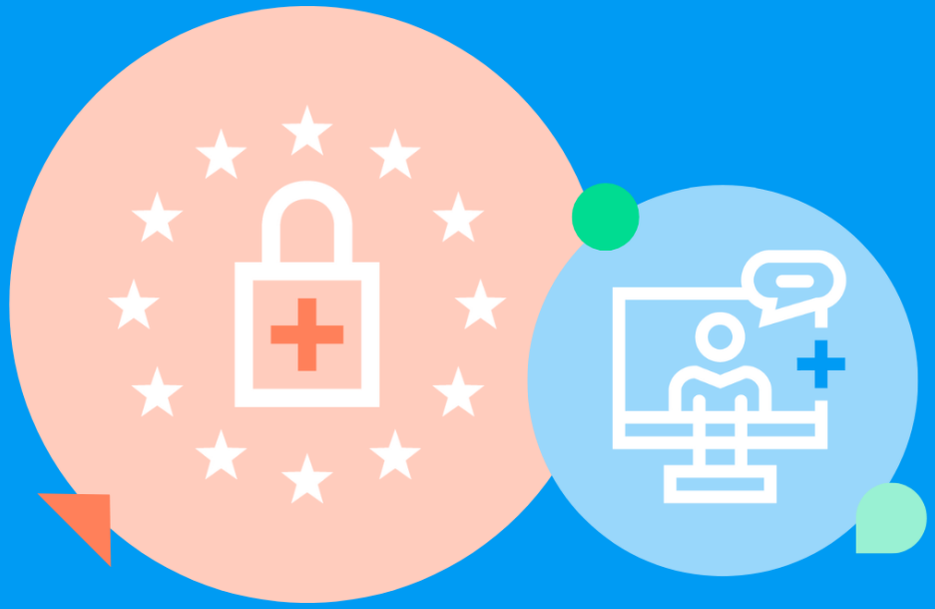
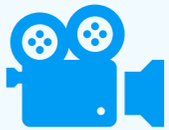
Auf die Plätze, fertig, NIS2!

So erfüllen Sie die NIS2-Anforderungen effektiv und heben Ihre IT-Security auf den Stand der Technik.



Housekeeping Rules



Das Webinar wird aufgezeichnet

Teilnehmer sind während des Webinars stummgeschaltet

Fragen bitte während des Webinars in das Q&A-Fenster stellen

Herzlich willkommen

Ihre Experten

Daniel Graßer

Senior Director of
Security Services

Peter Weber

Technical Account
Manager Security

Agenda

- Housekeeping
- Was Sie jetzt schon wissen sollten
- Ihre IT als Ausgangspunkt – „Das Haus der IT“
- Konzepte der Risikoanalyse & IT-Sicherheit
  - Security als Prozess
  - NIS2-Assessment
- Schutzmaßnahmen
  - Security Scanner
  - Workload Protection
  - Endpoint Security
  - Security Operations Center
- Backup & Disaster Recovery

Was Sie jetzt schon wissen sollten...

... oder gerne nachholen: Whitepaper lesen & Webinar „A beginner‘s Guide to NIS2“ ansehen

Bin ich betroffen?

Zum Whitepaper

Security ist geschäftskritisch

80 %
der Unternehmen
haben **Schaden** erlitten

8 von 10
Unternehmen
häufiger angegriffen

52 %
sehen Existenz bedroht

Umsetzung, Motivation, Sanktionen

Umsetzung:

Gesetz muss bis 17.10.2024 verabschiedet sein

Motivation:

Angemessene Sicherheitsmaßnahmen für Organisationen in kritischen Sektoren

Bessere Zusammenarbeit der EU-Mitgliedsstaaten zur Stärkung der Cybersecurity in Europa

Sanktionen:

Hohe Geldstrafen bei Verstößen + Geschäftsführer in Haftung

Zum Webinar

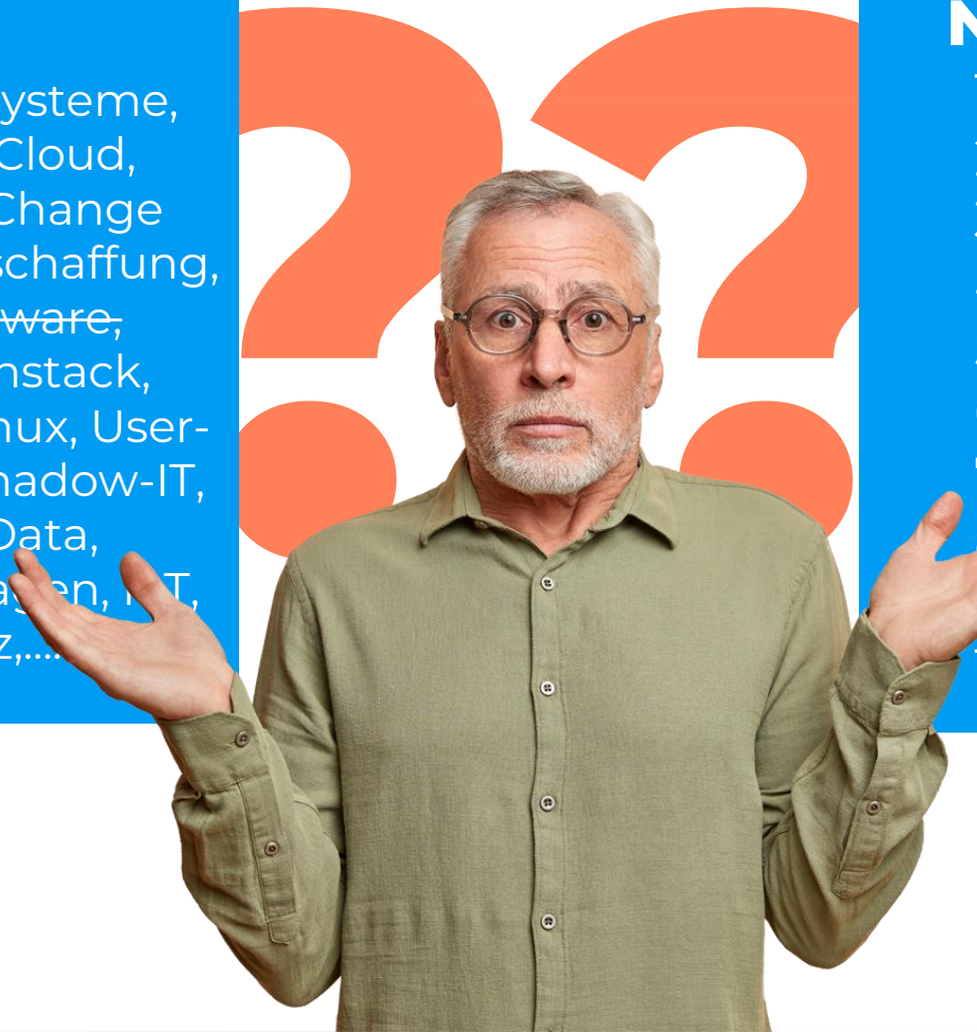
plusserver

Meine IT vs NIS2-Anforderungen

Wie finde ich mich zurecht?

Meine Jobs:

Rechenzentrum, Legacy-Systeme, Digitalisierung, DSGVO, Cloud, Hyperscaler, Mitarbeiter, Change Management, Einkauf & Beschaffung, Budget??, Prozesse, ~~VMware,~~ VMware/Broadcom, Openstack, Hyper-V, KVM, Windows, Linux, User-Management, ERP, CRM, Shadow-IT, Webseite & Shop, Big Data, Operation Technology, Anlagen, IoT, Künstliche Intelligenz,...



NIS2-Anforderungen

1. Blah!
2. Blah! Blah!
3. Unleserlich!
4. Hm,...
5. Wie bitte?
6. Das auch noch?
7. Soso,...
8. Och nö,...
9. Echt jetzt?
10. Jetzt reichts aber!

plusserver

Kurzgesagt
1. Konzepte: Risikoanalyse & IT-Sicherheit
2. Bewältigung von Sicherheitsvorfällen
3. Backup & Disaster Recovery
4. Supply-Chain
5. Schutzmaßnahmen inkl Schwachstellen-Management
6. Wirksamkeit von Risikomanagement
7. Schulung/Cyberhygiene
8. Kryptographie
9. Physische Anlagen: Zugriffskontrolle/Management
10. Authentifizierung & Kommunikation

§ 30 Abs.

Maßnahmen

Technik einha

und internatio

müssen auf ei

beruhen. Die

Folgendes um

lie Sicherheit in der

agement und

management,

sbezogener Aspekte

ungen und ihren

und Wartung von

n und Prozessen,

Schwachstellen,

amkeit von

icherheit in der

iene und

mationstechnik,

ografie und

kontrolle und für das

entifizierung oder

kontinuierlichen Authentifizierung, **gesicherte Sprach-, Video- und Textkommunikation** sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

***aktueller Referentenentwurf**

plusserver

Scope dieses Webinars

10 Anforderungen in 50 Minuten? -> Scope des Webinars auf technische Security reduzieren

NIS2-Anforderungen
1. Konzepte: Risikoanalyse & IT-Sicherheit
2. Bewältigung von Sicherheitsvorfällen
3. Backup & Disaster Recovery
4. Supply-Chain
5. „Sicherheitsmaßnahmen“ inkl Schwachstellen-Management
6. Wirksamkeit von Risikomanagement
7. Schulung/Cyberhygiene
8. Kryptographie
9. Physische Anlagen: Zugriffskontrolle/Management
10. Authentifizierung & Kommunikation

Scope des Webinars (Rest: über Partner-Ökosystem)
Konzepte: Risikoanalyse & IT-Sicherheit
Bewältigung von Sicherheitsvorfällen
Backup & Disaster Recovery
Supply-Chain
Schutzmaßnahmen inkl. Schwachstellen-Management
Wirksamkeit von Risikomanagement -> z.B. Pentesting
Schulung/Cyberhygiene
Kryptographie
Physische Anlagen: Zugriffskontrolle/Management
Authentifizierung & Kommunikation

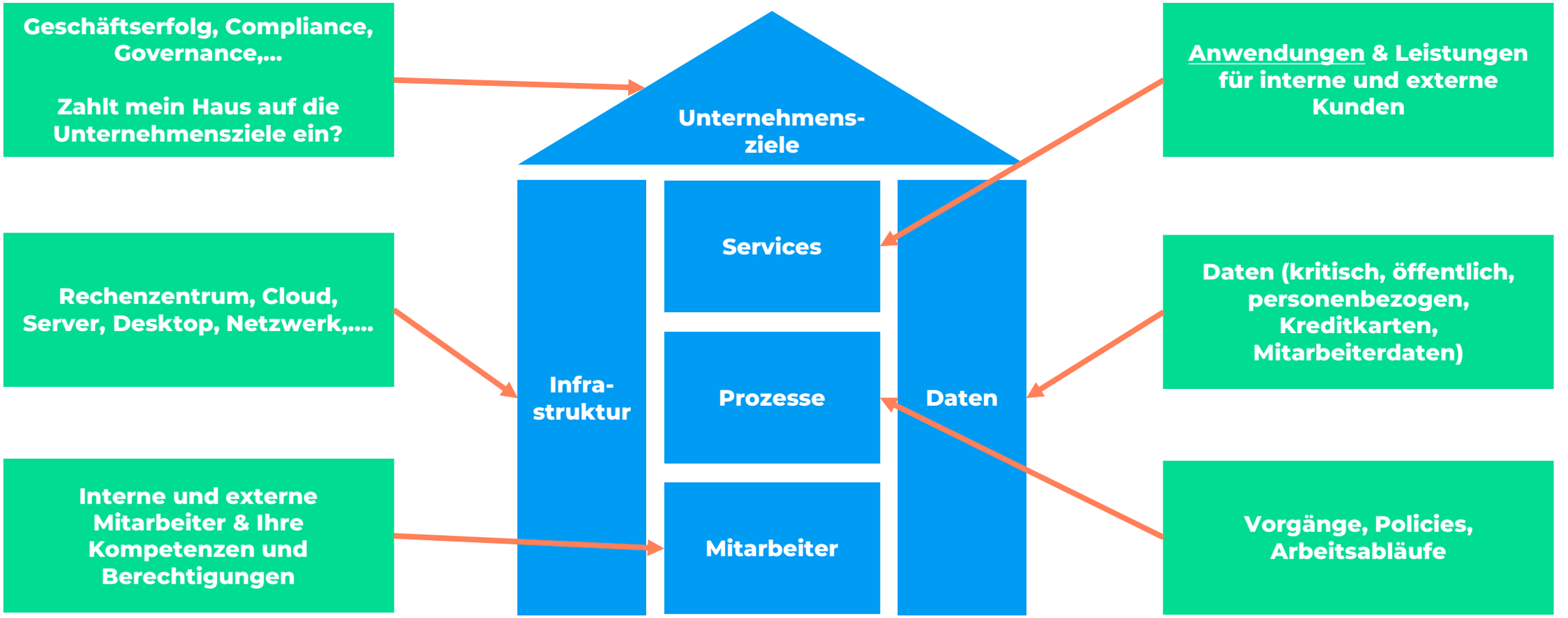
plusserver

Ihre IT als Ausgangspunkt

„Das Haus der IT“

plusserver

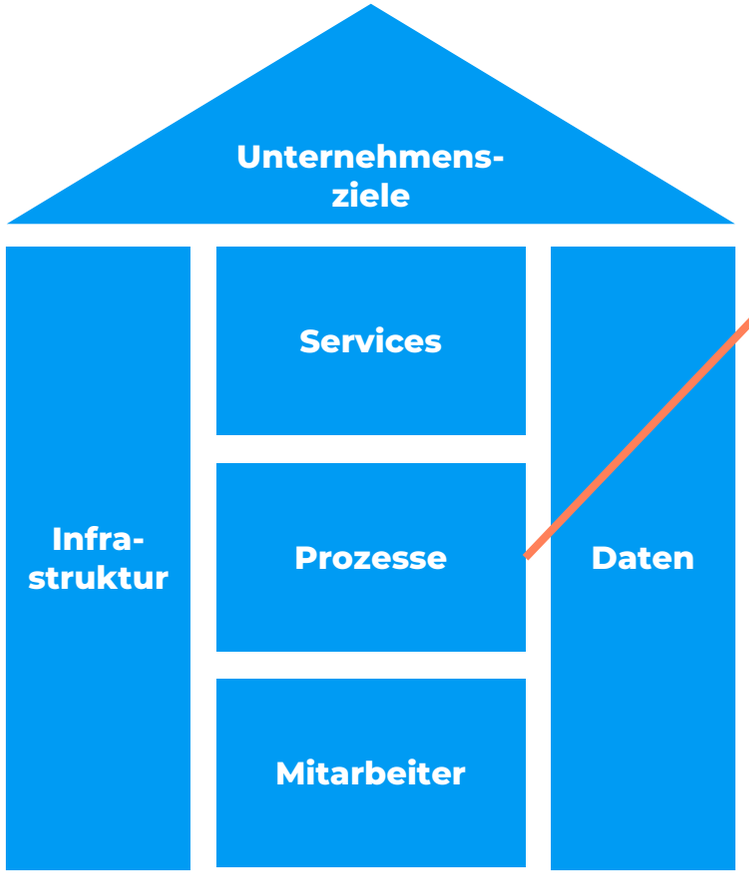
Stellen Sie sich Unternehmens-IT als ein Haus vor



plusserver

Risikoanalyse & IT-Sicherheit

Security als Prozess verstehen



Risikomanagement

+ NIS2 Assessment
+ Security Consulting

Schutzmaßnahmen

+ EDR, Security Scanner, Firewalls,
+ Workload Protection
+ DDoS-Protection
+ WAF

Security
Automation
360 Grad
Prozesse

GRC
(Governance, Risk, Compliance)

Wiederherstellung

Backup & Disaster Recovery

Transparenz

24x7 Detektion & Reaktion

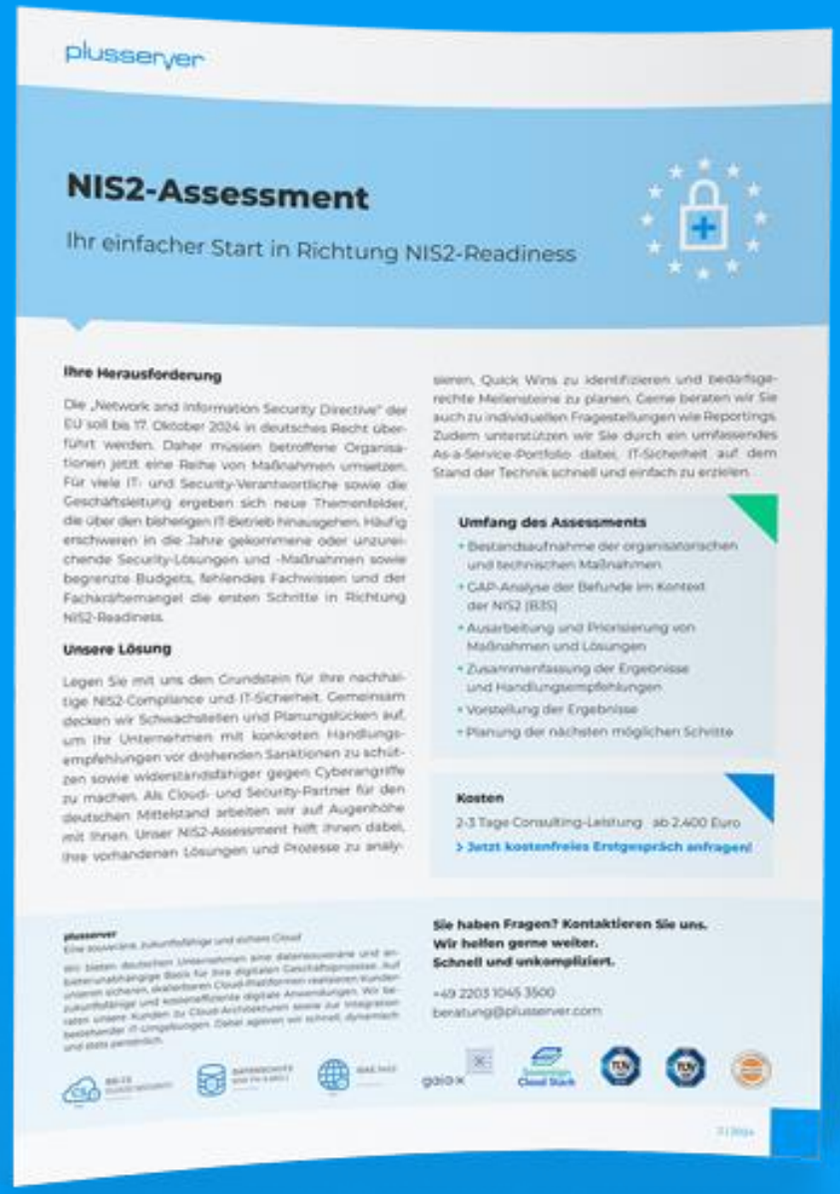
+ Security Operations Center

NIS2-Assessment

...den Einstieg finden!

+ Bestandsaufnahme der organisatorischen und technischen Maßnahmen
+ GAP-Analyse der Befunde im Kontext der NIS2 (B3S)
+ Ausarbeitung und Priorisierung von Maßnahmen und Lösungen
+ Zusammenfassung der Ergebnisse und Handlungsempfehlungen
+ Vorstellung der Ergebnisse
+ Planung der nächsten möglichen Schritte

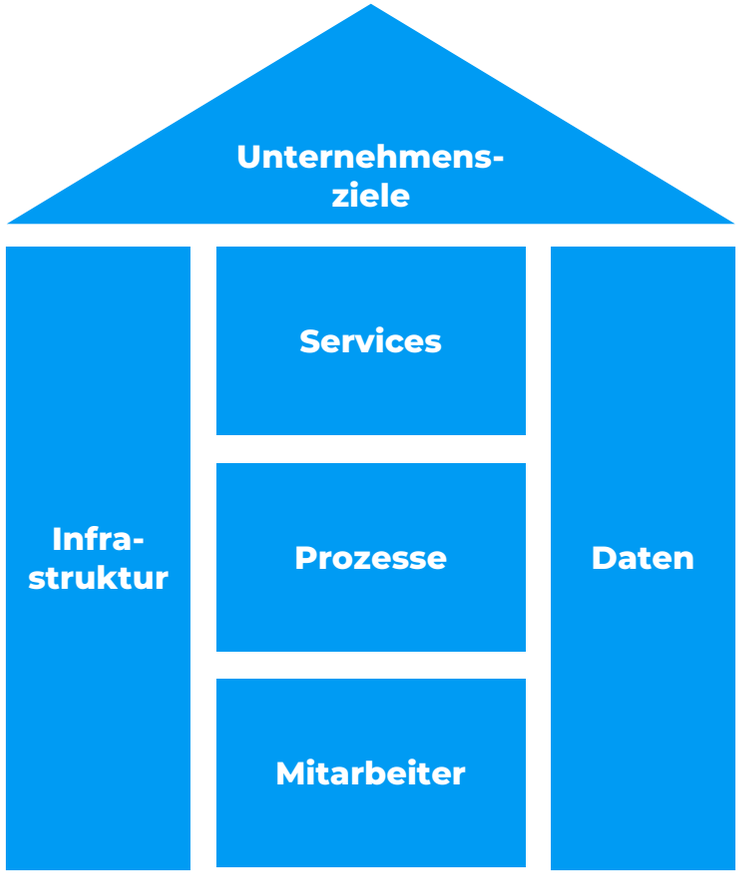
Jetzt kostenfreies Erstgespräch anfragen



plusserver

Risikobasierte Schutzmaßnahmen

Security als Prozess verstehen



Risikomanagement

+ NIS2 Assessment
+ Security Consulting

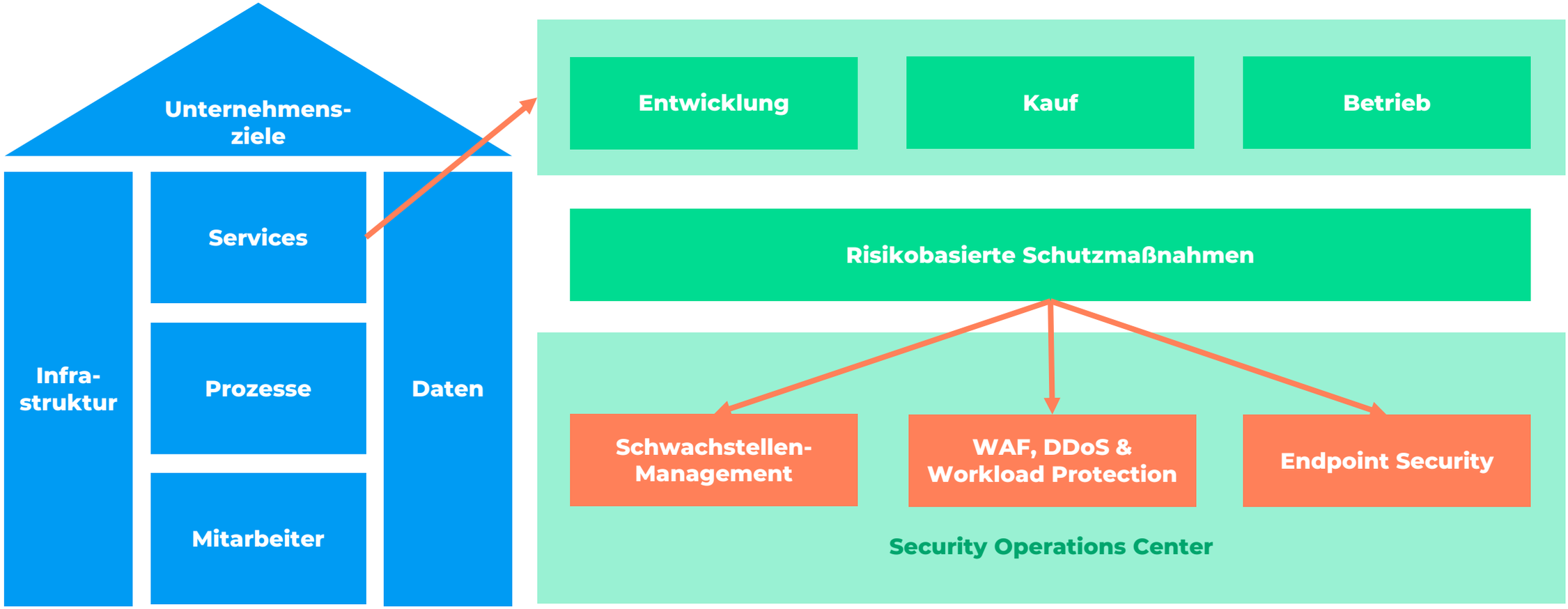
Schutzmaßnahmen

+ EDR, Security Scanner, Firewalls,
+ Workload Protection
+ DDoS-Protection
+ WAF

plusserver

Schutzmaßnahmen

Anwendungen erstellen, kaufen und betreiben



Security Scanner as a Service

Zuverlässiges Schwachstellenmanagement

Funktionsweise

+ Scannt öffentliche IPs (HTTP), kann auch interne IPs und IP-Bereiche scannen (Applikationen, OS, Peripherie)
+ Erkennung von Schwachstellen durch netzwerkbasierte Scans (IPv4 & IPv6)
+ Veränderungen im Netzwerk werden sofort sichtbar

Meine Vorteile

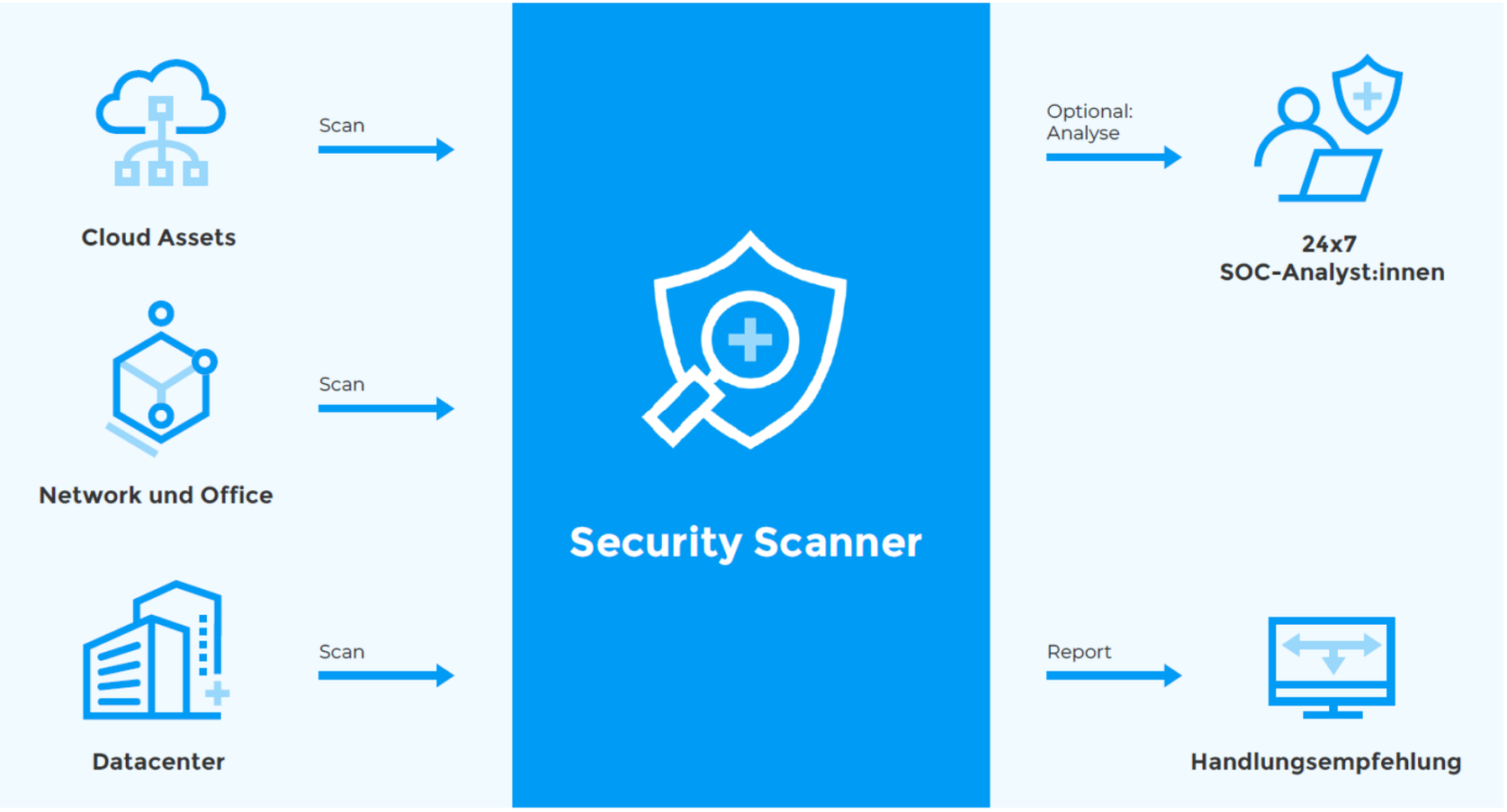
+ Steigerung der Transparenz des Security-Levels
+ Berichte über erkannte Schwachstellen -> Alarmierung
+ Self-Service-Produkt
+ 24/7 Support
+ Einbindung in Ihr oder unser Security Operations Center

Jetzt kostenfreies Demo anfragen

plusserver

Security Scanner as a Service

Einsatzmöglichkeiten & Produktdetails



plusserver

Cloud-Anwendungen von Beginn an schützen

DevSecOps, Kubernetes, Hyperscaler, ...

Entwicklung

Risikobasierte Schutzmaßnahmen?

Workload Protection as a Service

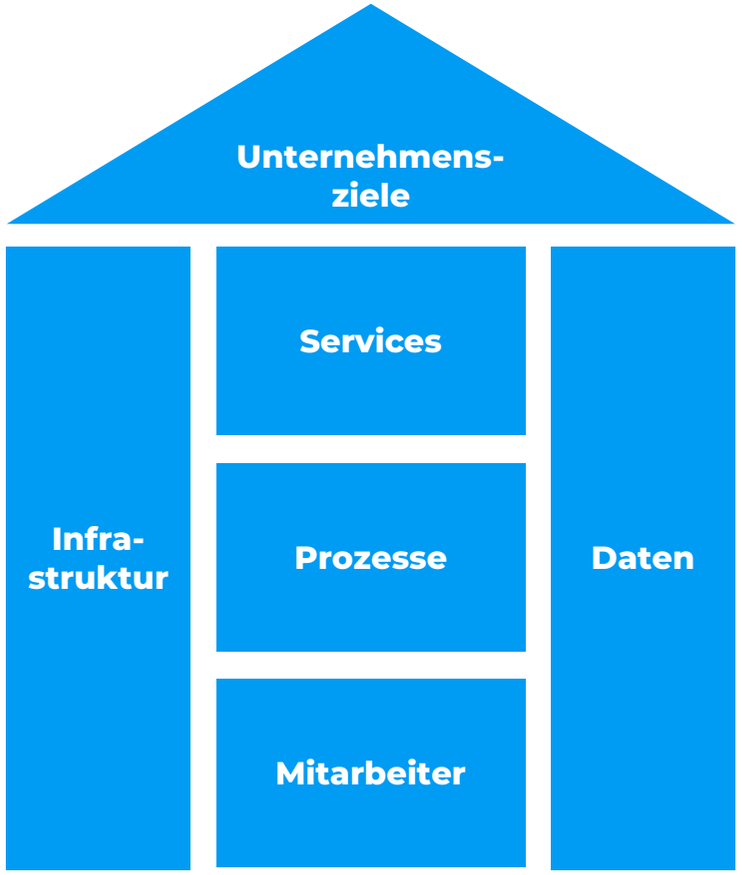
Webcast ansehen

- **DevSecOps**
  - Werkzeuge zur Implementierung von IT-Sicherheit in der Software-Entwicklung
- **Kubernetes/Container-Security**
  - Schwachstellenprüfung von Containern und Images
  - Laufzeitschutz für Prozesse und Anwendungen in Containern
  - Web Application und API Firewall zur Verhinderung von Angriffen
- **Posture Management**
  - Ganzheitliche Sicht auf Multi-Cloud-Infrastrukturen inkl. automatisierter Inventarisierung
  - Deckt Konfigurationsfehler bei den Hyperscalern auf

plusserver

Von Schutzmaßnahmen zur Bewältigung von Vorfällen

Schützen, erkennen, handeln mit Endpoint Detection & Response as a Service



Schutz an den Endpunkten des Netzwerks

Clients, Server, Cloud-OS
Mail- & Web-Malware-Schutz
Daten, Prozesse, Netzwerk

Endpoint Detection & Response

Erkennen & bewerten von Vorfällen

Erkennung von Anomalien
Überwachung von Daten, Prozessen und Netzwerkzugriffen zur Angriffs- und Malware-Erkennung

Handeln erfordert Experten

Maßnahmen ergreifen

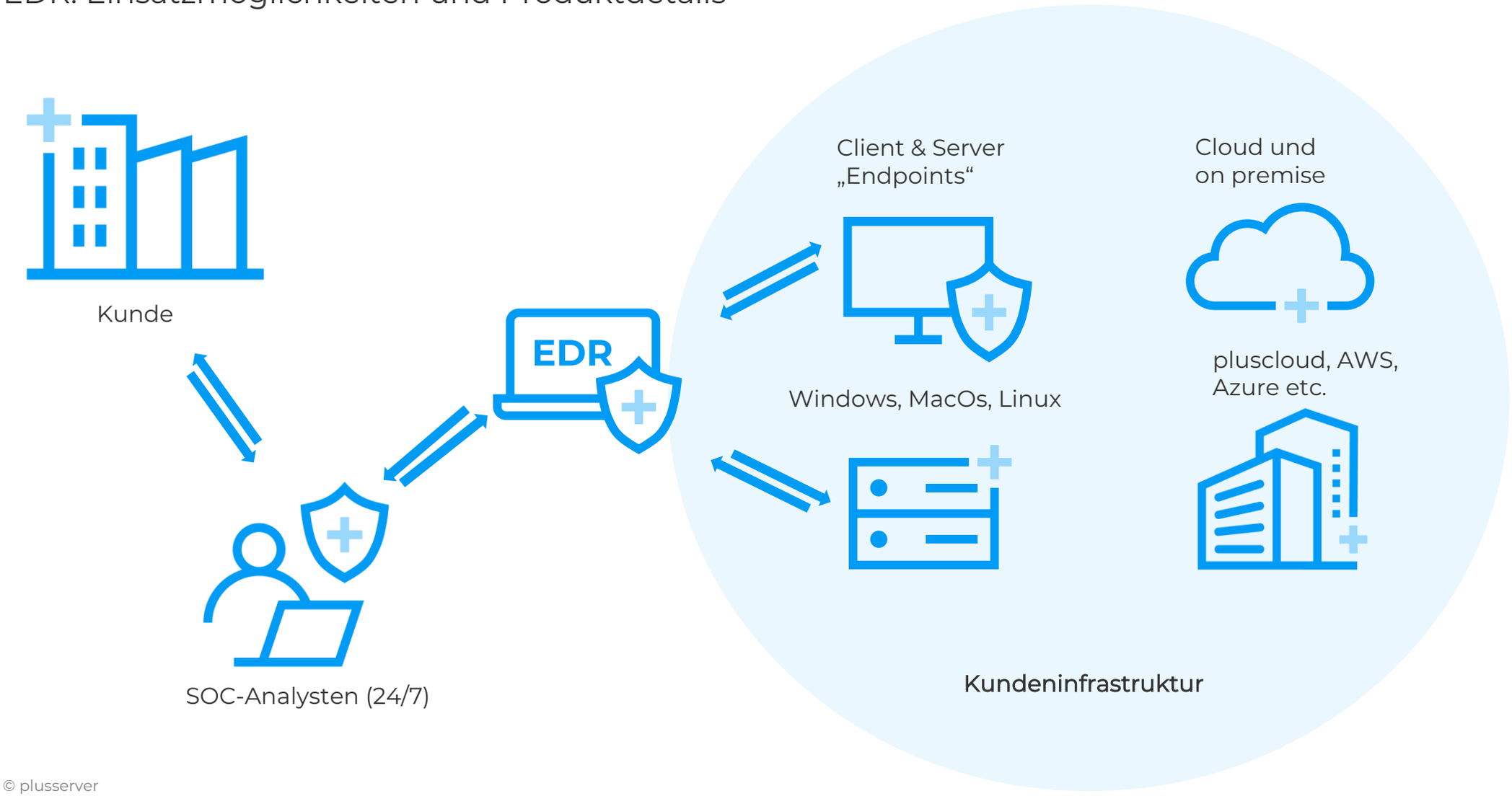
Automatische Quarantäne
... und dann?

Security Operations Center
Individuelle Maßnahmen!

plusserver

Von Schutzmaßnahmen zur Bewältigung von Vorfällen

EDR: Einsatzmöglichkeiten und Produktdetails



Endpoint Detection & Response (EDR)

Moderne Endpoint und Server Protection

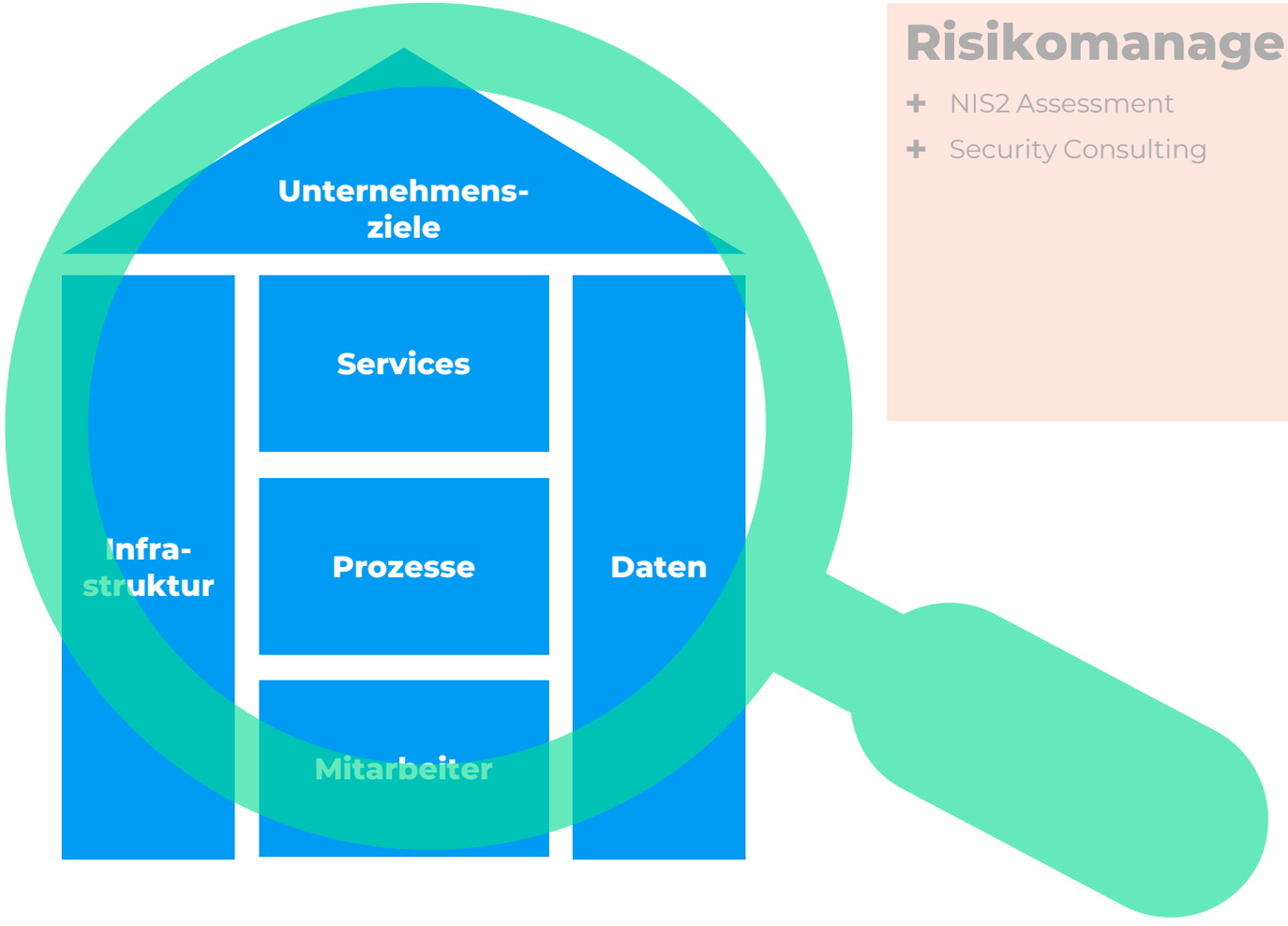
- Schutz von **Daten, Prozessen, Netzwerkverkehr auf Servern und Endpoints**
- **Abwehr** von Malware, Netzwerkangriffen, Phishing sowie Schutz des E-Mail-Clients und Browsers
- **Steigerung** des **Security Levels durch Malware und Ransomware Protection**
- Erkennung von **zielgerichteten Attacken in der Infrastruktur**
- EDRaaS als Full-Management-Produkt mit 24/7 Support
- SOC-Integration für Advanced Monitoring

Mehr zu Endpoint Detection & Response as a Service

plusserver

Bewältigung von Sicherheitsvorfällen erfordert Transparenz

Die Rolle eines Security Operations Center



Risikomanagement

+ NIS2 Assessment
+ Security Consulting

Schutzmaßnahmen

+ EDR, Security Scanner, Firewalls,
+ Workload Protection
+ DDoS-Protection
+ WAF

Transparenz

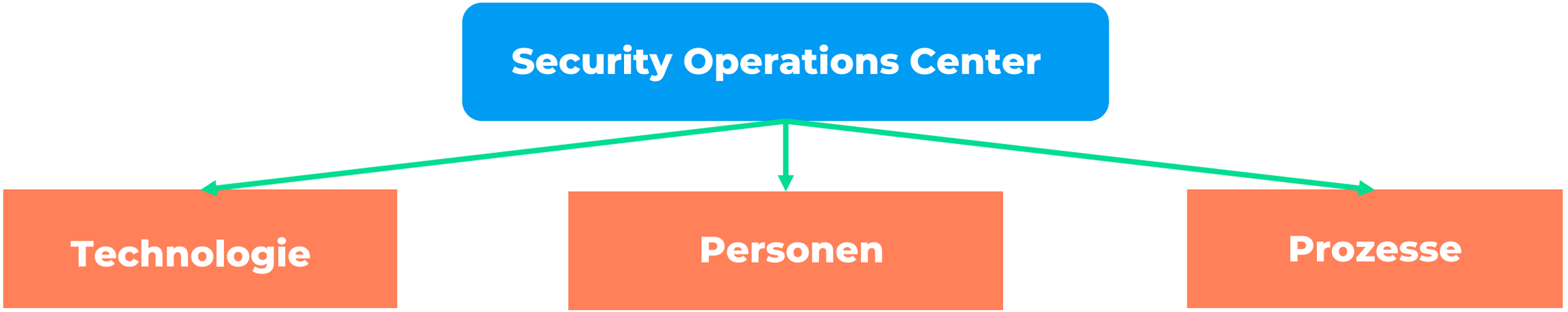
24x7 Detektion & Reaktion

+ Security Operations Center

plusserver

Was ist ein Security Operations Center (SOC)?

Ganzheitliche Abbildung der operativen Sicherheit im Unternehmen



- SIEM-Plattform
- Bereitgestellt auf pluscloud VMware (BSI-C5-Typ2-testiert)
- Threat Intelligence Feeds
- Event- & Flow-Collector

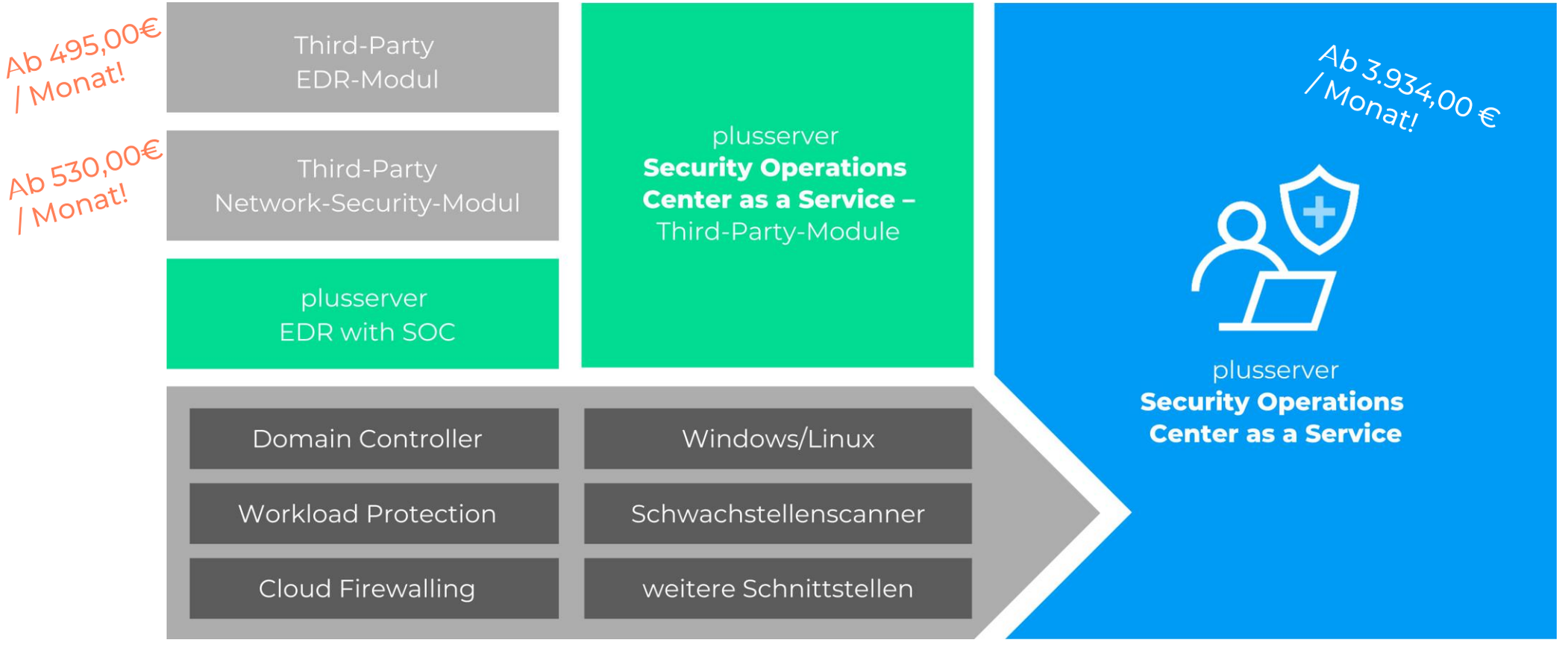
- 1st- und 2nd-Level-Analysten
- Forensik (Partner)

- Incident-Prozess
- Schwachstellen-Prozess
- SOC Board
- Use Cases

plusserver

Einfacher und schneller Einstieg – jederzeit erweiterbar

SOC mit modularem Aufbau



plusserver

SOC vs. SOC as a Service

Selber machen oder als Service beziehen?

Ihre Kosten für eigene Technik und Personal

100.000 €

SIEM-Plattform

5.000 € p. a.

Wartung

>200.000 € p. a.

Analysten-Team (min. 4-5 MA)

Kosten für das Jahr 1

>300.000 €

Kosten ab Jahr 2

>200.000 € p. a.

SOC as a Service
Mehr erfahren

Unser Angebot

plusserver SOC aaS
ab 47.000,00 € p. a.

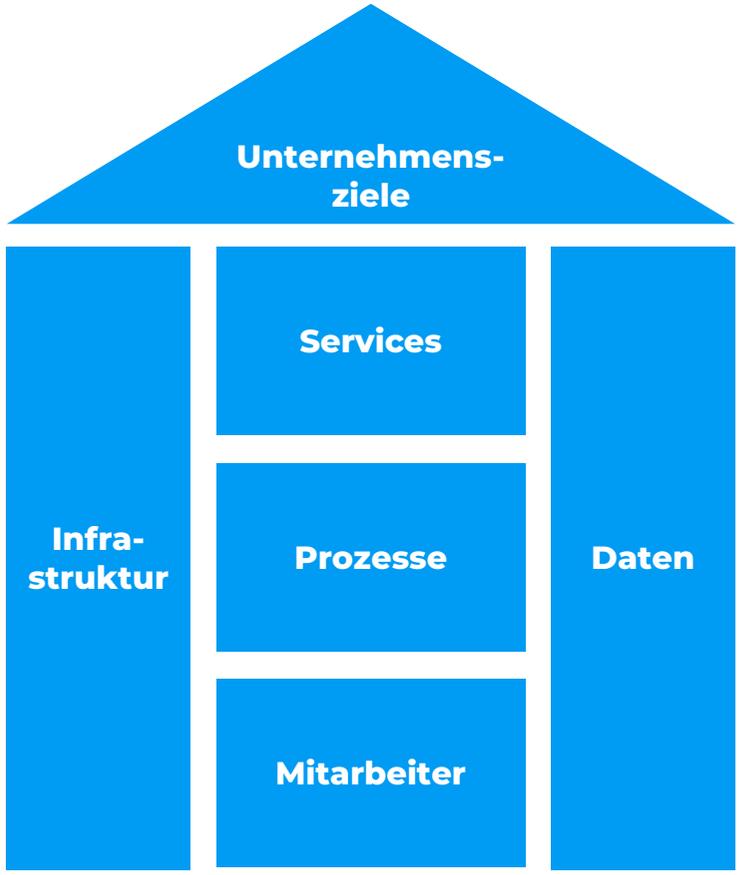
Berechnungsbeispiel:

- Unternehmen mit 600 Mitarbeitenden
- Anbindung Log-Quellen des Kunden: Windows Server, Linux Server, Firewall und EDR-Plattform
- 500 Events per Second (Standard)
- Monatliche Kosten: **3.934,00 €**

plusserver

Wiederherstellung

Handlungsfähig bleiben, wenn alle Stricke reißen



Risikomanagement

+ NIS2 Assessment
+ Security Consulting

Schutzmaßnahmen

+ EDR, Security Scanner, Firewalls,
+ Workload Protection
+ DDoS-Protection
+ WAF

Wiederherstellung

Backup & Disaster Recovery

Transparenz

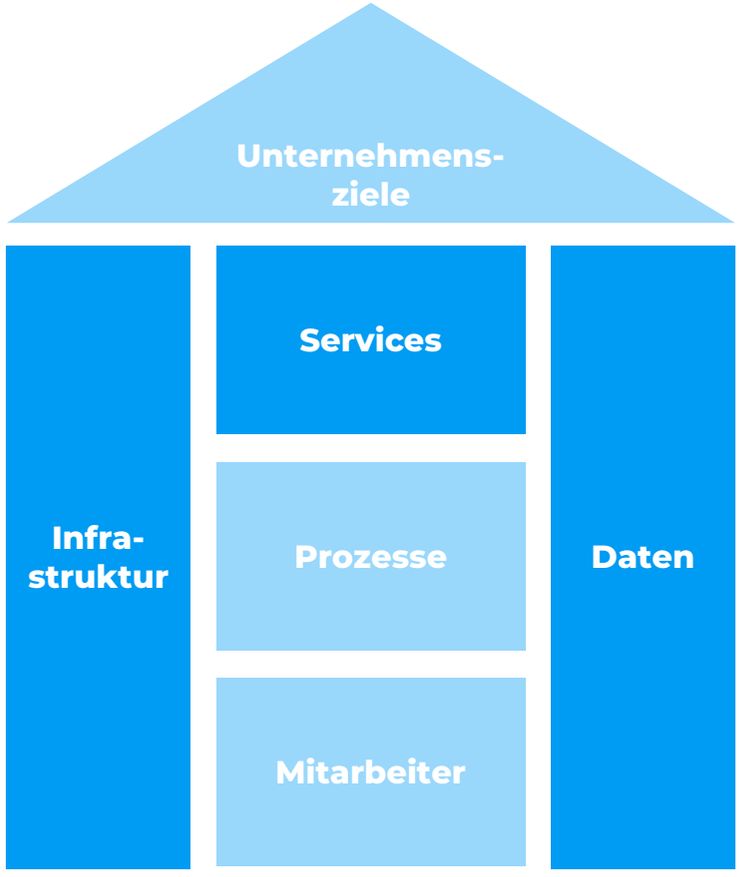
24x7 Detektion & Reaktion

+ Security Operations Center

plusserver

Backup und Disaster Recovery

Handlungsfähig bleiben, wenn alle Stricke reißen



Datenklassifizierung:
Geschäftskritische Daten müssen identifiziert und gesichert werden!

Backup ⟷ **Disaster Recovery**

Schutz vor Datenverlust:
Vollständigkeit der Daten /lückenlose Historie entscheidend?

Schutz vor Betriebsausfällen:
Schnelle Fortführung des Geschäftsbetriebes entscheidend?

Tipps:

3-2-1-Regel:
3 Kopien, 2 Medien, 1 Extern (Georedundanz)

WORM/Immutable Backups
Backups können nicht (z.B. durch Ransomware) verändert werden

Georedundanz:
BSI empfiehlt 200 km für Georedundanz (für viele Szenarien anwendbar)

plusserver

plusbackup ermöglicht Backups aller Daten aus jeder Infrastruktur

… egal, wo Ihre Primärdaten liegen

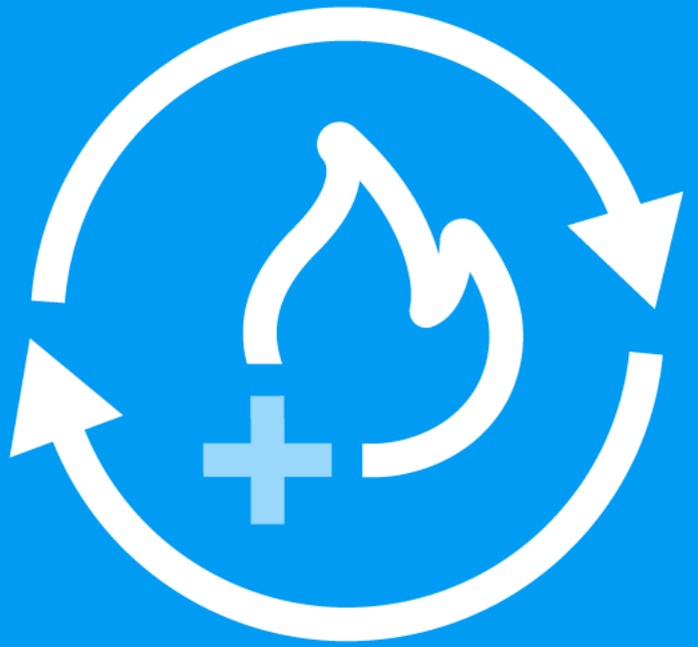
- Für Server und Workstation Clients mit Windows, Linux und MacOS
- Für Ihre Daten in beliebigen Clouds
- Sichern Sie mit Backup as a Service ganze Systeme oder Teile wie ausgewählte Verzeichnisse oder Dateien
- Basierend auf Veeam-Backup-Technologie

Disaster Recovery

+ Mit plusbackup haben Sie die Möglichkeit, Ihre Produktivumgebung (basierend auf VMware) zu replizieren und diese im Notfall in unserer pluscloud VMware wiederherzustellen.

+ Die Cloud-Umgebung wird erst im Fall der Fälle für Sie gestartet und erzeugt somit keine dauerhaften Kosten.

+ Dieses Angebot ist aufgrund unserer deutschlandweit verteilten Rechenzentren auch für Kunden mit pluscloud VMware als Primärumgebung interessant.



plusserver

Wie kann plusserver unterstützen?

Security Services, gemeinsam mit unseren Partnern

Security-Beratung/ Consulting

+ Security Consulting
+ Security Assessments
+ NIS2 Assessments
+ Pentests und Audits

Security-Lösungen

+ SOC as a Service
+ EDR as a Service
+ Schwachstellenmanagement
+ Next Gen Firewall
+ DDoS-Schutz
+ Backup/Disaster Recovery

Zertifizierte Infrastruktur

+ Standorte in DE
+ ISO 27001
+ BSI C5 (Typ-II)

Q&A

Wir helfen gerne!

plusserver

Vielen Dank für Ihre Aufmerksamkeit!

www.plusserver.com

Unsere Security-Initiative wird unterstützt von

VEEAM IBM