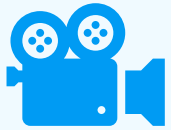
Agil, innovativ – und resilient

So werden moderne Cloud-Architekturen zum sicheren Erfolg

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

Tarek Nemri

IT Security Consultant

Peter Weber

Technical Account
Manager Security

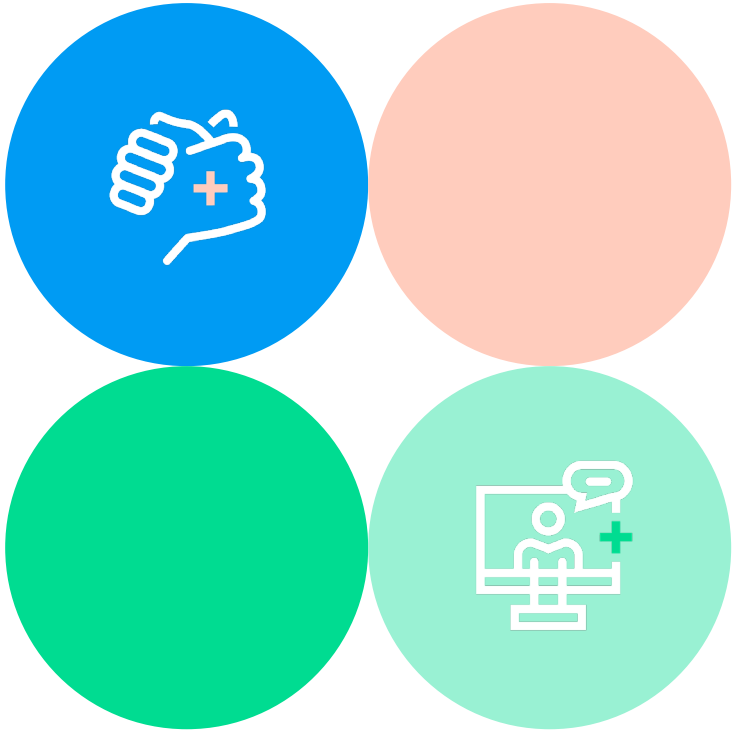
Florian Neus

Senior Partner
Marketing Manager

Agenda

Agil, innovativ – und resilient

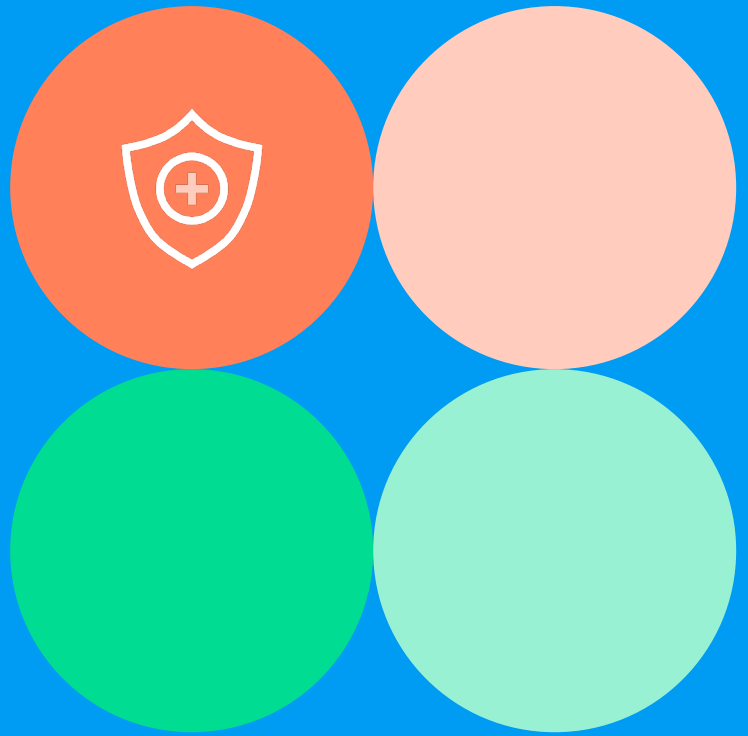
- NIS2 Wrap Up
- Vorstellung der Workload Protection als ergänzende technische Maßnahme zur Umsetzung der NIS2-Richtline
- Live Demo
- Q & A



plusserver

Umsetzungsszenarien und Projektmöglichkeiten

Security Services



plusserver

Wie kann plusserver unterstützen?

NIS2-Assessment (plusserver oder Partner)

Security-Beratung/ Consulting

+ Feinkonzeption und Design von Security-Maßnahmen und -Architekturen
+ Pentests und Audits

Security-Lösungen

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

Zertifizierte Infrastruktur

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

Sales Cases mit NIS2

Einfache Beispiele

Security auf dem Stand der Technik	→	NIS2-Assessment und Security Services als Projekttreiber zur Reduzierung von Komplexität
Incident Management	→	Security Scanner, SOC-Module, Security Operations Center aaS, EDR, ***Workload Protection***
Business Continuity	→	plusserver Cloud Services (made in Germany / certified) mit Backup as a Service in Kombination mit Cloud Security

plusserver

360-Grad-Ansatz

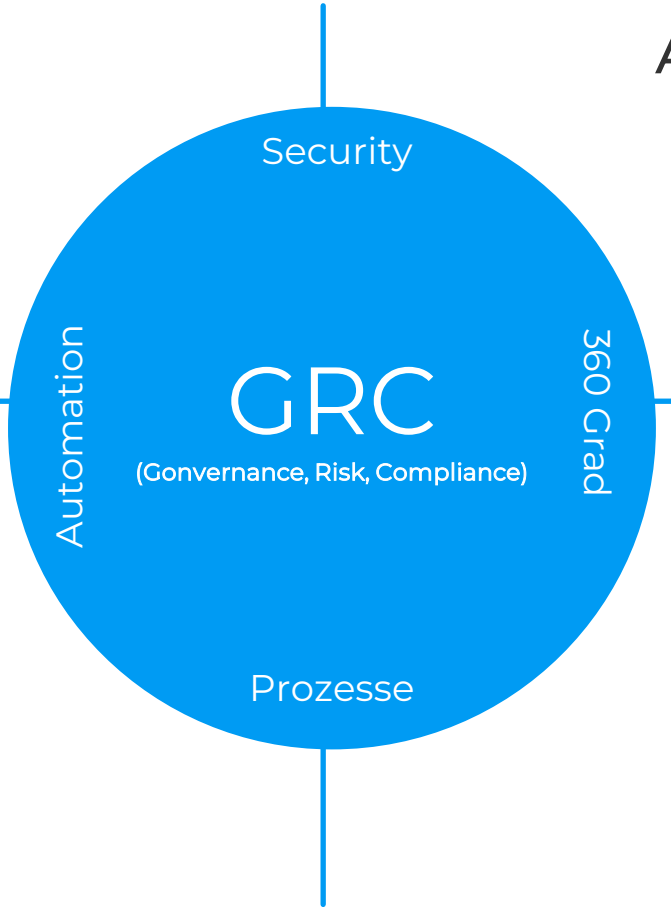
Security als Prozess etablieren

Wiederherstellung (Recovery)

- Backup as a Service

Analyse und Risikomanagement

- IT-Security Consulting
- Audits und Penetrationstests (@-Yet)



Detektion & Reaktion

- SOC as a Service
- Security Scanner
- Endpoint Detection with SOC

Prävention nach Schutzbedarf

- Next Generation Firewall (Cloud)
- Endpoint Detection and Response
- Workload Protection
- DDoS und WAF (Akamai und Link11)

Inhalte für Ihre Kommunikation

Kostenfreie Verwendung, hochwertige Inhalte

Nutzen Sie unsere Assets für die Ansprache Ihrer Kunden oder für die eigene LeadGen. Zum Thema NIS2 und unseren Security-Produkten bieten wir verschiedene Inhalte, die Sie passend zu den Bedürfnissen Ihrer Kunden einsetzen können.

+ **(Produkt-)Datasheets für den ersten Kontakt mit den Kunden**

+ **Präsentationen und Playbooks für Ihre Gespräche mit den Kunden**

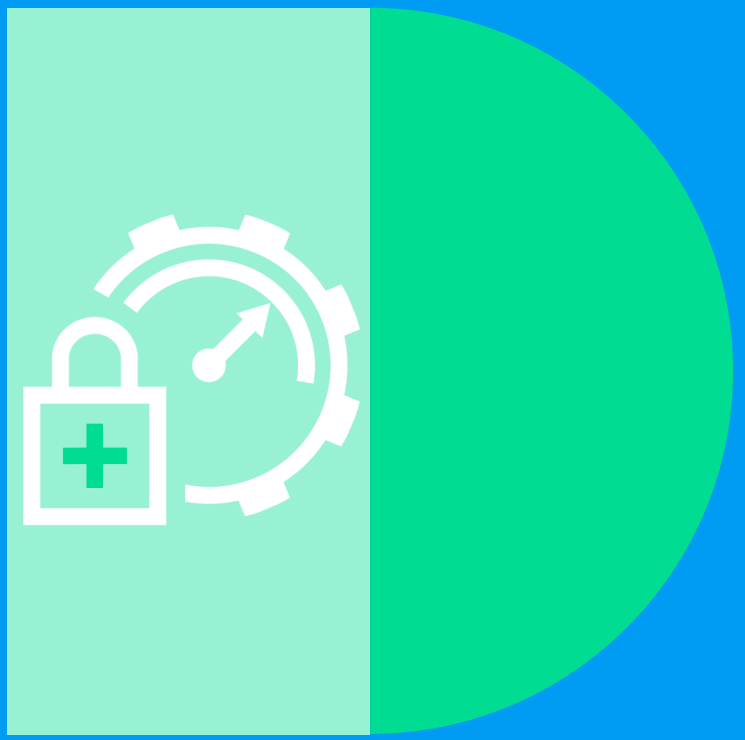
+ **Checklisten und Blog-Beiträge für den Wissensaustausch**

Alle Inhalte finden Sie in unserem neuen MarketingHub und auf der Landingpage zur NIS2-Initiative.

plusserver

Wie erhalte ich Transparenz in Multi-Cloud-Umgebungen und wie sichere ich containerisierte Umgebungen richtig ab?

Welchen Mehrwert bringt mir Workload Protection im Bezug auf NIS2?



plusserver

Herausforderungen im Hybrid- und Multi-Cloud-Umfeld

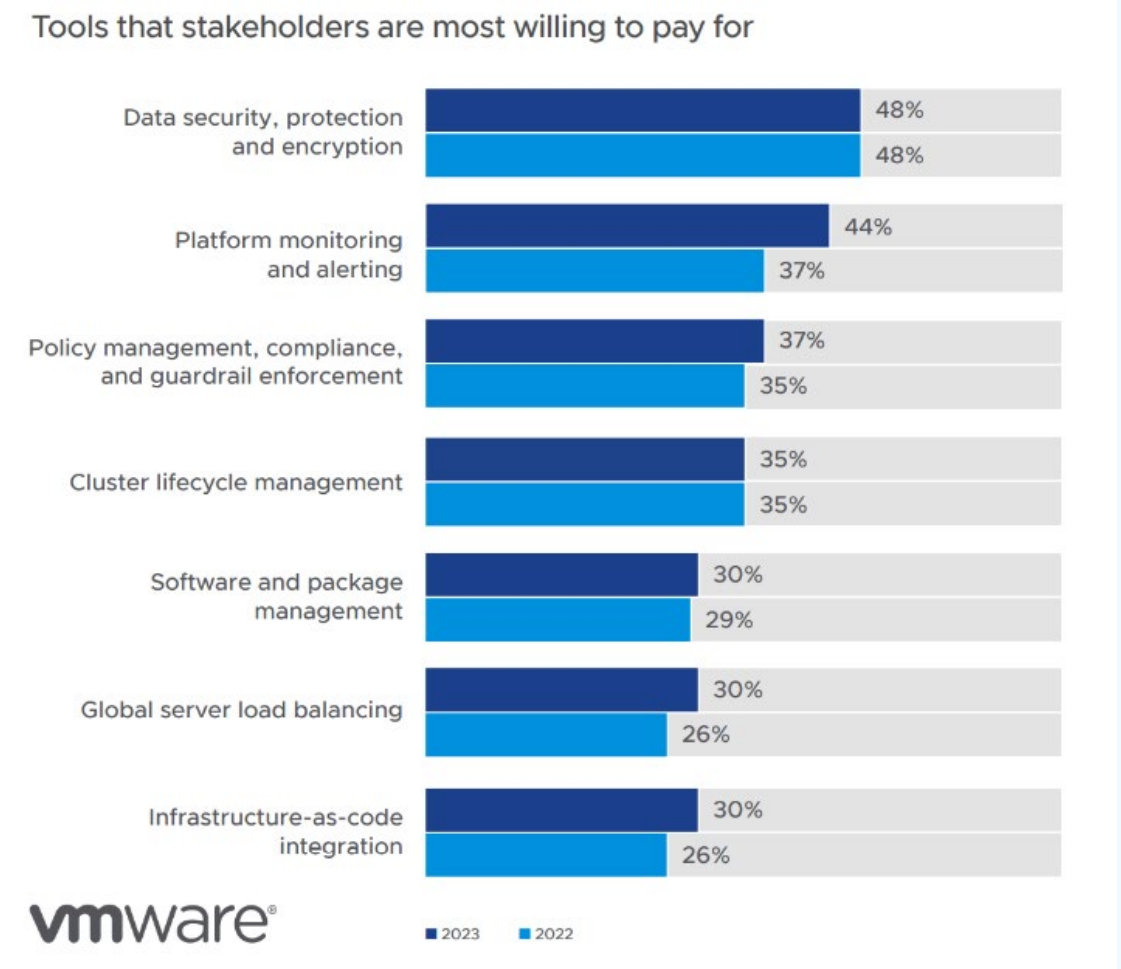
Problemstellung: Traditionelle IT-Sicherheitslösungen sind nicht Cloud-ready

1. Hybrid- und Multi-Cloud-Umgebungen erhöhen die **Komplexität**
2. Die Sichtbarkeit (**Inventarisierung**) der Cloud-Ressourcen und des **Netzwerkverkehrs** ist nur bedingt möglich
3. **Sicherheitsfunktionen** der Komponenten stehen ggf. nicht auf allen Plattformen bereit
4. Verschiedene IT-Sicherheitslösungen und **Standards** erschweren Aufgaben der **Compliance** und operativen Sicherheit

Security-Challenges beim Kubernetes-Betrieb

Verstärkt durch komplexer werdende Architekturen (Multi-Cloud)

- 52 % geben an, Schwierigkeiten im Hinblick auf Security- und Compliance-Anforderungen zu haben
- 55 % nennen Fehlkonfigurationen/Schwachstellen als größtes Problem
- Knapp die Häfte der Entscheider ist bereit, für Lösungen, die Security-Herausforderungen in Container/Kubernetes-Umgebungen adressieren, zu bezahlen.



(Quelle: The State of Kubernetes 2023, VMware)

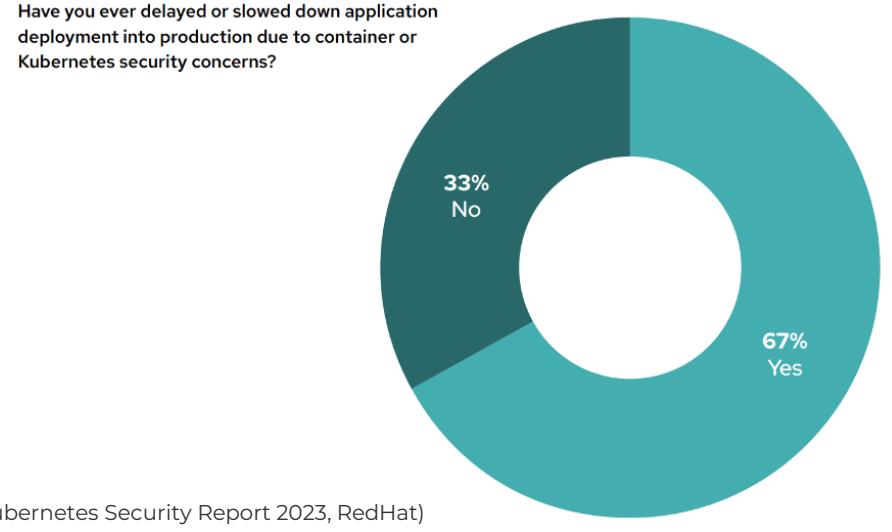
plusserver

Security-Challenges beim Kubernetes-Betrieb

… haben direkten Einfluss auf die Wettbewerbsfähigkeit!

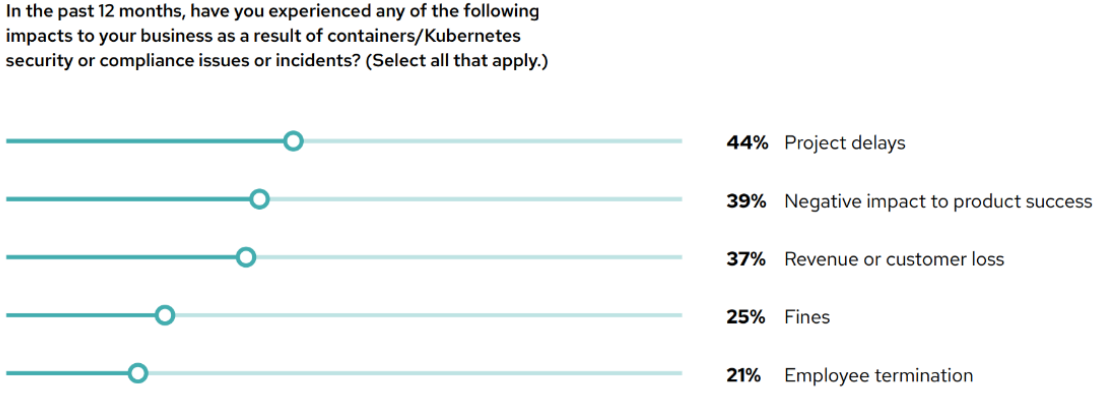
„Wenn Security zur Nebensache wird, wird die durch die Containerisierung gewonnene Agilität […] zunichte gemacht.“

+ 67% der Befragten mussten ihre Anwendungsbereitstellung aufgrund von Sicherheitsbedenken in der Vergangenheit verzögern (= längere Time-to-Market)



(Quelle: State of Kubernetes Security Report 2023, RedHat)

+ Security-Incidents in Kubernetes-Umgebungen haben Business Impact:
  + verzögerte Projekte
  + Produkte weniger erfolgreich
  + verlorene Umsätze und Kunden
  + Strafen
  + verlorene Mitarbeitende



Warum Workload Protection?

1

+ Seien Sie nicht im Blindflug unterwegs. Transparenz in Multi-Cloud-Umgebungen und dedizierte Absicherung von veröffentlichtem Content ist ein MUSS.

+ Hohes Risiko

2

+ Stellen Sie sich der Herausforderung zur Absicherung von containerisierten Umgebungen, um Security konsequent durchzusetzen

+ Ohne Detektion keine Reaktion

3

+ Schnell und effektiv ein unattraktives Ziel werden!

+ Zahlt direkt auf die Ziele, Maßnahmen und Anforderungen von NIS2 ein

plusserver

Workload Protection as a Service - Schlüsselbegriffe

Container (Kubernetes)

DevSecOps

Software-Entwicklung

Cloud-native-Ökosysteme

Web-Anwendungen

Cloud (Hyperscaler)

Workload Protection as a Service

Transparenz über die Sicherheit Ihrer Multi-Cloud und Cloud-native-Anwendungen

+ Ganzheitliche Sicht auf Multi-Cloud-Infrastrukturen
+ Automatisierte Inventarisierung von Cloud-Ressourcen

➔ **Transparenz über alle Layer und Umgebungen, um diese auch entsprechend absichern zu können**

+ Erkennung und Blockieren von Angriffen auf Container, Web-Applikationen oder Hyperscaler-Ressourcen
+ Benachrichtigung bzgl. sicherheitsrelevanter Ereignisse über diverse Schnittstellen (E-Mail, SMS, Syslog, SIEM)

➔ **Erweiterung der Security auf bislang intransparente Workloads und Umgebungen**

+ Benchmarks nach Industrie-Standards (CIS, NIST, PCI-DSS etc.)

➔ **Gewährleistung von Nachweispflichten aufgrund von Regularien, die gegenüber Geschäftspartnern erbracht werden müssen**

plusserver

Workload Protection as a Service

Multi-Cloud-Sicherheit

Jede Cloudplattform besitzt einen eigenen technologischen Unterbau, damit entstehen technologische Inseln.

➔ Unternehmen haben keine ganzheitliche Sicht auf Ihre heterogene Infrastruktur

Was sind die Mehrwerte einer Multi-Cloud-Sicherheit?

+ Sichtbarkeit der gesamten Infrastruktur
+ Zusammenführung aller Informationen verschiedener Cloudplattformen
+ Ganzheitliches Risikomanagement möglich (NIS2)

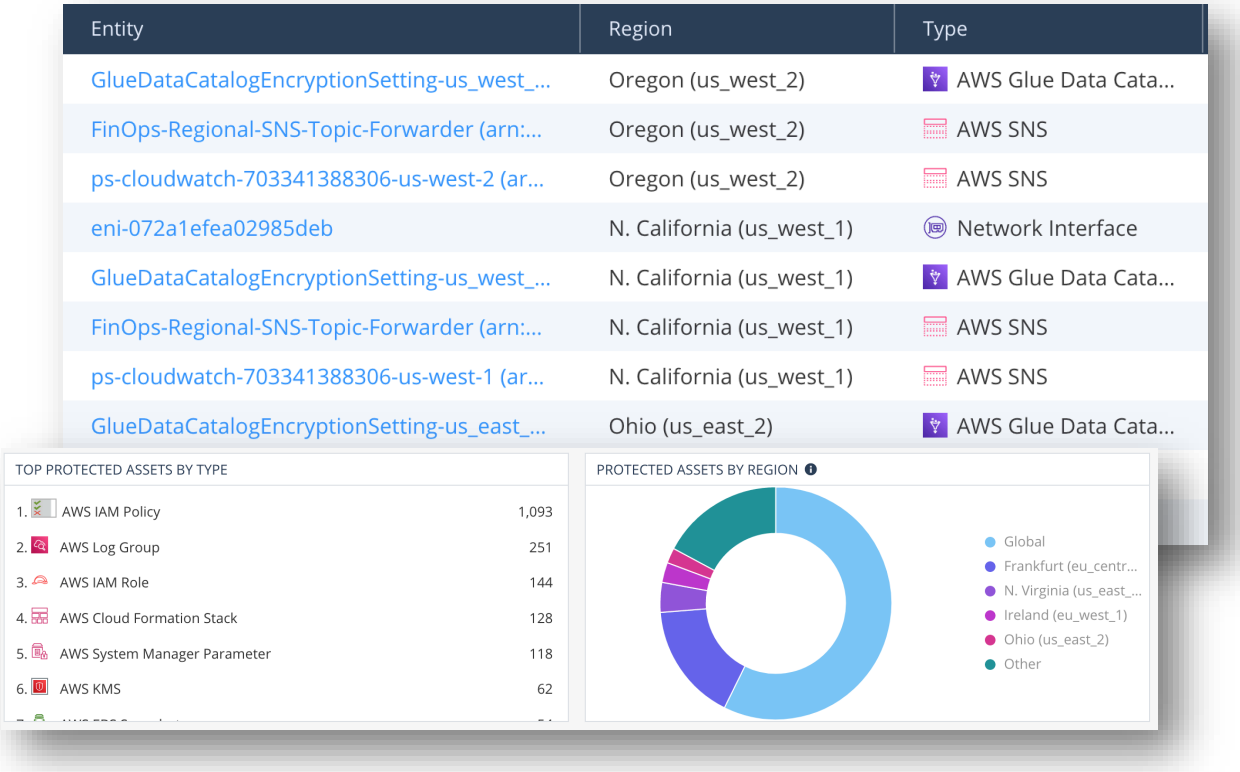
Amazon Web Services

Google Cloud Plattform

Oracle Cloud Infrastructure

Azure

Alibaba Cloud



plusserver

Workload Protection as a Service

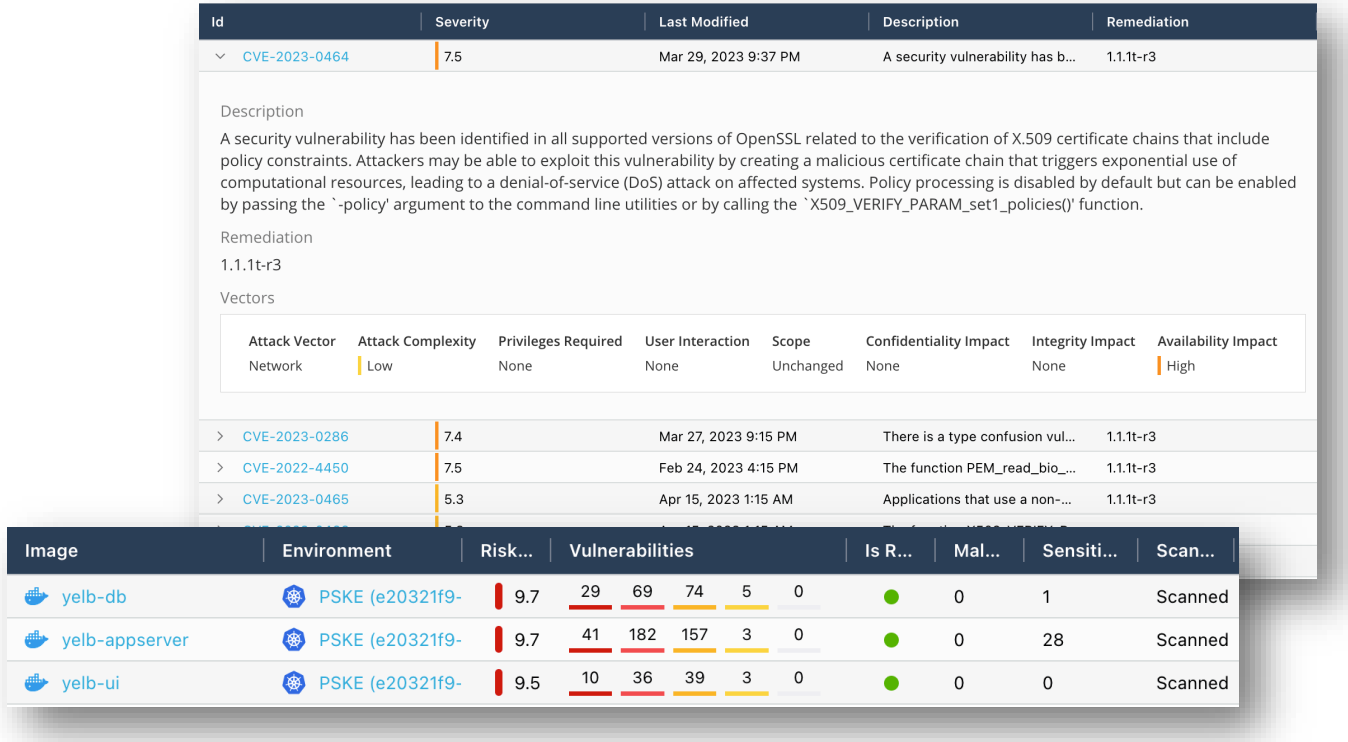
Container-Sicherheit

Warum ist Container-Sicherheit wichtig?

+ Klassische IT-Sicherheitslösungen wie z.B. Virenscanner & EDR können in Containern nicht installiert werden

Was erreiche ich mit einer dedizierten Absicherung durch WPaaS?

+ Transparenz über Schwachstellen auf Container-Plattformen
  - ➔Schließen von offenen Einfallstoren
+ Compliance (NIS2) der Einstellungen wird überprüft
+ Berichte über die Sicherheit nach Standards (z.B. ISO27001, BSI IT-Grundschutz) kann ggü. der Geschäftsleitung vorgestellt werden



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				

Image	Environment	Risk...	Vulnerabilities					Is R...	Mal...	Sensiti...	Scan...
yelb-db	PSKE (e20321f9-	9.7	29	69	74	5	0		0	1	Scanned
yelb-appserver	PSKE (e20321f9-	9.7	41	182	157	3	0		0	28	Scanned
yelb-ui	PSKE (e20321f9-	9.5	10	36	39	3	0		0	0	Scanned

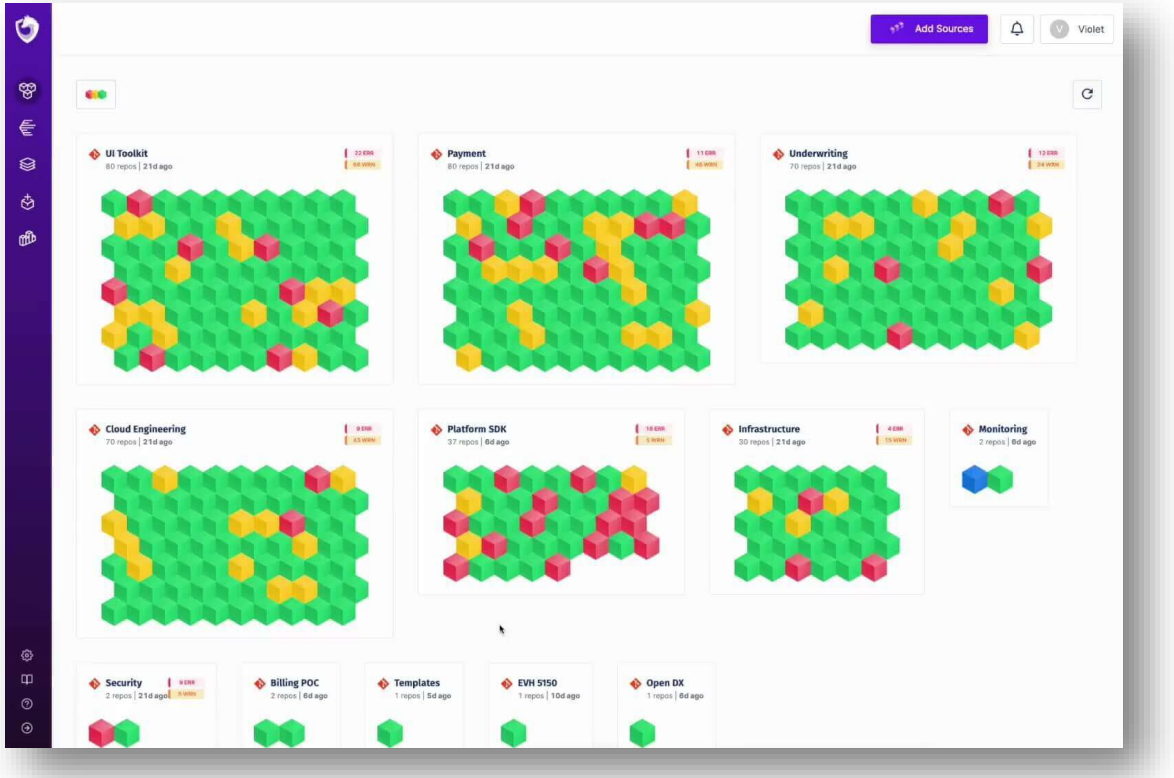
Google Amazon Harbor jFrog Azure

plusserver

Workload Protection as a Service

DevSecOps

- Schwachstellen in Software entstehen bereits bei der Programmierung
- Je früher Schwachstellen aufgedeckt werden, **desto günstiger** ist die Entfernung der Schwachstelle!
- **Steigerung der Geschwindigkeit** innerhalb der Software-Entwicklung durch frühzeitige Erkennung von Fehler in der Software
- Die Software-Entwicklung wird durch Workload Protection durch **Automatisierung** entlastet



Workload Protection as a Service

WAF, Applikations- und API-Sicherheit

- Web-Anwendungen (Webseiten, Webshop, etc.) müssen vor Angriffen geschützt werden.
  - Nur Web-Application-Firewalls sind darauf zugeschnitten!
- Web-Application-Firewall mit **Machine Learning** beschleunigt die Konfiguration und Entlastet die IT
- **IPS**: Schutz vor der Ausnutzung von Schwachstellen
- Einfache Integration einer WAF auf vorhandenen Systemen hat Vorteil für Time-to-Market!

-> IT-Abteilungen müssen keine externe WAF betreiben

Wann ist Workload Protection by plusserver für den Kunden DIE Lösung?

1

Arbeitet der Kunde in Multi-Cloud Umgebungen und hat derzeit keine Transparenz und Übersicht über alle Umgebungen ?

2

Handelt es sich um ein Softwareentwicklungs-unternehmen, das mit containerisierten Umgebungen arbeitet?

3

Gibt es eine Nachweispflicht von Compliance-Regularien (NIS2) gegenüber Geschäftspartnern oder der Geschäftsführung?

Q&A

Wir helfen gerne!

Gemeinsam wachsen!

Jetzt mit der Umsetzung starten. Wir unterstützen Sie gerne.

Sie haben Fragen oder Anregungen zu unserer NIS2-Initiative? Wenden Sie sich gerne an folgende Kontakte:

Bei Fragen zur Initiative, Kommunikationsmitteln und unseren Webinaren:

partner.marketing@plusserver.com

Bei Fragen zu Produkten und technischen Details:

partner.technik@plusserver.com

Bei Fragen zu Projekten, Deal-Registrierungen und Sales-Unterstützung:

partner.sales@plusserver.com

plusserver

Vielen Dank für Ihre Aufmerksamkeit!

14. Mai **A Beginner's Guide to NIS2**

4. Juni **Auf die Plätze, fertig, NIS2!**

Unsere Security-Initiative wird unterstützt von

VEEAM IBM