TEHTRIS

FACE THE UNPREDICTABLE

Ahead of time and cybersecurity

NIS2 + KRITIS 2.0 translated into XDR/MDR + SIEM

TEHTRIS

UNSERE MISSION

Als europäisches Unternehmen

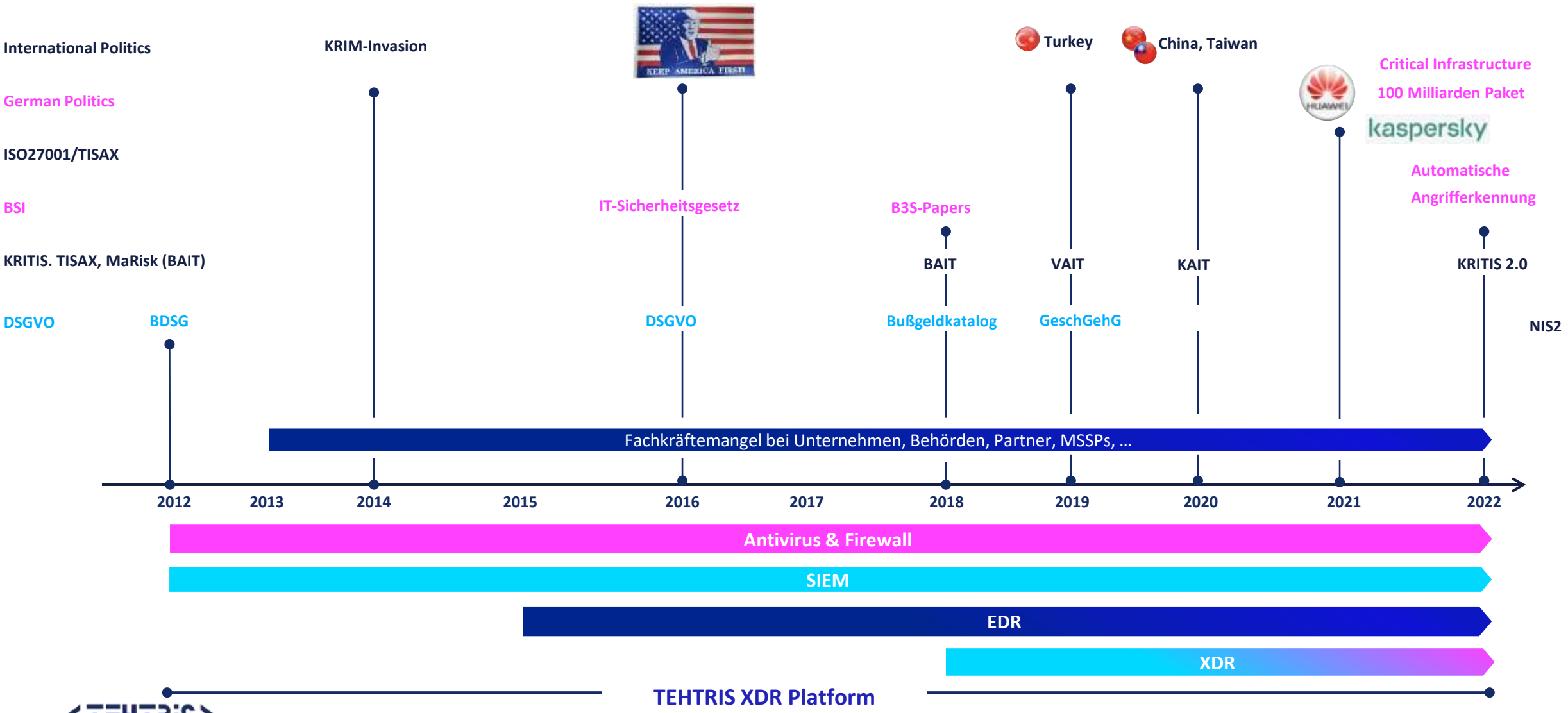
SCHÜTZEN WIR EUROPA

MIT **AUTOMATISIERTER NEUTRALISATION**

VON CYBERANGRIFFEN UND CYBERSPIONAGE

IN **ECHTZEIT**

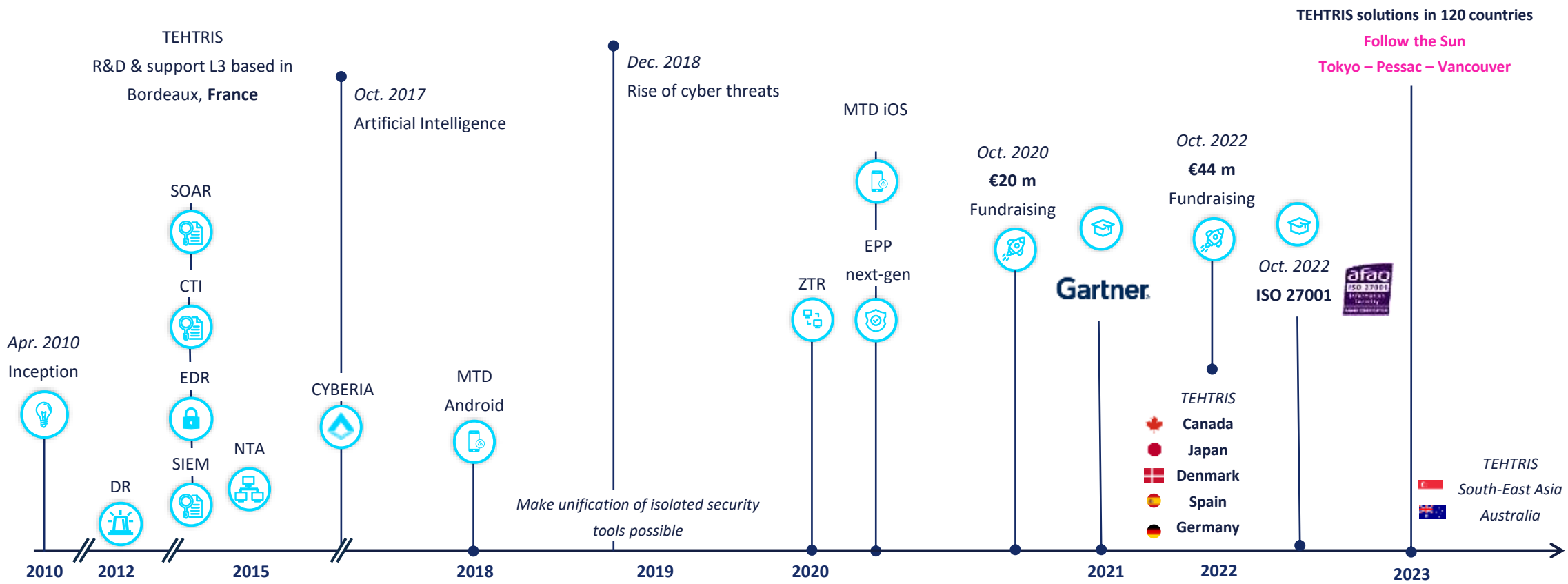
Heutige Anforderungen versus Stand der Technik



Created the first XDR Platform & strengthened it for 10 years

MADE IN EUROPE

Pentest — **TEHTRIS XDR Platform**



Private and public customers, from SMEs to large organizations (+200k endpoints)


TEHTRIS
XDR
Automation
Response - Workflow
APIs
Artificial Intelligence (CYBERIA)
Cyber Threat Intelligence
Threat Hunting
UEBA
Unified Console
Advanced Analytics
Compliance Audits
SOAR Orchestration
Ticketing System
Cyber warehouse
EDR
EPP
MTD
SIEM
NTA
Deceptive Response
DNS Firewall
Zero Trust
CWPP
Email Protection
Identity Access Management
TECHNICAL LANDSCAPE
CLOUD
aws
Azure
Google Cloud
OVH
SYSTEMS
Endpoints
Servers
Mobile
IoT
NETWORKS
SD-Wan
Firewalls
VPN
Network flows

TEHTRIS XDR Module

TEHTRIS R&D

(MCO + MCS)

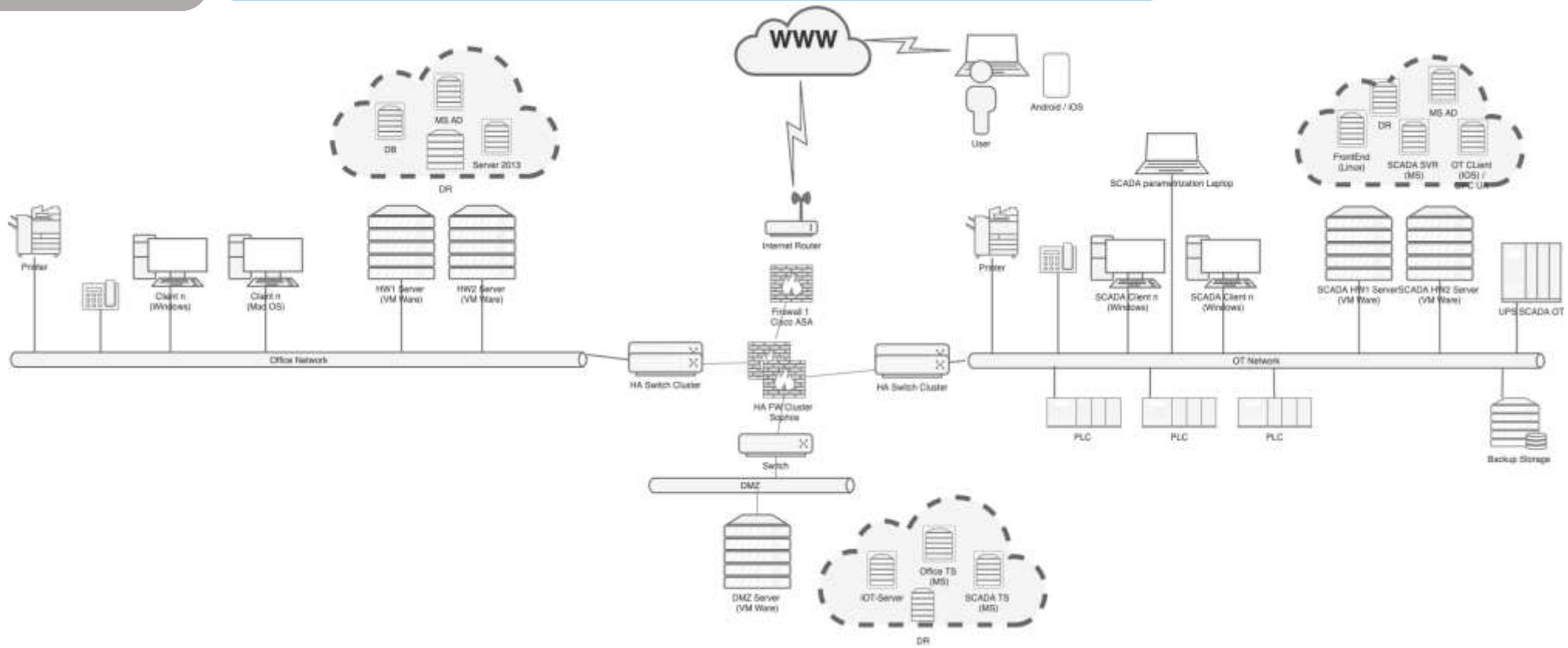
SOC

OVH Frankfurt / **CLIENT DEDICATED SERVERS**

TEHTRIS XDR Platform

Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE



TEHTRIS XDR Module

TEHTRIS R&D

(MCO + MCS)

Endpoint Detection & Response + Endpoint Protection Platform

SOC

OVH Frankfurt / **CLIENT DEDICATED SERVERS**

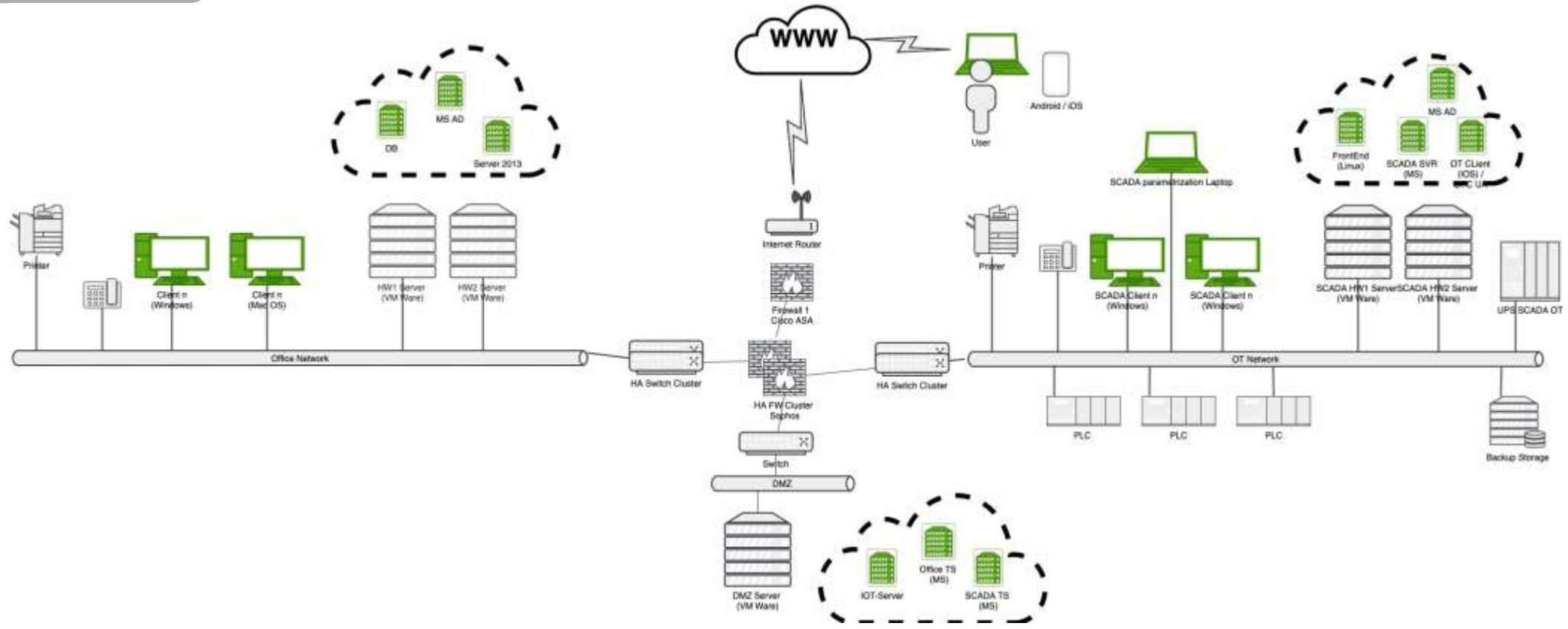
TEHTRIS XDR Platform

Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE

EDR

EPP



TEHTRIS XDR Module

EDR

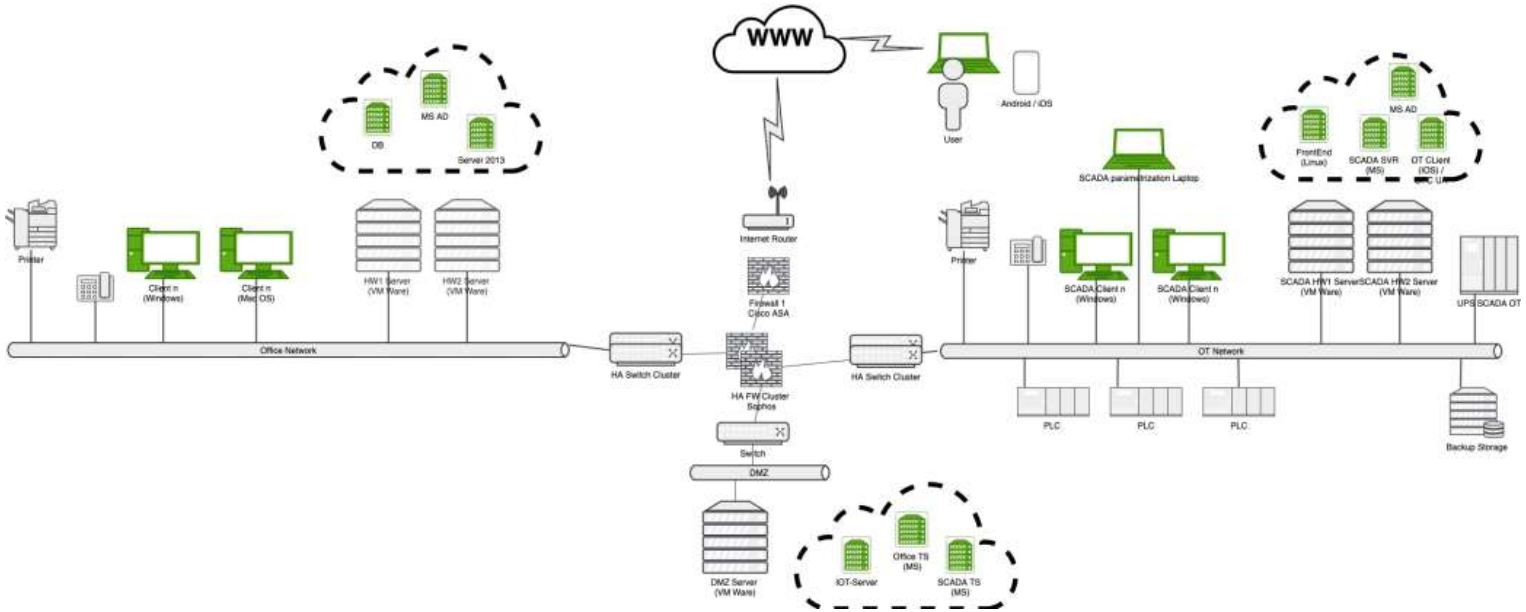
ENDPOINT DETECTION & RESPONSE

- 24x7 Erkennung und Neutralisierung ohne menschliche Interaktion
- ScanDisk: Analyse statischer Dateien
- Suspend, Quarantäne, Kill
- Neuronale Netze (Deep Learning) Personalisierung der Automatisierung
- Zugang zur TEHTRIS XDR Plattform und ihren Funktionen (SOAR, CTI, CYBERIA)
- Dashboards & Reporting
- On-Premise oder in der Cloud
- Schutz all Ihrer Betriebssysteme
- In alle IT- & OT-Umgebungen integrierbar via APIs

EPP

ENDPOINT PROTECTION & PLATFORM

- 24x7 Erkennung und Neutralisierung ohne menschliche Interaktion
- Antivirale Erkennung
- Verhaltensanalyse auf z. Bsp. Prozess- und Speicherebene
- Anti-Exploitation zum Schutz vor der Ausnutzung ungepatchter oder unbekannter Schwachstellen
- Firewall inklusive schon vordefinierter Regeln
- Zugang zur TEHTRIS XDR Plattform und ihren Funktionen (SOAR, CTI, CYBERIA)
- Dashboards & Reporting
- On-Premise oder in der Cloud
- Schutz all Ihrer Betriebssysteme
- In alle IT- & OT-Umgebungen integrierbar via APIs



TEHTRIS XDR Module

TEHTRIS R&D

(MCO + MCS)

Security Information Event Management

SOC

OVH Frankfurt / **CLIENT DEDICATED SERVERS**

TEHTRIS XDR Platform

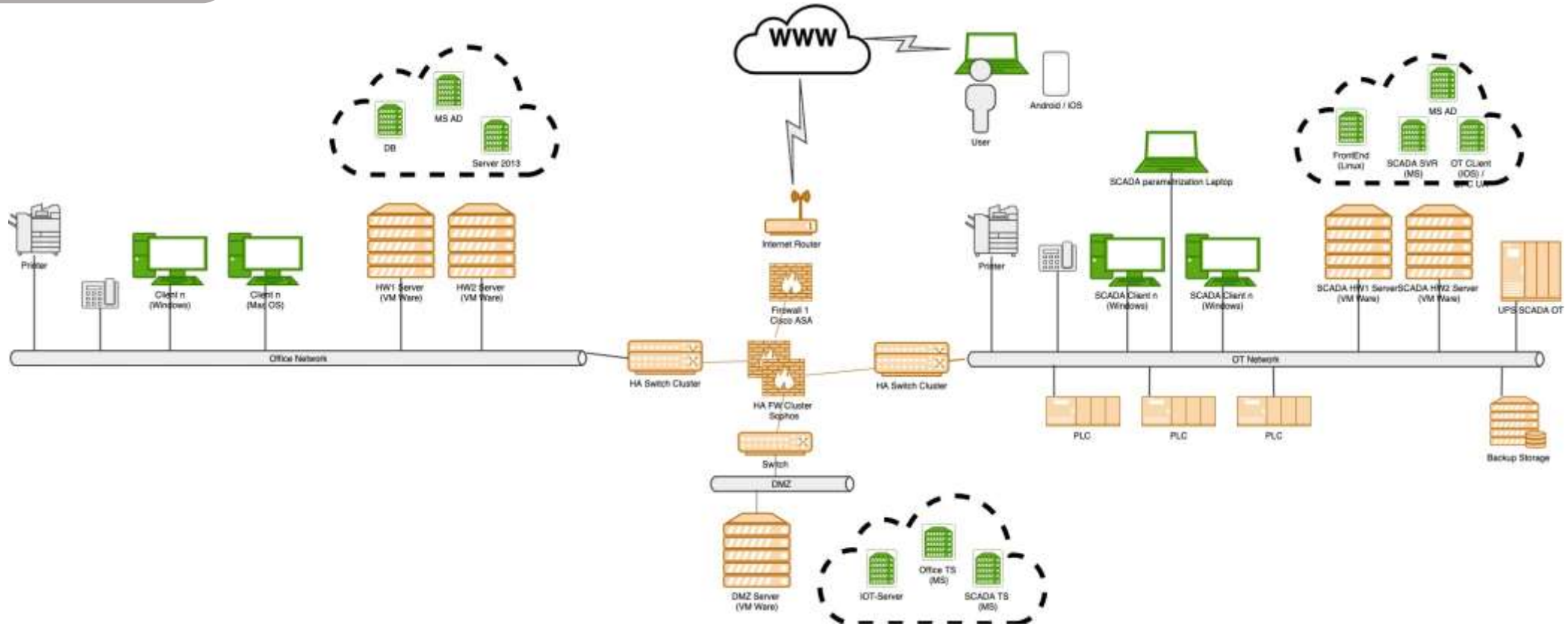
Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE

EDR

EPP

SIEM



TEHTRIS XDR Module

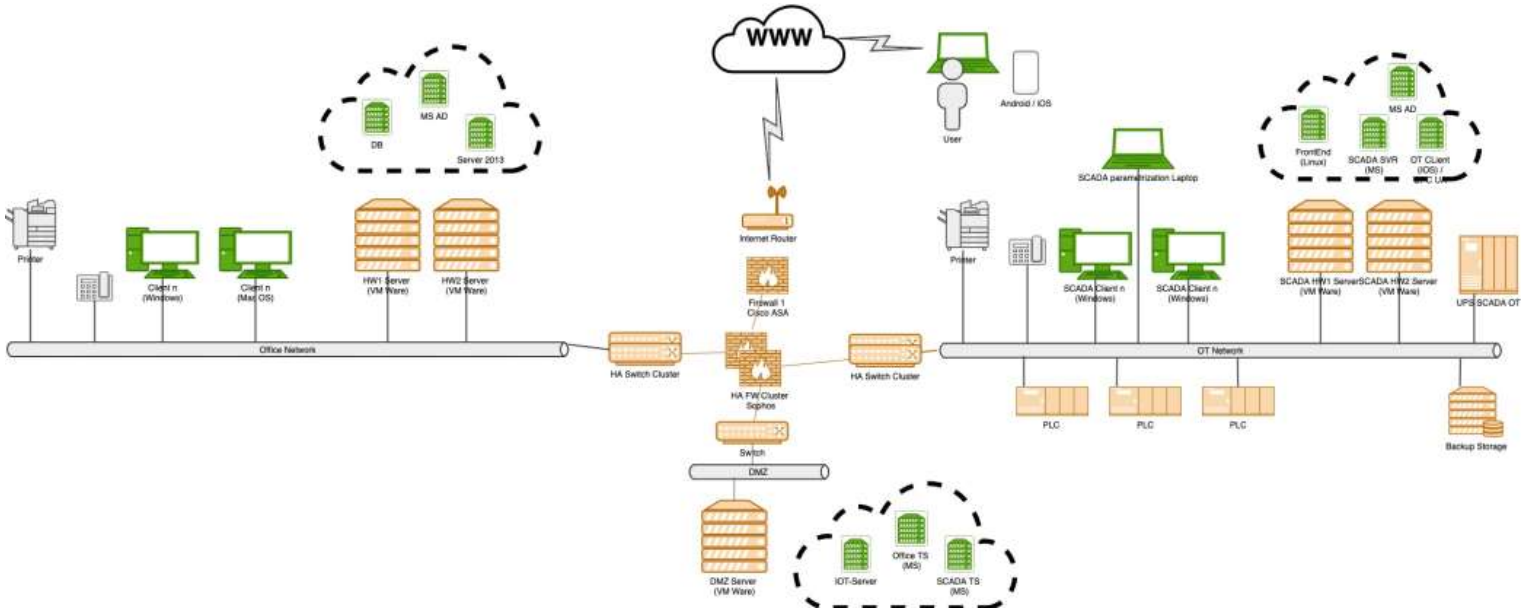
SIEM

Security Information & Event Management

- 24x7 Echtzeit-Überwachung und Monitoring
- Ermöglicht eine ausgedehnte Forensik und Abgleich mit den MITRE ATT&CKen
- Dient der Beweissicherung und Nachweißpflicht in Bezug auf die Eihaltung des Datenschutzes und des Geschäftsgeheimnisgesetzes
- Unabhängig von Ihren Quellen und deren Formaten (Syslog, Leef, CEF, JSON, CSV, KVP, XML...)
- Katalog von über 1 600 Korrelationsregeln
- Zugang zur TEHTRIS XDR Plattform und ihren Funktionen (SOAR, CTI, CYBERIA)
- Dashboards & Reporting
- On-Premise oder in der Cloud

Security Information & Event Management für Microsoft 365

- 24x7 Echtzeit-Überwachung und Monitoring ihrer MS 365 Cloud-Umgebung
- Ermöglicht eine ausgedehnte Forensik und Abgleich mit den MITRE ATT&CK Wegen
- Dient der Beweissicherung und Nachweißpflicht in Bezug auf die Eihaltung des Datenschutzes und des Geschäftsgeheimnisgesetzes
- Zugang zur TEHTRIS XDR Plattform und ihren Funktionen (SOAR, CTI, CYBERIA)
- Dashboards & Reporting



TEHTRIS XDR Module

TEHTRIS R&D

(MCO + MCS)

SOC

Network Traffic Analysis

OVH Frankfurt / **CLIENT DEDICATED SERVERS**

TEHTRIS XDR Platform

Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

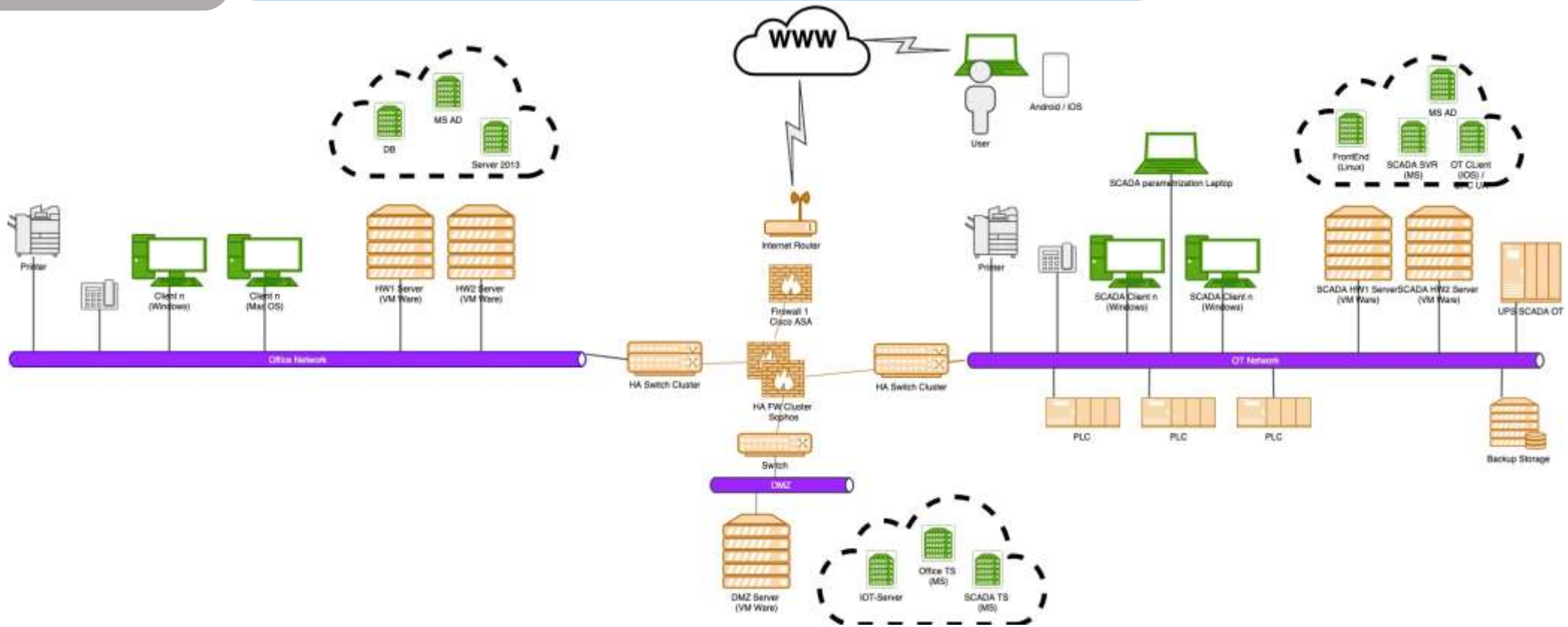
CYBER DATA LAKE

EDR

EPP

SIEM

NTA

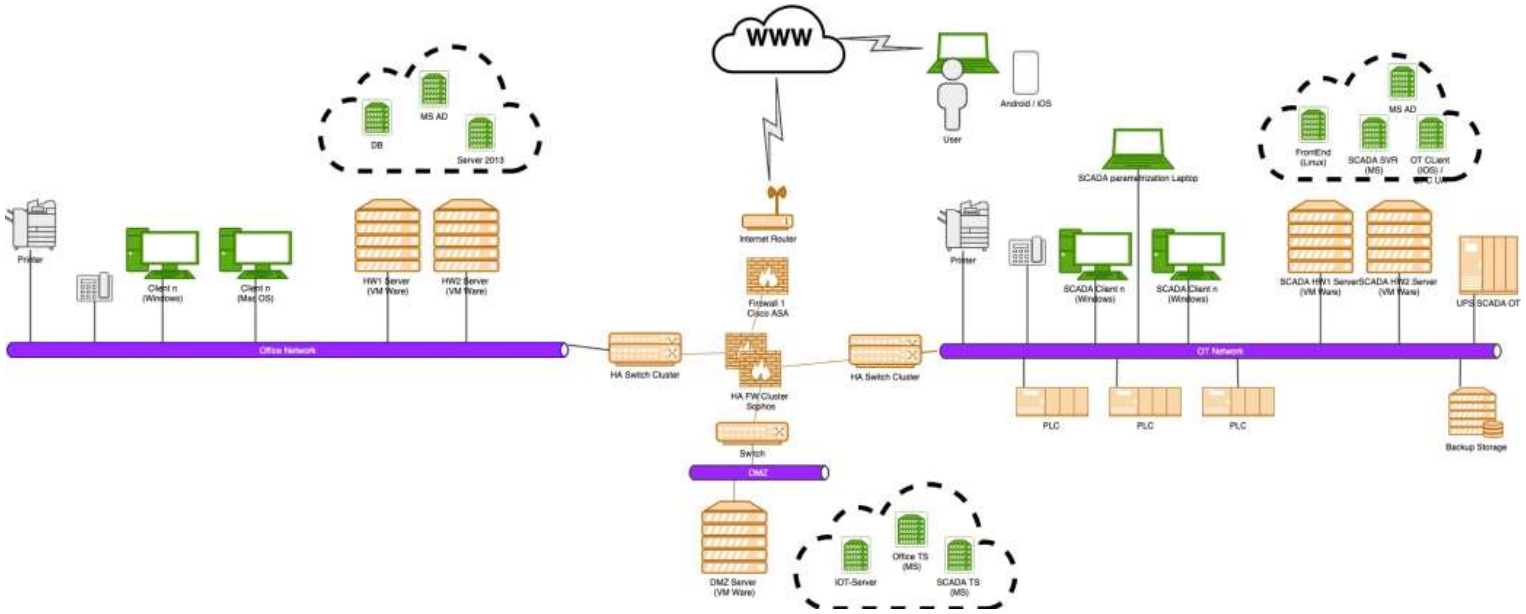


TEHTRIS XDR Module

NTA

Network Traffic Analysis

- 24x7 Echtzeit-Überwachung und Monitoring Ihrer Netzwerke
- Ermöglicht eine ausgedehnte Forensik und Abgleich mit den MITRE ATT&CKen
- Datenbank von über 60.000 qualifizierten Regeln
- Rückwirkungsfreies Monitoring in IT- und OT-Umgebungen
- Erkennt anormale Verkehrsaktivitäten mit Hilfe der Analyse von Netzwerksignaturen und Verhaltensanalysen (TEHTRIS CYBERIA Artificial Intelligence)
- Es sind keine zusätzlichen Integrationsprozesse
- Zugang zur TEHTRIS XDR Plattform und ihren Funktionen (SOAR, CTI, CYBERIA)
- Dashboards & Reporting
- On-Premise



TEHTRIS XDR Module

TEHTRIS R&D

(MCO + MCS)

Mobile Threat Detection

SOC

OVH Frankfurt / **CLIENT DEDICATED SERVERS**

TEHTRIS XDR Platform

Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE

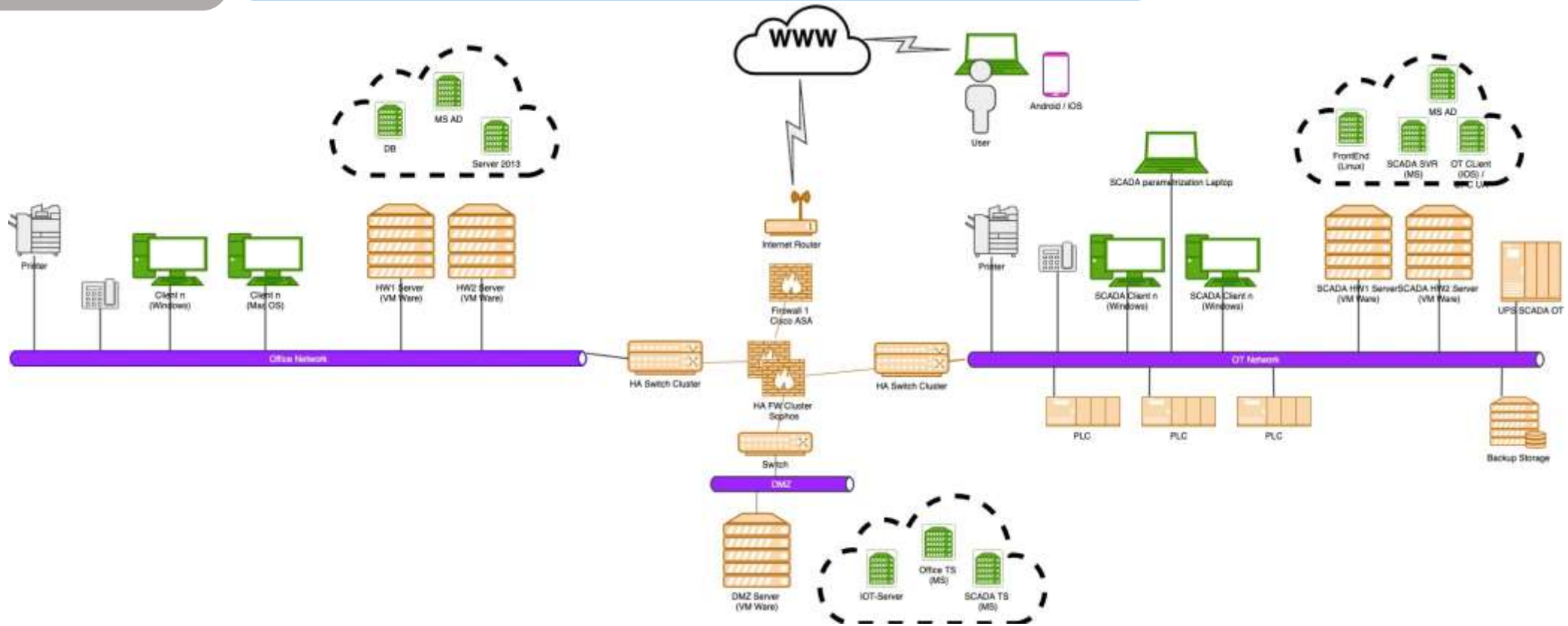
EDR

NTA

EPP

MTD

SIEM

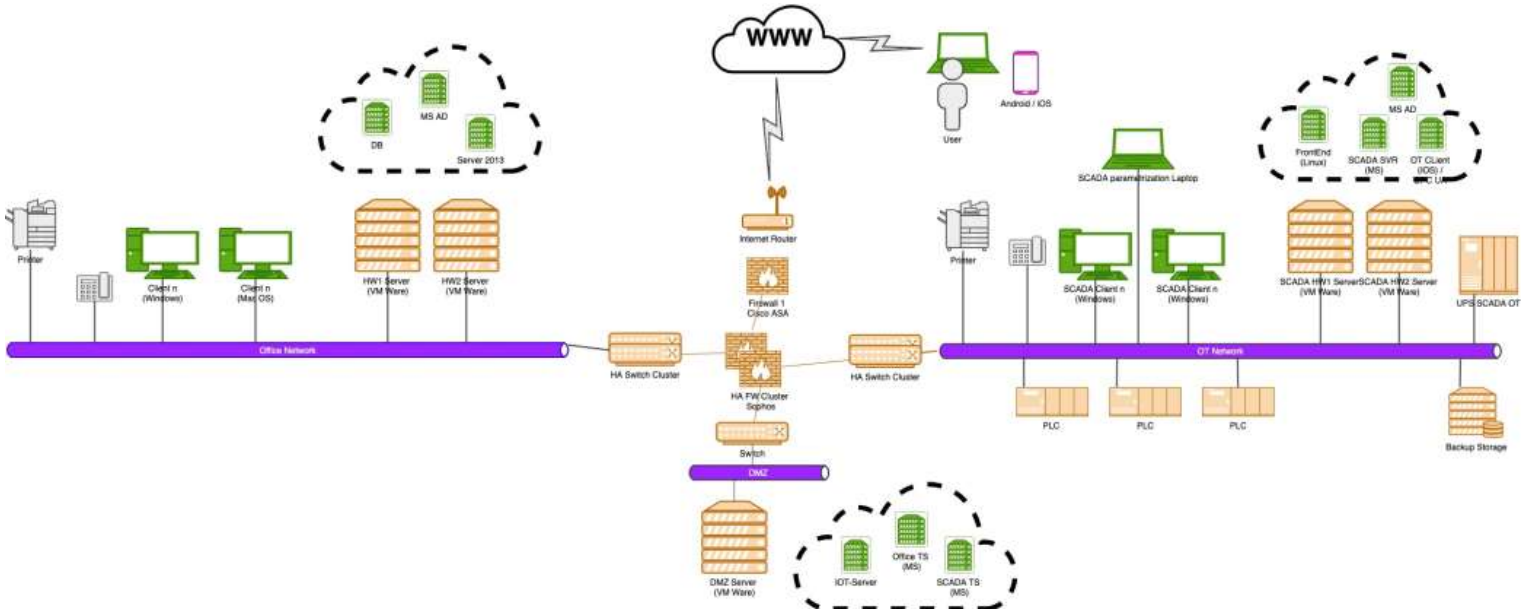


TEHTRIS XDR Module

MTD

Mobile Threat Defense

- Kontrollieren Sie Ihre Anwendungen von der Installation bis zum Update
- Verfügbar für Android, iOS, iPadOS und Chrome OS
- Schützen Sie Ihre Smartphones mit Telefon-Port-Scans, Telefon-Root-Erkennung, Erkennung von alternativen Stores, Erkennung bösartiger Bibliotheksinjektionen...
- Schwarze Liste bösartiger Websites mit der integrierten TEHTRIS DNS-Firewall
- Im Falle einer Kompromittierung können Sie die TEHTRIS MTD-Funktionen nutzen, um bösartige APKs aus der Ferne zu deinstallieren oder eine DNS-Isolierung des kompromittierten Geräts vorzunehmen
- Erstellen Sie Ihre eigenen benutzerdefinierten SOAR-Playbooks für DNS-Isolierung und Push-Benachrichtigung
- Behalten Sie die Kontrolle über die Sicherheit Ihrer Flotte mit den exklusiven Benachrichtigungen von TEHTRIS MTD mit anpassbaren Warnschwellenwerten



TEHTRIS XDR Module

TEHTRIS R&D

(MCO + MCS)

SOC

Deceptive Response

OVH Frankfurt / **CLIENT DEDICATED SERVERS**

TEHTRIS XDR Platform

Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE

EDR

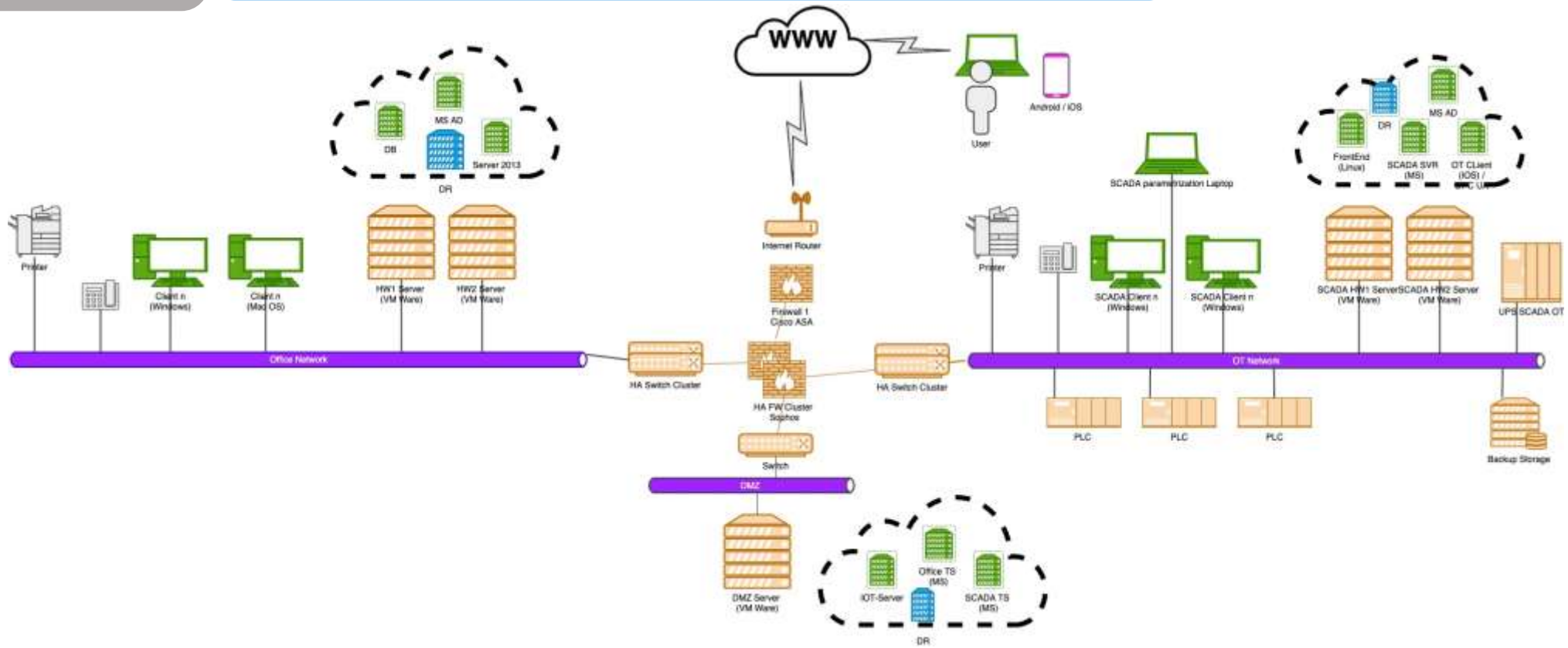
EPP

SIEM

NTA

MTD

Deceptive Response

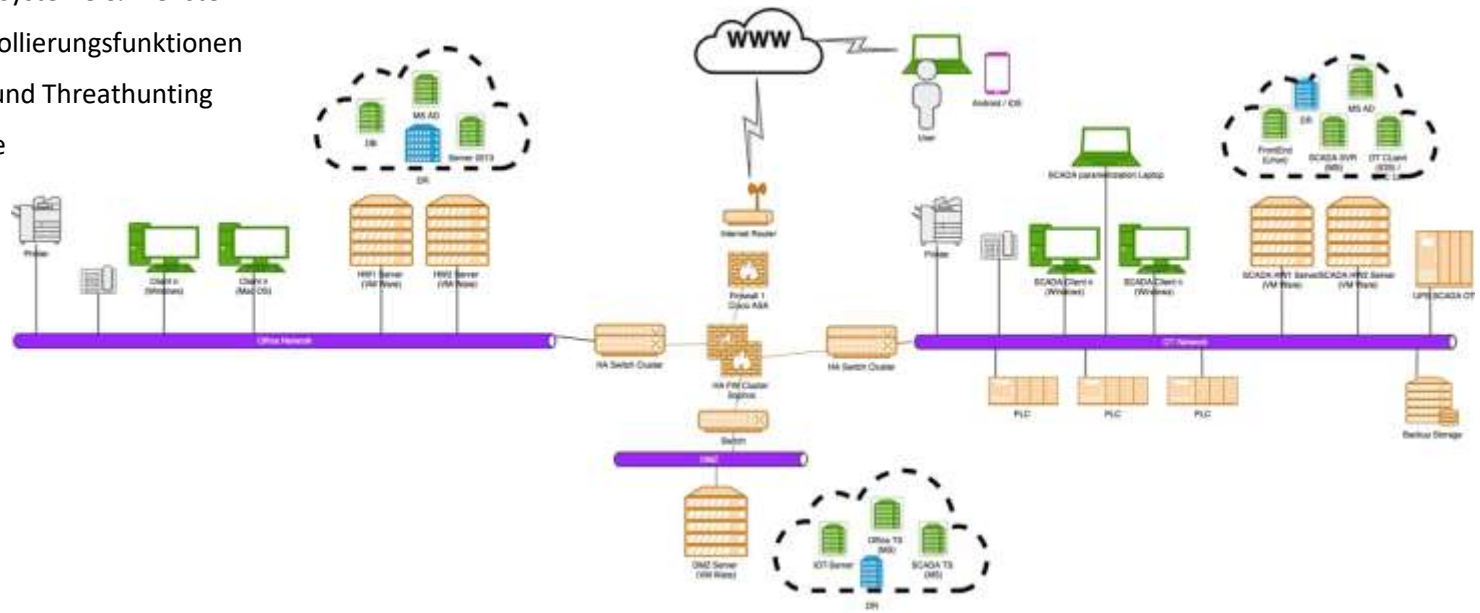


TEHTRIS XDR Module

Deceptive Response

Deceptive Response

- Honeypots, die gefälschte Dienste simulieren, um schwache Signale zu erkennen
- Vereinfachte Log-Analyse trotz der ausgefeilten Honeypot Technologie
- Videos von Befehlszeilen, die von Angreifern eingegeben werden
- Schneller MTTD (Mittlere Zeit bis zur Erkennung)
- Schnellere MTTR (Mittlere Zeit bis Behebung)
- Ferngesteuertes & zentralisiertes Verwaltung (SaaS)
- Einfach zu implementieren und einfach zu Verwenden
- TEHTRIS Deceptive Response virtuelle Maschine, die einfach auf der Hardware des Hardware des Kunden (VMware ESXi Hypervisor)
- TEHTRIS Deceptive Response virtuelle Maschine, die über das Internet mit der TEHTRIS XDR-Plattform verbunden (Trace Monitoring und Wartung im SaaS-Modus)
- Gefälschte Betriebssysteme & Dienste
- Verbesserte Protokollierungsfunktionen
- Datenspeicherung und Threathunting
- Cloud & On Premise



TEHTRIS XDR Module

TEHTRIS R&D
(MCO + MCS)

SOC

Modular die Sicherheit erhöhen!

OVH Frankfurt / **CLIENT DEDICATED SERVERS**

TEHTRIS XDR Platform

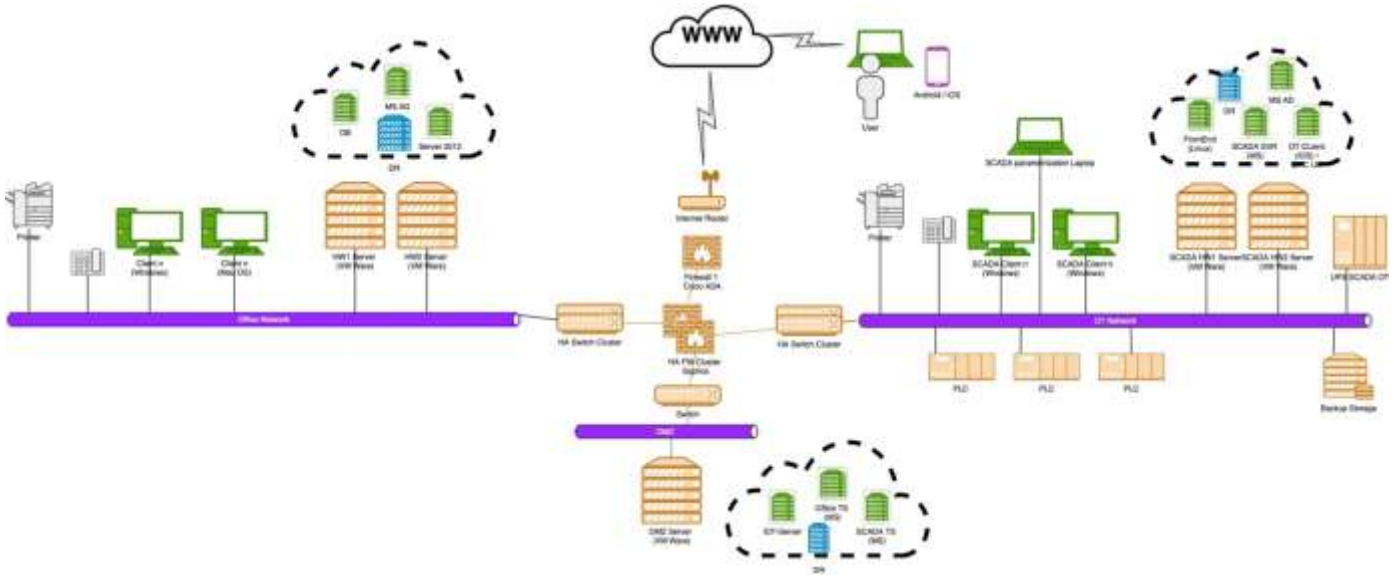
Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE

EDR | NTA | EPP | MTD | SIEM | Deceptive Response

Empfehlung: Mindestmaßnahmen

Ausbaustufe 1 POC	Ausbaustufe 2	Ausbaustufe 3 …
EDR	NTA	MTD
SIEM		Deceptive Response
		EPP



Vorteile unserer XDR Plattform:

- **Modular /Flexibel**
- **Skalierbar / Cloud / on Prem**
- **Intern verschlüsselt und gehärtet**
- **Schützen ihre Investitionen**
- **Erfahren in OT Umgebungen**

TEHTRIS XDR Module

TEHTRIS R&D

(MCO + MCS)

Modular die Sicherheit erhöhen!

OVH Frankfurt / **CLIENT DEDICATED SERVERS**

TEHTRIS XDR Platform

Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE

EDR

EPP

SIEM

NTA

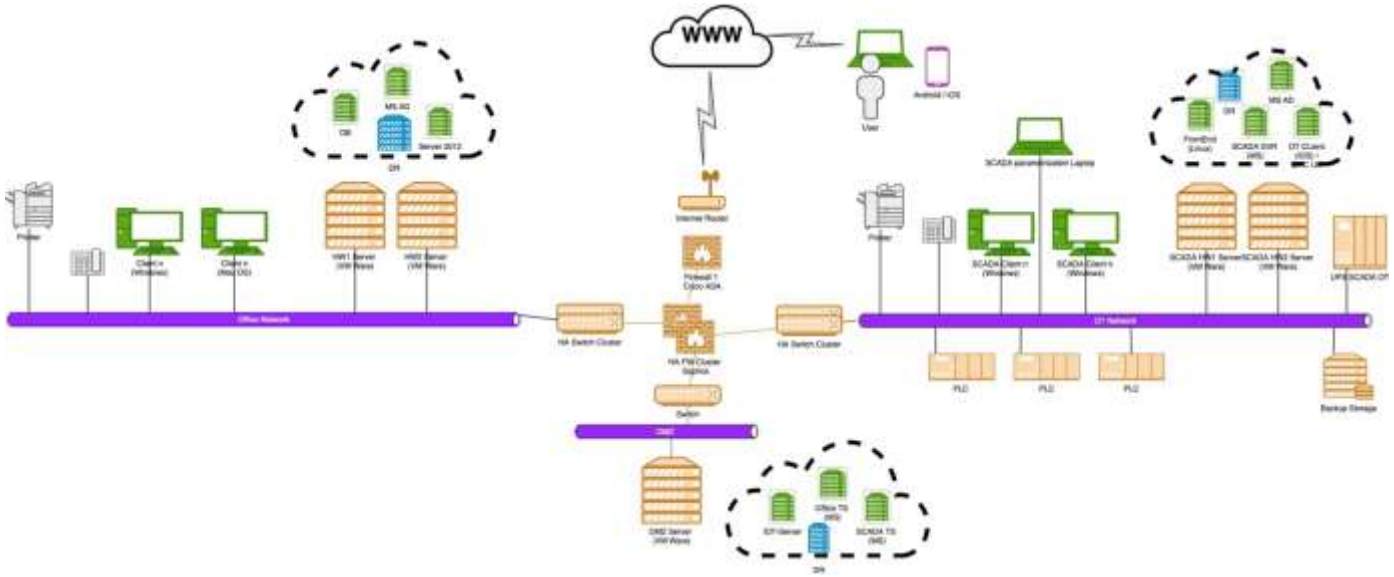
MTD

Deceptive Response

SOC

Partner

Eigenes Team



TEHTRIS EDR – COMPATIBILITY

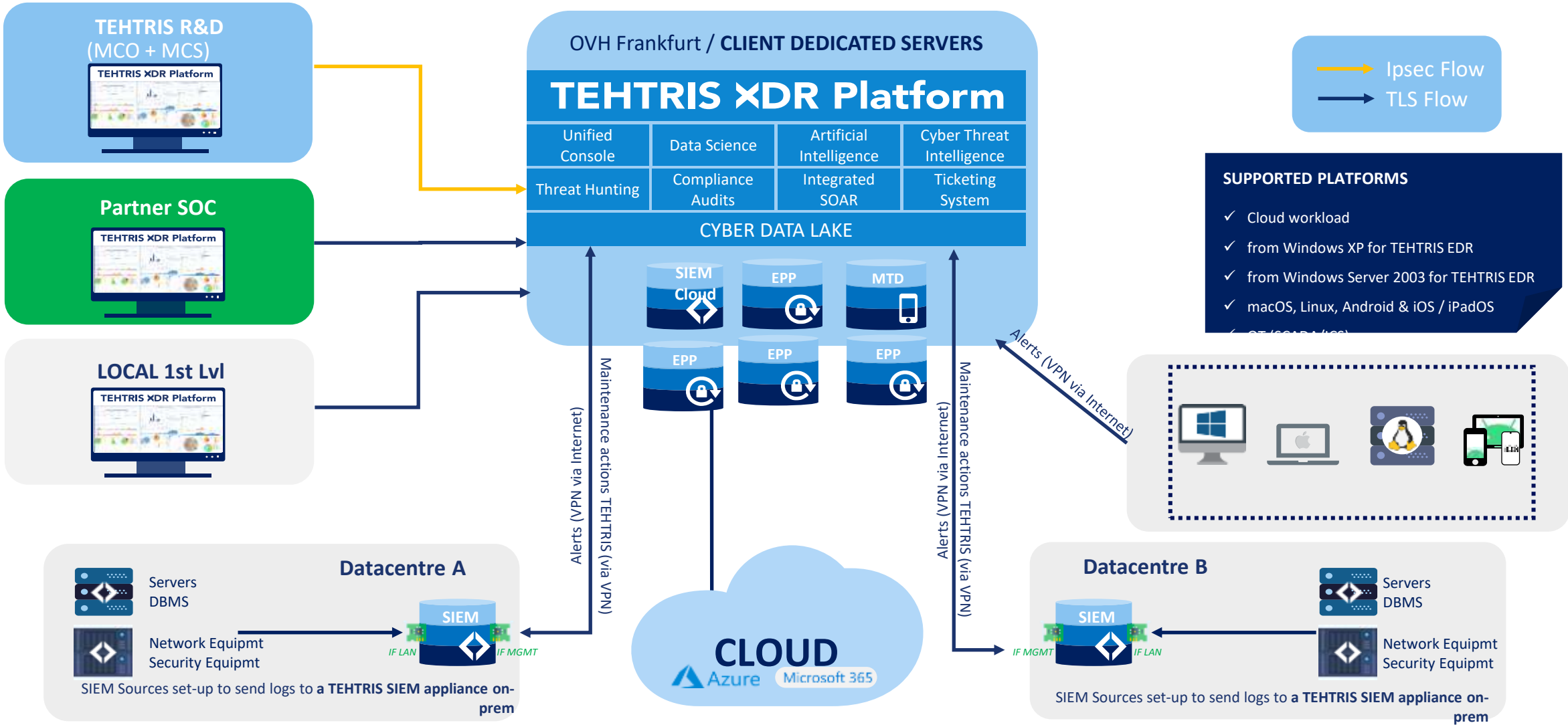
	32Bits	64Bits
Windows XP **	✓	✓
Windows Vista	✓	✓
Windows 7	✓	✓
Windows 8	✓	✓
Windows 10+11	✓	✓
Windows Server 2003 **	✓	✓
Windows Server 2008	✓	✓
Windows Server 2008 R2	✓	✓
Windows Server 2012		✓
Windows Server 2012 R2		✓
Windows Server 2016		✓
Windows Server 2019		✓

	64Bits
CentOS 5.3	✓
CentOS 5.11	✓
CentOS 6.9	✓
CentOS 7.5	✓
Ubuntu 8.04	✓
Ubuntu 14.04	✓
Ubuntu 16.04	✓
Ubuntu 18.04*	✓
RedHat 5, 6, 7 & 8	✓
macOS Sierra	✓
macOS High Sierra	✓
macOS Mojave	✓
macOS Catalina	✓

* The Linux distribution list is not exhaustive, Debian variants are also supported for instance

** Microsoft Visual C++ 2008 Redistributable Package might be installed : http://www.microsoft.com/en-us/download/details.aspx?id=29

Technische Architektur



FACE THE UNPREDICTABLE

Contact us!

Olaf.Mueller-Haberland@tehtris.com