VIVAVIS

Hausmesse 2025

Transformation sicher und zuverlässig umsetzen

Sicherer Hafen im Cybersturm

Lösungsansätze und Dienstleistungen für sicherheitskritische Infrastrukturen

Viktor Greve

50 Jahre

VIVAVIS

Neuer Slogan „IT meets Energy“ …

… aber was heißt das nun?

Inhalt

Auf der Fahrt in einen sicheren Hafen

1. Aktuelle Herausforderungen für Netzbetreiber
2. Cybersecurity Bedrohungslage
3. Gesetzliche Anforderungen und Regulatorien
4. VIVAVIS IT & Security Service Portfolio
5. Partnernetzwerk
6. Zusammenfassung

Cybersecurity im Spannungsfeld des Kerngeschäfts von Energieversorgern

- Steigende regulatorische Anforderungen
- Massive Zunahme von Cyberangriffen
- Komplexität der IT- und OT-Systeme
- Fachkräftemangel bei IT und Security Experten
- Strengere Haftung und Meldefristen
- Deutlich höhere Anforderungen an Systemintegration und Betrieb

-> Cybersecurity ist kein Nebenjob

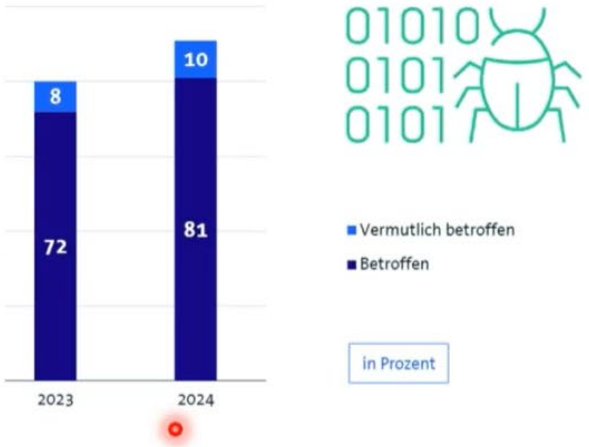
Die Cyber-Bedrohungslage für kritische Infrastrukturen

bitkom

Gesamtschaden für deutsche Unternehmen durch Cyberangriffe

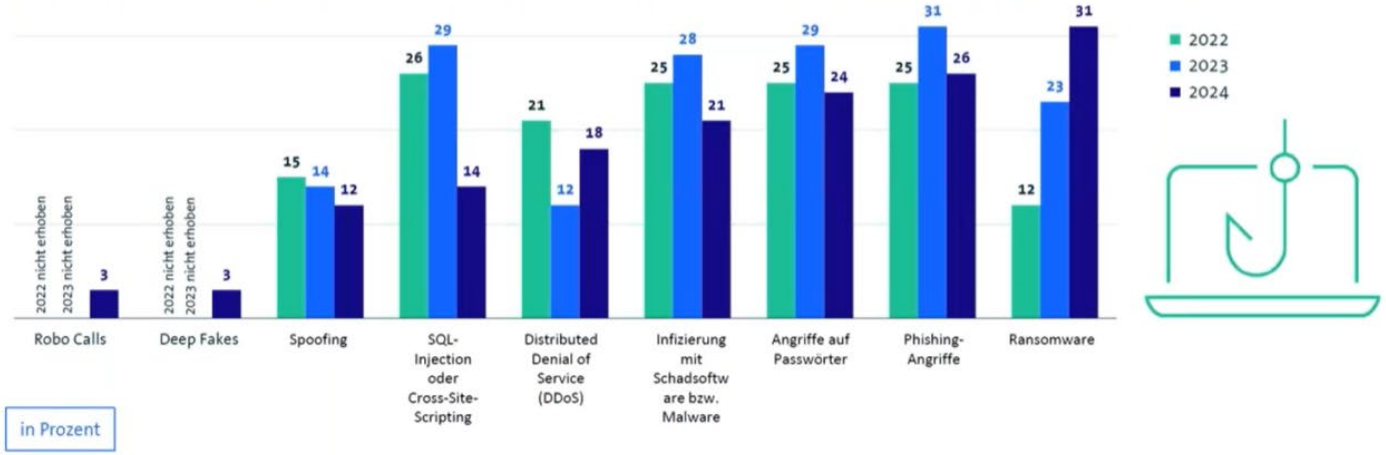
178,6 Mrd Euro

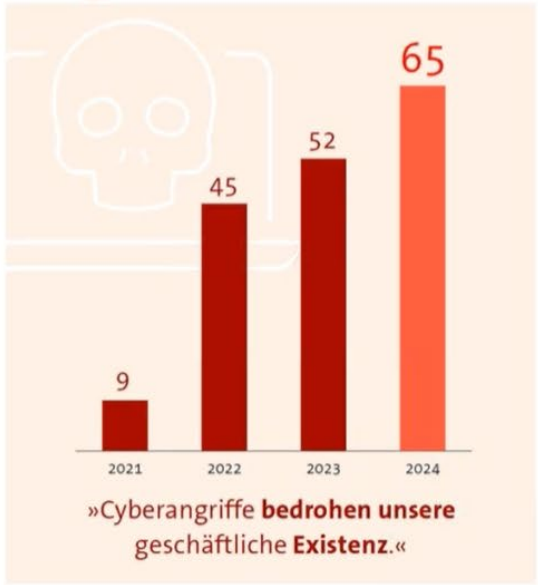
War Ihr Unternehmen innerhalb der letzten 12 Monate von (Daten-) Diebstahl, Industriespionage oder Sabotage betroffen?



Ransomware verursacht häufiger Schäden

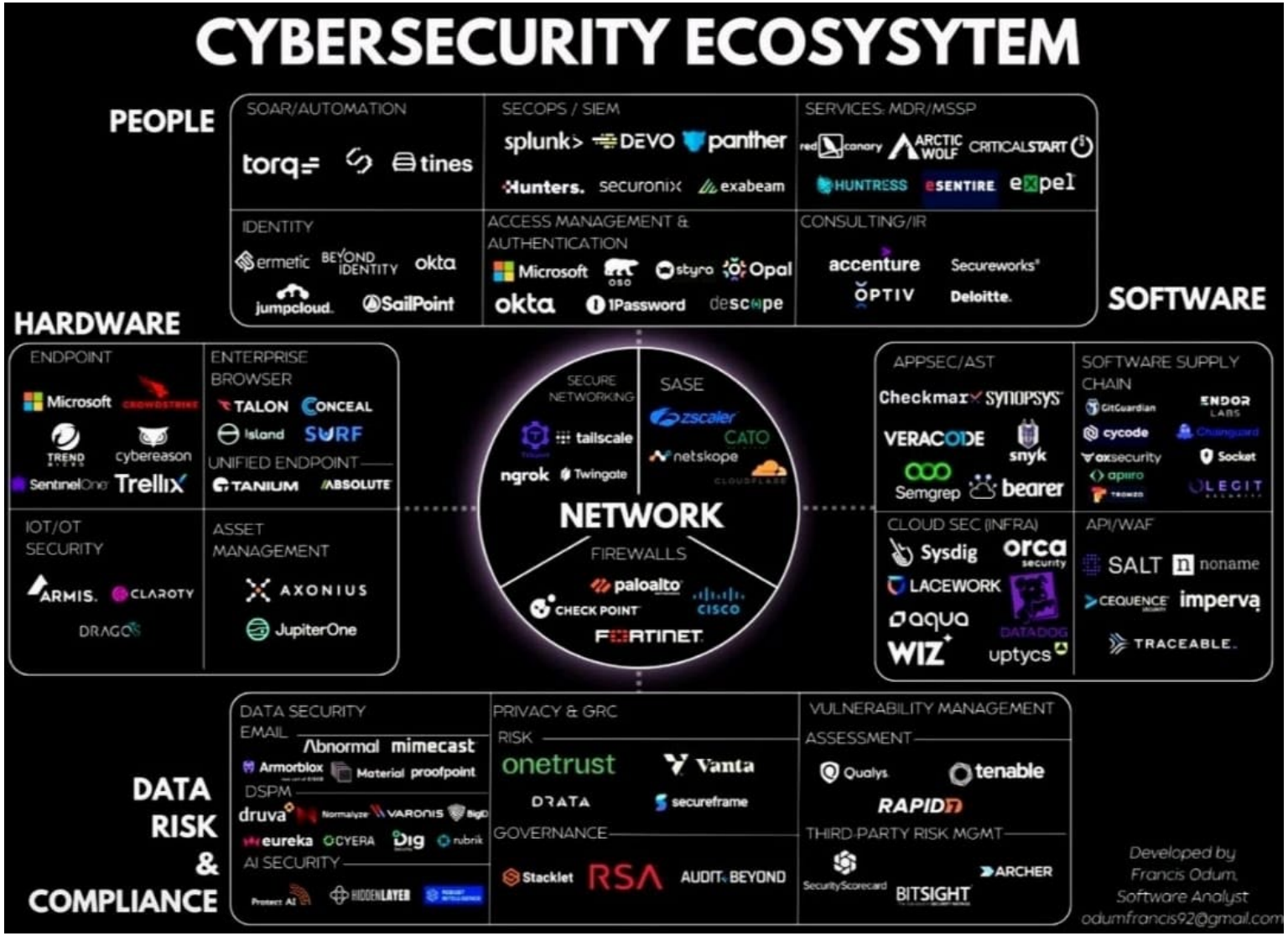
Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monate in Ihrem Unternehmen einen Schaden verursacht?





Quelle: Dr. Ralf Wintergerst, Bitkom-Präsident im August 2024 (https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf) SOPHOS
Datenbasis: Unternehmen in Deutschland mit mindestens 10 Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr

Soll das die Antwort sein?



NIS2 Deutsches Umsetzungsgesetz

Auswirkung auf das EnWG (E) §5c Absatz 4 – Vorgaben für den IT-Sicherheitskatalog

1. **Risikoanalyse** und **IT-Sicherheitskonzepte** entwickeln und dokumentieren
2. Bewältigung von **Sicherheitsvorfällen**
3. **Backup-Management und Wiederherstellung nach einem Notfall**
4. Sicherheit der **Lieferkette**
5. **Sicherheitsmaßnahmen** bei **Erwerb, Entwicklung und Wartung** von IT-Systemen
6. **Risikomanagementmaßnahmen**
7. **Cyberhygiene und Mitarbeiterschulungen** zur **IT-Sicherheit**
8. **Kryptografie und Verschlüsselung**
9. **Zugriffskontrolle** und das **Management** von Anlagen
10. **Multi-Faktor-Authentifizierung** für kritische Systeme einsetzen
11. Einsatz von **Systemen zur Angriffserkennung**
12. **Cybersicherheitszertifizierung** gemäß europäischer Schemata -> **CSA**

Wir sitzen im selben Boot …

Wir haben bereits ein ISMS und sind ISO 27001 zertifiziert … - reicht das nicht?

❌Nein leider nicht, weil ….

🛡️ Es gibt **höhere Mindestanforderungen** bei Risikoanalyse, Business Continuity Management, …

🔍Das **BSI hat erweiterte Befugnisse** für Prüfungen, Anordnungen und Sanktionen erhalten.

👨‍💼 Der **Vorstand trägt die Haftung** und führt jährlich ein Management-Review gemäß Artikel 21 durch

⏱️ **Kürzere Meldefristen** für Angriffserkennung und Schwachstellen

🔗 Die **Zuliefererkette** muss verschärfte Sicherheitsanforderungen erfüllen und überwacht werden

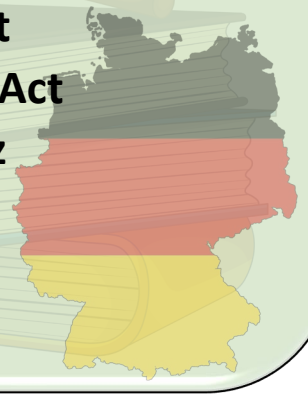
💸 **Umsatzbezogene Strafen** bis 2% des Jahresumsatzes

Wir analysieren, strukturieren und ordnen die Gesetz- und Normenlandkarte um und richten unser Service Portfolio danach aus

Regulatorische Anforderungen und Normen für Betreiber und Lieferanten Kritischer Infrastrukturen

Regulatorische Anforderungen für den deutschen Markt

- **BSIG**
- **EnWG**
- **NIS2 - EU**
- **NIS2 – deutsches Umsetzungsgesetz**
- **KRITIS Dachgesetz**
- **Cybersecurity Act**
- **Cyber Resilience Act**
- **Sicherheitsgesetz**
- **Data Act**
- **UpKritis**
- **DSGVO**

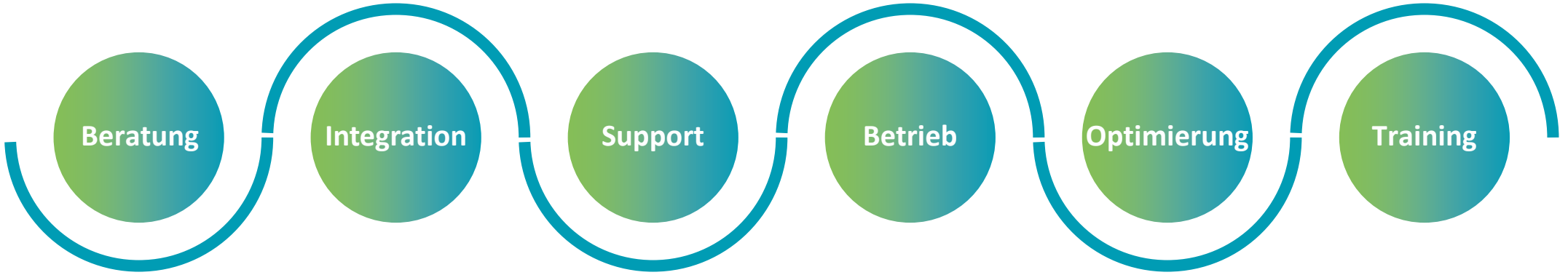


Normen und etablierte Standards mit umsetzbaren Sicherheits-kontrollen und Prozessen

- **ISO 27001**
- **ISO 27002**
- **ISO 27019**
- **BDEW 3.0**
- **IEC 62443**

VIVAVIS IT & Security Service Portfolio

Portfolio Übersicht und Struktur



VIVAVIS IT & Security Portfolio

Segment: Beratung

Heute:

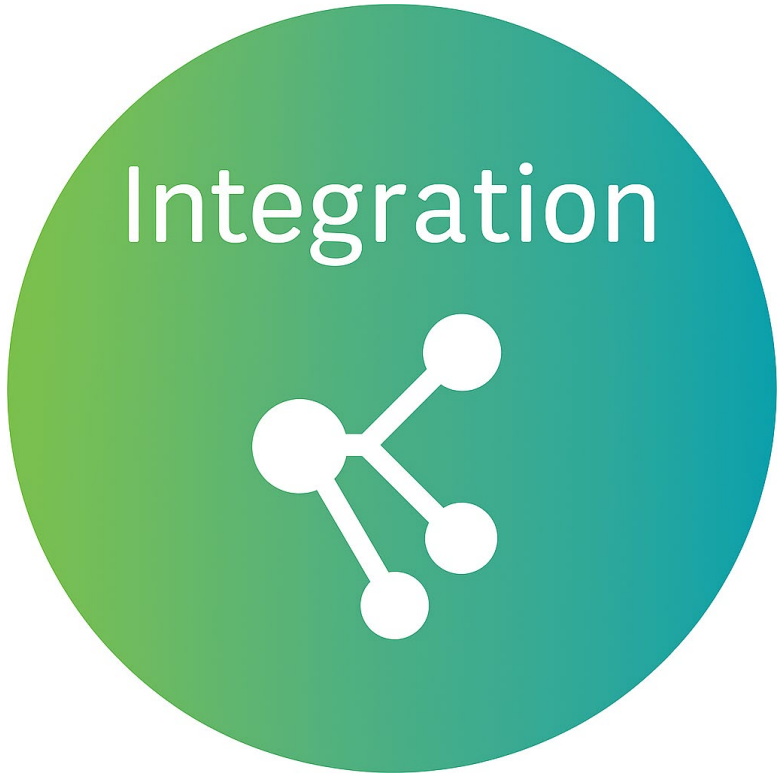
1. Beratung zur Leistellen System Planung
2. IT Infrastruktur Design für Netzleittechnik Systeme
3. Dokumentation der Netzleittechnik Systeme
4. OT System Architektur Design für BDEW 3.0 Compliance

Morgen:

- OT System Architektur für NIS2 Compliance
- Compliance as a Service
- Compliance Readiness Assessments
- HIGH-LEIT Migration Services

VIVAVIS IT & Security Portfolio

Segment: Integration



Heute:

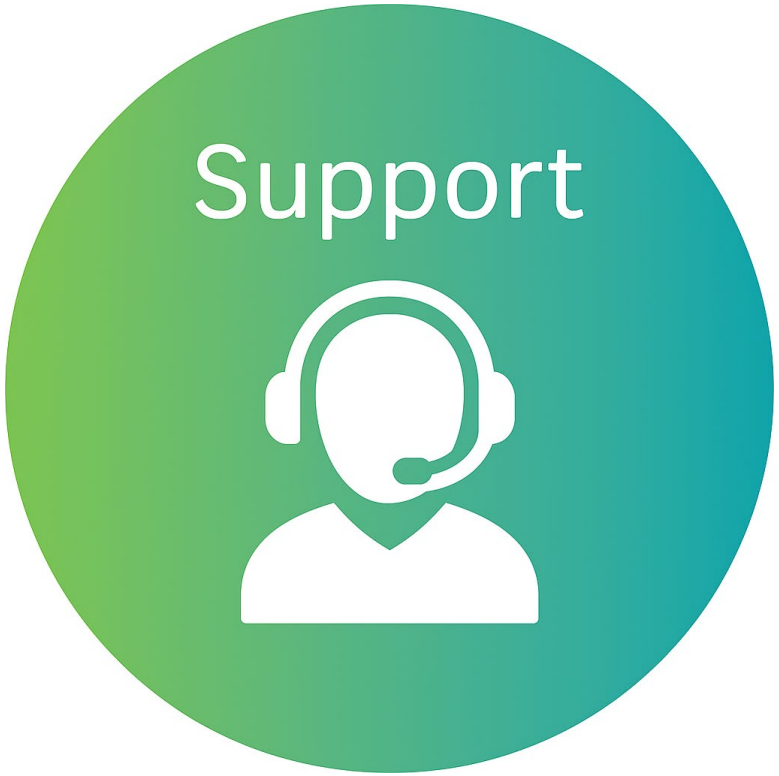
1. Systeme zur Angriffserkennung
2. Netzwerk Anomalie Erkennung
3. Firewall IDS/IPS
4. System Backups
5. Logging
6. Netzwerk Monitoring
7. Windows / Linux Integrations Services
8. AD Integration Services
9. Netzwerk Traffic Verschlüsselung
10. IPSec VPN Tunneln
11. PKI Einrichtung

Morgen:

- SIEM für OT-Systeme
- Next-Generation Firewall

VIVAVIS IT & Security Portfolio

Segment: Support



Heute:

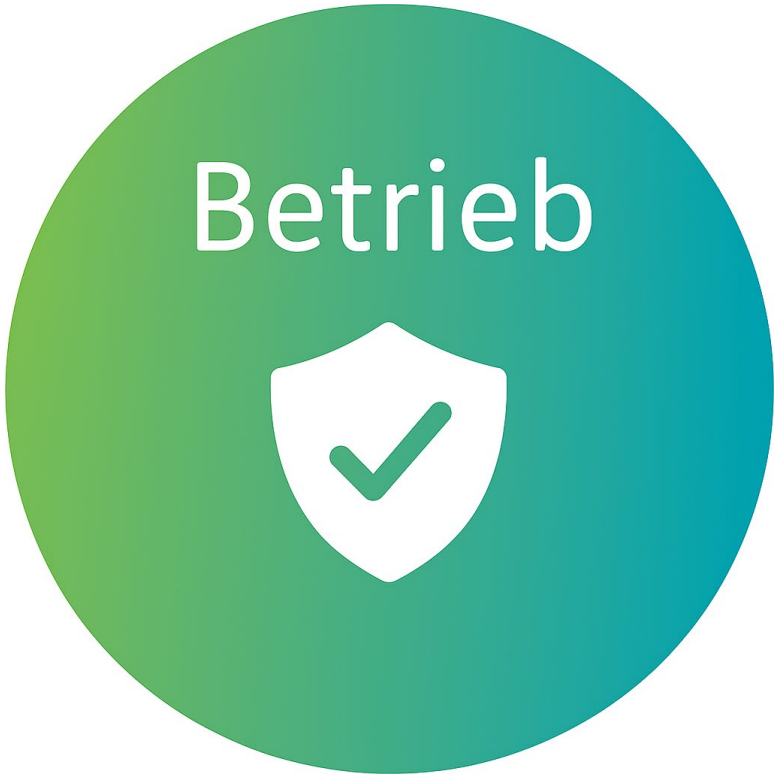
1. Service Desk
2. Schwachstellen Management
3. Patch Management
4. Begleitung von Kunden- und Auditoren Audits
5. Vorbeugende Wartung (Vor-Ort, Remote)
6. Microsoft Windows Support
7. Debian Linux Support
8. HIGH-LEIT Release Updates
9. Asset Inventory
10. Hypercare Support

Morgen:

- Container Plattform Support
- Erweiterter Cybersecurity Support

VIVAVIS IT & Security Portfolio

Segment: Betrieb



Heute:

1. Managed SOC

Morgen:

- Managed Detection and Response (MDR)
- Endpoint Detection and Response (EDR)
- Schwachstellen Management
- Attack Surface Management (ASM)
- Xtended Detection and Response (XDR)
- Security Orchestration, Automation and Response SOAR)
- Websecurity

VIVAVIS IT & Security Portfolio

Segment: Optimierung

Heute:
1. Schwachstellen Scans (Netzwerk)
2. DR-Verfahren und Tests für HIGH-LEIT

Morgen:
- Automatisierte Pen-Tests
- Schwachstellen Scans (System)

VIVAVIS IT & Security Portfolio

Segment: Training

Heute:
1. VIVAVIS HIGH-LEIT System Schulung
2. VIVAVIS Netzwerk Security Architektur Schulung
3. VIVAVIS Schulung S310 - IT-Sicherheit in der Netzleittechnik
4. VIVAVIS Schulung S332 - ISMS Lieferanten-Audit S332

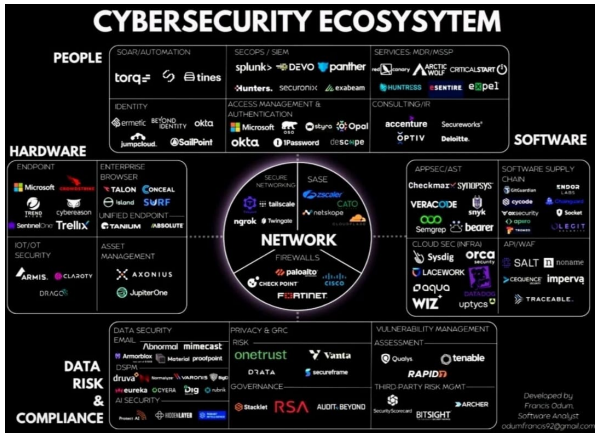
Morgen:
…

Aktuelles Partnernetzwerk im Bereich IT und Security

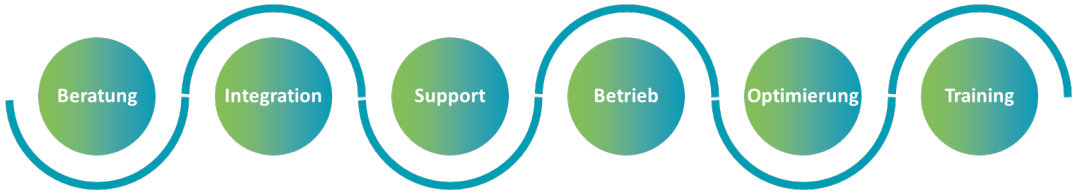


Warum VIVAVIS der beste IT Service Partner für ihre OT-Systeme ist

- ✓ Wir verstehen die spezifischen Anforderungen der Energieversorger
- ✓ Wir haben jahrelange Erfahrung in der Planung und Integration von OT und IT-Systemen
- ✓ Wir investieren in Skills, Tools und Prozesse zur Sicherung unserer Applikationen und ihrer Systeme
- ✓ Wir evaluieren die passenden Partner Produkte und Services und integrieren sie in ihr Netzleitsystem
- ✓ Wir haben die lokale Präsenz mit überregionaler Expertise



➢ Wir sorgen für die Sicherheit in Ihren OT-Systemen



VIVAVIS

VIVAVIS AG
Nobelstraße 18
76275 Ettlingen
Deutschland

www.vivavis.com
info@vivavis.com

Viktor Greve
Geschäftsbereichsleiter Digital Platform Services
VIVAVIS AG

Manuel Laufer
Produktmanager IT & Security Services
VIVAVIS AG

Wir unterstützen Sie mit branchenspezifischen Services, die ihre Netzleitsysteme sicher, gesetzeskonform und zukunftssicher machen

1. Machen Sie einen Termin mit unseren Experten
2. Geben Sie uns Feedback. Wünsche? Anforderungen?
3. Wir informieren Sie regelmäßig über Neuerungen in unserem Portfolio