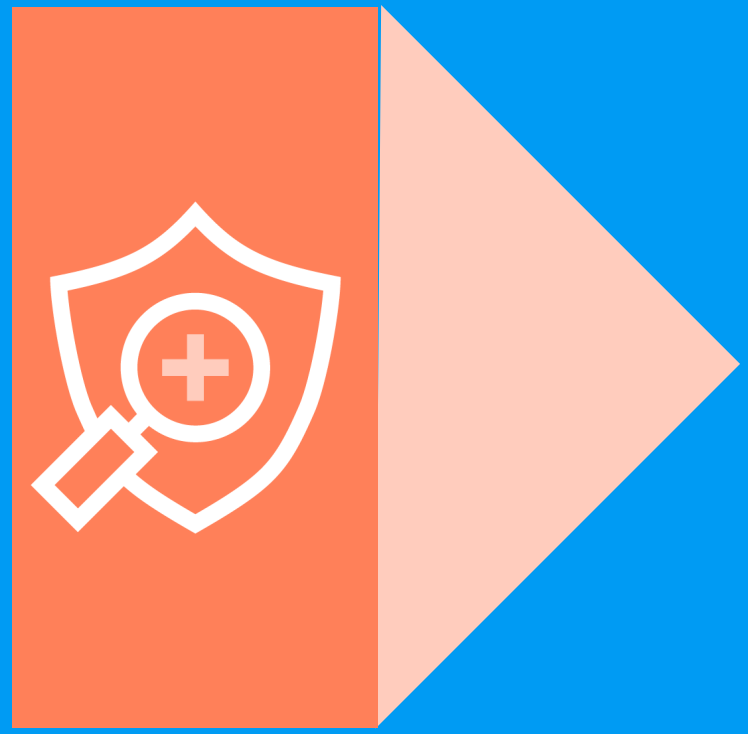
plusserver

Security Scanner Sales Playbook für intern und Partner

Version 1.2, März 2024

NICHT FÜR ENDKUNDEN

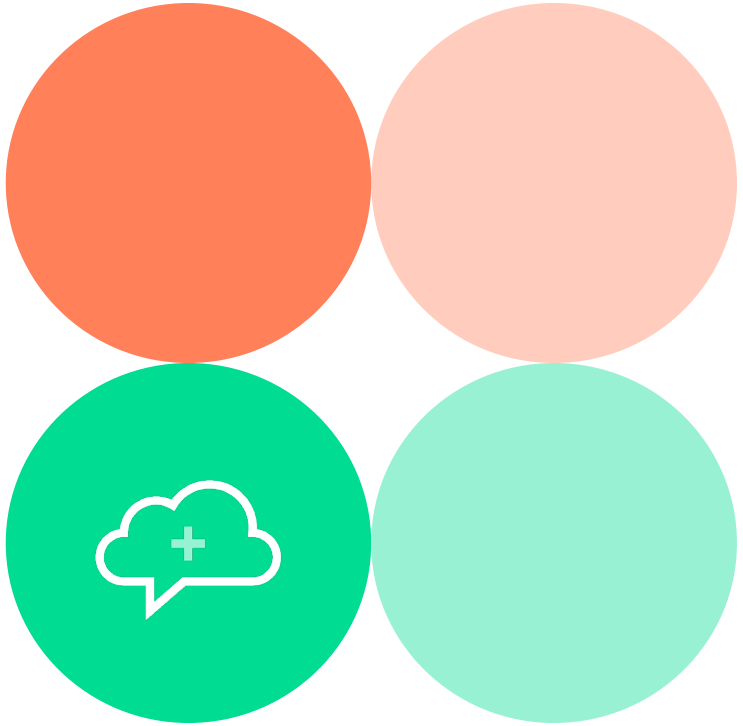


Was ist ein Sales Playbook?

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?



Security Scanner

... für eine schnelle Vorbereitung eines Kundentermins.

- Security-Verantwortliche in Unternehmen haben oft einen unzureichenden Überblick über vorhandene Schwachstellen in ihren IT-Systemen. Veränderungen in der Cloud-Umgebung werden nicht oder verspätet sichtbar. Daher werden Lösungen zum Schwachstellenmanagement nachgefragt, die:
  - komplette IT-Infrastrukturen überwachen
  - Transparenz und Sicherheitslevel steigern
  - das Risikomanagement unterstützen

- Unsere Lösung Security Scanner as a Service bietet darüber hinaus:
  - Schnelles Setup sowie SaaS-Ansatz
  - Deutsches Produkt als Plattform (DSGVO etc.)
  - SOC-Integration möglich
  - MRR- und Opex-Ansatz (sehr flexibel) sowie On-demand-Modell möglich

- Der Zeitraum zwischen der Erstveröffentlichung einer neuen Schwachstelle und der Ausnutzung dieser durch Angreifer beträgt im Schnitt nur zwölf Tage. Geschwindigkeit und Präzision sind daher die Treiber eines effizienten Schwachstellenmanagementprozesses.

Vorteile & Potenziale des Security Scanner as a Service

Unser Service für Ihre Zukunftsfähigkeit

Technologische Vorteile

- Schwachstellenprüfung von IP-basierten Systemen
- Automatisierte Prüfung nach Zeitplan
- Alarmierung über gefundene Schwachstellen
- Verschiedene Berichtsformate (auch Management Summary)
- Tägliche Aktualisierung der Schwachstellentests (100.000 NVTs)
- Hochverfügbare Management-Oberfläche
- Security-by-Design – beinhaltet die kontinuierliche Aktualisierung der Plattform
- Auditfähig

Potenziale für Kunden

- Vermeidung von Datenverlust und finanziellen Schäden
- Erkennung von Schwachstellen (z. B. Log4J)
- Veränderungen in der Cloud-Umgebung werden sofort sichtbar
- Steigerung der Transparenz des Security-Levels
- Der Security Scanner as a Service entlastet die Betriebsmannschaft des Kunden
- Technologisch immer vorn dabei durch permanente Weiterentwicklung der Lösung
- DSGVO-konform und Cloud-Act-neutral
- Deutschsprachiger 24/7 Support

Pricing-Modell

- IP-basierte Lizenzierung. Mindestbestellanzahl 30 IP-Adressen
- Commitment-Modell mit attraktiven Preisnachlässen
- Opex-Modell

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.

- **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 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 und die Wartung sowie Absicherung der zugrundeliegenden Infrastruktur kümmern müssen.
- **Fehlendes Budget:** Der Aufbau und die Wartung einer eigenen Infrastruktur sind mit hohen Investitions- und Wartungskosten verbunden.
- **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.

Die Lösung liefert plusserver

Vulnerability-Management leicht gemacht!

Der plusserver Security Scanner überprüft Ihre Zielsysteme auf bekannte und aktuelle Schwachstellen. Auf Basis dieser Informationen lässt sich die Bedrohungslage im Unternehmen gezielter einschätzen und geeignete **Schutzmaßnahmen ableiten**.

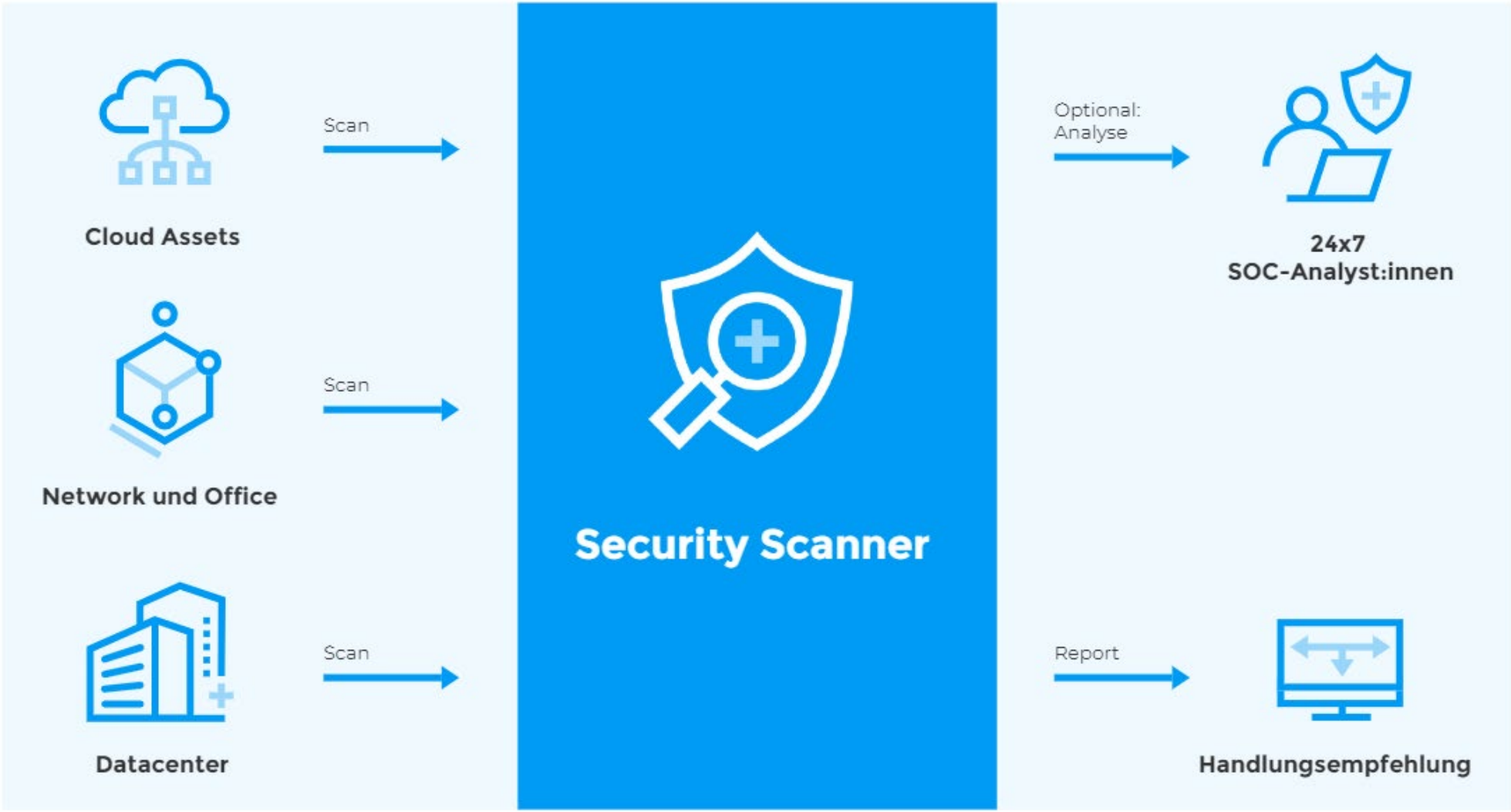
Darüber hinaus ermöglicht Ihnen der Security Scanner, aktuelle Schwachstellen in Ihrer IT-Umgebung zu **dokumentieren**. Um Bedrohungen noch effektiver zu reduzieren, bieten wir Ihnen zusätzlich die Möglichkeit, die gewonnenen Informationen durch unser **Security Operations Center (SOC)** analysieren zu lassen. Auf diese Weise können notwendige Handlungsempfehlungen für Ihre IT-Umgebung abgeleitet werden.

Durchleuchten Sie mit unserem Security Scanner **alle geschäftskritischen IT-Systeme**, egal wo sich diese befinden. In der Cloud, im eigenen Rechenzentrum, Colocation oder Hosting sowie auch im Office. Der **Report** zeigt ein übersichtliches Bild des Status quo und entsprechende Handlungsmöglichkeiten auf.

plusserver

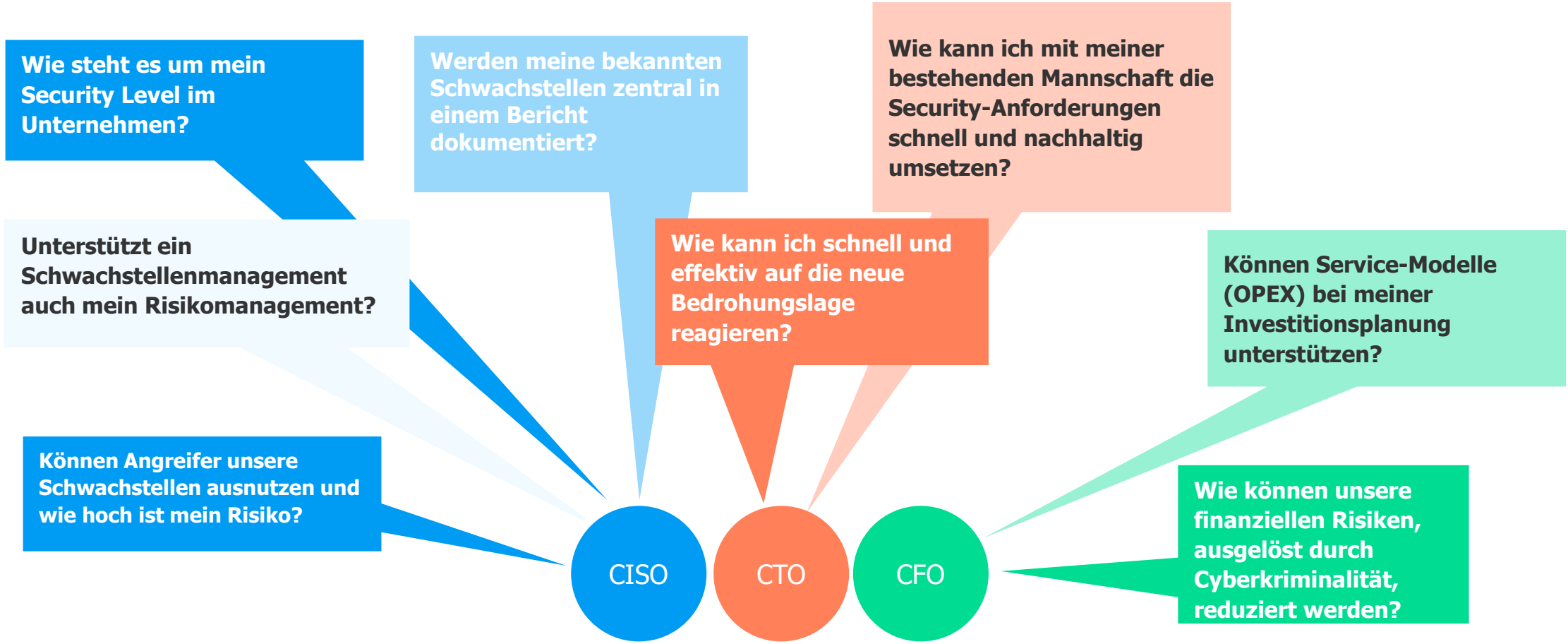
Security Scanner

Der Sicherheitscheck für alle Ihre Systeme



plusserver

Fragen von Entscheidenden



plusserver

Antworten auf zentrale Fragestellungen

Können Angreifer unsere Schwachstellen ausnutzen und wie hoch ist mein Risiko?	Jede Schwachstelle kann ein Einfallstor für Cyberkriminelle bieten, vergleichbar einem Loch im Sicherheitszaun. Dabei schützt selbst regelmäßiges Patching nicht vor Schwachstellen, da Systemabhängigkeiten bei unternehmenskritischen Applikationen oft keinen aktuellen Patch zulassen. Gleichzeitig können Updates wiederum für neue Schwachstellen sorgen.
Wie steht es um mein Security Level im Unternehmen?	Oftmals fehlt in Unternehmen die Transparenz über das Security Level. Der Security Scanner liefert einen ausführlichen Report und schafft so Klarheit über Schwachstellen und nötige Maßnahmen.
Werden meine bekannten Schwachstellen dokumentiert?	Ja, jeder Scan erzeugt einen umfassenden Report mit einer Dokumentation der Schwachstellen, einer Priorisierung und den entsprechenden Handlungsempfehlungen.
Unterstützt ein Schwachstellenmanagement auch mein Risikomanagement?	Selbstverständlich, denn das Ziel ist es, Schwachstellen schnell und effektiv zu erkennen und zu eliminieren, sodass diese kein Risiko mehr darstellen können. Der Scanner führt Tests auf dem zu prüfenden Netzwerk aus und erkennt so vorhandene Sicherheitslücken. Diese werden nach ihrem Schweregrad bewertet, was das Priorisieren der Beseitigungsmaßnahmen ermöglicht.
Wie kann ich schnell und effektiv auf die neue Bedrohungslage reagieren?	Unser Security Scanner as a Service ist nach der Installation einer virtuellen Appliance in der Kundeninfrastruktur direkt einsatzbereit und innerhalb von wenigen Minuten eingerichtet. plusserver übernimmt dies für den Kunden. Die Ergebnisse können direkt genutzt werden, um die eigene digitale Widerstandsfähigkeit zu verbessern.
Wie kann ich mit meiner bestehenden Mannschaft die Security-Anforderungen schnell und nachhaltig umsetzen?	Der Security Scanner ist eine Lösung, mit der Schwachstellen in der eigenen Netzwerkinfrastruktur innerhalb von wenigen Schritten aufgespürt und Anweisungen zu deren Behebung in Form von Berichten aufgezeigt werden. Fachkräfte oder spezielles Know-how sind nicht erforderlich.
Können Service-Modelle (OPEX) bei meiner Investitionsplanung unterstützen?	Sie haben keine Investitionsausgaben, keine Hardwarekosten, benötigen kein zusätzliches Personal und beziehen unsere Lösung im flexiblen On-demand-Modell.
Wie können unsere finanziellen Risiken, ausgelöst durch Cyberkriminalität, reduziert werden?	Je früher Schwachstellen in IT-Systemen aufgedeckt und behoben werden, desto geringer das Risiko eines erfolgreichen Angriffs, der hohe Kosten verursachen und im schlimmsten Fall existenzbedrohlich sein kann.

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