Compliance Management für die Cloud

Überblick, Einsicht und Kontrolle

Christoph Puppe

Besonders bei Cloud-Diensten reicht ein falscher Klick, um alle Daten zu veröffentlichen oder Angreifern Tür und Tor zu öffnen. Wenn in großen Umgebungen viele Server im eigenen RZ und Tausende Clients hinzukommen, ist es schwierig, alle Einstellungen im Blick zu behalten. Compliance-Management-Werkzeuge versprechen hier Abhilfe.

Eine IT-Weisheit lautet: Was man nicht messen kann, kann man managen. Sicherheit messen wird oft versucht und nur selten sind es die ausgewählten Key-Performance-Indikatoren (KPI), die tatsächlich Überblick, Einsicht und Kontrolle ermöglichen. So sagt beispielsweise die Zahl der Portscans oder gefundener Viren auf dem Mail-Gateway wenig über die reale Sicherheit der Organisation aus. Schon deutlich aussagekräftiger ist die Zahl der Schwachstellen auf den Systemen, aber auch das ist nur ein Teil der Wahrheit.

Viele Einbrüche sind die Folge falscher Systemparameter. Besonders bei Cloud-Diensten drohen bei kleinen Nachlässigkeiten fatale Folgen. Ob es nun nur das eigene Rechenzentrum ist oder eine Multicloud: Alle Einstellungen zu überwachen ist manuell faktisch nicht möglich. Hier kommen Begriffe wie Security Configuration Compliance (SCC), Secure Configuration Assessment (SCA), Cloud Security Posture Management (CSPM) oder Security Orchestration Automation and Response (SOAR) ins Spiel. Die Namen sind unterschiedlich, die Bedeutung ist mit kleinen Unterschieden ähnlich.

Ausgangspunkt für diesen Artikel war die Suche nach einem Produkt, das in einem typischen IT-Betrieb mit VMware, Windows AD und -Clients, Kubernetes sowie Public-Cloud-Diensten wie AWS, Azure und GCP alle Teile der IT-Landschaft auf fehlerhafte Einstellungen überwachen und diese auch beheben kann. Ein

Marktübersicht Compliance Management – Schwachstellenscanner				
Name	**InsightVM**	**tenable.io**	**Qualys SCA & CSA**	**SAINT Security Suite**
Anbieter	Rapid7	Tenable	Qualsys	Carson & SAINT
Typ	Schwachstellenscanner	Schwachstellenscanner	Schwachstellenscanner	Schwachstellenscanner
Lizenz	kommerziell	kommerziell	kommerziell	kommerziell
SaaS / on Premises	✓/–	✓/✓	✓/✓	✓/✓
Beheben	✓	–	–	–
Agents	✓	✓	✓	✓
AWS	✓	✓	✓	✓
Azure	–	✓	✓	✓
GCP	–	✓	✓	–
Windows AD	✓	✓	✓	✓
Windows-Systeme	✓	✓	✓	✓
Linux/Unix	✓	✓	✓	✓
Docker	–	✓	✓	–
Kubernetes	–	✓	✓	–
VMware	✓	✓	✓	–

Dashboard für alle Ergebnisse mit Planung der automatisierten Behebung ist der Traum jedes Chief Information Security Officer (CISO). Endlich alle Risiken auf einen Blick, und das auch über alle Umgebungen und Betriebssysteme hinweg.

Cavirin, Tripwire Configuration Compliance Manager, ServiceNow Configuration Compliance, Nessus und Qualys SCA können die genannten Systeme überwachen und gehen zumeist noch weit darüber hinaus. Allen im Artikel vorgestellten Produkten ist gemein, dass sie nicht nur über eine Weboberfläche zu bedienen sind, sondern auch eine API bereitstellen, mit der man sie in die eigenen Prozesse automatisiert einbinden kann. So wie auch die Verwaltung der Benutzer sind diese Aspekte daher nicht in der Tabelle enthalten.

Ein unübersichtlicher Markt

Der Markt ist riesig – Anlass genug, hier einen Überblick zu geben und die grundlegenden Funktionen sowie einige der Unterschiede aufzuzeigen. Für diesen Artikel hat der Verlag Testlizenzen bei rund zwei Dutzend Herstellern angefragt. Eine Lizenz stellten zur Verfügung: Aqua Security (Enterprise), Trend Micro (Conformity), Palo Alto Networks (Prisma), Rapid7 (InsightVM), Runecast und Sysdig (Secure). Für die anderen Produkte flossen die öffentlich verfügbaren Informationen in Tabelle und Kurzvorstellung ein. Kommerzielle, proprietäre Angebote dominieren den Markt für viele Sicherheitsprodukte, während Open-Source-Software keine nennenswerte Rolle spielt.

Um einen Überblick über die Werkzeuge zu erhalten, die ja selbst Überblick verschaffen sollen, sind zuerst vier Gruppen zu benennen. Die bekannteste Gruppe sind Werkzeuge zum Verwundbarkeitsmanagement, die schon früh angefangen haben, die verwalteten Systeme auf fehlerhafte Einstellungen zu untersuchen. Dann ist da noch die Gruppe der reinen SCC-Tools (Security Configuration Compliance). Die dritte Gruppe sind CWPP-Produkte (Cloud Workload Protection Platform). Und die vierte Gruppe sind jene Tools, die die Hersteller bei ihren Produkten mit anbieten.

Keiner Gruppe zugehörig, aber dennoch zu erwähnen ist SolarWinds' Network Configuration Manager, der die Netzwerkprodukte von Cisco und Palo Alto Networks auf unsichere Konfigurationen überwacht und sie auch einrichtet. Dazu bieten diverse Managementwerkzeuge den Check gegen die Benchmarks des Center for Internet Security (CIS). Diese sind in der Auflistung nicht enthalten. Auch existieren einige Tools, die nur ein Produkt auf Einhaltung beispielsweise der CIS-Benchmarks überprüfen, auch diese bleiben unberücksichtigt, da sie zu speziell sind.

Einsicht

Die Produkte sind entweder als SaaS oder in der eigenen Umgebung zu betreiben, bei einigen funktioniert beides. Die Tabellen geben einen groben Überblick über die Optionen und Funktionen. Grundsätzlich erwarten alle Pakete einen Zugang zur zu überwachenden Umgebung. Das erfordert in allen Fällen für den Zugang zur API entweder einen Account oder einen Agenten. Diese benötigen sehr weitreichende Berechtigungen auf alle Elemente, zumindest müssen sie alle Einstellungen auslesen können.

Sofern der Zugang über einen Account erfolgt, fragt die Software die Einstellungen über die API der zu überwachenden Technik ab. Das funktioniert natürlich nur, sofern diese eine API hat und alle interessanten Einstellungen auch darüber bereitstellt. Die Alternative, die aber auch

X-TRACT

- Ohne leistungsfähige Tools zum Compliance Management ist ein Überblick über den Stand der Sicherheit in allen Umgebungen inklusive Cloud möglich.
- Die unterschiedlichen technischen Schwerpunkte spiegeln sich in diversen Produktkategorien wider, etwa Security Configuration Compliance (SCC), Secure Configuration Assessment (SCA), Cloud Security Posture Management (CSPM) oder Security Orchestration Automation and Response (SOAR).
- Je spezialisierter die Tools sind, desto besser integrieren sie sich in die jeweiligen Umgebungen.
- Eine kombinierte Überprüfung auf sichere Konfiguration und auf Schwachstellen zeigt fast alle Risiken.

Marktübersicht Compliance Management – Werkzeuge zum Einsatz in der Cloud

Name	Aqua Security Enterprise	NeuVector	Prisma	StackRox	Sysdig Secure	CloudGuard Dome9	Cloud One Conformity	Cavirin Free Edition
Anbieter	Aqua Security	NeuVektor	Palo Alto Networks	StackRox	Sysdig	Check Point	Trend Micro	Cavirin
Typ	Cloud-Multitool	Cloud-Multitool	Cloud-Multitool	Cloud-Multitool	Cloud-Multitool	Cloud-Multitool	Cloud-Compliance	Cloud-Compliance
Lizenz	kommerziell	kommerziell	kommerziell	kommerziell	kommerziell	kommerziell	kommerziell	kommerziell
SaaS / on Premises / sonstige	✓/✓/Air-gapped	–/✓/–	✓/✓/–	–/✓/–	✓/✓/–	✓/✓/–	✓/–/–	✓/✓/–
Beheben	–	–	✓	–	–	✓	–	–
Agents	✓	✓	✓	✓	✓	–	–	–
AWS	–	–	✓	–	–	✓	✓	✓
Azure	–	–	✓	–	–	✓	✓	✓
GCP	–	–	✓	–	–	✓	–	✓
Windows AD	–	–	–	–	–	–	–	✓
Windows-Systeme	–	–	–	–	–	–	–	✓
Linux / Unix	✓	–	✓	✓	✓	–	–	✓
Docker	✓	✓	✓	✓	✓	–	✓	✓
Kubernetes	✓	✓	✓	✓	✓	✓	✓	✓
VMware	–	–	–	–	–	–	–	✓

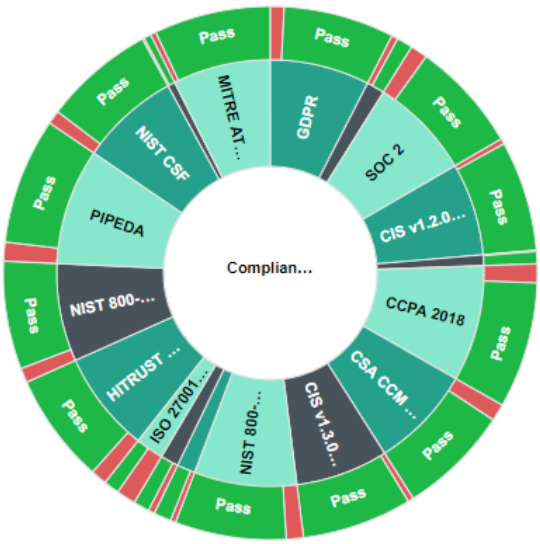
manchmal kombiniert wird, ist das Installieren eines Agenten in der zu überwachenden Umgebung. Der kann als lokaler Prozess beispielsweise direkt mit dem Betriebssystem interagieren und oft auch zusätzlich mit einem Account die Einstellungen über eine API abfragen. Besonders wenn der Scanner die API nicht direkt ansprechen kann, ist über den Agenten der Zugang doch möglich.

Dies ist beispielsweise dann der Fall, wenn ein Kubernetes-Cluster abgeschottet in einem eigenen Netzbereich agiert und die API nur innerhalb dieses Netzes erreichbar ist. Der Agent wird dann als Container im Cluster betrieben und fragt dort die Einstellungen der Nodes, der lokalen Container-Runtime, des Kubelets und letztlich der Kubernetes-API ab. Zusätzlich kann der lokale Agent eine Liste der auf dem Node gespeicherten Images im Cache auslesen und direkt den Kernel befragen. Damit ist ein Großteil der interessanten Konfigurationseinstellungen nur für den Agenten zugänglich, da die Kubernetes-API diese Informationen nicht hat.

Bei anderen Technologien wie Public-Cloud-Angeboten, Microsoft Active Directory oder VMware vSphere sind alle relevanten Daten über die API les- und schreibbar. Oder es lassen sich über die API Befehle absetzen, die die Konfiguration etwa auf den IaaS-Servern abfragen und so die Überwachung aller Elemente ermöglichen. Agenten sind dann nicht notwendig. Allerdings ist zu beachten, dass alle Produkte bis auf die Gruppe der reinen SCC-Werkzeuge auch noch einige andere Funktionen haben, die teilweise Agenten voraussetzen. So interagieren beispielsweise die CWPP mit dem Linux-Kernel auf den Servern, um Sicherheitsvorgaben durchzusetzen.

Überblick und Kontrolle

Die Scans selbst sortieren die Produkte nach Compliance-Gebieten und bieten dabei für die diversen Sicherheitsstandards abgestimmte Richtlinien. Für unterschiedliche Technologien dienen jeweils eigene Pakete mit Tests. Die Tabellen „Marktübersicht Compliance Management – …“ zeigen, welches Produkt welche Technik scannen kann. Dieser Artikel bietet aber keine Übersicht über die von den Paketen beherrschten Standards, da die Produkte sich hier sehr ähneln. Besonderheiten wie die Messung der Compliance nach BSI-Grundschutz-Kompendium sind – sofern vorhanden – jeweils im Textabschnitt erwähnt.



Das umfangreiche Beispiel Palo Alto Networks Prisma zeigt eine Übersicht der zur Messung der Compliance herangezogenen Sicherheitsstandards (Abb. 1).

Alle Produkte stellen die Ergebnisse der Scans als Übersicht und auch mit zeitlichem Verlauf vor. Die Ergebnisse lassen sich immer als Übersicht in einem Dashboard betrachten oder sortiert nach Umgebung, Art der Systeme und Kritikalität. Weiter geben alle Tools in den Ergebnissen Hinweise zum Beheben der Schwachstellen. Auch eine Ausgabe als Bericht beherrschen alle Produkte. Wichtig für den Überblick in großen Umgebungen ist die Darstellung mit Herkunft der Ergebnisse. Damit lässt sich schnell einschätzen, welcher Teil der Landschaft besonderer Aufmerksamkeit bedarf.

Probleme zu erkennen ist natürlich nur die halbe Miete. Sie zu beheben ist der eigentlich relevante zweite Schritt. Alle Produkte bieten hierfür Hinweise und Empfehlungen, manche können die Probleme auch selbstständig beseitigen. Dafür benötigen sie Berechtigun-

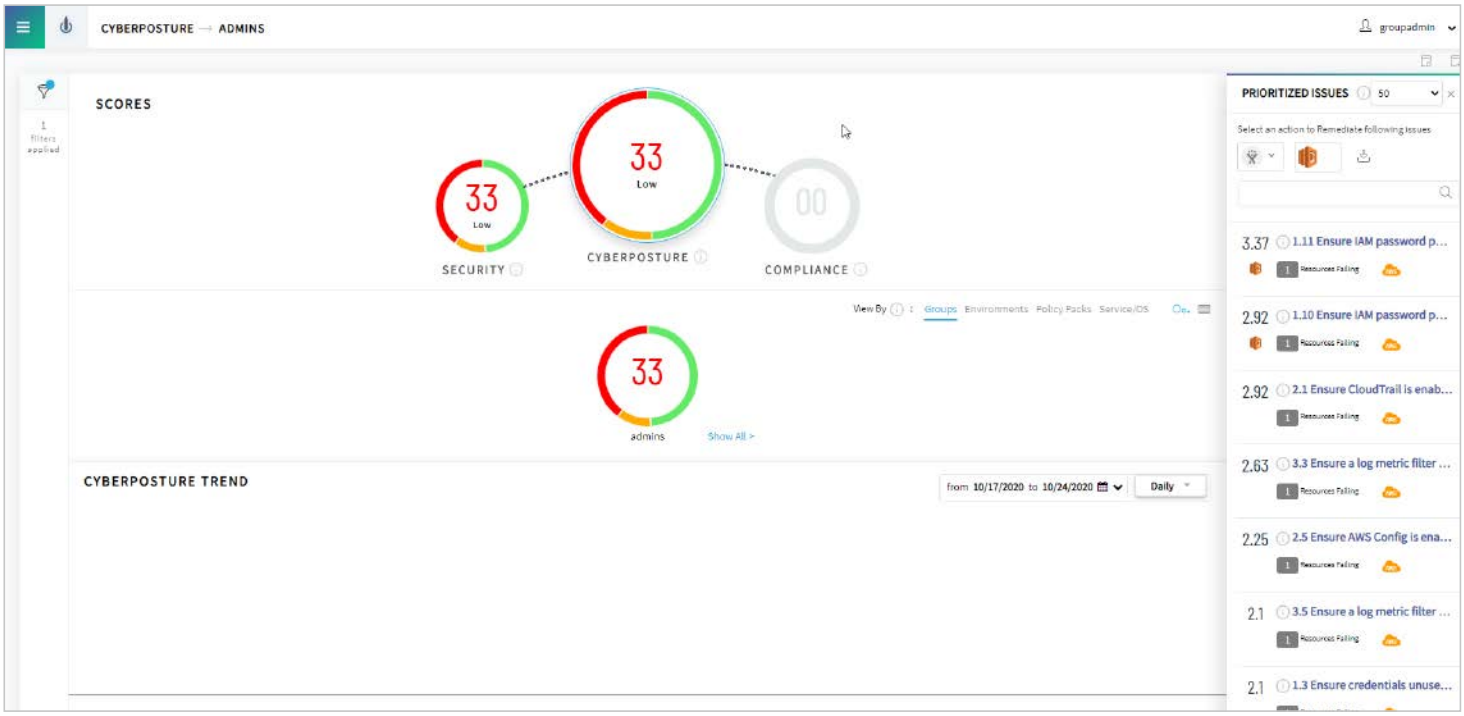
	Cloud Control	CloudSploit / Aqua Wave	Runecast	Configuration Compliance Manager	Network Configuration Manager	Configuration Compliance
	C3M	Aqua Security	Runecast	Tripwire	SolarWinds	ServiceNow
	Cloud-Compliance	Cloud-Compliance	Cloud-Compliance	Cloud-Compliance	Netzwerk-Compliance	Operations Automatisation
	kommerziell	Open Souce / kommerziell (siehe Text)	kommerziell	kommerziell	kommerziell	kommerziell
	✓/✓/–	✓/✓/–	–/✓/–	✓/✓/–	–/✓/–	✓/–/–
	✓	✓	–	✓	✓	✓
	–	–	–	✓	–	✓
	✓	✓	✓	✓	–	✓
	✓	✓	–	✓	–	✓
	✓	✓	–	✓	–	✓
	–	–	–	✓	–	✓
	–	–	–	✓	–	✓
	–	–	–	✓	–	✓
	–	–	✓	✓	–	✓
	–	–	✓	✓	–	✓
	–	–	✓	✓	–	✓

gen zum Verändern der Konfiguration, die beim Einrichten des Accounts für den Zugang zu hinterlegen sind. Dies geschieht entweder halbautomatisch, indem der Bearbeiter mit einem Klick die Aktion anstößt, die das Tool dann ausführt, oder vollautomatisch ohne eine menschliche Interaktion nach festgelegten Regeln. Letzteres bezeichnet man als SOAR (Security Orchestration, Automation and Response).

Sobald also der Scan ein Problem erkannt hat, wird es sofort behoben, was besonders zu Zeiten teilweise unbetreuten 24/7-Betriebs von Bedeutung ist. Wie bei jedem Automatismus lassen sich aber Fehler nicht ausschließen. Wenn etwa eine Einstellung eigentlich per Policy verboten ist, aber für den Betrieb notwendig, dann wird der Automatismus den Betrieb verhindern. Die Regel entsprechend anzupassen, eine Ausnahme hinzuzufügen oder ein Problem zu akzeptieren, muss dann Teil der Scannerkonfiguration sein. Aber auch wenn dies nicht immer funktioniert, ist es oft preiswerter, einen kurzen Ausfall hinzunehmen, statt sich mit den langwierigen und teuren Folgen eines Einbruchs beschäftigen zu müssen.

Konfiguration und Testumgebung

Zur Konfiguration der Produkte gehört immer das Anlegen von Benutzern, die mit dem Produkt arbeiten sollen. Dabei ist es



Das Dashboard der Free Edition von Cavirin ist definitiv nicht überladen (Abb. 2).

Usus, auch rollenbasierte Berechtigungen einzusetzen. Dann sind die Zugänge zu den überwachten Umgebungen einzurichten. Dashboards sind zumeist schon vorkonfiguriert und lassen sich nur selten anpassen. Es gibt bei den größeren Produkten oft noch eine Auswahl der zu untersuchenden Standards zu wählen und, sofern der Betrieb Abweichungen erfordert, entsprechende Ausnahmen einzutragen. Viele Produkte erlauben auch die Zusammenstellung eigener Regelpakete aus den vorhandenen Tests sowie das Anlegen eigener Tests. Zum Schluss ist die Weiterleitung der Ergebnisse in ein SIEM-, Chat- oder Ticketsystem zu konfigurieren.

Zwar ist der Wartungsaufwand der Produkte relativ gering, allerdings ist auch hier das Patch-Management nicht zu vergessen. Einerseits müssen die Regelsätze und auch die Software selbst immer aktuell gehalten werden und andererseits ist darauf zu achten, wirklich alle Umgebungen in die Überwachung einzubeziehen. Besonders Letzteres ist nicht immer einfach, da jeder Mitarbeiter mit einer Kreditkarte einen Cloud-Dienst anmieten kann und so eine neue Umgebung schafft, die vielleicht unerkannt und unbeobachtet zum Teil der IT-Landschaft wird.

Der Autor hat die teilnehmenden Produkte in einer heute typischen Umgebung ausprobiert. Es gab ein AWS-Projekt mit einem öffentlichen S3-Bucket, ein GCE mit einem GKE-Cluster inklusive darauf laufendem GitLab sowie Azure mit einem AD in einem Tenant. Die Screenshots der Produkte stammen aus diesen Scans. Die Umgebung lief etwa zwei Wochen größtenteils unverändert, auch wenn zwischendurch der Node-Pool des GKE-Clusters abgeschaltet war.

Compliance-Scanner

Die Compliance-Spezialisten dieser Marktübersicht bieten keine weiteren Funktionen. Das merkt man zumeist an der Zahl der implementierten Technologien und Standards.

Cavirin

Von allen Produkten ist dieses laut Webseite eines der Produkte mit der umfangreichsten Abdeckung aller Technologien. Eine kostenlose Version lässt sich innerhalb weniger Minuten etwa in der GCP aus dem Marketplace installieren und ermöglicht so erste Einblicke in Produktumfang und Bedienung. Die freie Version erlaubt allerdings nur einen Zugangsaccount und nur eine eingeschränkte Zahl von Policy-Paketen. Aber auch sie liefert schon ansehnliche Ergebnisse. VMware vSphere in einem internen Netzwerk konnte es allerdings nicht erreichen, da es keine Agenten nutzt und den vSphere-Server direkt hätte erreichen müssen. Der Hersteller ist Mitglied des CIS und arbeitet auch an deren Benchmarks mit.

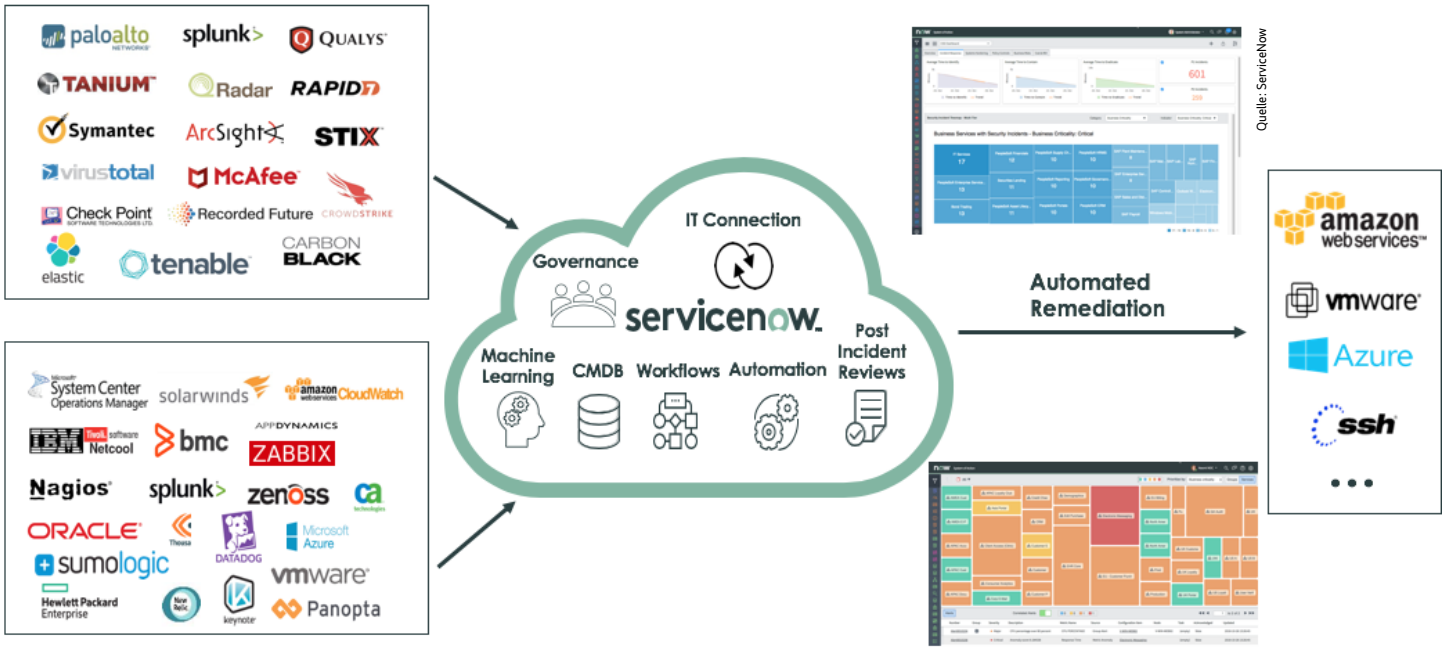
Die Bedienung ist angenehm und schnell. Flugs ist ein Account für AWS eingerichtet, der Scan durchgeführt, der Account wieder gelöscht und der Vorgang mit einem Account für GCP wiederholt. Der Scan der GCP funktionierte nicht, warum, war aus den Logfiles nicht ersichtlich. Das Löschen dieser Gruppe verwirrte den Dienst völlig und erforderte einen Neustart der VM. Azure lief einwandfrei; mehr Tests erlaubt die freie Version nicht.

C3M Cloud Control

C3M legt den Fokus klar auf das Beheben der Schwachstellen. Der Hersteller vermarktet dies als SOAR, also als Automatisierung der Reaktion. Das Produkt scannt dafür über die API die drei großen Cloud-Dienste und durchsucht auch die Protokolldaten auf Hinweise. Sobald es einen Policy-Verstoß entdeckt, wird ein Skript aktiv, das eine hinterlegte Aktion ausführt. Es kann Einstellungen ändern, Objekte anlegen und löschen und auch Mitarbeiter über diverse Wege informieren. Der Hersteller präsentierte sein Produkt in einer Besprechung, stellte aber für den Artikel keine Lizenz zur Verfügung.

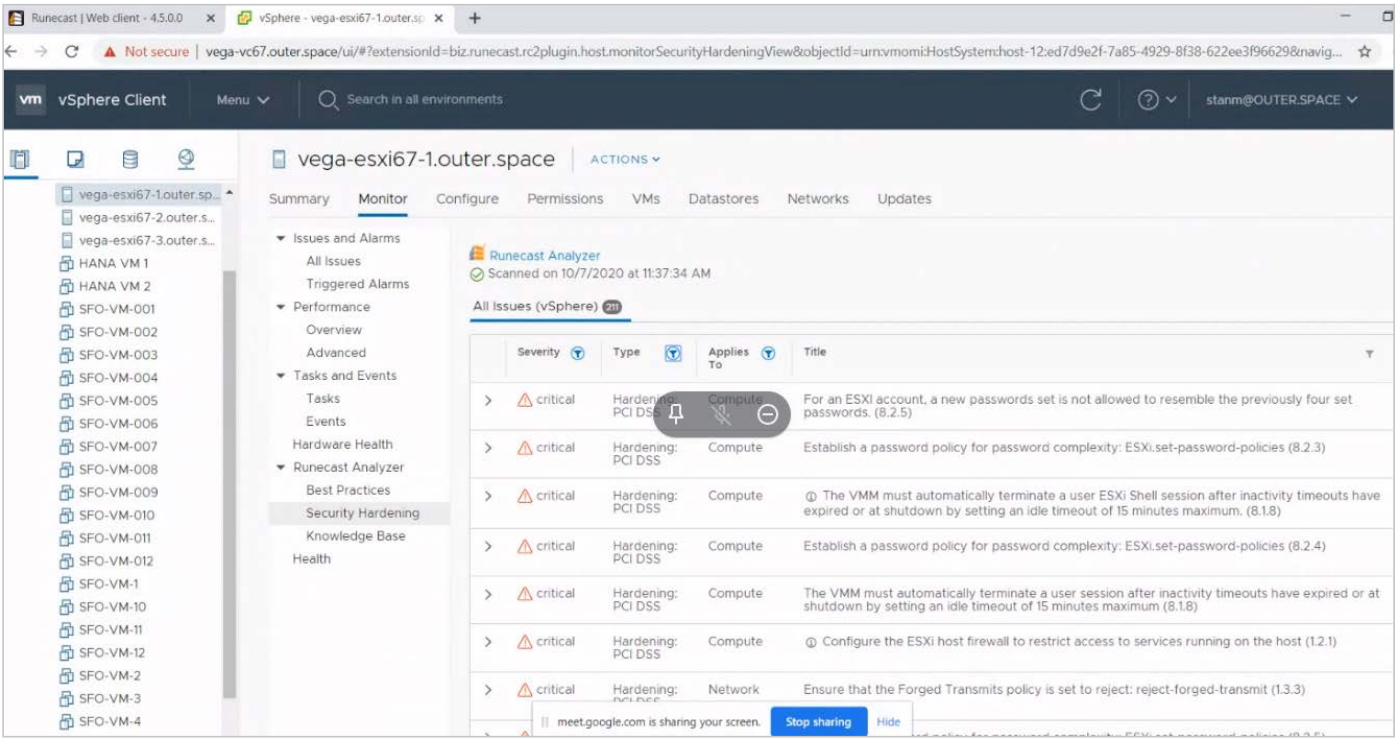
CloudSploit von Aqua Security

Als eines der wenigen Open-Source-Angebote ist CloudSploit die kleinere Version eines Teils des SaaS-Angebots von Aqua Security. Es scannt die drei großen



ServiceNow aggregiert die Ausgabe fast aller Hersteller und überführt sie in einen Workstream (Abb. 3).

Quelle: Runecast



Die Spezialisierung von Runecast zeigt sich in der sehr tiefen Integration in die Produkte von VMware (Abb. 4).

Cloud-Anbieter und – etwas ungewöhnlich – auch das Cloud-Angebot von Oracle. Policies sind die CIS-Benchmarks, HIPPA und PCI-DSS. Gestartet wird das Tool auf der Kommandozeile; es bietet keine Weboberfläche. Es beherrscht auch das Beheben der Feststellungen und nutzt dafür vom Anwender hinterlegte Skripte. Als kommerzielles Angebot ist es in Aqua Wave enthalten, kombiniert mit der Dynamic Threat Analysis (DTA) und dem Image Scanner von Aqua Enterprise.

ServiceNow Configuration Compliance

ServiceNow bietet ein sehr umfangreiches Paket zum Verwalten von Diensten und Anwendungen an. Das Modul Configuration Compliance erlaubt das Erkennen und Beheben von Konfigurationsfehlern. Auch bindet es fast alle SCA-Produkte ein, um deren Ergebnisse in die Übersicht aufzunehmen und Fehler zu beseitigen.

Runecast

Der Hersteller Runecast hat sich auf das gleichnamige Produkt spezialisiert und ist damit neben Cavirin derzeit der einzige, der VMware vSphere untersuchen kann. Diese Spezialisierung zahlt sich aus: Runecast bietet den Scan sowohl von vSphere als auch von NSX-T, Horizon, vSAN und NSX und sogar eine Kompatibilitätssimulation der Hardware gegen eine geplante Release. Relativ neu sind Scans für Kubernetes und AWS. Die anderen Cloud-Anbieter sollen laut Aussage des Herstellers bald folgen. Bereits jetzt funktioniert der Scan von SAP HANA.

Die Fehlerbehebung erfolgt aus dem vRealize Orchestrator heraus. Dort trägt Runecast seine Ergebnisse ein. Der Administrator kann den Vorgang manuell anstoßen oder automatisiert erledigen lassen. In vSphere finden sich die Ergebnisse im Tab „Compliance“.

Als Policies sind die des CIS und auch einige eigene enthalten. Als Besonderheit verfügt Runecast hier neben den üblichen Kandidaten (NIST, DISA, HIPPA et cetera) über einen Compliance-Check gegen das BSI-Grundschutz-Kompendium. Darüber hinaus untersucht das Produkt auch die Logfiles nach Hinweisen auf Schwachstellen. Der Hersteller hat eine unlimitierte Lizenz zum Testen bereitgestellt und sein Produkt in einer Videokonferenz vorgestellt.

Conformity von Trend Micro Cloud One

Conformity ist einer von sechs Diensten der Cloud-One-Suite. Es scannt allerdings nur AWS und Azure. Die Installation laut Anleitung verläuft problemlos, erfordert aber etwas Handarbeit. Die Beschreibung zu Azure ist nicht ganz aktuell. Mit einem Installationsskript aus GitHub sind die Rollen und Rechte eingetragen.

Eine Besonderheit ist der Scan von CloudFormation-Templates. Die Scans erzeugen Alerts, die man zwar kommentieren, aber nicht aus dem Reporting herausnehmen kann. Verschiedene Benachrichtigungen sind möglich und über den AWS Simple Notification Service (SNS) kann ein Alert in eine Lambda-Funktion wandern, die dann die Behebung der Feststellung übernimmt. Es gibt zwar eine anschauliche Übersicht aller Regionen, allerdings wird eine in allen Regionen vorhandene Fehlkonfiguration nicht überall angezeigt.

Regelsätze lassen sich über das Bauen eigener Profile anpassen. Sie sind umfangreich und haben die eingebauten Fehler gefunden. In der Realtime-Einstellung reagiert der Scanner sofort auf alle Änderungen. Automatisiertes Beheben beherrscht Conformity nicht, aber die Beschreibungen sind umfangreich und enthalten Codebeispiele. Auch Trend Micro hat eine unlimitierte Lizenz bereitgestellt und das Produkt in einer Videokonferenz präsentiert.

Network Configuration Manager

Der zur Plattform SolarWinds Orion gehörende Network Configuration Manger

ist spezialisiert auf Netzwerkequipment von Cisco und Palo Alto Networks. Er überwacht die Einstellungen aller Geräte und kann diese auch auf die gewünschte Konfiguration setzen.

Tripwire Configuration Manager

Der Configuration Manager von Tripwire nutzt die CSI-Benchmarks für das Überwachen von Azure und AWS. Er erlaubt ein automatisiertes Beheben der Feststellungen. Laut Support-Policy kann das Tool noch 115 weitere Betriebssysteme und Anwendungen untersuchen. Allerdings stehen die großen Cloud-Anbieter nicht auf dieser Liste, denn deren Scan übernimmt das Modul Cloud Management Assessor. Der Hersteller hat nicht am Test teilgenommen.

CWPP – Cloud Workload Protection Platforms

Die Produkte dieser Kategorie bieten die Compliance-Scans als eine Funktion unter vielen. Der Fokus liegt dabei auf den Scans der Container-Images auf Verwundbarkeiten und Verstöße gegen Betriebsrichtlinien. Auch gehören die Steuerung der clusterinternen Firewall, die Überwachung des Betriebs der Container und der Orchestrierung zu den Kernfunktionen dieser Produkte. Eine detaillierte Vorstellung findet sich im Artikel „Blitzableiter und Regenschirme“ des *iX* kompakt Container [1].

Aqua Security Enterprise

Seine Stärken zeigt Aqua Security beim Absichern von Containern und Kubernetes-Clustern und bietet Funktionen wie „virtual Patching“, das das Ausnutzen bekannter Schwachstellen verhindert. Die Scans der Konfiguration beschränken sich auf die Server, Docker, Kubernetes und die Images der Container nach den einzustellenden Richtlinien. Kurz vor Redaktionsschluss gab Aqua Security die Erweiterung seines Posture Managements um Microsoft Azure bekannt. Auch Compliance zu PCI DSS, NIST und weiteren ist enthalten. Die Software greift mit auf allen Nodes als DaemonSet laufenden Agenten direkt auf die Clusterserver zu. So hat sie einen guten Einblick und kann auch Einstellungen überprüfen, die über die Kubernetes-API nicht erreichbar sind.

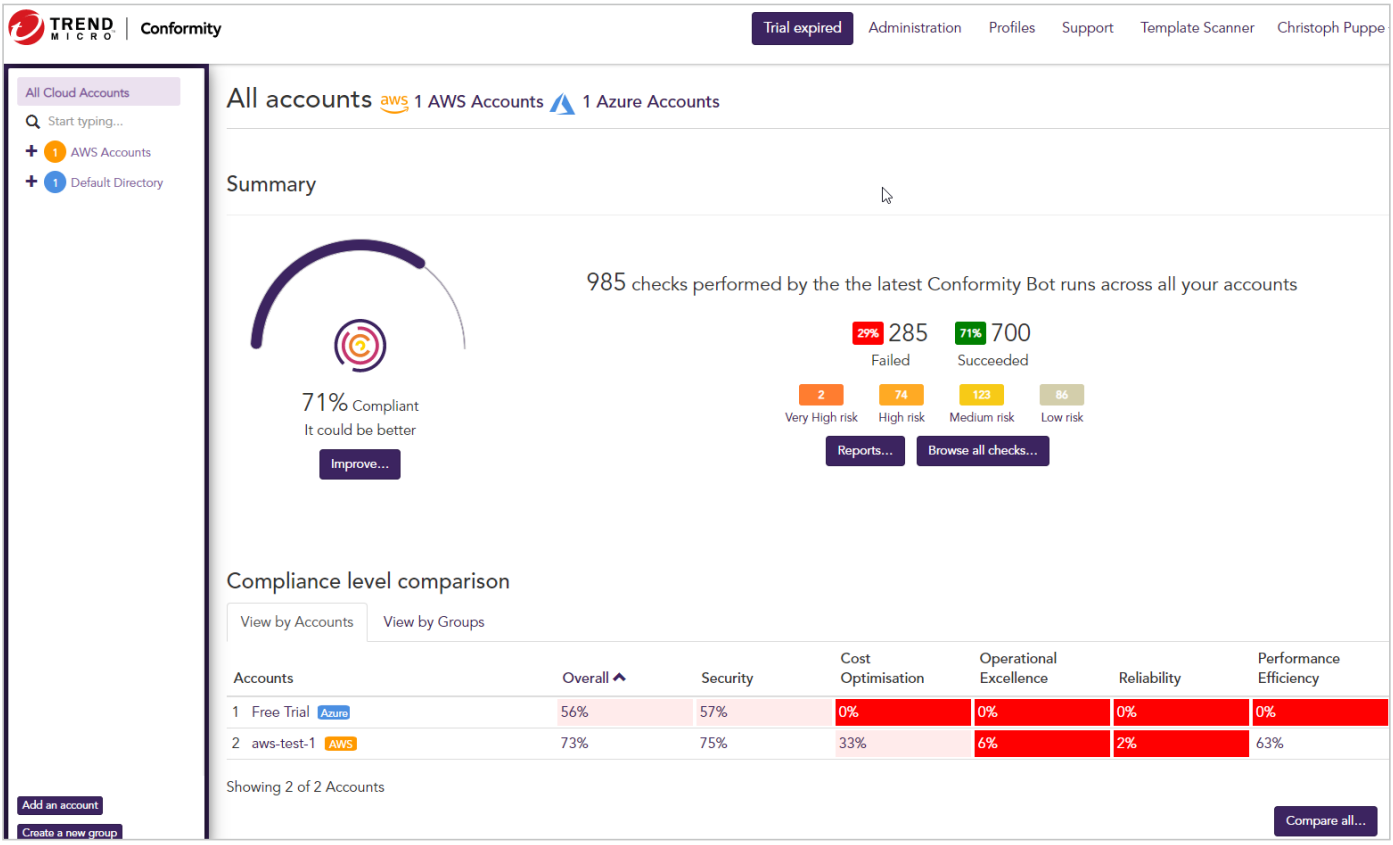
Die Installation ist „Air-gapped“, also ohne Netzverbindung, on Premises sowie als SaaS möglich. Manche Funktionen wie Dynamic Threat Analysis (DTA) funktionieren aber nur in der Cloud. Aqua Security hat sich zwar nicht direkt in den Test eingebracht, der Autor hatte aber noch eine Lizenz aus einem früheren Test zur Verfügung.

NeuVector

Auch NeuVector überprüft die zu überwachenden Kubernetes-Cluster mit den CIS-Benchmarks für Kubernetes und Docker. Zur Überwachung der Cluster gehört auch bei NeuVector der Scan der Images auf Sicherheitslücken und Richtlinien. Weitere Scans enthält das Tool laut Webseite nicht. Mangels Lizenz stammen die Produktinformationen aus Onlinequellen.

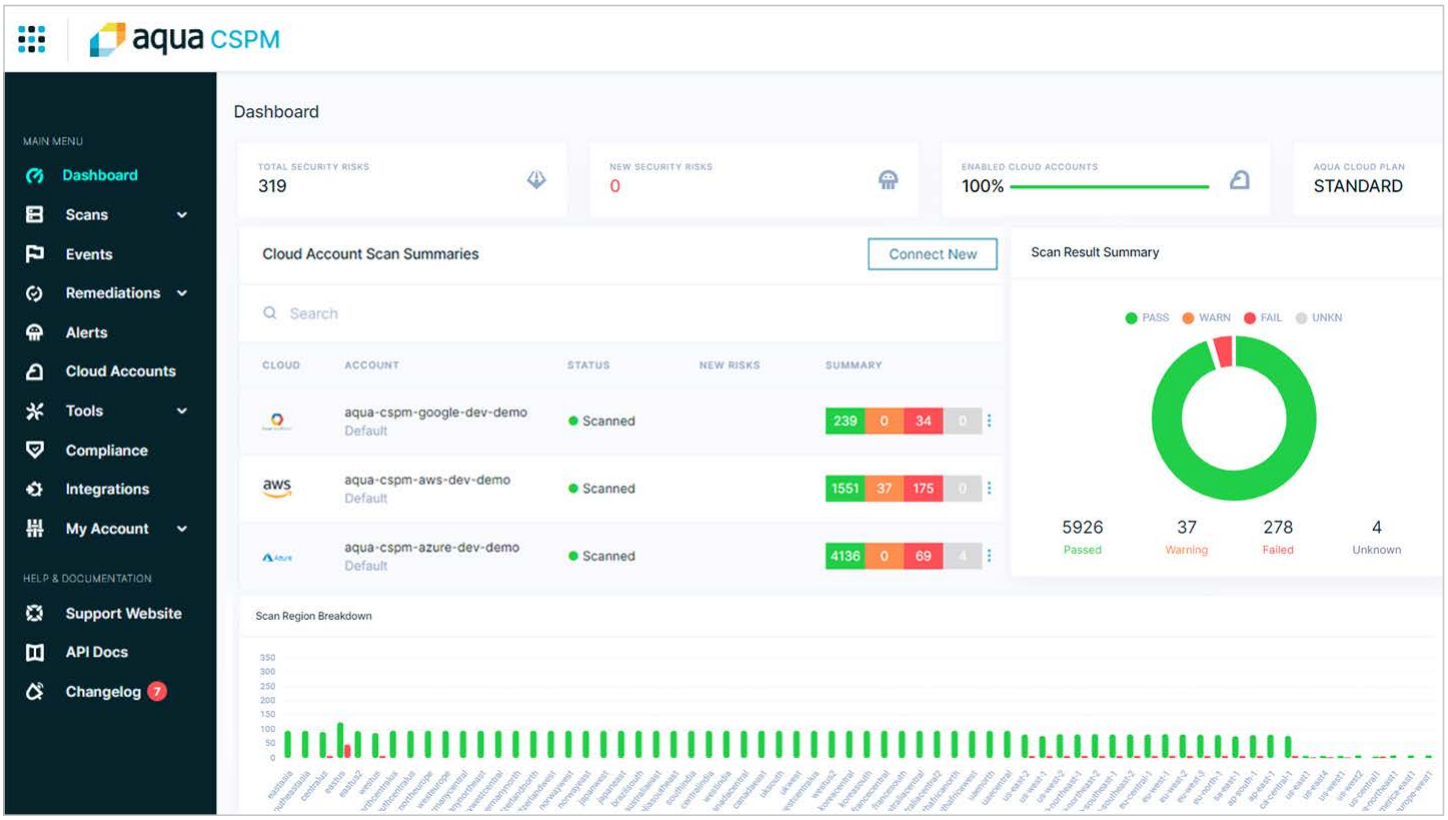
Prisma Cloud

Prisma Cloud ist eine von 16 Anwendungen, die Palo Alto Networks (PAN) als SaaS anbietet. Der Hersteller hat eine unlimitierte Lizenz bereitgestellt und sein Produkt in einer Videokonferenz vorgestellt. Das Portfolio reicht hier von PAM (Privileged Access Management) über DLP (Data Leakage Prevention) bis zum auto-



Conformity gehört zur Cloud-One-Suite von Trend Micro (Abb. 5).

Quelle: Aqua Security



Aqua Security eignet sich besonders gut für Kubernetes-Cluster (Abb. 6).

matisierten Erkennen und Beheben von Schwachstellen als SOAR mit Cortex. Kürzlich hat PAN die Akquisition der Firma Expanse Inc. angekündigt. Die bietet quasi ein kommerzielles Shodan, das das gesamte Internet scannt und den Firmen eine Übersicht ihrer angreifbaren Systeme gibt. Wie die meisten dieser Dienste ist auch Prisma Cloud ein Zukauf. Es besteht je zur Hälfte aus dem ehemaligen CWPP Twistlock und dem ehemaligen CSPM RedLock.io. Den Twistlock-Teil gibt es weiterhin auch on Premises.

Schon beim Einrichten überzeugt PAN mit einer automatisierten Installation auf GCE, Azure und AWS mit Terraform. Das Skript bietet fast zwei Dutzend Aktionen. Zugänge und Berechtigungen sind damit schnell angelegt und nur der Twistlock-Agent ist manuell einzuspielen. Ein Webformular unterstützt den Admin dabei und baut die Befehlszeile mit allen Optionen. Im Test nahm es die Flow-Logs allerdings nicht mit auf, das hätte eine Auswertung der Aktionen auf den drei Plattformen ermöglicht.

Prisma Cloud besitzt im Lieferumfang sehr viele Scanprofile für Sicherheitsstandards, inklusive der gängigen wie PCI DSS und NIST; die CIS-Benchmarks sind natürlich auch enthalten. Eigene Profile lassen sich ebenfalls erstellen. Alle Funde kann das Tool an externe Dienste wie Mail, Slack et cetera weiterleiten. Sie zu akzeptieren oder die Bearbeitung zu verschieben klappt innerhalb der Oberfläche. Prisma Cloud bietet wo immer möglich eine Problembehebung an und kann sie auch automatisch ausführen. Als Workflow lässt sich eine Automatisierung einrichten, auch mit manueller Bestätigung und Vieraugenprinzip. Den öffentlichen S3-Bucket hat Prisma Cloud gefunden, einen Alert erstellt und den Fehler nach einem Klick behoben.

Die Software bietet auch einen Scan von Terraform-, YAML- und CloudFormation-Templates an, die dafür im GIT liegen müssen. Die üblichen Funktionen eines CWPP wie Scan der Images auf Richtlinien, Verwundbarkeiten und Überwachung des Betriebs sind dank der Integration von Twistlock weiterhin möglich und sehr umfangreich. Hervorzuheben ist die Integration externer Tools, denn Prisma Cloud exportiert nicht nur, sondern kann auch die Ergebnisse von Qualys und Tenable importieren. Auch scannt es Alibaba Cloud, was sonst kein anderes Produkt bietet.

StackRox

Das Tool bezeichnet sich als „kubernetes Native“ und dementsprechend liegt sein Fokus auf den Funktionen eines CWPP. Besonderheit hier wäre, dass StackRox auch die Rollen und Rechte auditiert und Accounts mit besonders weitgehenden Rechten erkennt. Auch kontrolliert es die Container während der Ausführung, überwacht deren Netzwerkverkehr und die Zugriffe auf den Kernel und die Secrets. Richtlinien für Container und Images sind ebenfalls enthalten. Für Compliance-Scans dienen die Benchmarks der CIS für Kubernetes und Docker. Dazu gibt es weitere Scanprofile wie für HIPPA, PCI DSS und NIST. StackRox hat sich am Test nicht beteiligt.

Sysdig

Wie die meisten CWPP ist auch Sysdig Cloud-native und konzentriert sich auf Kubernetes und Container. Hier zeigt es seine Stärken bei der Absicherung von Clustern und Containern. Scans für Letztere und deren Images nach vorgegebenen Richtlinien sowie das Überwachen gehören ebenfalls zum Funktionsumfang. Sysdig hat mit Falko auch ein Open-Source-Werkzeug zum Erkennen von Einbrüchen im Angebot. Als Compliance-Scans kommen auch hier die CIS-Benchmarks für Kubernetes und Docker zum Einsatz sowie PCI DSS, NIST und AICPA SOC2.

Der Hersteller hat eine unbeschränkte Lizenz bereit- und sein Produkt in einer Videokonferenz vorgestellt.

CloudGuard

Check Point hat das Tool Dome9 2018 gekauft und bietet es jetzt als CloudGuard an. Neben den üblichen Scanprofilen für PCI DSS, CSI Benchmarks, NIST und weitere kann man eigene erstellen. Dies geschieht in der GSL (Governance Specification Language). CloudGuard ist allerdings kein vollständiges CWPP, da es beispielsweise keine Container-Images scannt. Es verwaltet aber die Serverless-Funktionen in AWS und die Cloud-Identitäten sowie -Firewalls. Letzteres als „Macro-Segmentation", also auf der SDN-Ebene des Cloud-Anbieters und nicht auf der SDN-Ebene in den Kubernetes-Clustern. CloudGuard kann die Protokolle hinsichtlich Hinweisen auf unübliches Verhalten und Fehler in den Sicherheitseinstellungen überwachen. Das automatisierte Beheben erfolgt über CloudBots, die es für AWS, Azure und GCP gibt.

Seine Ergebnisse gibt CloudGuard über AWS SNS an Splunk oder an Ticketsysteme wie PagerDuty, Slack, ServiceNow und andere weiter. Eine Besonderheit ist die Mandantenfähigkeit der Oberfläche. Als Managed Service Provider kann man über einen speziellen Zugang mehrere Kunden verwalten und administrieren. Der Hersteller hat sich nicht am Test beteiligt, aber die Handbücher sind online und bieten einen guten Einblick in die Möglichkeiten dieses sehr umfangreichen Werkzeugs.

Verwundbarkeitsmanagement

Diese Gruppe ist die älteste und ihre Anbieter haben früh erkannt, dass es nicht ausreicht, die Systeme auf veraltete Software hin zu überwachen, sondern dass auch die Konfiguration auf Fehler zu kontrollieren ist. Hier sind Produkte am Markt, in die teilweise über 20 Jahre Erfahrung einfließen. Leider hat sich nur Rapid7 mit einer Lizenz für InsightVM am Test beteiligt. Die anderen Hersteller bieten keine frei verfügbaren Testversionen an.

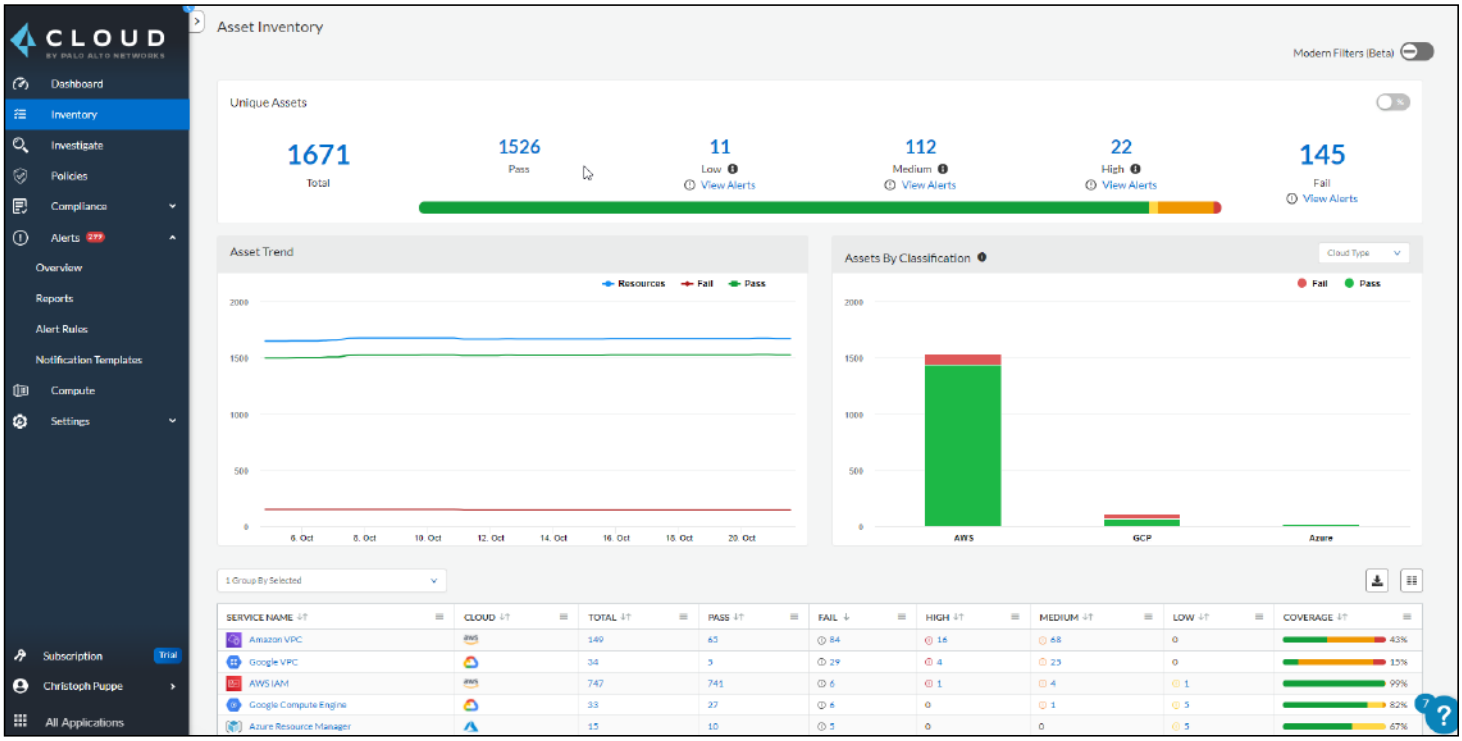
tenable.io

Nessus hat Ende der 1990er-Jahre als Open Source angefangen und der Autor dieses Artikels ist bis heute stolz, damals Code beigetragen zu haben. Aus den Anfängen hat sich eine umfangreiche Testsuite entwickelt, die stark beim Schwachstellenmanagement ist und auch die Compliance der Systeme schon früh mit im Blick hatte. Bereits 2017 hat Tenable den CIS-Kubernetes-Benchmark eingebaut. Die Zahl der Integrationen, mit denen Tenable auf die Dienste zugreift, ist groß: von ServiceNow über Intune bis zu den etablierten Cloud-Anbietern ist alles dabei.

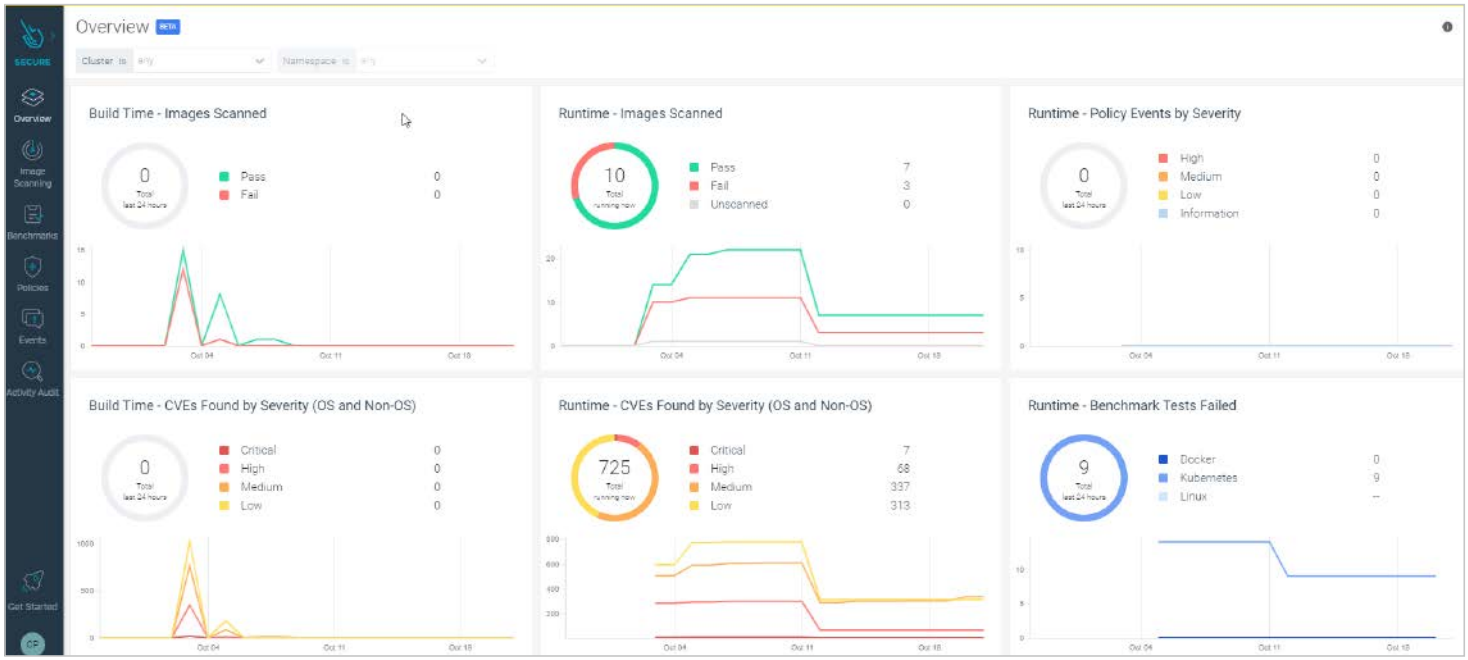
Die Suite greift für die Scans lesend auf manche Dienste zu und exportiert die Ergebnisse beispielsweise in die Sicherheitscenter von ServiceNow, Azure und GCE. So lassen sie sich in eine gemeinsame Ansicht überführen. Wer dies selbst betreiben möchte, kann hierfür Splunk nutzen. Auch Tenable hat keine Lizenz zum Test beigetragen, allerdings stehen die Handbücher online und bieten einen guten Einblick in die Möglichkeiten dieses leistungsfähigen Tools.

Qualys SCA & CSA

Für Kunden ihres Verwundbarkeitsmanagements bietet Qualys mit dem Security Configuration Assessment (SCA) die Möglichkeit, eine große Bandbreite von Systemen und Anwendungen auf Einhaltung der CIS-Benchmarks zu überwachen. Es ist ein SaaS-Angebot, das sich mithilfe von Appliances aber auch in geschlossenen Netzwerken nutzen lässt. Mit 129 CIS-basierten Scanprofilen bietet Qualys eine weit größere als die in der Tabelle dargestellte Reichweite bei der Überwachung. Ergebnisse der Scans sind Teil der Verwaltung von Schwachstellen und es kann diese entweder in der Webanwendung bearbeiten oder an externe Werkzeuge wie Slack, E-Mail oder Ticketsysteme weitergeben.



Prisma Cloud bietet eine Übersicht über die überwachten Systeme und Clouds (Abb. 7).



So sehen die Daten der Testumgebung im Dashboard von Sysdig Secure aus (Abb. 8).

Mit dem Cloud Security Assessment (CSA) bietet Qualys die Überwachung von Public-Cloud-Diensten an. Das führt, wie auch Container Security als zusätzliche App aus dem umfangreichen Portfolio, die Ergebnisse in einer Managementoberfläche zusammen. Auch Qualys konnte sich nicht z ueiner Lizenz für den Test durchringen.

SAINT Security Suite

Schon seit über 20 Jahren ist SAINT im Markt aktiv. Angefangen hat es als Open-Source-Software unter dem Namen SATAN und bietet eine umfangreiche Palette an Funktionen für das Schwachstellenmanagement, aber auch Forensik und Compliance. Es verwendet die CCE (Common Configuration Enumeration) der Mitre, die für 33 Anwendungen und Betriebssysteme vorliegen – jedoch entwickelt Mitre CCE seit 2013 nicht mehr weiter. Die Webseite führt PCI DSS als Thema auf und auch der Scan von AWS wird erwähnt. Der Hersteller hat nicht am Test teilgenommen.

Rapid7 InsightVM

Mit Nexpose ist Rapid7 seit Anbeginn im Markt der Schwachstellenscanner aktiv. InsightVM bietet Compliance für Betriebssysteme und Anwendungen. Auch hier sind die CIS-Benchmarks im Einsatz, aber neben den üblichen Scanprofilen nach PCI DSS und NIST gehören auch HIPPA, GDPR, NY DFS, FISM und einige mehr mit zum Lieferumfang. Der Einstieg in die Cloud-Welt ist hier noch etwas zögerlich, Scans von AWS erst als Preview vorhanden. Die Installation ist im Handbuch gut beschrieben, aber manuell und leider auch fehleranfällig. Etwas irritierend ist auch, dass die Weboberfläche zwischen der lokalen Konsole und der SaaS-Anwendung hin- und herspringt. Hier ist noch einige Arbeit notwendig.

Für die gefundenen Schwachstellen bietet InsightVM auch eine automatische Behebung oder einen Workflow an. Neben InsightVM hat Rapid7 noch ein SIEM und das wohl bekannteste Pentest-Framework Metasploit im Angebot. Der Hersteller bietet auf seiner Webseite eine Demoversion zum Download an, die hier zum Einsatz kam. Die Preview des Cloud-Compliance-Scans brachte aber keine für einen Screenshot ausreichenden Ergebnisse.

Werkzeuge der Hersteller

Auch die großen Public-Cloud-Anbieter bieten als Teil des Self-Service ein Werkzeug zur Absicherung, Überwachung und Kontrolle der Compliance. Alle können die jeweils eigene Umgebung betrachten und sind tief in diese integriert. Für einen Vergleich dieser umfangreichen Werkzeuge AWS Systems Manager Configuration Compliance, Azure Security Center und GCP Security Command Center wird es in einer späteren Ausgabe einen eigenen Artikel geben.

Auch die Hersteller von Betriebssystemen geben ihren Kunden Werkzeuge an die Hand. Hier sind für Linux Red Hats OpenSCAP und für Windows Microsofts DSC Environment Analyzer zu nennen.

Fazit

Automatisierung ist tatsächlich die Antwort auf die brennendsten Fragen der IT. Die Landschaften nehmen an Komplexität ständig zu, die Abhängigkeiten voneinander auch. Gleichzeitig ist das Personal, das diese Komplexität versteht und kontrollieren kann, rar und zumeist überlastet. Hier bietet SOAR als Weiterentwicklung der reinen Erhebung der Schwachstellen einen vielversprechenden, aber auch kostspieligen Ansatz, schnell auf menschliche Fehler zu reagieren. (avr@ix.de)

Quellen

Christoph Puppe; Blitzableiter und Regenschirme; Tools zur Absicherung von Containern; *iX* kompakt – Container 2020, S. 22

Christoph Puppe

ist Security Consultant bei SVA, Auditteamleiter für ISO 27001 nach Grundschutz, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.