MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Cloud-Sicherheit: Cloud Security Operations Center im Vergleich

24.06.2021 06:15 Uhr Christoph Puppe

"Sicherheit ist kein Projekt, sondern ein Prozess", sagt sich leicht. Die Umsetzung im IT-Alltag ist oft nicht so einfach. Werkzeuge helfen in Cloud-Umgebungen.

Es ist kompliziert, die Sicherheit komplexer Cloud-Umgebungen zu gewährleisten. Dazu muss man die Cloud-Infrastruktur kontinuierlich überwachen, Lücken beim Durchsetzen der Sicherheitsrichtlinien aufdecken und diese möglichst automatisiert schließen.

Alle großen Hyperscaler haben hierfür ihre Security Operations Center (SOC), aber auch eine größere Schar von Drittanbietern bietet eine Vielzahl an Werkzeugen unterschiedlichster Ausrichtung – für SaaS, IaaS oder PaaS (Software-/Infrastructure-/Platform-as-a-Service) –, aus denen man sich die fürs eigene Unternehmen geeigneten heraussuchen muss.

Gartner prägte für diese Produktkategorie den Begriff Cloud Security Posture Management (CSPM) und beschreibt sie als Sicherheitsprodukte, die Anwendern helfen können, die Sicherheitsprozesse zu automatisieren und die Compliance in der Cloud zu gewährleisten.

Sicherheit als Prozess

Für die prozessorientierte Betrachtung von Sicherheitsaspekten haben sich einige Eckpunkte etabliert:

- Umsetzung von Sicherheitsmaßnahmen kontrollieren,
- Sicherheitsvorgaben bei jeder Konfiguration einhalten,
- Updates verwalten,

- Codequalität überwachen,
- versuchte und erfolgreiche Angriffe erkennen.

Werkzeuge, die den aktuellen Stand der Sicherheit messen, hat der Artikel **"Übersicht Compliance Management: Tools für die Cloud und Schwachstellenscanner" [1]** im Rahmen einer Übersicht von Compliance-Management-Tools zum Analysieren, Verwalten, Überwachen und Einstellen sicherheitsrelevanter Konfigurationsoptionen bereits vorgestellt. Diese Tools eignen sich gut sowohl für die interne IT als auch für die Cloud und alles dazwischen.

Gartners CSPM fasst eigentlich alles zusammen, was die Sicherheit von Anwendungen und Daten in der Cloud betrifft. Das reicht von der Überwachung der Konfiguration (SCC, Security Configuration Compliance) über die automatisierte Reaktion auf Vorfälle und Probleme (SOAR, Security Orchestration, Automation and Response) bis zur Absicherung der Container Workloads (CWPP, Cloud Workload Protection Platform). Die Security Operations Center (SOC) sind dabei die jeweilige Kommandozentrale, die den Überblick gibt, aber auch die zentrale Stelle, die Reaktionen festlegt und die Bearbeitung der Vorfälle steuert.

IX-TRACT

- Hyperscaler helfen ihren Kunden mit vielen Werkzeugen und einem Security Operations Center (SOC) beim Absichern der Cloud.
- Die Verantwortung für die Sicherheit liegt auch beim Kunden, der diese Werkzeuge sinnvoll einsetzen sollte.
- Während Azure viele Features mitbringt, sind Multi-Cloud-Umgebungen eine reine Domäne externer Werkzeuge für SCC, SOAR, CWPP und CSPM.

Große *-as-a-Service-Anbieter, die Hyperscaler, haben allerdings auch eigene Dienste, die die Sicherheit bei der Nutzung der eigenen Angebote signifikant erhöhen können und die genannten Bereiche mehr oder weniger gut abdecken. Dieser Artikel stellt die Angebote von Amazons AWS, Microsofts Azure und Googles Cloud Platform (GCP) vor.

Ein paar Begriffsbestimmungen

Ein Security Operations Center soll dem IT-Sicherheitsmanagement helfen, alle Informationen zusammen zu betrachten, und bei der Bewertung der aktuellen Situation unterstützen. Für den Aufbau eines SOC in der eigenen Infrastruktur stehen viele Werkzeuge zur Verfügung, deren Integration aber oft ein kostspieliger Prozess ist, da hier sehr viele unterschiedliche Datenquellen erst zusammen ein vollständiges Bild ergeben.

Bei Public-Cloud-Angeboten sind (fast) alle Datenquellen Dienste, die man per Klick oder API-Aufruf buchen kann. Die drei großen Hyperscaler und auch die an Großkunden gerichteten Clouds haben ein virtuelles SOC im Angebot. AWS ist hier mit dem **Security Hub [2]** vertreten, Azure hat das **Security Center [3]** und GCP das **Security Command Center [4]**.

Der erste und zweite Eckpunkt für ein SOC sind das Überwachen und die Umsetzung der Sicherheitsmaßnahmen. Hier gilt es, drei der Konzepte zu beachten: SCC, SOAR und CWPP.

SCC und CSPM

Alle drei Hyperscaler bieten Security Configuration Compliance für die interne und externe Cloud, also ein Cloud Security Posture Management. Hier ist die Überwachung aller sicherheitsrelevanten Einstellungen gemeint, die Anwender in einem der *aaS vornehmen können. GCE hat dazu vergleichsweise wenig Regeln und keine Flexibilität, da es keine eigenen Regeln erlaubt. AWS bietet mehr vordefinierte Regeln und kann jede Änderung

einer Konfiguration oder eines Status automatisch in eine Lambdafunktion leiten, wo selbst geschriebener Code auf die Veränderung reagiert.

Mit Abstand die meisten Funktionen bietet Azure bereits mit dem kostenlosen Angebot. Die Zahl der vordefinierten Regeln in den Checklisten ist sehr groß und deckt die meisten Dienste ab. Auch kann Azure bei vielen Regeln verhindern, dass verbotene Einstellungen passieren, wo etwa AWS nur nachträglich – wenn auch schnell – darauf reagiert.

SOAR

Security Orchestration, Automation and Response (SOAR) erweitert SCC um die Automatisierung der Reaktion auf das Verletzen der Sicherheitsvorgaben oder auf das Entdecken eines Sicherheitsvorfalls. Auch hier kann Azure punkten, da ein Vorfall, ein Regelverstoß oder eine Empfehlung eine Logic App starten kann. AWS bietet mit den Lambdafunktionen die gleiche Flexibilität, allerdings mit dem größeren Aufwand. GCP hat hier noch einiges aufzuholen, da zumindest die Basisedition keine automatische Reaktion erlaubt. Die Premium-Version kennt Trigger für Cloud-Functions auch bei Ereignissen der Angriffserkennung.

CWPP

Cloud Workload Protection Platform definiert sich vor allem über den Schutz von Containern und deren Betriebsumgebung. Gartner hätte es besser "Container Protection" genannt, aber der Begriff steht nun im Raum und wird von allen Anbietern mit Produkten in dem Bereich genutzt. Für den Vergleich der SOC der Hyperscaler ist hier die Überwachung der Kubernetes-Dienste und der in diesen laufenden Container relevant.

Google hat zwar im Basispaket keine Überwachung der Images vorgesehen, aber der Registry-Dienst von GCP bietet dies standardmäßig. Der Funktionsumfang ist allerdings begrenzt auf wenige Basis-Images. AWS und Azure bieten hier einen umfangreichen Scan der Images auf Verwundbarkeiten, was ein guter erster Schritt ist. Die Image- und Runtime-Policy-Optionen eines ausgewachsenen CWPP wie **AquaSec [5]** oder **Palo Alto Prisma Cloud [6]** bieten sie allerdings nicht. Die Nase vorn hat dennoch auch hier Azure mit dem Defender, der auf Qualys aufsetzt und damit eine der besten Scan-Engines auf dem Markt nutzt. Der Defender ist allerdings nicht umsonst, und ohne die kostenpflichtige Aktivierung steht kein Scan der Images zur Verfügung.

Statische Codeanalyse

Der dritte Eckpunkt für ein SOC soll verhindern, dass der eigene Code Schwachstellen enthält. Dies ist schwer zu automatisieren und die Ergebnisse der statischen Codeanalyse sind keine abschließende Antwort auf das Risiko, aber sie senken es zumindest. Hier haben alle drei Hyperscaler keine eigenen Angebote, können aber Drittanbieter einbinden, die Integrationen sind leider noch etwas holprig.

Angriffe erkennen und darauf reagieren

SOAR ist die Weiterentwicklung von SCC und SIEM. Es kombiniert die Erkennung eines Angriffs mit der Reaktion; da Angriffe heute automatisiert und schnell sind, muss es auch die Reaktion sein. Hier bieten alle drei Hyperscaler kostenpflichtige eigene Dienste und auch Drittanbieter für SIEM und IDS lassen sich in das SOC integrieren.

AWS hat mit GuardDuty für Log-Analyse, Detective für die Forensik, CloudWatch für Anomalieerkennung von Betriebsparametern und dem IoT Device Defender ein breites Angebot an Diensten im Programm. GCP bietet Threat Detection als Teil des Premiumpakets und analysiert die Logs, geht allerdings noch einen Schritt weiter und überwacht auch die Kernel-Calls der Container in den Kubernetes-Clustern.

Azure hat mit den kostenpflichtigen Zusatzangeboten Defender und Sentinel zwei leistungsstarke Services im Portfolio, die die komplette Umgebung und Dienste inklusive IoT auf "Indicators of Compromise" überwachen.

MEHR ZU UNTERNEHMENS-IT UND SECURITY

Allerdings verfügt Sentinel bei Aktivierung zunächst über nur wenige Regeln. Eine aktive Community auf GitHub hilft hier, ein eigenes Regelset zu erstellen. Die Vorfälle sind im Security Center zu bearbeiten und WorkBooks helfen dabei. Dazu bietet Azure die Angriffserkennung für das Active Directory und den CASB (Cloud App Security Broker), der beispielsweise nicht erlaubte Nutzung der Cloud-Dienste von Drittanbietern durch Mitarbeiter erkennen kann.

[28]

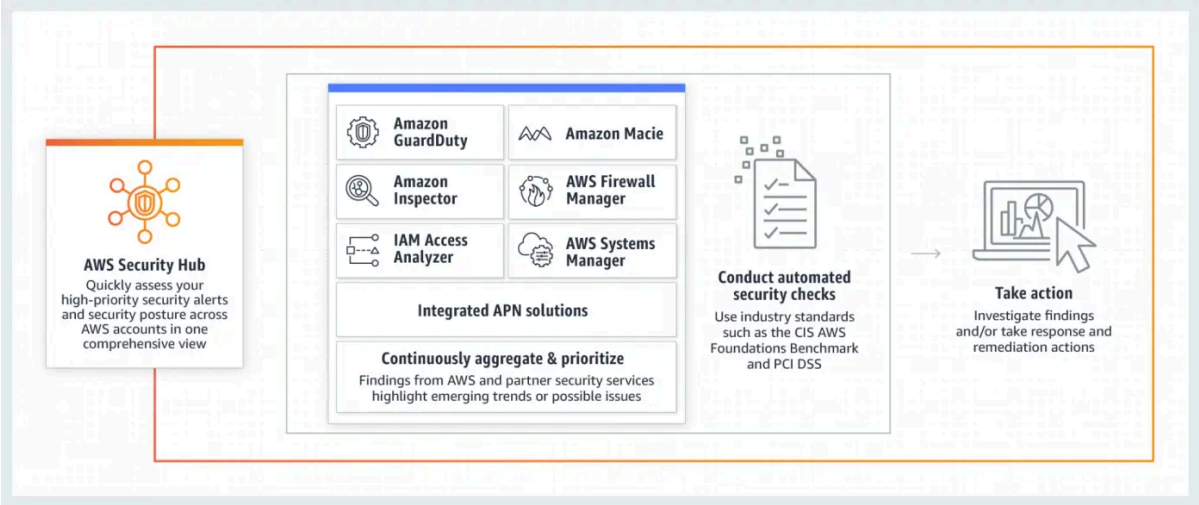
AWS Security Hub

Amazon hat mit AWS die Public Cloud erfunden, wie wir sie heute kennen. Das ist gut für den Marktanteil, aber bei manchen Diensten leider auch zu merken. Die immer noch starke Fokussierung auf die Regionen und dass manches erst nachträglich eingebaut wurde, macht die Benutzung des Security Hub ziemlich umständlich. Dieser Entstehungsgeschichte ist es wohl geschuldet, dass es mehrerer Dienste für eine Aufgabe bedarf.

Um den Security Hub überhaupt zu starten, muss zuerst AWS Config die Konfiguration der Ressourcen aufzeichnen. Sobald dies aktiviert ist, kann AWS CloudWatch jede Veränderung einer Konfiguration gegen die hinterlegten Regeln prüfen. Es kann daher fehlerhafte Einstellungen nicht verhindern, sondern nur nachträglich warnen oder die Fehler direkt beheben. Dann ist es allerdings vielleicht bereits zu spät. Immerhin ist die Reaktion sehr schnell. Jede Regel ist bei AWS eine Lambdafunktion, was es ermöglicht, auch eine Funktion als Regel zu hinterlegen und damit auf beliebige Konfigurationsereignisse zu reagieren. Diese Flexibilität ist allerdings nicht umsonst. So berechnet AWS pro Bewertung einer Regel 0,1 US-Cent, auch bei einer größeren Installation sind die Kosten also überschaubar.

Auch der Historie und der regiozentrischen Sicht geschuldet ist der Umstand, dass Konfigurationsereignisse aus unterschiedlichen Regionen nur in der jeweiligen Region vorliegen. Wer Regeln auf alle Ressourcen anwenden will, muss diese mit dem Konfigurationsaggregator von AWS Config zusammenführen. Dies funktioniert dann auch über mehrere Konten hinweg und eine Organisation kann dies zum Aufbau einer zentralisierten Sicht nutzen.

Mit den Conformance Packs bietet AWS die Option, ein unveränderliches Regelset in allen Konten der Organisation zu nutzen. Es kann sich um vorgegebene, aber auch um eigene Regeln handeln.



Im AWS Security Hub fasst Amazon die verschiedenen Komponenten und Methoden zur Absicherung zusammen. (Bild: Amazon)

Wie auch bei den unverpackten Regeln zeigt der Security Hub alle Regelverstöße und somit eine Übersicht über die Einhaltung der Compliance an. Ein Dashboard ist hier natürlich ebenfalls enthalten. Das zeigt auch alle anderen Meldungen an, die der Hub aus einer der Partnerintegrationen erhält. Hier hat AWS mit dem AWS Security Finding Format (ASFF) eine für den Erfolg ausschlaggebende Grundlage gelegt. ASFF legt präzise fest, wie eine Meldung aussehen muss, zu welcher Taxonomie sie gehört, was der Ursprung und der Inhalt ist.

Partnerlösungen wie Splunk, ServiceNow, Evident.IO, CloudCheckr, RedSeal Networks und Red Hat CloudForms sind nur ein paar Beispiele aus der Liste der verfügbaren externen Integrationen. Allerdings fallen auch für diese Meldungen die oben genannten Preise an. Neben den externen Integrationen gibt es AWS-interne Integrationen für GuardDuty, Inspector, Macie, IAM Access Analyzer, Systems Manager Patch Manager und Firewall Manager. Über diese sammelt der Hub Meldungen aus allen sicherheitskritischen Diensten von AWS und präsentiert sie im Dashboard. Zum Bearbeiten dieser Meldungen verlinkt das Dashboard dann auf die Konsolen dieser Dienste.

Neben den Meldungen an den Hub kann eine Integration auch der Empfänger sein, der diese Informationen dann entweder für Berichtswesen oder Reaktion nutzen kann. Der Fantasie sind bei dieser Art der Automatisierung des Compliance Reporting und der automatischen Reaktion keine Grenzen gesetzt und die Wahrscheinlichkeit ist hoch, dass bereits ein Tool existiert, das die eigenen Vorstellungen umsetzt. Für das Compliance Reporting sei hier auf die Produktübersicht im Artikel **"Übersicht Compliance Management: Tools für die Cloud und Schwachstellenscanner" [29]** verwiesen, denn diese Werkzeuge nutzen die ASFF-Meldungen ebenfalls. APN-Partner-Anwendungen wie ServiceNow, Evident.IO, Splunk, CloudCheckr, RedSeal Networks und Red Hat CloudForms stellen für Daten aus AWS Config voll integrierte Angebote bereit.

Beim ersten Aktivieren des Hub startet dieser bereits mit den Regelsätzen "AWS Foundational Security Best Practices" und "CIS AWS Foundations Benchmark" jeweils in den aktuellen Versionen. Auch ist sofort eine Auswertung zu sehen, welche S3-Buckets öffentlich schreib- oder lesbar sind. Hier hat AWS aus einer ganzen Serie unabsichtlich veröffentlichter Daten gelernt und erschwert es heute, diese Fehler zu begehen oder nicht zu bemerken. Praktisch ist auch die Übersicht aller aus dem Internet erreichbaren Ports auf EC2-Instanzen und die Aufschlüsselung von Befunden nach Konten und Nutzern. Zur genaueren Analyse lassen sich alle Meldungen durchsuchen und die Suchen als Insight speichern. Dieser ist dann zusammen mit den 32 bereits vorhandenen Einblicken in der Übersicht aufgeführt, steht aber nicht auf der Startseite im Dashboard.

Die Qualität der Ergebnisse hängt hauptsächlich von den genutzten und aktivierten Sicherheitsdiensten ab. Wer alle Register zieht und von CloudWatch bis Firewall Manager alles nutzt, erhält – sofern die Meldungen zusammengeführt sind – eine sehr umfangreiche Übersicht über die Sicherheit seiner AWS-Ressourcen. Hier merkt man im Guten wie im Schlechten das Alter von AWS.

Einerseits sind die Dienste ausgereift und sehr umfangreich. Andererseits merkt man, dass die Zusammenfassung in den Hub und auch die Integration der Verwaltungseinheit Organisation eine nachträgliche Entwicklung ist. Auch die Regionalität erfordert zusätzlichen Konfigurationsaufwand. Mit dem AWS Security Hub lassen sich sehr umfangreiche Auswertungen, Berichtswesen und Complianceüberwachung realisieren, die auch für sehr große Installationen gute Ergebnisse liefern – selbst wenn manchmal eine Meldung etwas länger braucht, als man sich wünschen würde.

Azure Security Center

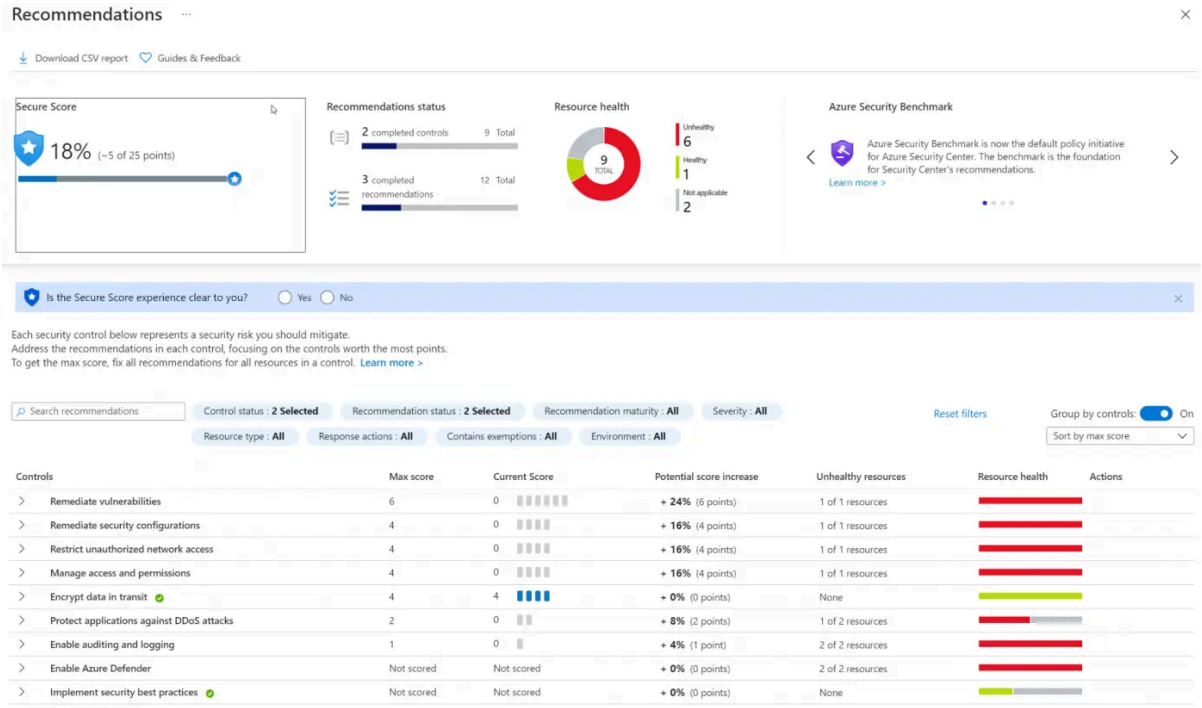
Bei Azure merkt man auch im Security Center, dass Microsoft hier auf den Erfahrungen anderer Hyperscaler aufbauend einen Dienst entwickelt hat, der besonders die Bedürfnisse großer Firmen erfüllen soll. So wie die Group Policy unter Windows die Verwaltung sehr vieler Server und Clients ermöglichte, eignen sich auch die Managementstrukturen von Azure für Umgebungen, in denen ein Kunde mit vielen Abteilungen und Arbeitsgruppen Ressourcen in einer zentralen Verwaltung benötigt.

Das Security Center ist hier nicht ein nachträglicher Aufsatz, sondern eine zentrale Komponente. Auch das Berechtigungsmanagement für die Sicherheitsfunktionen folgt diesem Ansatz. So sind die Rollen Security Reader und Security Administrator relativ neu, aber die Idee des ganzheitlichen Managements aller sicherheitsrelevanten Funktionen zieht sich durch alle Produkte und wird im Security Center gebündelt dargestellt.

Bewertungen und Empfehlungen inklusive Richtliniensätzen für ein Dutzend Compliance-Frameworks von CIS bis HIPAA sind kostenfrei enthalten. Wer mehr will, braucht den Defender, der pro überwachter Ressource etwa zwei Euro-Cent pro Stunde kostet. Dazu kommen die Kosten der weiteren Sicherheitsdienste wie Sentinel, Web-Application-Firewalls und Firewall Manager.

Die Grundlage der Sicherheit sind auch bei Azure die Policies, die Azure entweder einzeln oder als Set auf Ressourcen anwendet. Besonderheit ist hier, dass es auch Policies gibt, die bestimmte Einstellungen verhindern und nicht erst nach der Konfiguration aktiviert werden, wie es bei AWS der Fall ist. Ressourcen verwaltet Azure immer in Subscriptions, die dann Ressourcengruppen enthalten, in denen die eigentlichen Dienste Storage, Server, PaaS oder IaaS liegen. Eine Subscription ist üblicherweise eine Umgebung eines Projekts. Das wird schnell unübersichtlich und zur besseren Verwaltung gibt es Management Groups, die Subscriptions oder wiederum andere Management Groups enthalten.

So bildet sich eine Hierarchie, wie man sie aus dem heimischen AD kennt. Für die Policies ist dies relevant, denn sie gelten entweder für die Ressource, die Ressourcengruppe, die Subscription oder eine Management Group. Wer GPO kennt, findet sich in diesem Konstrukt umgehend zurecht. Das Erstellen einer globalen Richtlinie für alle Ressourcen und spezieller Richtliniensets für einzelne Abteilungen, Projekte oder Umgebungen ist auf diese Weise einfach möglich. Auch lassen sich Richtliniensets an Test- und Staging-Subscriptions oder den diese enthaltenden Managementgruppen testen, bevor sie ein Administrator auf die Produktion anwendet. Gut für das Erproben ist auch die Option, einen Regelsatz zuerst im Audit-only-Modus anzuwenden, auf Meldungen zu warten und dann auf Enforcing scharf zu schalten.



Im Azure Security Center finden sich Empfehlungen zur aktuellen Sicherheitssituation, hier für eine kleine Umgebung mit wenig Ressourcen.

Jede Regel ist dabei die Quelle entweder für eine Nachricht als Alert oder Empfehlung oder sie triggert eine Logic App, die beliebigen Code enthalten kann, der direkt auf das Ereignis reagiert. Ein SOAR ist so für Angriffe und für Abweichungen der Konfiguration vom gewünschten Zustand realisierbar. Für sehr oft auftretende Ereignisse, etwa das Fehlen einer Einstellung, bieten viele Regeln das Ereignis DeployIfNotExists, also "Installiere es, wenn es noch nicht da ist".

Die Bedienung ist übersichtlich und alle Ressourcen, auf die der angemeldete Mitarbeiter zugreifen kann, sind sofort sichtbar, wenn auch nicht alle zu überwachenden Ereignisse sofort für das Security Center oder den Defender bereitstehen. So kann es nur überwachen, was auch protokolliert wird. Alle Subscriptions benötigen also einen "Log Analytics Workspace" der die Aktivitäten aufzeichnet. Zu diesem verbindet sich das Security Center und erstellt dann die Alerts. Die Sicherheitsregeln für die Konfiguration wendet es sofort nach dem Aktivieren des Regelsatzes an und zeigt die Empfehlungen allen Mitarbeitern, die das entsprechende Recht auf diese Ressourcen haben.

Um über diese kostenfreien Funktionen hinaus einen tieferen Einblick in die sicherheitsrelevanten Ereignisse zu erhalten, muss der kostenpflichtige Defender aktiv sein. Der kann von SQL-Servern bis IaaS alle Ressourcen überwachen. Dies umfasst von Patch-Management bis zu Anomalien im Betrieb eine umfangreiche Bandbreite von Messpunkten. Wer noch mehr und auch eigene Regeln auf alle Ereignisse will, benötigt den ebenfalls kostenpflichtigen Dienst Sentinel, ein zentrales SIEM, dem aber alle Ressourcen ihre Diagnose-Logs schicken müssen, was mit einer Policy pro PaaS-Typ etwa für alle in einer Managementgruppe oder Subscription erledigt ist.

Das Security Center stellt dann alles zusammengefasst dar, was für diesen Mitarbeiter zugänglich ist. Es gibt Aufschlüsselungen über die Compliance zu bestimmten Regelsätzen oder pro Subscription. Sehr managementfreundlich ist auch der Overall Secure Score. Zum Vereinfachen des Sicherheitsstatus beziehungsweise von Empfehlungen oder der Bearbeitung von Vorfällen kann es auch Produkte von Drittanbietern einbinden oder die Sicherheitsadministratoren nutzen die mitgelieferten Workbooks.

Eine Besonderheit ist sicherlich, dass Microsoft auch an Kunden mit Multicloud gedacht hat. So ist Azure das einzige Produkt, das auch AWS und GCP überwachen kann. Auch Azures SIEM Sentinel kann Logdaten von AWS

und anderen Anbietern verarbeiten.

Google GCP Security Command Center

Der dritte im Bunde nach Marktanteil hat einige Umbauten hinter sich, die auch das Security Command Center betreffen, mit dem Google in GCP einen Überblick über die Sicherheit aller Ressourcen in der Cloud bietet. Der Bericht über dieses Angebot muss leider recht kurz ausfallen, da Google für diesen Artikel keinen Zugang zum Premiumangebot bereitstellte. Bei Kosten von mindestens 25 000 US-Dollar kam ein eigens für diesen Artikel angelegter Account nicht infrage.

Immerhin erhalten alle Kunden der GCP ein Basisangebot, das zumindest eine Funktion bietet. Dies nennt sich Security Health Analytics und enthält bereits einige Sicherheitsregeln für diverse Dienste und die Benutzerverwaltung auch der neuen "Organisationen" genannten Verwaltungseinheit. Leider ist die Liste der Regeln nicht einsehbar und auch durch Hinzufügen von PaaS-, IaaS- und STaaS-Diensten (Storage as a Service) erhöhte sich die Zahl der vom SCC gefundenen Sicherheitsprobleme nicht.

Um also in der Konsole der GCP den SCC zu aktivieren, ist es zuerst notwendig, eine Organisation zu erstellen. Dafür sind eine Firma und eine Domain anzugeben. Es wird ein Benutzerverzeichnis erstellt, das für alle eine email@Domain erfordert. Wer hier schon einen Google Workspace hat, wird sich schnell zurechtfinden, auch die Administration dieser Organisation ist unter admin.google.com erreichbar. Sobald ein erster Account als Inhaber eingerichtet ist, kann dieser in der Konsole Projekte initiieren und dort Dienste starten.

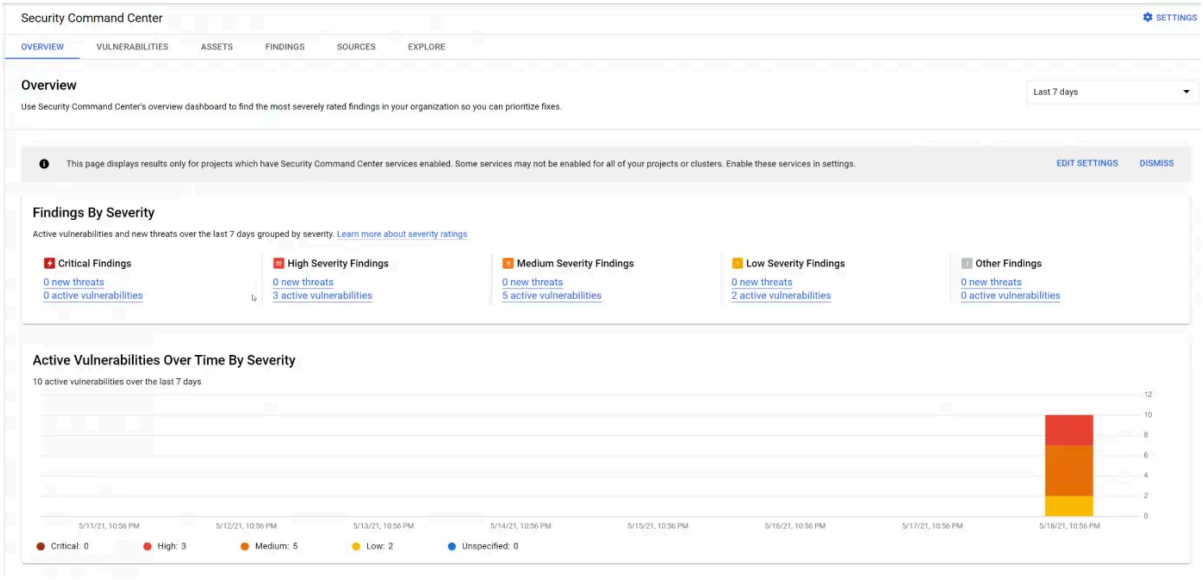
Etwas verwunderlich ist, dass Google Zahlungsdaten dann erst in den Projekten akzeptiert. Hier wäre eine Abrechnung über den Firmenaccount eher zu erwarten gewesen. In der Administration der Organisation finden sich auch Sicherheitsregeln, wenn auch nicht die, die im SCC auftauchen. Aber immerhin gelten diese Regeln dann für alle Mitglieder und es gibt auch die Möglichkeit, sie weiterzuleiten oder in einer Übersicht anzusehen.

Verwaltung und Integrationsoptionen

SCC nur mit konfigurierter Organisation sinnvoll

Nach dem Konfigurieren der Organisation ist der SCC mit wenigen Klicks aktiviert. Dies geht nur, wenn man den Kontext der Konsole auf die Organisation setzt. Hier merkt man, dass Google die Organisationen nachträglich zu GCP hinzugefügt hat und diese nun ein Überbau über die eigentlich verwendeten Projekte sind. Die Integration ist gelungen, und auch mehrere Organisationen gleichzeitig zu verwalten, ist für einen Admin-Account ohne Schwierigkeiten möglich.

Dass man zwei Konsolen für die Verwaltung benötigt, ist wie auch die ständig neuen Tabs im Alltag ziemlich lästig und der Nutzen nicht erkennbar. Für die Organisation ist im Admin-Interface eine Untergruppe eingerichtet, die sich beim Zugang über die Webkonsole und der Zuordnung der Projekte nicht wiederfindet. Ob ein Projekt Teil einer Untergruppe sein und ob es zwischen den Untergruppen wandern kann, ist nicht ersichtlich. Hier sind die Azure Management Groups sehr viel klarer und ermöglichen es auch großen Organisationen, die genutzten Ressourcen übersichtlich zu verwalten.



Googles Security Command Center bietet auch in der kostenfreien Basisversion ein Dashboard.

Auch in einer völlig leeren Organisation findet der SCC-Basiszugang bereits einige Verbesserungsvorschläge. Allerdings zeigt die Übersicht mit den Quellen der Verwundbarkeiten auch nicht im Basis-SCC enthaltene Features an – ohne dies irgendwie kenntlich zu machen. Nach dem Aktivieren von Functions, einem K8s-Cluster, einer Bigtable und diverser Buckets in einem Projekt kamen jedoch kaum neue Feststellungen hinzu – die SCC-Standardeinstellungen sind schon sehr sicher.

Testweise ein Bucket auf Public zu stellen, führte zum gewünschten Ergebnis und es gab sofort einen High Alert. Das Problem per Klick zu beheben, bietet die Weboberfläche zwar nicht an, sie zeigt aber den auf der Kommandozeile auszuführenden Befehl auf Wunsch an. Ein automatisiertes Beheben für SOAR ist nicht vorgesehen. Für Anthos gibt es einen eigenen Menüpunkt zur Sicherheit, dies scheint nicht im SCC mit enthalten zu sein, das zu testen war wegen des eingeschränkten Zugangs nicht möglich. Zumindest führte das Aktivieren von Anthos nicht zu neuen Feststellungen im SCC.

Integrationsoptionen für Software von Drittanbietern

Erwähnenswert ist die große Zahl der Integrationen für den SCC. Hier sind alle namhaften Hersteller von CWPP, CSPM, CASB, SCC et cetera aufgeführt, die auch die kostenpflichtigen Funktionen des SCC selbst teilweise ersetzen. So ist CSPM nach den Benchmarks des CIS mit **Cavirin [30]**, **Dome9 [31]** oder **Tenable.io [32]** genauso möglich wie mit den Funktionen des SCC.

Allerdings war eine Integration des SCC mit den anderen GCP-Sicherheitsfunktionen wie Chronicle für Logsammlung, DLP oder VPC Service nicht zu erkennen. Der Web Security Scanner, den das SCC eigentlich nur im Premiumpaket enthält, ließ sich in den Projekten aktivieren und lieferte dann auch seine Ergebnisse an den SCC. Den Scan auf die eine Funktion mit dem JavaScript-Beispiel "Hello World" startete es allerdings nicht, da hier eine dynamische IP-Adresse im Einsatz war, die nicht dem Projekt zugeordnet war, was für diesen Funktionstyp auch nicht möglich ist.

Insgesamt hinterließ der SCC einen unfertigen Eindruck, was darauf zurückzuführen sein kann, dass nur die sehr eingeschränkte Basisversion zur Verfügung stand. Aber auch dann kann GCP mit einem Security Hub von AWS oder dem Azure Security Center mit vielen Optionen, definierbaren Regeln und Automatisierung bei Weitem nicht mithalten.

Fazit und Vergleichstabelle

Die Cloud bietet sicherheitsbewussten Nutzern durchaus große Vorteile. So entfallen viele Betriebsaufgaben, die jetzt der Cloud-Anbieter übernimmt und durch die Automatisierung oft auch zuverlässiger und schneller erledigt,

als das für die meisten Firmen möglich ist. Die Verantwortung für die Qualität des eigenen Codes und für die Einstellungen verbleibt aber weiterhin beim Kunden. Auch hier ermöglichen Produkte wie die im **Artikel Anfang des Jahres 2021 [33]** vorgestellten oder die Haus-Anwendungen der Hyperscaler eine bessere Verwaltung und einen tieferen Einblick in die Konfiguration sowie eine stark verbesserte Überwachung.

Unabhängig von der Wahl des Werkzeugs sind Anwender allerdings auch in der Pflicht, diese Angebote zu nutzen und auf die Empfehlungen zu regieren, sonst ist ein Sicherheitsvorfall schnell passiert. Der oft beschworenen, auch im Artikel **"Cloud-Betrieb: Maßnahmen zur sicheren Nutzung von Public Clouds" [34]** detaillierter vorgestellten, geteilten Verantwortung für die Cloud müssen Kunden sich bewusst sein und dafür auch die entsprechende Kompetenz mitbringen. Die Werkzeuge vereinfachen diese Arbeit schon relativ stark, da die Empfehlungen bei fast allen Angeboten sehr ausführlich und konkret sind.

Ob es ein Werkzeug eines Drittanbieters oder eines der hier vorgestellten SOC sein soll, ist in der Praxis oft eine Preisfrage. Nur bei GCP ist die eigene Software teurer als die der Drittanbieter, und die Hyperscaler helfen auch mit den kostenfreien Funktionen schon gut beim Absichern. Wer allerdings maximale Sicherheit benötigt, wird um zusätzliche Produkte wie ein vollständiges CWPP für Container nicht herumkommen.

Vergleichstabelle

Cloud Security Operations Center und kommerzielle Tools für Cloud Security Posture Management

Name	Aqua Wave	AWS Security Hub	Azure Security Center
Anbieter	Aqua Security	Amazon	Microsoft
Typ	Cloud-Multitool	herstellereigenes SOC	herstellereigenes SOC
Varianten	SaaS	SaaS	SaaS
AWS	✓	✓	✓
Azure	✓	–	✓
GCP	✓	✓	–
SOAR	✓	✓	✓
Windows AD	–	–	✓
Windows-Systeme	–	✓	✓
Linux/Unix	✓	✓	✓
Docker	✓	–	✓
Kubernetes	✓	–	✓
Container-Images	✓	✓	✓
IoT	✓	✓	✓
VMware	–	–	✓
Anmerkungen	IoT auf ARM ist in der Enterprise Edition möglich.	CIS Benchmarks des „Inspector“ sind für Windows	Defender als Teil von ASC ist kostenpflichtig

		und Unix verfügbar. CloudWatch und andere Dienste sind hier mit enthalten.	für fast alle Umgebungen verfügbar.
URL	**www.aquasec.com/products/cspm/ [35]**	**aws.amazon.com/de/security-hub/ [36]**	**azure.microsoft.com/en-us/services/security-center/ [37]**

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

(avr [49])

URL dieses Artikels:

https://www.heise.de/-6110834

Links in diesem Artikel:

[1] https://www.heise.de/tests/Uebersicht-Compliance-Management-Tools-fuer-die-Cloud-und-Schwachstellenscanner-4989174.html

[2] https://aws.amazon.com/de/security-hub/?aws-security-hub-blogs.sort-by=item.additionalFields.createdDate&aws-security-hub-blogs.sort-order=desc

[3] https://azure.microsoft.com/en-us/services/security-center/

[4] https://cloud.google.com/security-command-center

[5] https://www.aquasec.com/products/CSPM/

[6] https://www.paloaltonetworks.com/prisma/cloud

[7] https://www.heise.de/hintergrund/Wie-Angreifer-dank-psychologischer-Tricks-in-Unternehmen-eindringen-7317970.html

[8] https://www.heise.de/tests/Sicherheits-und-Incident-Management-mit-Wazuh-7218423.html

[9] https://www.heise.de/hintergrund/BSI-Warnungen-zur-IT-Sicherheit-ernst-nehmen-7143015.html

[10] https://www.heise.de/hintergrund/Ukrainekrieg-Auswirkungen-auf-die-IT-Sicherheit-in-Deutschland-6668405.html

[11] https://www.heise.de/hintergrund/IT-Versicherungsschutz-fuer-kleine-Unternehmen-und-Freelancer-6489094.html

[12] https://www.heise.de/ratgeber/Security-Ransomware-Angriffsmuster-und-wie-man-sich-vor-ihnen-schuetzt-6457415.html

[13] https://www.heise.de/ratgeber/Security-So-laufen-Ransomware-Angriffe-heute-ab-6457906.html

[14] https://www.heise.de/ratgeber/Security-So-arbeiten-Incident-Response-Teams-nach-einem-Ransomeware-Angriff-6473782.html

[15] https://www.heise.de/hintergrund/IT-Recht-Sicherheitsanforderungen-und-Rechtsfragen-zu-Ransomware-Attacken-6474409.html

[16] https://www.heise.de/hintergrund/OWASP-Top-10-Sicherheitsrisiken-in-Web-Anwendungen-6332056.html

[17] https://www.heise.de/hintergrund/OKR-Einfuehrung-in-Firmen-Haeufige-Fehler-und-wie-es-dennoch-klappt-6291471.html

[18] https://www.heise.de/ratgeber/Unternehmens-IT-Wie-sich-Managed-Services-wandeln-6233929.html

[19] https://www.heise.de/ratgeber/Endgeraetesicherheit-und-EDR-Tools-Gefahren-schnell-erkennen-und-reagieren-6222034.html

[20] https://www.heise.de/hintergrund/Cybercrime-Ransomware-Entwicklung-fuehrt-zu-neuen-Bekaempfungsstrategien-6220960.html

[21] https://www.heise.de/hintergrund/Identity-and-Access-Management-der-Zukunft-Digitales-Business-Zero-Trust-SASE-6203741.html

[22] https://www.heise.de/hintergrund/IT-Sicherheit-Ransomware-Attacken-verhindern-durch-Security-Learning-Center-6204081.html

[23] https://www.heise.de/hintergrund/IT-Grundschutz-BSI-Anforderungen-fuer-Container-und-Kubernetes-6200393.html

[24] https://www.heise.de/hintergrund/IT-Security-Trainings-als-Vorbereitung-fuer-Sicherheitsvorfaelle-im-Unternehmen-6196247.html

[25] https://www.heise.de/ratgeber/IT-Security-PetitPotam-und-andere-Wege-die-Kontrolle-ueber-das-AD-zu-uebernehmen-6170976.html

[26] https://www.heise.de/hintergrund/Netzwerksicherheit-im-Active-Directory-So-enttarnen-Sie-Angreifer-durch-Logs-6141370.html

[27] https://www.heise.de/hintergrund/Cloud-Sicherheit-Cloud-Security-Operations-Center-im-Vergleich-6110834.html

[28] https://www.heise.de/ix/

[29] https://www.heise.de/tests/Uebersicht-Compliance-Management-Tools-fuer-die-Cloud-und-Schwachstellenscanner-4989174.html

[30] https://www.cavirin.com/

[31] https://www.checkpoint.com/products/cloud-security-posture-management/

[32] https://de.tenable.com/products/tenable-io?tns_redirect=true

[33] https://www.heise.de/tests/Uebersicht-Compliance-Management-Tools-fuer-die-Cloud-und-Schwachstellenscanner-4989174.html

[34] https://www.heise.de/hintergrund/Cloud-Betrieb-Massnahmen-zur-sicheren-Nutzung-von-Public-Clouds-4994040.html

[35] https://www.aquasec.com/products/cspm/

[36] https://aws.amazon.com/de/security-hub/

[37] https://azure.microsoft.com/en-us/services/security-center/

[38] https://www.cavirin.com/

[39] https://www.c3m.io/compliance

[40] https://www.checkpoint.com/products/cloud-security-posture-management/

[41] https://store.servicenow.com/sn_appstore_store.do#!/store/application/29691e1f0212471dad08668c1e39932b/11.0

[42] https://cloud.google.com/security-command-center

[43] https://www.rapid7.com/de/products/insightvm/features/policy-assessment/

[44] https://www.qualys.com/apps/security-configuration-assessment/

[45] https://www.runecast.com/

[46] https://tenable.io/

[47] https://www.trendmicro.com/de_de/business/products/hybrid-cloud/cloud-one-conformity.html

[48] https://www.tripwire.com/products/tripwire-configuration-manager

[49] mailto:avr@ix.de