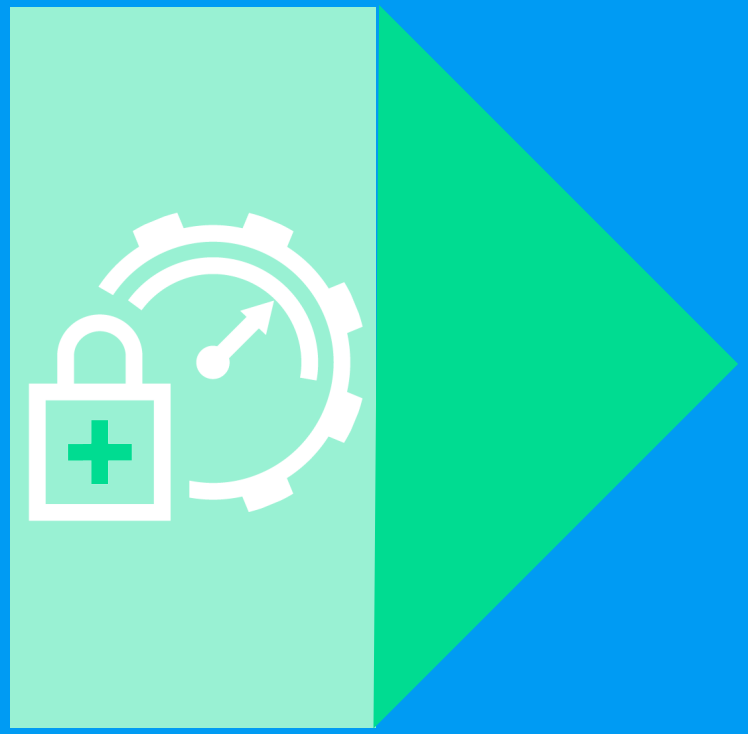
Workload Protection Sales Playbook für intern und Partner

Version 1.2, März 2024

NICHT FÜR ENDKUNDEN

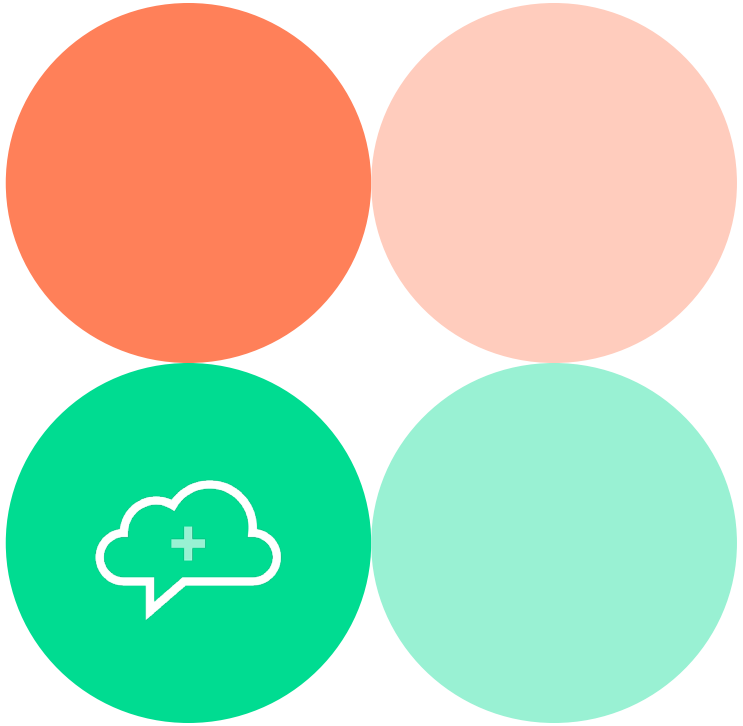


Was ist ein Sales Playbook?

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?



Workload Protection

... für eine schnelle Vorbereitung eines Kundentermins.

- Ganzheitliche Sicht auf Multi-Cloud-Infrastrukturen (Niemand kann schützen, was er nicht sieht.)
- Automatisierte Inventarisierung von Cloud-Ressourcen
- Erkennen und Blockieren von Angriffen auf Container, Web-Applikationen oder Hyper-scaler-Ressourcen
- Benchmarks nach Industrie-Standards (CIS, NIST, PCI DSS etc.)
- Risikomanagement zur Priorisierung von Bedrohungen
- Netzwerksicherheit durch Einsicht in Datenflüsse über Container- und Cloud-Umgebungen inkl. Einstellen von Firewallregeln (herstellerunabhängig)
- Meldung von sicherheitsrelevanten Ereignissen über diverse Schnittstellen (E-Mail, SMS, Syslog, SIEM)
- Plattformbetrieb und Onboarding durch plusserver
- Deutschsprachiger 24/7 Support
- Integration in ein SOC möglich (plusserver oder eigenes)
- Anwendbar z. B. auf der pluscloud open, plusserver Kubernetes Engine (PSKE), AWS, Azure

Vorteile & Potenziale

Unser Service für Ihre Zukunftsfähigkeit

Technologische Vorteile

- Inventarisierung von Ressourcen im Kubernetes-Cluster
- Prüfungen von Containern, Container Images & Container Registries auf Schwachstellen, Malware oder Anmeldedatenlecks
- Laufzeitschutz (Runtime Protection) von Prozessen und Anwendungen in Containern
- DevSecOps: Prüfung von Softwarecode
- Applikations- und API-Sicherheit
- Zentrales Dashboard für Alarmierung und Reporting
- Benachrichtigung über sicherheitsrelevante Ereignisse mittels diverser Schnittstellen (E-Mail, SNS, Syslog, SIEM)
- plusserver-SOC-Integration (auf Anfrage)

Potenziale für Kunden

- Schutz der plusserver Kubernetes Engine PSKE (Produkt-Add-on)
- Transparenz über die Sicherheit Ihrer Multi-Cloud sowie Cloud-nativen Anwendungen
- Erfüllung von Compliance & Regularien in Multi-Cloud- Umgebungen
- Plattform-Service, nutzbar auch ohne zusätzliches Fachpersonal
- Deutschsprachiger 24/7 Support
- Standardisiertes Onboarding und Bereitstellung der Client-Pakete, begleitet durch Consulting
- Erfüllung von Compliance-Vorgaben in der Multi-Cloud- Umgebung

Pricing-Modell

- Assetbasierte Lizenzierung (nach Bedarf und Nutzung, pro Monat)
- Opex-Modell
- Standardisiertes Onboarding (einmalige Gebühr)

Technische Kombinationsmöglichkeiten der pluscloud open

... mit anderen plusserver-Produkten

Security & Storage

Security

- EDR as a Service
- SOC as a Service
- Security Scanner
- DDoS-Schutz
- Web Application Firewall

Storage

- S3 Storage / Object Storage
- Network Storage

Backup & Cloud

Backup

- Backup as a Service

Cloud

- pluscloud open
- pluscloud VMware
- Dedicated Server
- AWS, GCP, Azure

Datenbanken & Container

Datenbanken

- MariaDB as a Service
- MySQL as a Service
- PostgreSQL as a Service

Container

- plusserver Kubernetes Engine

Ausgangssituation

… von Unternehmen und öffentlichen Auftraggebern

Der Einsatz von Multi-Cloud- sowie Container-Technologie ist für die Digitalisierung ein bedeutender Schritt, fordert aber ein generelles Umdenken.

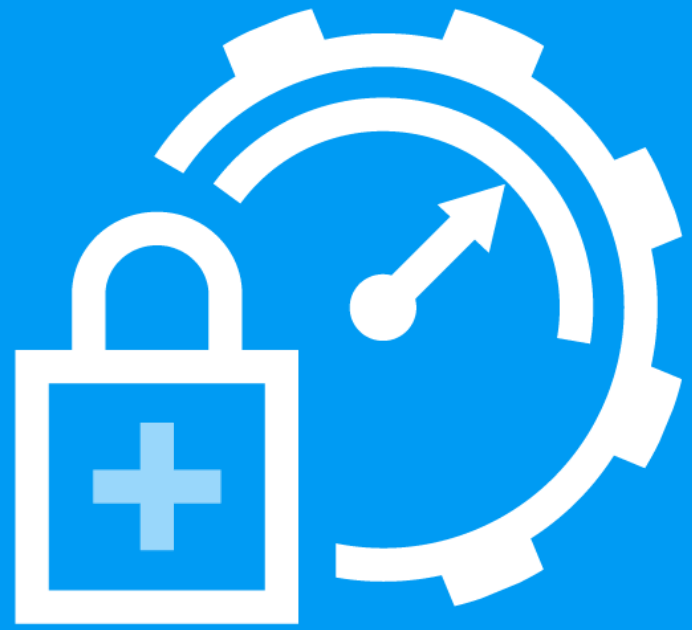
Security-Verantwortliche stehen vor der Herausforderung, vor dem Hintergrund einer steigenden Bedrohungslage im Kontext der Digitalisierung die richtigen Entscheidungen zur Absicherung von Multi-Cloud-Umgebungen abzuleiten. Beispielsweise ist es unabdingbar, Konfigurationsprobleme in einer Multi-Cloud-Umgebung schnell aufzudecken und zu beseitigen. Mit dem Einsatz von z. B. Container-Plattformen wird ein Schutz zur Absicherung von East-West Traffic (Traffic innerhalb eines Firmennetzwerks/Datacenters) benötigt.

Die Lösung liefert plusserver

mit Workload Protection as a Service

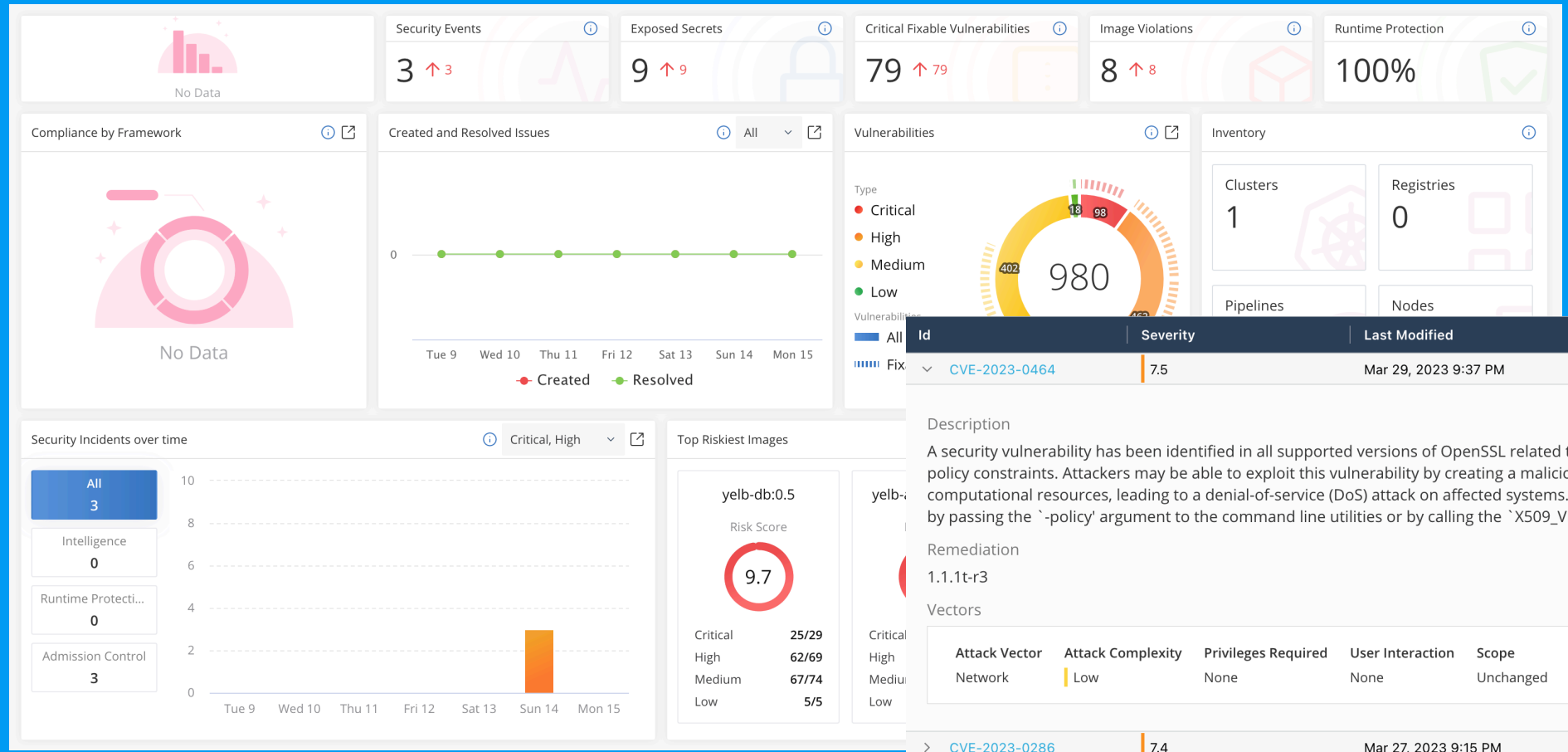
Das Produkt Workload Protection ist ein grundlegender Baustein zur Analyse, Erkennung sowie Verhinderung von Risiken innerhalb von Multi-Cloud-Umgebungen oder Containern. Es kann bei der frühzeitigen Erkennung von Cyberattacken in der Container-Umgebung sowie der Source-Code-Überprüfung (DevSecOps) in der Entwicklung unterstützen.

+ Transparenz über die Sicherheit Ihrer Multi-Cloud sowie Cloud-native-Anwendungen
+ Ganzheitliche Sicht auf Multi-Cloud-Infrastrukturen und automatisierte Inventarisierung von Cloud-Ressourcen
+ Inventarisierung von Ressourcen im Kubernetes-Cluster
+ Prüfungen von Containern, Container Images & Container Registries auf Schwachstellen, Malware oder Anmeldedatenlecks
+ Laufzeitschutz (Runtime Protection) von Prozessen und Anwendungen in Containern
+ DevSecOps-Prüfung von Softwarecode
+ Applikations- und API-Sicherheit
+ Erfüllung von Compliance & Regularien in Multi-Cloud-Umgebungen
+ Reduzierte Komplexität durch Servicemodell (Fachkräftemangel)



plusserver

Dashboard und Berichte



Id	Severity	Last Modified	Description	Remediation
CVE-2023-0464	7.5	Mar 29, 2023 9:37 PM	A security vulnerability has b...	1.1.1t-r3

Description

A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function.

Remediation

1.1.1t-r3

Vectors

Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	Unchanged	None	None	High

CVE-2023-0286	7.4	Mar 27, 2023 9:15 PM	There is a type confusion vul...	1.1.1t-r3
CVE-2022-4450	7.5	Feb 24, 2023 4:15 PM	The function PEM_read_bio_...	1.1.1t-r3
CVE-2023-0465	5.3	Apr 15, 2023 1:15 AM	Applications that use a non-...	1.1.1t-r3
CVE-2023-0466	5.3	Apr 15, 2023 1:15 AM	The function X509_VERIFY_P...	
CVE-2022-4304	5.9	Feb 24, 2023 6:13 PM	A timing based side channel ...	1.1.1t-r3

plusserver

Workload Protection im Überblick

Was ist enthalten?

Transparenz
- Dashboards
- Inventarisierung von Cloud-Ressourcen
- Risikomanagement zur Priorisierung von Bedrohungen
- Compliance

Container-Sicherheit
- Images & Container (Schwachstellenüberwachung)
- Runtime Protection (XDR, File-Überwachung etc.)

Applikationssicherheit / DevSecOps
- Source Codes Scans (DevSecOps)
- IAC Scans (Infrastucture as a Code Scanning)

Multi-Cloud-Sicherheit
- Plattform-Protection (z. B. AWS, Azure und GCP)
- Serverless-Funktionen
- File-Storage (z. B. S3)

Standardisiertes Onboarding

Für einen reibungslosen Start des Kunden

Das Onboarding dauert ca. einen Tag und wird mit einmalig 1.320 Euro berechnet. Beim Produkt Advanced Workload Protection (mit SOC, auf Anfrage) kommt ein Onboarding-Tag hinzu.

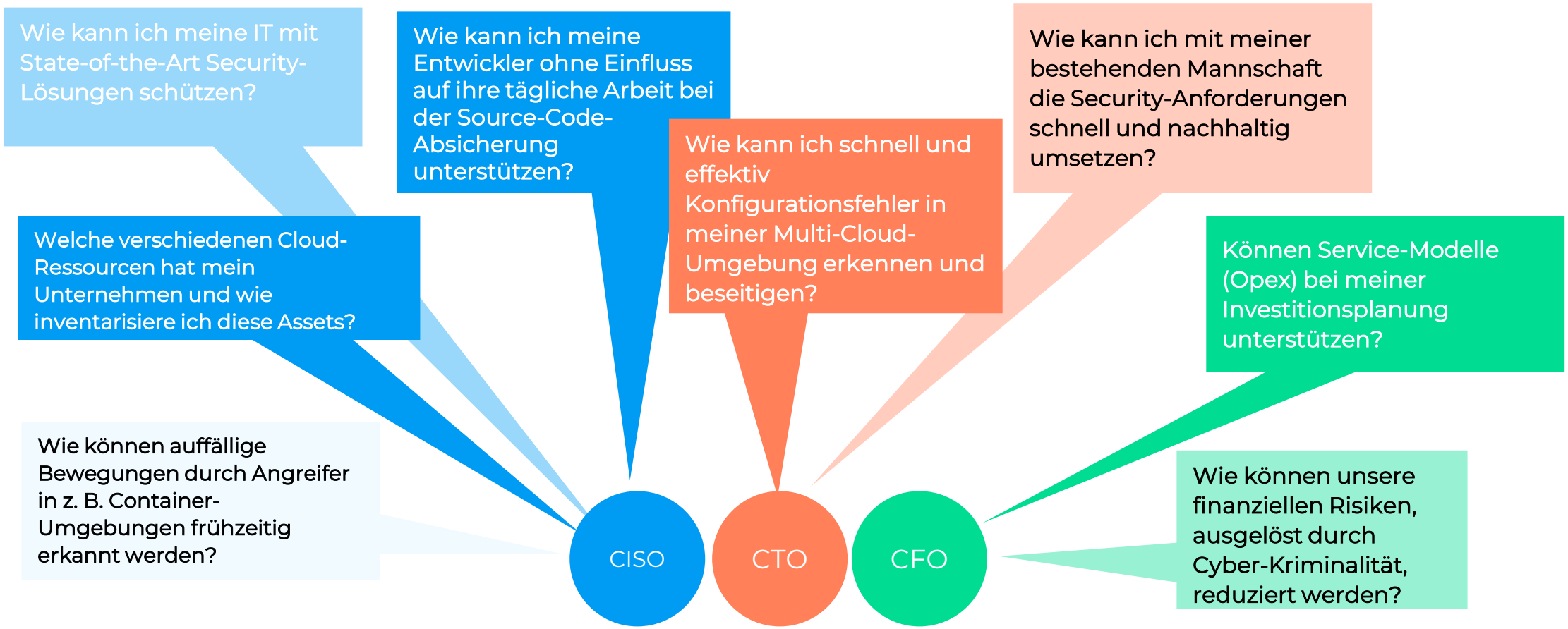
Kick-off-Meeting mit dem Kunden
Vorstellung der Plattform sowie Lösung mit allen relevanten Funktionen
Aufzeigen von Best Practices zu einer möglichen Implementierung durch den Kunden
Vorstellung der Herstellerdokumentation

Im Rahmen des Onboardings findet keine Implementierung oder weiterführende Beratung durch plusserver statt.

Erweiterte Professional-Service-Leistungen können durch das Security Consulting Team nach Rücksprache mit dem Kunden kostenpflichtig erbracht werden.

plusserver

Fragestellungen von Entscheidenden



plusserver

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …		… weitere wesentliche Mehrwerte	
Wie können auffällige Bewegungen durch Angreifer in z. B. Container-Umgebungen frühzeitig erkannt werden?	+ Durch eine richtlinienbasierte Zugriffskontrolle werden Workloads, die in Kubernetes ausgeführt werden, vor unbefugtem Zugriff geschützt. Unternehmen erhalten eine granulare Kontrolle darüber, welche Workloads aufeinander und auf das Internet zugreifen können.	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. ✓ Sind
Welche verschiedenen Cloud-Ressourcen hat mein Unternehmen und wie inventarisiere ich diese Assets?	+ Workload Protection as a Service bietet Ihnen eine ganzheitliche Sicht auf Multi-Cloud-Infrastrukturen und automatisierte Inventarisierung von Cloud-Ressourcen. Dazu steht Ihnen ein komfortables Dashboard zur Verfügung.		

plusserver

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …		… weitere wesentliche Mehrwerte	
Wie kann ich mit meiner bestehenden Mannschaft die Security-Anforderungen schnell und nachhaltig umsetzen?	+ Mit Workload Protection as as Service erhalten Sie einen Full-Managed Service, sodass Ihr IT-Team nachhaltig entlastet wird. Zudem werden Sie durch ein individuelles Onboarding unterstützt und können reibungslos mit der Lösung starten.	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. ✓ Sind
Können Service-Modelle (OPEX) bei meiner Investitionsplanung unterstützen?	+ Ja, Sie nutzen die volle Flexibilität im On-demand-Modell. Statt in eigene Software und Personal zu investieren, können Sie mit unserem vorteilhaften Service-Modell (Opex) noch einfacher Ihre Investitionen planen.		

plusserver

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie …		… weitere wesentliche Mehrwerte	
Wie kann ich meine Entwickler ohne Einfluss auf ihre tägliche Arbeit bei der Source-Code-Absicherung unterstützen?	+ Mit Workload Protection as as Service können Sie Security unmittelbar in Ihre DevOps-Prozesse einbinden (=DevSecOps). Der Code wird automatisch auf Sicherheitsrisiken hin untersucht. Durch die Verlagerung der Security-Kontrolle in die Phase der Codeerstellung (shift left) erzielen Organisationen neben höherer Sicherheit auch eine schnellere Time-to-Market ihrer Anwendungen und von neuen Features.	Cyber-versicherungen	✓ Um sich gegen Cyberattacken versichern zu können, müssen bereits umfangreiche Schutzmaßnahmen bestehen. ✓ Moderne Cybersecurity-Versicherungen verlangen einen entsprechenden Nachweis über Security-Systeme auf dem Stand der Technik. ✓ Workload Protection ist dabei ein hilfreiches Element und kann weitere Lösungen wie ein EDR innerhalb eines 360°-Security-Ansatzes ergänzen.
Wie kann ich schnell und effektiv Konfigurationsfehler in meiner Multi-Cloud-Umgebung erkennen und beseitigen?	+ Unser Produkt hilft dabei, die Governance über Multi-Cloud-Ressourcen und -Services zu wahren. Dazu gehört eine Visualisierung und Bewertung der Sicherheitslage sowie die Erkennung von Fehlkonfigurationen. So setzten Sie Best Practices und Compliance-Frameworks optimal durch.		

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