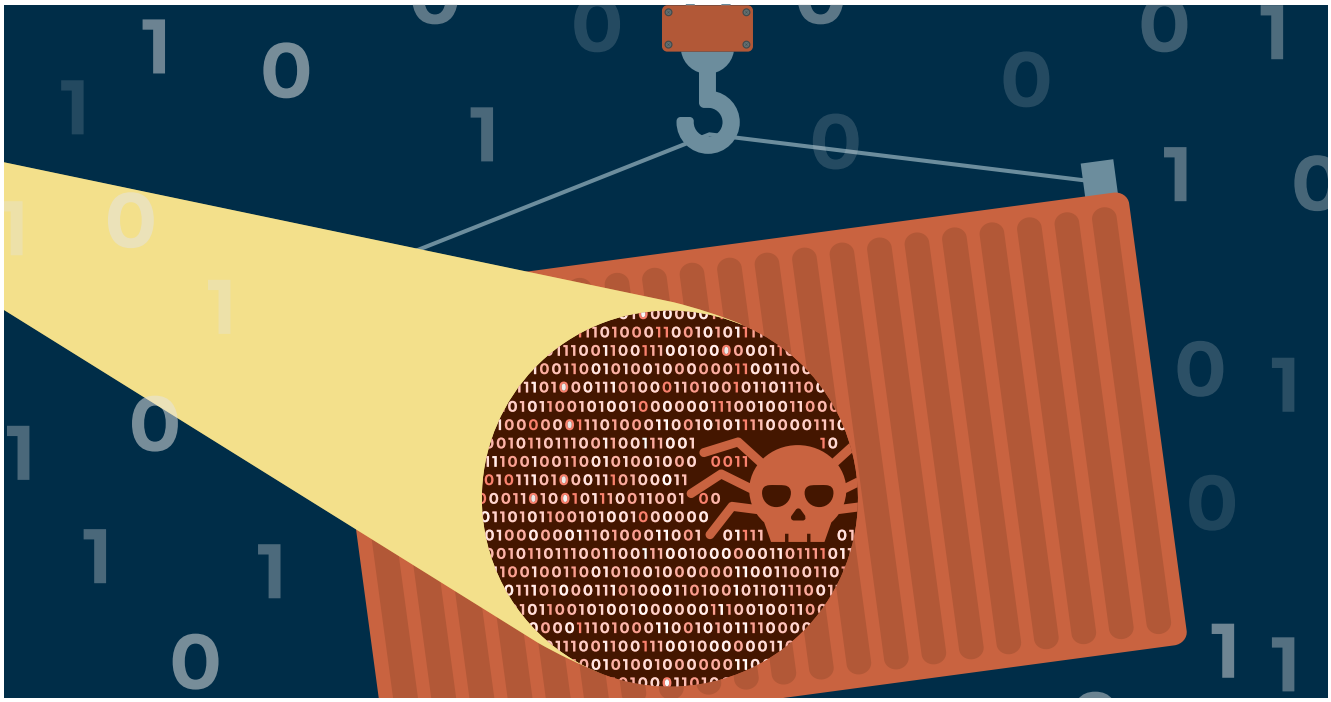

Marktübersicht: Sicherheitsscanner für Container-Images

Container bieten viele Vorteile bei der Entwicklung und Bereitstellung, aber ihre inhärenten Eigenschaften – gemeinsamer Kernel, geschichtetes Dateisystem – bergen auch einzigartige Risiken. Eine robuste Containersicherheitsstrategie kann diese mindern.

Von Christoph Puppe

Die in diesem Artikel vorgestellten Tools untersuchen Container-Images auf bekannte Schwachstellen, veraltete Software, Fehlkonfigurationen und eingebettete Malware. Ein proaktives Containerscanning ermöglicht den Entwicklungs- und Sicherheitsteams, Probleme zu erkennen, bevor sie im Produktivbetrieb landen. Dieser vorausschauende Ansatz verringert das Risiko von Sicherheitsverletzungen und Complianceverstößen und stellt die Integrität der containerisierten Anwendungen sicher. Alle Angaben in diesem Artikel stammen aus der Dokumentation der Hersteller und einem Kurztest, an dem 15 Hersteller teilgenommen haben.

Risiken beim Einsatz von Containern und einer CI/CD-Pipeline

Jede Schutzmaßnahme sollte konkret eines oder mehrere Risiken in ihren Auswirkungen oder ihrer Eintrittshäufigkeit reduzieren. Die wichtigsten hier im Überblick. Viele Container-Images werden auf Basis öffentlich verfügbarer Images erstellt. Sie können Malware, bekannte und unbekannte Schwachstellen enthalten. Bleiben diese unentdeckt, werden sie in die eigenen Container eingebettet. Auch selbst geschriebener Code für containerisierte Anwendungen und Bibliotheken von Drittanbietern können Anfälligkeiten für Angriffe wie SQL-Injection oder Remote Code Execution (RCE) mit sich bringen. Viele Risiken gehen auch von fehlerhaften Konfigurationen aus, wie die Ausführung als Root, zu viele Mounts auf dem Node oder nicht eingeschränkte Syscalls.

Auch die CI/CD-Pipeline, das Rückgrat der modernen Entwicklung, birgt einzigartige Sicherheitsrisiken für Container. Angreifer können Build-Systeme kompromittieren oder bösartige Abhängigkeiten einschleusen, um Container-Images mit Malware oder Backdoors zu infizieren. Ein enormes Risiko besteht auch, wenn vertrauliche Daten wie Secrets, private Schlüssel, API-Schlüssel oder Datenbankzugangsdaten versehentlich oder absichtlich in Container-Images gelangen. Wer dann Zugriff auf ein solches Image hat, kann diese Secrets für Angriffe ausnutzen. Diese Risiken sind

iX-TRACT

- Container-Security-Scanning identifiziert und behebt Schwachstellen in verschiedenen Phasen des Containerlebenszyklus.
- Viele der verfügbaren Produkte bieten zusätzliche Sicherheitsfunktionen.
- Im Kurztest zeigten sich erhebliche Unterschiede bei der Qualität der Schwachstellenerkennung.

Zentrale Funktionen für Container-Image-Scanner

Die meisten Produkte in diesem Artikel bieten folgende Basisfunktionen in unterschiedlichen Ausprägungen an.

Scannen auf Schwachstellen: Die Kernfunktion von Container-Image-Scannern identifiziert bekannte Schwachstellen (CVE) im Betriebssystem und in den im Image enthaltenen Softwarepaketen. Sie zielt auf häufige Angriffsvektoren ab, bei denen Angreifer bekannte Schwachstellen ausnutzen, um Zugriff zu erlangen oder Schaden anzurichten.

Kontrolle bei der Bereitstellung / Admission Controller: Ein Admission Controller ist wie ein Agent eine Software des Anbieters, die im Cluster – oder zumindest für diesen gut erreichbar – installiert wird. Ein benutzerdefinierter Admission Controller erlaubt dem Scanner, die Bereitstellung von Images zu blockieren, die nicht den Sicherheitskriterien entsprechen. Er erzwingt Sicherheitsrichtlinien in der Bereitstellungsphase und verhindert, dass unsichere Images in die Produktivumgebung gelangen.

Scan nach Secrets: Diese Funktion sucht nach sensiblen Daten wie API-Schlüsseln, Passwörtern und anderen Anmeldeinformationen, die möglicherweise ungewollt in Container-Images eingebettet wurden. Das verhindert die versehentliche Offenlegung von Geheimnissen, die zu unberechtigtem Zugriff oder Datenlecks führen könnte.

Suche nach Malware: Das Erkennen von in Container-Images eingebetteter Malware ist unerlässlich, da Images bösartige Nutzdaten enthalten können, die zur Ausführung in der Zielumgebung bestimmt sind. Die Suche blockiert die Bereitstellung von mit Malware belasteten Images und schützt so vor Kompromittierung.

Erstellen einer SBOM: Eine Software Bill of Materials (SBOM) ist wie eine Zutatenliste für ein Container-Image. Sie listet alle Komponenten, deren Versionen und Abhängigkeiten auf. SBOMs helfen dabei, Schwachstellen zu verfolgen und bei ihrer Behebung die richtigen Entscheidungen zu treffen. Sie bieten Einblick in die Zusammensetzung von Images und ermöglichen eine schnellere Reaktion auf Schwachstellen, die bestimmte Komponenten betreffen.

Nutzung von Paketmanagerinformationen zur Schwachstellenbewertung: Die Integration in Paketmanager ermöglicht Scannern, bekannte Schwachstellen (etwa in Distributionen) mit den in den Images verwendeten Paketen zu vergleichen. Es zielt auf Schwachstellen in gängigen Anwendungen, die Angreifer häufig ausnutzen.

Scannen aller Paketabhängigkeiten in Risikobewertungen: Das Eintauchen in tiefe Abhängigkeiten deckt ein breiteres Spektrum an Schwachstellen auf, da Probleme in Bibliotheken existieren könnten, von denen die Images indirekt abhängen. Es bietet eine umfassendere Bewertung potenzieller Risiken, die sich aus mehreren Abhängigkeitsebenen ergeben.

Umfassende Scans aller Dateien in einem Image: Eine gründliche Untersuchung aller Dateien hilft nicht nur, bekannte Schwachstellen, sondern auch potenzielle Fehlkonfigurationen, eingebettete bösartige Skripte oder andere Anomalien zu erkennen. Sie bietet ein breiteres Sicherheitsnetz, um Probleme zu erkennen, die nicht unbedingt mit bekannten Schwachstellen zusammenhängen.

Image-Richtlinien: Um nur Images zu betreiben, die den Vorgaben, den sogenannten Quality Gates, entsprechen, erstellt man Richtlinien, die die Software auf die Images anwendet. Das kann etwa das Verbot sein, einen sshd im Image zu haben, oder die Vorgabe, dass keine Schwachstellen über einem definierten CVSS-Grad enthalten sein dürfen. Auf diese Weise wird die Sicherheit verbessert, indem die Software nicht nur den Inhalt des Image überprüft, sondern regelt, was überhaupt enthalten sein darf. So kann man den Betrieb verwundbarer oder anderweitig unsicherer Images automatisch ausschließen. Bekannte Open-Source-Vertreter für die Durchsetzung solcher Richtlinien sind Kyverno und der Open Policy Agent (OPA).

nicht nur bei Eigenentwicklungen vorhanden, sondern auch bei externer Software, die oft direkt als Container kommt.

Im Rahmen einer Strategie für Software Supply Chain Security ist es notwendig, auch die Container der Lieferanten zu scannen und Schwachstellen oder SBOMs zu überwachen. Dass diese Software frei von Schwachstellen ist und der Hersteller Sicherheitslücken auch schnell behebt, ist entsprechend in den Verträgen festzuhalten.

Praktiken zum Scannen der Containersicherheit

Das Scannen von Container-Images in den CI/CD-Pipelines ist wichtig, um Schwachstellen schon früh im Entwicklungszyklus zu erkennen. Das ist jedoch keine isolierte Aufgabe, sondern ein kontinuierlicher Prozess, der in den gesamten Containerlebenszyklus integriert ist. Mit geeigneten Tools, der Implementierung von Best Practices und der Förderung einer sicherheitsbewussten Entwicklungskultur können Organisationen das Angriffsrisiko auf ihre containerisierten Umgebungen deutlich reduzieren.

Neben dem Scan der Images – also der statischen Kontrolle des Dateisystems, aus dem der Container gestartet wird – empfiehlt es sich auch, Werkzeuge zur Laufzeitkontrolle zu nutzen. Sie überwachen das Verhalten der Container, erkennen Anomalien oder verhindern bösartige Aktivitäten. Wie der Artikel „Marktübersicht EDR-Systeme: Sicherheit auf den Punkt“ [1] zeigt, ist dies auf den Clients bei Endpoint Security seit vielen Jahren Standard. Server hinken hier leider etwas hinterher.

Wie bei jedem Betriebssystem und jeder Anwendung hilft das Prinzip der geringsten Rechte, Angriffe einzudämmen. Container sollten nur die für ihre Funktion erforderlichen Berechtigungen erhalten. Aber auch die Kontrolle der Herkunft von Container-Images und das Nutzen digitaler Signaturen verringern das Risiko unerwünschter Software.

Last, but not least: Nur wer bei Bekanntwerden von Schwachstellen die Images schnell neu erstellt, hat überhaupt eine Chance, seine Umgebung abzusichern. Das gilt natürlich auch für die Sicherheitssoftware. Ein Scan der Produkt-Images auf Verwundbarkeiten sollte immer erfolgen, wenn eine Lösung zur Absicherung getestet wird – egal, ob mit oder ohne Agent. Der Kasten „Zentrale Funktionen für Container-Image-Scanner“ fasst die in diesem Segment üblichen Funktionen zusammen. Sie sind in den meisten Produkten mehr oder weniger stark ausgeprägt vorhanden und zur besseren Übersicht nicht in der Tabelle mit Kurztests aufgeführt.

Agenten, ja bitte

Alle Produkte in dieser Marktübersicht scannen Images in den Registries oder auch als Teil der Build-Pipeline. Manche bieten auch die Option, zusätzlich Agenten auf allen Nodes in der Containerbetriebsumgebung zu installieren. Dies führt zu einem deutlich erweiterten Schutz. Nur ein Hersteller (Aqua Security Enterprise) kann den Agenten optional als Sidecar in Pods integrieren. Das kann in Umgebungen, in denen man keine Agenten auf den Nodes installieren darf, ein großer Vorteil sein.

Erst Agenten ermöglichen die oben erwähnte Überwachung, aber auch eine Reglementierung zur Laufzeit des Con-

Der Highscore der Verwundbarkeiten der Scanner im Vergleich zum zwei Jahre alten Test-Image zeigt deutliche Unterschiede auf.

tainers. Agenten, die mit Funktionen zur Verhaltensanalyse ausgestattet sind, können aktive Exploits identifizieren, die die Image-Analyse umgangen haben. Durch das Blockieren oder Beenden bösartiger Prozesse zur Laufzeit können Agenten Angreifer daran hindern, Persistenz zu etablieren oder ihre Ziele wie Datendiebstahl oder laterale Verbreitung zu erreichen. Die Überwachung kann Netzwerk, Syscalls, Dateisystem und Speicher umfassen. Agenten bilden auch die Grundlage für die Lernfähigkeit der Laufzeitüberwachung. Dabei wird ein normales Verhalten des Containers erlernt, als Policy gespeichert und diese im Betrieb erzwungen. Der Container darf dann keine Funktionen ausführen, die nicht in der Policy enthalten sind. Eine solche Laufzeitrichtlinie lässt sich natürlich auch manuell erstellen. Zu diesem Thema sei auf andere Artikel zur Absicherung von Containern verwiesen, da dieser Artikel nur die Scanfunktionen betrachtet [2, 3].

Darüber hinaus können nur Agenten detaillierte forensische Daten über Angriffsversuche sammeln. Diese wertvollen Informationen fließen in die Reaktion auf Vorfälle ein und ermöglichen eine gezielte Eindämmung und Ursachenanalyse, um zukünftige Angriffe zu verhindern. Neben der Überwachung können Agenten fein abgestufte Richtlinien auf dem Node selbst durchsetzen. Sie können Netzwerkverkehr, Dateisystemzugriffe und Prozessberechtigungen einschränken. Häufig verwenden sie dazu eBPF, um Filterlisten im Kernel zu hinterlegen. Damit gehen sie weit über die Möglichkeiten hinaus, die Kubernetes über den Security Context und SECCOMP-Profile bietet.

Ein weiterer Vorteil ist, dass Agenten auch Images scannen, nachdem sie auf Nodes gezogen wurden. So können sie Schwachstellen finden, die möglicherweise erst nach dem ursprünglichen Scan des Image entdeckt wurden. Diese Funktion bildet eine zusätzliche Verteidigungslinie. Sie erkennt Lücken, die sich ausnutzen lassen, wenn ein Angreifer Zugriff auf einen Node erhält und ein kompromittiertes zwischengespeichertes Image verwendet. Der Agent kann auch verhindern, dass ein Angreifer ein Image per `docker load` auf den Node lädt und es ohne Scan und Überwachung ausführt.

Einige Hersteller nutzen die Agenten auch, um die Schwachstellenanalyse auf Hostsysteme (Worker Nodes) auszuweiten. Die Images der Container sollten sich zur Laufzeit nicht verändern. Neue oder veränderte Dateien außerhalb des virtu-

Kurztest Container-Image-Scanner

Die Qualität der Sicherheitsscans ist nicht leicht zu beurteilen und es gibt derzeit keinen Service, der einen solchen Test durchgeführt hat. Daher haben wir im März 2024 eine Auswahl der Produkte auf den Prüfstand gestellt. Ein verwundbares Image für den Test ist schnell erstellt: Man nehme eine gut abgehangene Version einer beliebten Linux-Distribution, packe einen SSH-Secret-Key hinein und platziere eine verwundbare NPM-Library an eine Stelle, wo sie nicht hingehört. Ergänzt wird das test3 genannte Docker-Image noch um einen sshd und zum Schluss um einen EICAR-Test-String in der Datei txt.text:

```
FROM ubuntu:jammy-20221101
COPY .ssh/ /var/lib/.ssh/
COPY sshd /var/lib/.ssh/sshd
COPY ua-parser-js-0.7.31/ /var/spool/RUN
mkdir /usr/local/txt
COPY txt.text /usr/local/txt/
```

Dann wurde das Image in GitLab, GCP Artifactory, Azure ACR und GitHub hochgeladen. Die Registries scannen teilweise selbst und sind somit die ersten Testkandidaten. Die Image-Scans der anderen Produkte nutzten dann die Azure Container Registry, um an die Test-Images zu gelangen.

Sofern sich die Ergebnisse exportieren ließen, was bis auf Snyk wegen eingeschränkter Testlizenz bei allen funktionierte, erfolgte die Auswertung anhand der CVE. Jede gefundene CVE wurde dabei nur einmal gezählt. Eine manuelle Überprüfung der CVE kontrollierte alle Funde, die nicht bei allen Teilnehmern auftraten. Eine Verwundbarkeit (CVE-2024-28085) wurde erst während des Tests veröffentlicht und daher von einigen Scannern nicht erkannt. Um die Zahlen nicht zu verfälschen, geht sie bei allen Scannern nicht in die Bewertung ein.

Bei drei CVE waren die Informationen nicht eindeutig, sie sind in der Auswertung ebenfalls nicht enthalten (CVE-2021-46848, CVE-2022-41409, CVE-2023-31486). Nur Clair respektive Quay.io hatte diese drei gefunden. Nach allen Überprüfungen und Checks ist die korrekte Anzahl der CVE im Image 69, kein Scanner hat alle gefunden. Aqua Security Enterprise war mit 68 sehr nah dran, Sophos Cloud Optix, Snyk und Clair waren mit 67 auch sehr gut. NeuVector ist mit 65 ebenfalls im Spitzenfeld.

Bei Qualys ist zu beachten, dass sich die Art der Darstellung der Ergebnisse traditionell von der anderer Scanner unterscheidet. Qualys listet schon immer die verwundbaren Pakete auf und legt weniger Wert auf die CVE. Um dem gerecht zu werden, gab es eine Auswertung nach Anzahl der Pakete, bei der Qualys im Vergleich zu den anderen Produkten dennoch deutlich weniger Pakete im Export der Ergebnisse hatte. Diese Auswertung ist mangels Relevanz nicht im Artikel enthalten.

ellen /tmp sind also nicht erwünscht. Ein Agent auf dem Node kann dies überwachen. Er hilft dabei, Angriffe zu erkennen, die lokale Dateien – ausführbare oder andere – verändern oder neue Software auf das Image aufspielen.

Es ist zu beachten, dass nicht alle Agenten alle diese Funktionen bieten, aber sich diese Funktionen ohne Agenten nicht realisieren lassen. Agenten verbessern die allgemeine Sicherheitslage erheblich, ersetzen aber nicht die Image-Prüfung in der CI/CD-Pipeline. Für einen optimalen Schutz ist immer ein mehrschichtiger Ansatz zu empfehlen.

Agenten, nein danke

Es gibt aber auch gute Gründe, auf Agenten zu verzichten. Der Verzicht auf die Installation von Softwareagenten auf Kubernetes Worker Nodes vereinfacht die Bereitstellung, reduziert den Ressourcenbedarf und verringert das Risiko, dass die Agenten selbst Schwachstellen einführen. Alle Produkte greifen dabei von außen auf die APIs von Kubernetes und der Registry zu.

Einige Produkte bieten auch die Installation eines lokalen Agenten an, der als Vermittler fungiert. Dies ist eine Möglichkeit, in stark abgeschotteten Clustern die Nodes dennoch von einer zentralen Konsole aus zu überwachen. Solche Proxys für den API-Zugriff werden in diesem Artikel nicht als Agent gewertet, beispielsweise der von Tenable.

Auch wenn manche Hersteller damit werben, dass sie die Sicherheit ohne Agenten gewährleisten, ist es nicht möglich, die erhöhten Anforderungen des BSI aus den Bausteinen APP.1.6 Containerisierung und APP.4.4 Kubernetes vollständig ohne Agenten zu erfüllen.

Eigene Verwundbarkeiten

Auch die Images der Sicherheitssoftware sind für den Vergleich der Angebote interessant, denn auch diese selbst können Verwundbarkeiten enthalten. Daher wurden alle Produkte im Kurztest (siehe Kasten „Kurztest Container-Image-Scanner“) gescannt, ebenso alle anderen, sofern die Images frei verfügbar waren. Bei den SaaS-Angeboten umfassten diese Scans nur die Agenten, bei den On-Premises-Varianten auch die Images der Server. Wurde mehr als ein Image gescannt, liefert die Tabelle den Durchschnitt. Wo eine Trial-Version verfügbar war oder der Hersteller eine bereitstellt, sind die Ergebnisse des Kurztests in die Tabelle eingeflossen.

Glossar

CI/CD – Continuous Integration / Continuous Delivery (oder Deployment): Die Praxis, Codeänderungen, Builds, Tests und Bereitstellungen zu automatisieren, um Softwarereleaseprozesse zu rationalisieren.

CWPP – Cloud Workload Protection Platform: Eine umfassende Sicherheitslösung zum Schutz von Anwendungen und der darin verarbeiteten sensiblen Daten in Cloud-Umgebungen, einschließlich Container.

CSPM – Cloud Security Posture Management: Software, die Cloud-Konfigurationen (inklusive Containerumgebungen) kontinuierlich auf Fehlkonfigurationen, Schwachstellen und Verstöße gegen Compliancevorschriften überprüft.

CNAPP – Cloud-Native Application Protection Platform: Eine Suite von Sicherheitswerkzeugen, die sich auf den gesamten Lebenszyklus von Cloud-nativen Anwendungen (einschließlich Container) konzentrieren und Workload-Schutz, Schwachstellenscans, Complianceüberwachung und vieles mehr bieten.

CVE – Common Vulnerabilities and Exposures: Eine öffentlich zugängliche Datenbank mit bekannten Sicherheitslücken.

DLP – Data Leakage Prevention: Methoden zum Verhindern von Datenabfluss.

SBOM – Software Bill of Materials (Softwarestückliste): Eine detaillierte Auflistung aller Softwarekomponenten, Abhängigkeiten und ihrer Versionen innerhalb einer Anwendung oder eines Systems, die häufig zur Schwachstellenverfolgung verwendet wird.

WAF – Web Application Firewall: HTTP-Proxy, der Angriffe erkennt und unterbindet.

XDR – Extended Detection and Response: Eine Weiterentwicklung von EDR, die die Sichtbarkeit und Sicherheitskontrollen auf Netzwerke, Cloud-Umgebungen und andere Bereiche ausweitet.

Um die Image-Scans der hier vorgestellten Produkte besser mit den Scans der Managed-K8s-Angebote aus der letzten Artikelserie [4] vergleichen zu können, kamen wieder der gleiche Scanner (Aqua Security Enterprise) und dessen Risikobewertungen zum Einsatz. Zur Sicherheit wurden die Images auch mit Sophos gescannt. Die Tabelle „Marktübersicht Produkte zum Container-Image-Scanning – mit Kurztest“ zeigt die Ergebnisse von AquaSec.

Aqua Security Enterprise

Die SaaS-Variante von Aqua Security Enterprise liefert eine vollständige CNAP-, CSPM- und CWPP-Suite (siehe Kasten „Glossar“) mit einem starken Fokus auf selbstlernende Überwachung der Container und dem Verhindern von Einbrüchen. Eine der Registries anzubinden geht schnell. Die Auswahl des Repositorys ist dank eingebauter Suche sehr einfach. Wenige Minuten später liegt das Ergebnis vor und ist mit einem Klick heruntergeladen. Im Image test3 hat es die Malware nicht erkannt, da es nur ausführbare Dateien scannt. In einem geänderten Image, in dem wir die Datei mit dem EICAR in test.sh umbenannt und ausführbar gemacht haben, erkennt Aqua den EICAR-String. Auch die anderen Produkte scannten dann dieses Image, entdeckten die Malware aber weiterhin nicht. Bis auf eine etwas obskure Verwundbarkeit, die es nicht fand (CVE-2022-40735), hat Aqua Security Enterprise im Test am besten abgeschnitten.

Sophos Cloud Optix

Sophos liefert mit Cloud Optix eine CWPP-, CSPM-Lösung inklusive Anzeige der Kosten in den angebundenen Umgebungen. Es bietet Überwachung der drei großen Hyperscaler, Kubernetes-Cluster, Git und Container-Registries. Der Test erfolgt mit einem kostenlosen Testaccount ohne funktionale Einschränkungen. Als Registry ist nur Docker Hub möglich, was die Auswahl etwas einschränkt. Sofern bereits eine Cloud-Anbindung besteht, sind die dort enthaltenen Registries und ihre Repositorys automatisch sichtbar. Die Verbindung zu Azure ACR erfordert allerdings noch einen Service Principal. Das Anbinden an die CSPM-Funktionen ist mit zwei PowerShell-Befehlen erledigt und klappt auf Anhieb. Die drei Images wandern sofort in die Scan Queue, die Ergebnisse liegen fast augenblicklich vor und lassen sich mit einem Klick als CSV exportieren. Positiv fällt auf, dass Sophos die Nutzer zu einer FIDO2-MFA zwingt. Bei den weitreichenden Rechten, die CNAP- und CWPP-Anwendungen haben, sollte das eigentlich selbstverständlich sein. Zusammen mit dem sehr guten Ergebnis beim Scannen der Images ist das ein sehr überzeugender Auftritt im Test.

Snyk

Snyk verfolgt einen entwicklerorientierten Ansatz mit tiefer Integration in Entwicklungswerkzeuge und Repositorys. Im Gegensatz zu den meisten anderen

Marktübersicht: Produkte zum Container-Image-Scanning – mit Kurztest

Produktname	Anchore Enterprise	Aqua Security	Azure Defender für Containerregistrierung	Clair	Datadog Container Security	Elastic Container Registry / Elastic Scan
Hersteller	Anchore	Aqua Security Software	Microsoft	Red Hat	Datadog	Amazon
Beschreibung	Fokus auf richtlinienbasierte Image-Scans und Governance; lässt sich gut in CI/CD-Pipelines integrieren	umfassende Plattform für Image-Scans, Runtime-Schutz und Schwachstellenmanagement Trivy ist als OSS und Teil der Enterprise Edition verfügbar	native Integration in Azure Kubernetes Service (AKS), Schwerpunkt auf Azure-Umgebungen	Clair ist nur ein Verwundbarkeitsscanner ohne weitere Funktionen. Es wird unter anderem in Quay.io eingesetzt.	starker Fokus auf Observability und integrierte Überwachung für Container	in AWS enthaltene Container-Image-Registry
als Open Souce verfügbar	ja	(ja, Trivy)	nein	ja	ja	nein
Node Agent	nein	ja	ja	nein	nein	n. a.[1]
Admission Controller	ja	ja	nein	nein	ja	n. a.[1]
CVE korrekt	61	68	47	67	n. a.[2]	48
CVE False Negative	8	1	22	2	n. a.[2]	21
CVE False Positive	0	0	6	11	n. a.[2]	6
eigene Verwundbarkeiten	52	28	0	59	59	n. a.[1]
ParserJS gefunden	ja	ja	ja	nein	n. a.[2]	ja
Secret Key gefunden	nein	ja	nein	nein	n. a.[2]	nein
Malware gefunden	nein	ja	nein	nein	n. a.[2]	nein
Webseite	anchore.com	aquasec.com	microsoft.com	quay.github.io/clair/	securitylabs.datadoghq.com	aws.amazon.com

[1] Registry als SaaS, daher nicht anwendbar. [2] Im Test ist es nicht gelungen, ein Image zu scannen. [3] Die „Report"-Funktion war im Test nicht enthalten, daher kein Export der Verwundbarkeiten und

Produkten ist es auf Codesicherheit und SAST spezialisiert, scannt aber auch Container. Eine Laufzeitüberwachung mit Node Agents, einen Admission Controller oder weitere CNAP- und CSPM-ähnliche Funktionen hat es nicht. Der Test erfolgt mit einem kostenlosen Testaccount, der keine Reports erstellt, aber den vollen Funktionsumfang bietet.

Auch hier ist die Registry schnell verbunden und es wird eine Liste der gefundenen Repositorys gezeigt. Mit einem Klick ist der Scan gestartet. Optional lässt er sich auf der Kommandozeile starten. Das Ergebnis ist sehr schnell da, einen Download als CSV erlaubt die Testversion aber leider nicht. Der Abgleich nach mehrfachen CVE-Funden des Scans erfolgte daher über die sehr flotte und intuitive Weboberfläche. Positiv fiel auf, dass Snyk per Mail über eine neue, während des Tests bekannt gewordene CVE informierte. Auch die Ergebnisse des Scans überzeugten, allerdings fehlten die NPM-Verwundbarkeiten und auch das SSH-Secret hat Snyk nicht erkannt. Die Zahl der eigenen Verwundbarkeiten trübte das Bild zusätzlich.

Quay.io / Clair

Da Clair in Quay.io für die Containerscans im Einsatz ist und es recht komplex ist, die Open-Source-Variante von Clair selbst aufzusetzen, nutzt der Kurztest die Ergebnisse aus Quay.io für den Vergleich. Auch bei Quay.io startet direkt nach dem Hochladen der Scan. Immerhin wurden 161 CVE gefunden, davon wieder viele doppelt – nach dem Entfernen der doppelten blieben 81 übrig. Das etwas versteckte NPM-Paket fand Quay nicht. Auch die hohe Zahl der fehlerhaften Funde ist negativ zu bewerten. Das Image von Clair selbst enthält sehr viele Verwundbarkeiten. Beides sorgt für eine nicht ganz so positive Bewertung.

Sysdig Secure / Falco

Sysdig war schon immer ein starker Anbieter von Monitoringpaketen und brachte mit Falco sowie Sysdig Secure als einer der ersten Anbieter auch eine CWPP auf den Markt. Diese Herkunft ist heute noch in allen Produkten der Firma bemerkbar: Der Fokus liegt auf Überwachung, Auswertung und Präsentation. Die Funktionen zur selbstlernenden Laufzeitüberwachung setzen darauf auf. Leider lag keine Testlizenz vor, aber in GCP kostet ein Monat nur 72 Euro plus Nutzung. Nach dem Kauf schaltete Sysdig dann auch die angefragte Testlizenz frei. Mit dem Zugang zum SaaS-Angebot Sysdig Secure ist die Azure-Registry schnell angebunden und der Scan gestartet.

Die Images von Sysdig liegen in GitHub. Drei Images mit zusammen fünf High, 336 Medium und knapp 200 Low CVE sind eine überraschend hohe Zahl, die auch im Vergleich zu anderen Produkten nicht erklärbar ist. Auch in früheren Scans der Images der Sysdig ist bereits die hohe Zahl von Verwundbarkeiten aufgefallen [5]. Das Thema Sicherheit der eigenen Software scheint bei diesem Hersteller nicht so hoch priorisiert zu sein, was erstaunt, da die eigenen Produkte doch Kunden dabei helfen sollen, sichere Images zu betreiben. Das entwertet das ansonsten sehr gute Ergebnis im Test.

NeuVector

Seit der Übernahme durch SUSE Ende 2021 ist bei NeuVector relativ wenig passiert. Da es eine der ersten vollständigen CWPPs war, muss das nicht unbedingt schlecht sein. Die versprochenen Funktionen arbeiten weiterhin sehr gut. NeuVector legt seinen Fokus auf das Netzwerk, dessen Überwachung und Analyse. Es ist die einzige CWPP, die in Clustern IP-Pakete mitschneiden kann. Auch der WAF- und DLP-Sensor ist für eine CWPP unüblich. Es ist als einziges Produkt vollständig als Open Source verfügbar. Die Installation mit Helm klappt schnell und reibungslos, mit dem Parameter `manager.svc.type=LoadBalancer` ist das Web-UI auch aus dem Internet erreichbar.

Die im Test genutzte Registry hinzufügen ist unkompliziert. Eingabe eines Filters ist Pflicht, mit * scannt NeuVector

	GCP Artifact Registry	NeuVector	Qualys Container Security	Quay	Snyk Container	Sophos Cloud Optix	StackRox / Red Hat Advanced Container Security	Sysdig Secure	Trend Vision One
	Google	SUSE	Qualys	Quay.io	Snyk	Sophos	Red Hat	Sysdig	Trend Micro
	Die in GCP enthaltene Artifactory-basierte Registry speichert Artefakte aller Art und ist tief in GCP integriert.	Containersicherheit über den gesamten Lebenszyklus, mit Schwerpunkt auf Laufzeitschutz und Analyse des Netzwerksicherheitsverhaltens	etablierter Anbieter für Schwachstellenmanagement, jetzt mit soliden Funktionen für Containersicherheit	Quay nutzt Clair und daher sind die Ergebnisse identisch.	entwicklerorientierter Ansatz, tiefe Integration in Entwicklungswerkzeuge und Repositorys	etablierter Anbieter von Endpoint-Sicherheit mit Komponenten zum Schutz von Containern	auf Basis von StackRox tief in Red-Hat-OpenShift- und -Enterprise-Linux-Umgebungen integriert	umfassende Sicherheits- und Observability-Plattform mit starken containerspezifischen Funktionen	breit ausgelegte Sicherheitsplattform mit Modulen zum Schutz von Containern
	nein	ja	nein	ja	ja	nein	ja	ja	nein
	n. a.[1]	ja	ja	n. a.[1]	nein	nein	ja	ja	ja
	n. a.[1]	ja	ja	n. a.[1]	nein	nein	ja	ja	ja
	59	65	39	67	67	67	48	66	58
	10	4	30	2	n. a.[3]	2	21	3	11
	0	0	6	11	n. a.[3]	0	0	0	0
	n. a.[1]	3	17	n. a.[1]	41	n. a.[1]	40	179	0
	ja	nein	nein	nein	nein	ja	nein	nein	nein
	nein	ja	nein	nein	nein	ja	nein	nein	nein
	nein	nein	nein	nein	nein	nein	nein	nein	nein
	cloud.google.com	suse.com	qualys.com	quai.io	snyk.io	sophos.com	redhat.com	sysdig.com	trendmicro.com

keine Liste der Pakete möglich.

alle Images. Etwas unschön fällt auf, dass es keine Änderung des Defaultpassworts erzwingt. Die Scanergebnisse sind gut, auch wenn es die verwundbare NPM-Bibliothek oder die Malware nicht fand. Das SSH-Secret wird gefunden. Auch sind die Images von NeuVector fast ohne Schwachstellen und schneiden in dieser Kategorie sehr gut ab. Das Paket hat damit einen verdienten Platz in der Spitzengruppe, und wer kostenlos eine umfangreiche CWPP mit Node Agents und Admission Controller als Open Source betreiben möchte, ist hier gut aufgehoben.

Anchore

Anchore konzentriert sich auf Kubernetes und Container und bietet die für eine CWPP üblichen Funktionen und einen Admission Controller. Laufzeitüberwachung oder ein Node Agent sind nicht enthalten. Seine Stärken sind Tiefenanalyse von Images und eine flexible, aber auch komplexe Richtlinien-Engine. Als kostenlosen Trial bietet Anchore einen AWS CloudFormation Stack. Sofern es schon einen SSH-Key gibt, ist der auch schnell erstellt. Die ECS-VM enthält dann drei Images und eine Datenbank, die alle als Docker-Container laufen. Das Hinzufügen der Registry und des Repositorys ist einfach und übersichtlich.

Der Scan startet automatisch, die Ergebnisse gibt es direkt zum Download als CSV oder JSON. Anchore fand die NPM-Bibliothek und deren Verwundbarkeiten. Auch der SSHD ist in der SBOM enthalten. Im Default-Policy-Set fand Anchore das SSH-Secret oder die Malware nicht. Auch eine neue Policy, die explizit nach Secrets und Malware sucht, fand beides nicht. Vielleicht war die Policy auch nicht korrekt, der Editor ist komplex und hat viele Parameter. Dass es nicht alle CVE fand und selbst einige Verwundbarkeiten enthält, trübt den Gesamteindruck erheblich.

GCP Artifact Registry

Nach dem Hochladen des Image erfolgt sofort ein Scan mit der von Google bereitgestellten Container Scanning API. Zusätzliche Kosten entstehen dabei nicht, allerdings sind aktuell nur Scans von bekannten Linux-Distributionen sowie Go und Java mit Maven möglich. Die Registry selbst unterstützt von Docker-Images über NPM, Go und Python die üblichen Formate und Programmiersprachen. Wie alle Ressourcen bei GCP reicht eine Option, um die Registry nur in den eigenen Netzen bereitzustellen. Die Ergebnisse des Image-Scans liegen nicht in der Spitzengruppe, immerhin 10 CVE hat es nicht gefunden. Was positiv überrascht, ist, dass eigentlich keine NPM-Scans erfolgen, es aber die etwas versteckte verwundbare Bibliothek doch fand.

Trend Vision One

Trend Micro hat sein Angebot für CNAP, CWPP, CSPM, ZTSA, SASE (siehe Glossar) und automatisierte Reaktion auf Sicherheitsvorfälle mit XDR grundlegend überarbeitet. Seit Februar 2021 ist es als Managed XDR verfügbar. Trend Vision One benötigt für den Image-Scan laufende Container, alternativ lässt es sich aus einer CI/CD-Pipeline über API ansprechen. Es überwacht EKS, ECS, AKS, GKE und selbst betriebene K8s. Images direkt aus Registries laden kann One nicht.

Die Anbindung an AWS erfolgt mit CloudFormation und konnte im Test nicht erfolgreich abgeschlossen werden. Azure anzubinden ist noch in Preview und etwas aufwendiger, da erst ein Terraform-Skript herunterzuladen ist. Das war im ersten Anlauf gleich erfolgreich. Die ACR zeigt One allerdings nicht an und dementsprechend auch nicht das Test-Image. Sobald das Image in AKS gestartet ist, wird es angezeigt und auch gescannt. One findet nicht alle Verwundbarkeiten und auch die verwundbare NPM oder das SSH-Secret bleiben unentdeckt.

Da One auch nach Malware sucht, wurde auch das test4-Image mit der umbenannten EICAR-Datei in AKS gestartet. One fand auch in diesem Image keine Malware. Auch das Aktivieren von Log oder Deny bei Malware in der mitgelieferten Policy und einer selbst erstellten

Marktübersicht Produkte zum Container-Image-Scanning – ohne Kurztest

Produktname	CrowdStrike Falcon Cloud Security	GitHub	GitLab	Orca Security Platform
Anbieter	CrowdStrike	GitHub (Microsoft)	GitLab	Orca Security
Beschreibung	Teil einer umfassenderen Endpoint-Security-Suite, die Containersicherheit in diesem Kontext bietet	bekanntes SaaS-Angebot zum Verwalten von Quellcode, das auch die Speicherung von Images erlaubt	bekanntes SaaS-Angebot zum Verwalten von Quellcode, das auch die Speicherung von Images erlaubt	legt Wert auf agentenlose Sicherheit und konzentriert sich auf die schnelle Erkennung von Schwachstellen ohne Containerbereitstellungen
Node Agent	ja	n. a.[1]	n. a.[1]	nein
Admission Controller	ja	n. a.[1]	n. a.[1]	nein
Vorteile	Viele Image Policies vorhanden. Selbstlernende Runtime-Überwachung. Gut um Endpoint Security mit Containersicherheit zu erweitern. CrowdStrike hat sich mit KI-basierter Angriffserkennung einen Namen gemacht.	Scan ist Teil des Angebots.	Scan ist Teil des Angebots. GitLab gibt es auch als On-Premises-Version.	schnelle Einrichtung, breite Abdeckung von Cloud-Ressourcen
Nachteile	Anfrage nach Testversion nicht beantwortet	Scan des Image nur im Build-Vorgang möglich, daher hier nicht getestet	Scan des Images nur im Build-Vorgang möglich, daher hier nicht getestet	keine Agenten und damit keine Runtime-Überwachung
Webseite	www.crowdstrike.com/products/cloud-security/	github.com	gitlab.com	orca.security

[1] Registry als SaaS, daher nicht anwendbar

Policy halfen nicht. Es ist aber nicht auszuschließen, dass hier ein Bedienfehler vorlag. Der Scan der Images des Admission Controllers und des Scan Managers ergab keine Verwundbarkeiten. So sollte das immer bei Sicherheitssoftware sein.

StackRox / Red Hat Advanced Container Security

Red Hat übernahm Anfang 2021 die Firma StackRox und hat deren Produkt in das OpenShift-Bundle Advanced Container Security (ACS) integriert. Im Test enthalten ist daher das komplette Bundle. ACS ist eine klassische CWPP mit den üblichen Funktionen. Laufzeitüberwachung ist allerdings nicht enthalten, auch wenn es einen Node Agent gibt. Dieser sammelt allerdings nur Informationen über den Cluster. Es gibt eine Trial-Version, die innerhalb weniger Minuten eine Instanz in AWS erzeugt. Die ACR ist schnell angebunden und das Hinzufügen des Test-Image per komplettem Pfad verlief erfolgreich. Leider gibt es keine Suchfunktion für die Images. Der sshd findet sich weder in der Liste der Verwundbarkeiten noch in der SBOM.

Verwundbarkeitsmanagement ist entweder in Version 1 als ausgereiftes Produkt oder in Version 2 als Preview verfügbar. Die Ergebnisse des Scans unterscheiden sich nicht. An einigen Namen von Token und Variablen ist die Herkunft gut zu erkennen. Version 1 meldet auch noch, dass StackRox den Scan durchführt. Um auch die Verwundbarkeiten in ACS selbst zu untersuchen, war es notwendig, einen Cluster anzubinden. Der Scan untersuchte die dort zum Einsatz kommenden Images von ACS. Negativ fiel die geringe Zahl gefundener CVE auf. Die versteckte Library und den SSH-Secret-Key hat ACS auch nicht erkannt. Die ACS-Images enthalten viele Verwundbarkeiten, einige davon im main-Image mit Risikostufe High.

Elastic Container Registry

AWS bietet mit der ECR eine Registry für Container-Images, die exakt diesen Zweck erfüllt, aber auch nicht mehr. Für das Speichern anderer Artefakte sind andere AWS-Dienste verfügbar. Nachdem man sich erinnert hat, in welcher Region die ECR läuft, ist das Hochladen der Images einfach und auch das Scannen erfolgt umgehend. Es stehen mehrere Optionen zur Auswahl. Einerseits Basic, die Clair nutzt und kostenlos ist. In Basic gibt es auch einen verbesserten Modus als Vorschau. Kostenpflichtig ist die Scan-Option Verbessert. Der Test nutzte den verbesserten Modus aus Basic und die Option „Verbessertes Scannen“.

Bis auf CVE-2023-6237, die nur der kostenpflichtige Modus fand, sind beide Ergebnisse identisch. Beide fanden die verwundbare NPM-Bibliothek, aber nicht das SSH-Secret. ECR bildet mit Azure Defender for Container das Schlusslicht des Tests bei der Zahl der erkannten CVE. Für die kostenlose Variante vielleicht ein akzeptables Ergebnis, aber für einen „verbesserten“ und kostenpflichtigen Dienst inakzeptabel. Vielleicht erklärt dies aber auch die in der Serie über die Absicherung von K8s gefundene extrem hohe Anzahl von teils schwerwiegenden Verwundbarkeiten in AWS-Images, die EKS-Cluster verwalten. Hier wartet auf AWS noch einiges an Arbeit.

Azure Container Registry mit Defender für Container

Azure bietet mit der ACR eine funktionale Container-Image-Registry. Um den Scan mit Defender for Container zu aktivieren, ist der kostenpflichtige Defender Plan für die Registry zu aktivieren. Dann finden sich die Scanergebnisse etwas später auch im Defender for Cloud unter Workload Protection und der Registry. Der Defender for Container kann auch eine begrenzte Auswahl von anderen Registries scannen. Den Scan führt seit Anfang März nicht mehr Qualys, sondern die Microsoft-eigene Scan Engine durch. Getestet wurde das Image für den Defender Stable Pod Collector, das frei von Verwundbarkeiten war. Etwas überraschend ist, dass sehr viele False Positives die gleichen wie bei Qualys sind, obwohl doch die Scan Engine seit März eine andere ist. Insgesamt ist das Ergebnis fast identisch mit ECS und somit auch enttäuschend.

Qualys Container Security

Qualys bietet die wohl umfangreichste Plattform im Test. Wie bei den anderen Plattformen konzentrierte sich der Test nur darauf, die Images auf Verwundbarkeiten zu prüfen. Laufzeitüberwachung mit Node Agent und Admission Controller ist im Produkt enthalten, aber im Test nicht bewertet. Dank der Testversion ist ein Account schnell eingerichtet und gibt Zugriff auf alle Elemente der sehr umfangreichen Werkzeugkiste von Qualys.

	Prisma Cloud	SentinelOne Singularity Cloud	Symantec Cloud Workload Protection	Tenable.io	Wiz.io
	Palo Alto Networks	SentinelOne	Broadcom	Tenable	Wiz
	umfassende Cloud-Sicherheitsplattform mit robustem Modul (ehemals TwistLock) für Containersicherheit	Teil einer umfassenderen Endpoint-Security-Suite, die Containersicherheit in diesem Kontext bietet	breit ausgelegte Sicherheitssuite, die sich auf Containersicherheit erstreckt	etablierter Schwachstellenfokus, jetzt mit Containersicherheitsintegration	umfangreiche Suite mit Werkzeugen zum Absichern von Clouds und Containern
	ja	ja	ja	ja	ja
	Open Policy Agent	ja	ja	ja	ja
	TwistLock ist einer der ersten Anbieter von Containersicherheit gewesen.	Gut geeignet, wenn Containersicherheit eine Erweiterung der bestehenden Endpoint-Strategie ist. SentinelOne hat sich mit KI-basierter Angriffserkennung einen Namen gemacht.	gute Wahl für Anwender, die bereits mit Symantec-Tools arbeiten	eingebunden in eine umfangreiche Suite zum Schwachstellenmanagement	Fokus auf präzise Risikobewertung und Cloud-native Workflows
	Die Integration von TwistLock in Prisma ist vorhanden. Seit der Übernahme wenig neue Funktionen.	weniger spezialisiert auf eigenständige Container-anwendungsfälle	vor einiger Zeit von Broadcom übernommen worden	Anfrage nach Testversion nicht beantwortet	Admission Controller und Agents sind relativ neu, Anfrage nach Testversion nicht beantwortet.
	prismacloud.io	www.sentinelone.com	techdocs.broadcom.com	docs.tenable.com	wiz.io

Das Scannen eines Image erfordert einen als Container zu startenden Registry Agent und die Zugangsdaten für die Registry. Leider bietet das Web-UI keine Suche in der Registry, aber nach der manuellen Eingabe des Repository-Namens ist das Image geladen und wird gescannt. Ein Klick lädt eine Liste der Verwundbarkeiten herunter.

Etwas überraschend findet dieses Produkt eines doch sehr renommierten Anbieters von Verwundbarkeitsmanagement nur 39 Schwachstellen und entdeckt weder die Malware noch das SSH-Secret oder die verwundbare NPM-Bibliothek. Auch hier wurde das Ergebnis mit dem test4-Image überprüft, ohne die Malware zu finden. Positiv ist, dass das Container-Image des Qualys Broker, ohne den kein Scan möglich ist, nur 17 Verwundbarkeiten enthält. Allerdings sind fünf davon „high“. Da das Ergebnis überrascht, hab ich es mehrfach überprüft.

Datadog

Auch Datadog kommt wie Sysdig eher aus der Welt der Monitoringsoftware. In der sehr umfangreichen Werkzeugkiste sind Monitoring, Metriken, Integrationen in Dienste und auch Servicemanagement die zentralen Themen. Im Reiter Security sind ein Cloud SIEM und ein CSPM enthalten. Der Test erfolgt mit einem kostenlosen Testaccount, der keine funktionalen Einschränkungen hat. Auch hier ist das Einrichten eines Agenten Pflicht. Datadog kann sich auch per API mit den Kubernetes-Clustern verbinden und so die dort laufenden Images einsammeln und scannen.

Leider kann es sich nur mit der AWS-Registry verbinden. Will man einen Container überprüfen, ohne dafür einen Kubernetes-Cluster zu starten, muss das Image also dort liegen. Das Scannen statischer Images aus Registries ist ein neues Feature bei Datadog. Das Set-up, um die Images dann auch zu scannen, ist relativ komplex und benötigt das Editieren mehrerer Konfigurationsdateien des Agents. Im Test gelang es nicht, ein Image aus der Registry nach Verwundbarkeiten zu scannen. Zusammen mit der sehr hohen Anzahl an Verwundbarkeiten hinterließ Datadog somit keinen guten Eindruck.

Fazit

Die Wahl des richtigen Tools zum Scannen von Containern hängt von den spezifischen Anforderungen des Unternehmens ab. Faktoren wie Bereitstellungsumgebungen (Cloud, lokal, hybrid), Entwicklerworkflows, Complianceanforderungen, vorhandene Sicherheitsprodukte und Budgetbeschränkungen spielen eine entscheidende Rolle. Auch wenn die meisten Produkte immer die gleichen Funktionen bieten, gibt es doch Unterschiede. Hier stellt sich die Frage, ob eine Überwachung der Container zur Laufzeit und damit auch Agenten auf den Nodes gewünscht sind. Die Sicherheit der Umgebung steigt durch dieses etwas aufwendigere Feature erheblich.

Auch wenn die meisten Produkte immer die gleichen Funktionen bieten, gibt es doch Qualitätsunterschiede. Im Test hat nur ein Produkt 68 von 69 möglichen Verwundbarkeiten gefunden. Auch gibt es Kandidaten, die selbst viele Verwundbarkeiten mitbringen und deren Einsatz daher sehr kritisch zu betrachten ist. Letztlich sind neben den nicht erkannten Schwachstellen auch die fehlerhaft erkannten bei sehr bekannten Produkten problematisch. (avr@ix.de)

Quellen

[1] Kristian Kißling, Dominic Pfeil; Marktübersicht EDR-Systeme: Sicherheit auf den Punkt; iX 5/2024, S. 68

[2] Christoph Puppe; Besondere Schutzanforderung; Neuer Entwurf des BSI-Bausteins zu Containern; iX 5/2020, S. 88

[3] Christoph Puppe, Jan Walther; Kubernetes mit Capabilities, SECCOMP und SELinux; iX 12/2022, S. 60

[4] Christoph Puppe; OpenShift und Rancher nach BSI härten; iX 6/2023, S. 60

[5] Christoph Puppe; Blitzableiter und Regenschirme; Tools zur Absicherung von Containern; iX kompakt 2019 – Container, S. 98

CHRISTOPH PUPPE

ist Principal Enterprise Security Architect und Auditteamleiter für ISO 27001 nach Grundschutz bei NTT DATA Deutschland SE, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.