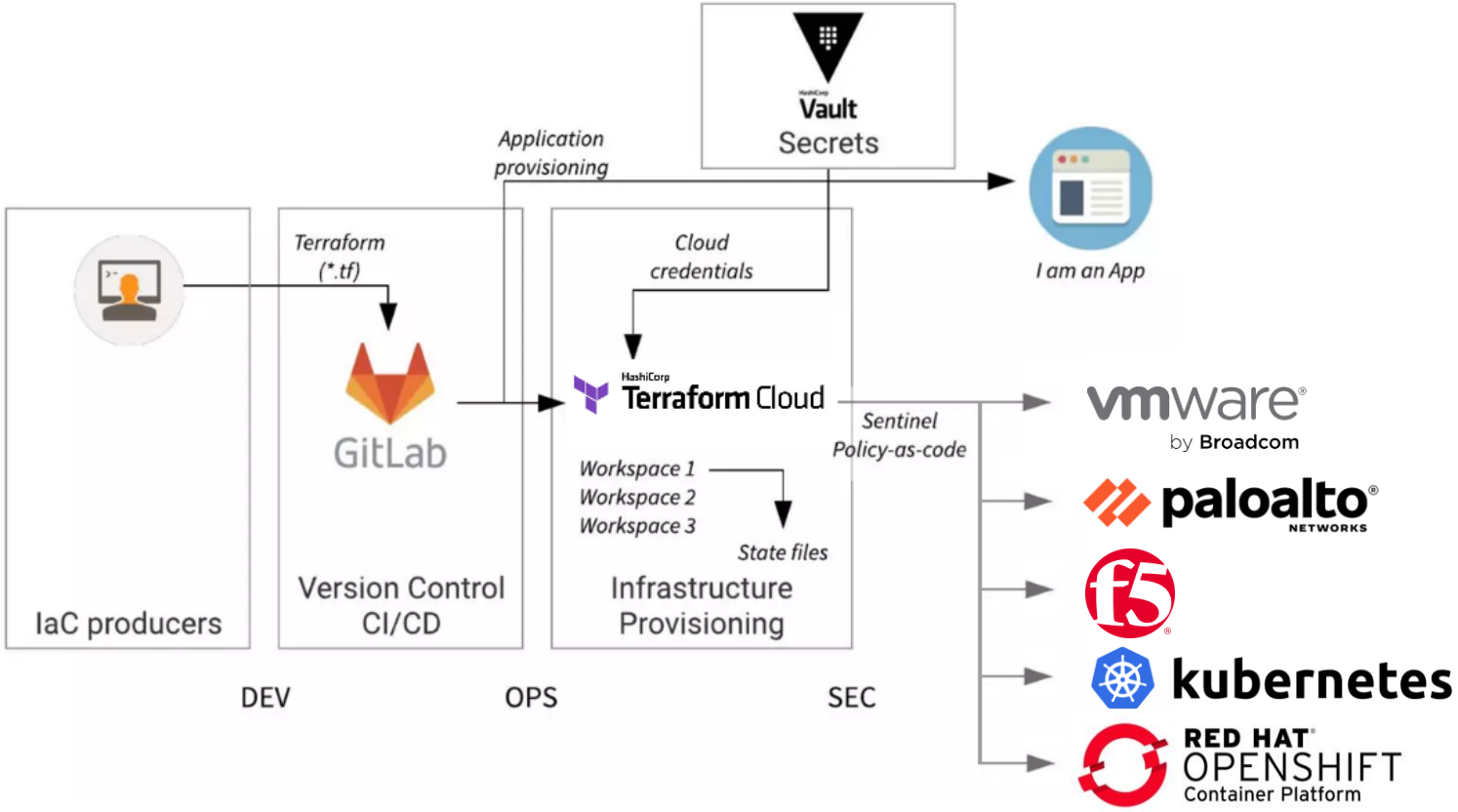


DEVSECOPS & INFRASTRUCTURE-AS-CODE

GITOPS ➔ PLATFORM-AUTOMATION

GitLab

HashiCorp



NTS


NTS
DEFENSE

NTS SECURITY SERVICES ÜBERBLICK

TDS | SIEM

SPLaaS (Splunk as a Service)

Defense Platform Operations | VM | TDS | MDR | IR

DEFENSE SERVICES

SECURITY OPERATIONS

cisco Partner | paloalto NETWORKS | FORTINET | splunk> | tenable | totemo securing data in motion

F5 DISTRIBUTED CLOUD

SECURE ALL APPS AND APIS EVERYWHERE

CONNECTIVITY FOR EVERY USER AND APP

RUN APPS ANYWHERE

app

API

VISIBILITY, ANALYTICS, AND CONTROL

010
1011

NTS NIS PACKAGE

Aufbauend auf **NTS I4ALL**

Portal zur Inventarisierung von Netzwerkkomponenten inkl. Konfigurationsbackups

NTS NIS PACKAGE

Onboarding

Vulnerability Modul

Compliance Modul

Consulting

→ Unterstützung bei NIS 2 Konformität