plusserver

SOC as a Service Sales Playbook für intern und Partner

Version 1.2, März 2024

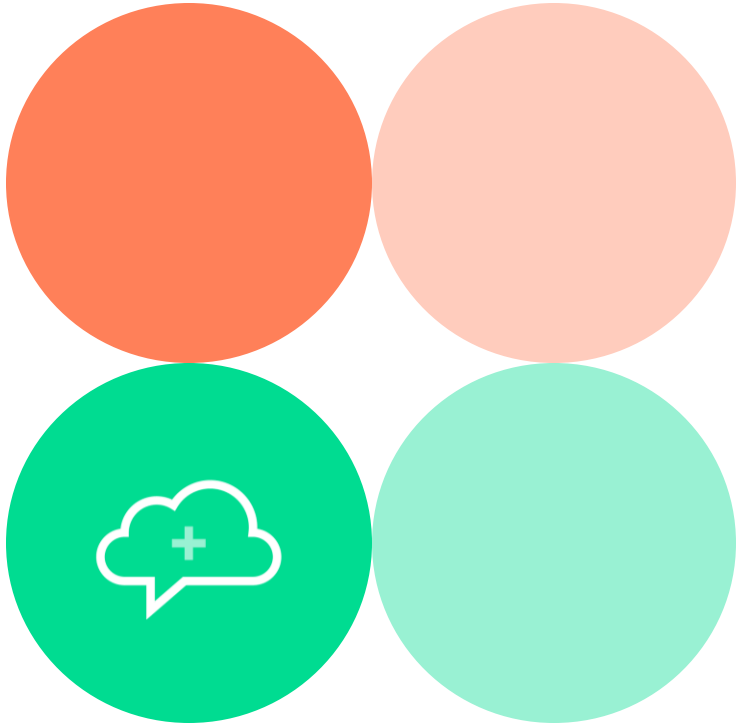
NICHT FÜR ENDKUNDEN

Was ist ein Sales Playbook?

Dieses Dokument dient der internen Benutzung bei plusserver und Partner-Unternehmen. Es enthält essenzielle Informationen zu Produkten und soll helfen, die Erstgespräche mit Kunden und Interessenten vorzubereiten.

Die Inhalte des Dokuments sind nicht zur Weiterleitung an den Kunden gedacht, dienen vielmehr dem Aufbau eigener Argumentationsketten und sollen u. a. folgende Fragen beantworten:

- Was kann das Produkt?
- Für wen ist das Produkt?
- Wie kann ich die Zielgruppe von den Vorzügen des Produkts überzeugen? Welche Argumente und Antworten helfen im Gespräch mit dem Kunden?
- Wie grenzt sich das Produkt vom Wettbewerb ab?



SOC as a Service

… für eine schnelle Vorbereitung eines Kundentermins

Unser SOC as a Service macht State-of-the-Art Security für jedes Unternehmen zugänglich. Sie benötigen kein zusätzliches Fachpersonal und können sich auf Ihre wichtigen geschäftskritischen Prozesse konzentrieren.

- Steigerung der Transparenz und Reaktionsfähigkeit im Hinblick auf Cyberattacken
- Schutz vor Ransomware und zielgerichteten Attacken
- Schutz vor Abfluss sensibler Daten
- Alarmierung und Reporting
- Managed Service durch plusserver entlastet Ihre IT
- Modulare Integration in weitere Security-Lösungen (z.B. EDR) oder eigene Infrastruktur
- Erfüllung von Compliance und Regularien (NIS2, IT-Sicherheitsgesetz 2.0, B3S, DSGVO, PCI DSS, TISAX, ISO 27001, PDSG etc.)
- Unterstützung des Business Continuity Managements im Unternehmen
- Nachweislicher Einsatz von State-of-the-Art-Security-Prozessen (z.B. bei Cyber-Versicherungen)

plusserver

Vorteile & Potenziale des SOCaaS

Unser Service für Ihre Zukunftsfähigkeit

Technologische Vorteile

- Konsolidierung und Korrelation von Logfiles und Events aus Security-Plattformen\-Lösungen
- Schnelle Einbindung von Log-Quellen durch Standards
- Zusätzliche Anbindung von Sicherheitslösungen oder Plattformen aus der Kundeninfrastruktur wie z. B. lokale Firewall, EDR oder Domain-Controller, Linux Server etc.
- State-of-the-Art und Best-Practise Use Cases auf Basis des MITRE Attack Frameworks
- SIEM-Plattform Managed Service
- Standardisiertes Onboarding

Potenziale für Kunden

- 24x7 Alarmierung und regelmäßige Reportings (inkl. Executive Summary)
- Steigerung der Transparenz und Reaktionsfähigkeit hinsichtlich Cyber-Attacken in der IT-Infrastruktur oder Cloud
- Schutz vor z. B. Ransomware oder zielgerichteten Attacken
- Kein zusätzliches Fachpersonal erforderlich
- Deutschsprachiges Analysten-Team (auch EN)
- Nachweis von State-of-the-Art Security-Tools und -Prozessen
- DSGVO-konform und CLOUD-Act-neutral
- Erfüllung von Compliance-Vorgaben (z. B. SIG 2.0)

Pricing-Modell

- Einzelne Module wählbar (auch Third-Party-Integration)
- Opex-Modell
- EPS*-Erweiterungen nach Bedarf (500 EPS enthalten)
- Standardisiertes Onboarding (einmalige Gebühr)

*Events per Second

Ausgangssituation

… von Unternehmen und öffentlichen Auftraggebern

Anforderungen von Unternehmen und öffentlichen Auftraggebern an Datenhoheit, Datensicherheit sowie Rechtsraumsicherheit rücken deutlich in den Vordergrund und dienen immer mehr als Entscheidungsgrundlage für Cloud-Infrastrukturen sowie Cloud-basierte Security.

+ **Vendor Lock-in:** Unternehmen haben den Wunsch, in die Cloud zu migrieren, sind aber durch Vendor Lock-ins und/oder externe Vorschriften geblockt, internationale Anbieter zu nutzen.
+ **Compliance:** Strenge Vorgaben gerade im Behördenbereich verlangen starken Datenschutz, lokale Datenhaltung und Transparenz bei der Auswahl einer geeigneten Lösung.
+ **Maintenance:** Unternehmen möchten sich auf ihr Geschäftsmodell konzentrieren. Der 24/7-Betrieb eines IaaS oder einer Security-Lösung bleibt oftmals außen vor und wird somit zu einem Risiko für das Unternehmen.
+ **Fehlendes Personal:** Der anhaltende Fachkräftemangel wirkt sich hierbei zusätzlich negativ aus, wenn Unternehmen und der öffentliche Sektor sich neben der Entwicklung von neuen Anwendungen auch um den Betrieb, die Wartung und die Absicherung der zugrundeliegenden Infrastruktur kümmern müssen.
+ **Kostendschungel:** Der Aufbau und die Wartung einer eigenen Infrastruktur sind mit hohen Investitions- und Wartungskosten verbunden, während intransparente Kostenübersichten bei manchen Cloud-Anbietern für Verwirrung und böse Überraschungen auf der Rechnung sorgen können.
+ **Auf dem Laufenden bleiben:** Unternehmen haben zwar den Wunsch, technologisch auf dem neuesten Stand zu sein. Den Überblick über die neuesten Updates und notwendigen Patches zu behalten, bleibt im Tagesgeschäft jedoch oft auf der Strecke und kann Risiken für den Betrieb bedeuten.

plusserver

Unternehmerische Herausforderungen...

und Chancen für unser Angebot

Security-Verantwortliche müssen sich gleichzeitig mit einer stetig steigenden Bedrohungslage (u. a. zunehmende Anzahl von Ransomware-Attacken) sowie neuen digitalen Geschäftsmodellen auseinandersetzen. Zusätzlich haben sie die Aufgabe, die weltweit neuesten Bedrohungen jederzeit zu beobachten und in Notfallsituationen zu reagieren, damit eine Cyber-Abwehrstrategie rund um die Uhr in vollem Umfang gewährleistet ist.

Hinzu kommen neue Sicherheitsgesetze (z. B. NIS2, SIG 2.0) oder die Datenschutzgrundverordnung (DSGVO). All diese Anforderungen an eine zeitgemäße Security-Strategie sind vor allem für kleinere und mittlere Unternehmen oder die öffentliche Verwaltung intern kaum zu bewältigen. Gleichzeitig stehen sie vor der Herausforderung, entsprechendes Personal zu finden, da Experten gerade im Bereich Security stark nachgefragt sind.

Potenzielle Kunden haben daher folgende Needs:

+ Bessere Detektions- und Reaktionsfähigkeit zur frühzeitigen Erkennung von Cyber-Angriffen (z. B. zielgerichteten Attacken oder Ransomware)
+ Höhere Transparenz über das Sicherheitslevel im Unternehmen
+ Erfüllung von Compliance-Vorgaben (NIS2, IT-Sicherheitsgesetz 2.0, B3S, DSGVO, PCI-DSS, TISAX, ISO 27001, PDSG etc.)
+ Reduzierung finanzieller Schäden infolge von Cyber-Angriffen
+ ... und dies alles ohne große Investitionen oder sonstige Einstiegshürden

Wir bieten eine Lösung

mit einem SOC as a Service

Das Produkt Security Operations Center as a Service, kurz SOCaaS, ist ein Kernelement zur Steigerung der Detektion & Reaktion sowie der Transparenz über das Schutzniveau im Unternehmen, Korrelation von Events und zur 24x7 Analyse, um Risiken und Angriffe in der IT-Infrastrukturumgebung oder Cloud zu erkennen und zu verhindern.

Anstatt das entsprechende Personal zur Analyse von Angriffen selbst beschäftigen zu müssen, können Unternehmen den Service einfach nach Bedarf buchen und profitieren dadurch von Kostenersparnissen und einem umfassenden Schutz sowohl für Infrastruktur bei plusserver, als auch für ihre eigenen Dritt-Systeme.

Diese können ebenfalls an unser SOCaaS angebunden und überwacht werden. Auch heterogene Systeme lassen sich so schützen, während der Kunde in eigener Geschwindigkeit seine IT modernisiert.

Werkzeugkasten vs. Handwerkerservice

Was ist ein SOC und was ist eine SIEM-Lösung?

Einsatz einer SIEM-Lösung (ohne SOC-Service)

+ Security-Lösungen wie z. B. eine Firewall werden an das SIEM-System angebunden.
+ Events werden durch die SIEM-Lösung erzeugt und der Kunde alarmiert. Es ist eine reine Detektion und Anzeige von einem Security-Vorfall.
+ Der Kunde muss eigenständig einschätzen, ob/welche Art von Cyber-Attacke vorliegt sowie nächste Schritte eigenständig ableiten!

Eine SIEM-Plattform ist die Bereitstellung eines „**Werkzeugkastens**“

SOC as a Service von plusserver

+ 24/7 Analyse-Service zur Bewertung der Events aus der SIEM-Plattform.
+ Bereitstellung der technischen SIEM-Lösung, des menschlichen Know-hows der Analysten, Prozessen sowie Use Cases zur effektiven Erkennung von Cyber-Attacken.
+ Proaktive Alarmierung, Handlungsempfehlungen sowie nächste Schritte für unsere Kunden.

Wir stellen unseren Kunden einen „**Handwerkerservice**“ bereit!

Technologische Basis

Unser SIEM-Plattformpartner IBM

Für unser Managed SOC setzen wir beim SIEM auf den Industriestandard von IBM QRadar. Die sicherheitsrelevanten Daten werden dabei in unserer eigenen datensouveränen sowie BSI-C5-testierten Cloud-Infrastruktur (pluscloud VMware) verarbeitet.

+ Plattformanbieter: IBM QRadar (zum 13. Mal in Folge als Leader im Gartner Magic Quadrant for SIEM geführt)
+ Sensorik: Security-Lösungen sowie Log-Collectoren - auch beim Kunden vor Ort (virtuelle Appliance)
+ Datenquellen: EDR, Windows, Linux, Firewall, Flow-Collectoren
+ Anbindung der Datenquellen: Auf Basis des IBM-Standards. Individuelle Use Cases auf Anfrage.

IBM Silver Partner

Gartner Magic Quadrant for Security and Information Management 2023

plusserver

Schutz der IT-Infrastruktur

Die drei Bausteine eines Security Operations Center

- SIEM-Plattform
- Bereitgestellt auf pluscloud VMware

  (BSI-C5-Typ2-testiert)
- Logfile-Kollektoren

- 1st- und 2nd-Level-Analyst:innen
- Partner (Forensik)

- SOC Board
- Use Cases
- Security-Prozesse

Auch eigene Datenquellen möglich

3rd-Party-Lösungen mit dem plusserver SOC

SOC as a Service mit Datenquellen von plusserver

+ Kunden aus dem SMB-Umfeld sind die Zielgruppe für dieses Modell
+ Herstellung eines Grundschutzes durch Anbindung der wichtigsten Datenquellen (hohe Standardisierung, geringer Einstiegspreis)
+ Geeignet für: Kunden in der Cloud von plusserver

Datenquellen		
EDR · EDR as a Service Advcanced (ESET)	Firewall · Virtual Cloud Firewall (FortiNet)	OS · Windows, Linux

SOC as a Service mit Datenquellen der Kunden & Partner (individuell)

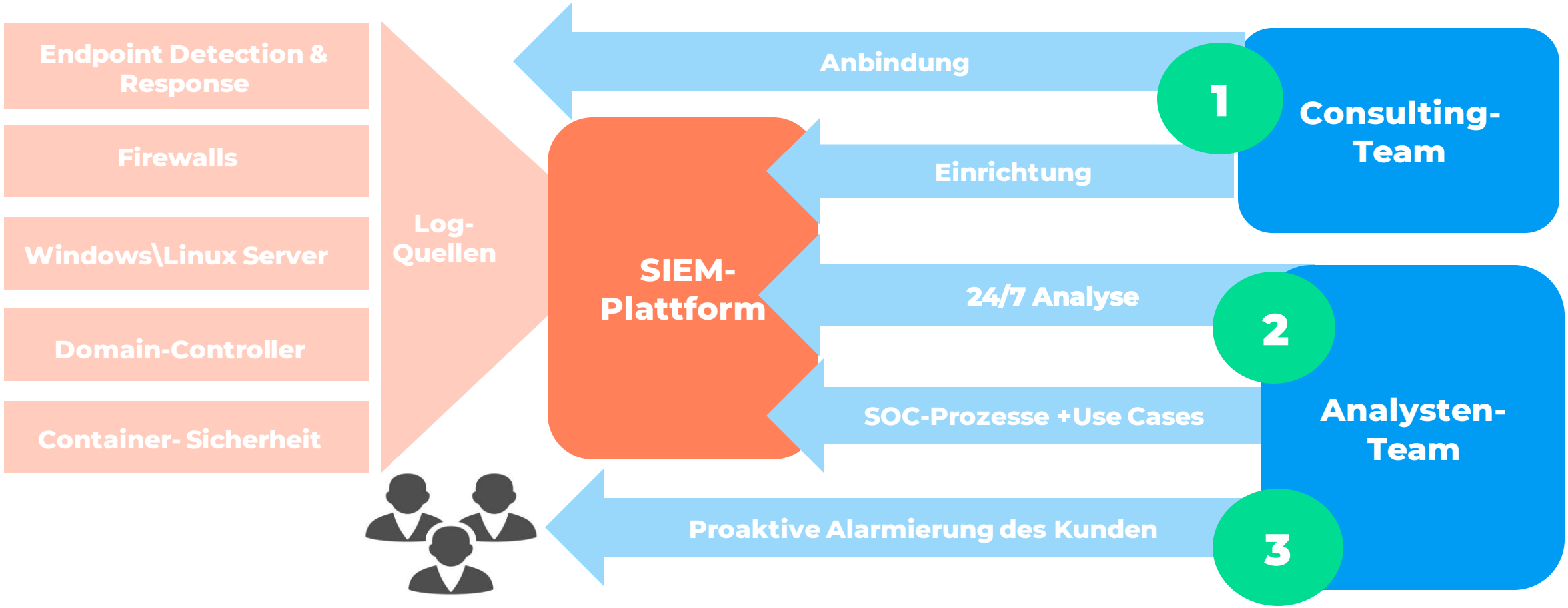
+ Kunden aus dem SMB-Umfeld sind die Zielgruppe für dieses Modell
+ Herstellung eines Grundschutzes durch Anbindung der wichtigsten Datenquellen (hohe Standardisierung, geringer Einstiegspreis)
+ Geeignet für: Kunden & Partner, die vorhande Datenquellen einbinden möchten oder außerhalb der Infrastruktur bei plusserver

Datenquellen		
EDR · Individuell	Firewall · Individuell	OS · Windows, Linux

plusserver

Schutz der IT-Infrastruktur des Kunden\Partners

Einsatzmöglichkeiten & Servicebeschreibung



Log-Quellen des Kunden oder von plusserver

plusserver SOCaaS-Servicemodule

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

=

Kosten für das Jahr 1

>300.000 €

Kosten ab Jahr 2

>200.000 € p. a.

Unser Angebot

plusserver SOC aaS für den Mittelstand

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: **3.930,00 €**

plusserver

Standardisiertes Onboarding

für einen reibungslosen Start

Das Onboarding dauert ca. 6 Tage und wird mit einmalig 7.500 Euro berechnet.

Individuelle Anpassungen können nach Rücksprache geplant und kostenpflichtig umgesetzt werden.

Kick-off-Meeting mit dem Kunden
Erstellung eines kundespezifischen Onboarding-Plans und Konzept (nach Standard)
Vorbereitende Tätigkeiten in der SIEM-Plattform
Aufbau Regelwerk nach aktuellem Best-Practice Standard (Detection & Prevention)
Implementierung und Aktivierung der Standardisierten Use-Cases (MITRE ATT&CK)
Definition von Prozessen mit dem Kunden
Early go live gemeinsam mit dem Kunden
Training und Tuning
Finale Dokumentation und Übergaben

plusserver

Fragestellungen von Entscheider:innen

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …		… weitere wesentliche Mehrwerte	
Wie erreiche ich mehr Transparenz über meine IT-Infrastruktur, um Cyber-Attacken frühzeitig zu bemerken und nachhaltig und angemessen zu reagieren?	+ Durch die gezielte Anbindung von Log-Quellen hat die SIEM-Plattform die Möglichkeit, Abhängigkeiten zu erkennen und Events zu generieren. + Die SOC-Analysten können auf Basis dieser Informationen erkennen, ob ein Cyber-Angriff erfolgt ist und Handlungsempfehlungen ausprechen.	**Entlastung von IT-Mitarbeitenden**	✓ Ein Security-System aufzusetzen und zu verwalten, braucht nicht nur das entsprechende Fachwissen, sondern ist auch arbeitsintensiv. IT-Abteilungen sind oft bereits mit der Maintenance von Systemen ohne den Security-Layer aus- oder sogar überlastet. ✓ Durch einen Security-Service wird die Verantwortung und operative Arbeit für die Aktualität der Plattform bis hin zur Analyse für Events an den Anbieter abgegeben.
Bekomme ich schnellstmöglich passendes Fachpersonal wie z. B. Consultants und SOC-Analysten?	+ Vielen Unternehmen im Mittelstand fehlt das nötige Personal, um ein SOC zu betreiben. + Beim Einsatz des SOCaaS ist kein eigenes zusätzliches Fachpersonal erforderlich, da plusserver die nötige Expertise zentral bereitstellt.	**Hilfe ohne Sprachbarriere und Zeitzonen-probleme**	✓ Durch deutschen 24/7 Support gibt es keine Missverständnisse. Für internationale Kunden bietet plusserver schnelle Hilfe auf Englisch. ✓ Bei ausgelagerten Support-Zentren in anderen Ländern, oft auf anderen Kontinenten, gibt es oft nicht nur Sprachprobleme. Durch die unterschiedlichen Zeitzonen kann es länger dauern, bis Hilfe vor Ort organisiert werden kann.

plusserver

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …		… weitere wesentliche Mehrwerte	
Wie kann ich meine unternehmenskritischen und sensiblen Informationen bestmöglich schützen?	+ Es ist wichtig, seine eigenen Unternehmensrisiken und Schutzbedarfe zu kennen und auf dieser Basis eine nachhaltige Security Strategie zu entwickeln. + Ein Kernelement ist der Einsatz eines SOC, um Transparenz über aktuelle Sicherheitslevel zu erhalten und mit dem nötigen Know-how auf kritische Situationen angemessen zu reagieren.	**Fachkräftemangel**	✓ Unternehmen sind händeringend auf der Suche nach passendem Fachpersonal. Security-Experten sind unter den IT-Spezialisten sogar noch gefragter. Um das eigene Security-Level nicht durch fehlendes Know-how/Personal zu riskieren, empfiehlt sich der Einsatz von Security-As-a-Service-Leistungen. ✓ Hier liefert der Anbieter das entsprechende Expertenwissen und das Unternehmen spart sich sowohl das Recruiting als auch die Bindung von Spezialisten.
Wie kann ich meine Investitionen für ein Security Operations Center (SOC) besser planen?	+ Neben dem Fachpersonal benötigt es auch Erfahrung im Aufbau und Betrieb einer SIEM-Plattform sowie die gezielte Definition von Use-Cases (z. B:. MITRE Attack Framework) oder Prozessen zum SOC-Betrieb. + Jedoch entfällt die Sorge um fehlendes Personal und Know-how mit dem SOC as a Service, da alle Leistungen zentral durch plusserver bereitgestellt werden.	**Security nach Augenmaß – nicht einfach „ganz oder gar nicht“**	✓ Unternehmen werden da abgeholt, wo sie sich auf ihrer Digitalisierungsreise gerade befinden. ✓ Ob schrittweise Legacy-Modernisierung oder Lift&Shift, durch die modulare Bauweise unserer Security- sowie weiterer Angebote können Unternehmen sich ihr System, begleitet durch unsere Beratung, so zusammenstellen, wie sie es brauchen. Made to fit, mit Raum für individuelle Anpassungen. Nicht ein Standard für alles.

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …	… weitere wesentliche Mehrwerte
Wie krieg ich meine alte IT-Landschaft gesichert, während wir modernisieren? + In der IT-Modernisierung ist es essenziell, die bestehende Infrastruktur gemeinsam mit der neuen (z. B. Cloud) abzusichern. + Wird ein SOC eingesetzt, sollten beide Welten mit entsprechender Sensorik (z. B. Firewall oder Anti-Virus) ausgestattet werden, um im SOC die nötigen sicherheitsrelevanten Informationen zu erhalten.	**Schutz vor Compliance-Strafen** ✓ Wenn es zu Datenvorfällen gekommen ist, müssen Unternehmen nachweisen, dass sie über einen ausreichend großen Schutz verfügt haben. ✓ Ist der Nachweis erfolgreich, können sie vorgeschriebenen Strafen entgehen, wie z. B. 4 % des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr oder bis zu 20 Mio. Euro bei DSGVO-Verstößen. Andere Richtlinien sind z.B. SIG2.0
Wie kann ich meine Investitionen für ein Security Operations Center (SOC) besser planen? + plusserver bietet hier ein vorteilhaftes As-a-Service-Modell und eine transparente Preisstruktur. + Durch ein Opex-Modell können Investitionen schneller und einfacher geplant werden. Der eigene Betrieb eines SOCs ist mit deutlich mehr variablen Kosten verbunden.	**Mehr Transparenz auch in heterogene Systeme** ✓ Durch die Anbindung von Sensorik wie u.a. ein EDR, Firewall und andere Systemkomponenten in einem SIEM erhalten Unternehmen zum einen eine Übersicht ihrer Logquellen ihrer kritischen Infrastrukturen und sichern gleichzeitig den Informationsfluss zu den Experten im SOC. ✓ Auf dieser Basis erfolgt die Gefahren-Einschätzung und Ableitung von Handlungsempfehlungen.

plusserver

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …	… weitere wesentliche Mehrwerte
Erfülle ich mit meiner Cyber-Abwehrstrategie neue Compliance-Vorgaben wie z. B. NIS2?	**Versicherungs-schutz**
+ Aktuelle Regularien schreiben Security-Lösungen auf dem Stand der Technik vor. Viele der Anforderungen lassen sich mit einem SOC erfüllen,	✓ Um sich gegen Cyberattacken versichern zu können, muss ein umfangreicher Schutz bestehen. ✓ Ein State-of-the-Art-Security-System ist dafür Voraussetzung. Ein SOC zum Schutz der Infrastruktur oder Cloud ist dabei ein hilfreiches Element. ✓ Moderne Cybersecurity-Versicherungen prüfen einen entsprechenden Nachweis über solche Security-Strategien mit entsprechenden Komponenten als Teil des Vertriebsprozesses.
Wie können unsere finanziellen Risiken, ausgelöst durch Cyber-Kriminalität, reduziert werden?	**SOCaaS ist Security als Abo**
+ Cyberangriffe können mit einem SOC frühzeitig erkannt und notwendige Schritte zur Abwehr oder Isolation eingeleitet werden. + Im Falle eines erfolgreichen Angriffs kann zusätzlich die Forensik unterstützt sowie der Schadensumfang einfacher ermittelt werden.	✓ Der Aufbau eines eigenen SOC bedeutet für Unternehmen ein hohen Kosten- und Personalaufwand (Einstiegs- und laufende Kosten). ✓ Mit einem SOCaaS entfallen diese Posten: State-of-the-Art-Technik und aktuellstes Know-how zu Security-Risiken werden zu einem fest kalkulierbaren Preis geliefert und können bei Bedarf auch skaliert werden.

Mehrwerte für Partner

Wie können Partner die Lösungen anbieten und eigene Services erbringen?

+ **Bereitstellung und Betrieb des Event- und Flow-Collectors** in der Infrastruktur des Kunden
+ **Anbindung von Datenquellen** aus der Infrastruktur des Kunden an den Event- und Flow-Collector
+ **Administration von Datenquellen/Use Cases** (z.B. EDR-Plattform, Firewall) und Integration gemeinsam mit dem SOC in das SIEM-System
+ **Eigenständiges Abbilden des Incident-Managements** – der Betrieb des SIEM-Systems verbleibt in der Verantwortung von plusserver

Sprechen Sie uns an

Wir unterstützen Sie gerne bei Ihren Kundenprojekten!

Melden Sie sich einfach bei unserem Channel-Team, um Ihre Projekte und Ideen mit uns zu besprechen. Sie haben Fragen zu unseren Produkten oder wollen Ihr Feedback mit uns teilen? Wir freuen uns über Ihre Nachricht.

Kontaktieren Sie uns jederzeit unter:

Tel.: +49 2203 1045 3500

Mail: partner.sales@plusserver.com