Technischer Leitfaden für AWS

Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS

Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS: Technischer Leitfaden für AWS

Table of Contents

Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS

Veröffentlichungsdatum: 23. November 2020 (Dokumentversionen)

Dieser Leitfaden bietet einen Überblick über die Grundlagen der Reaktion auf Sicherheitsvorfälle in der AWS Cloud-Umgebung eines Kunden. Er bietet zudem eine Zusammenfassung der Cloud-Sicherheit und Konzepte der Vorfallreaktion und er identifiziert Cloud-Funktionen, -Services und -Mechanismen, die Kunden zur Reaktion auf Sicherheitsprobleme zur Verfügung stehen.

Dieses Dokument richtet sich an technische Mitarbeiter unter der Voraussetzung, dass Sie mit den allgemeinen Prinzipien der Informationssicherheit vertraut sind, über ein grundlegendes Verständnis der Reaktion auf Vorfälle in Ihren aktuellen On-Premises-Umgebungen verfügen und mit Cloud-Services vertraut sind.

Einführung

Sicherheit bei AWS hat oberste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat. Die AWS Cloud verfolgt ein Sicherheitsmodell mit geteilter Verantwortung. AWS verwaltet die Sicherheit der Cloud. Sie sind verantwortlich für die Sicherheit in der Cloud. Das bedeutet, dass Sie die Kontrolle über die Sicherheitsmaßnahmen haben, die Sie implementieren möchten. Sie haben Zugriff auf Hunderte von Tools und Services, mit denen Sie Ihre Sicherheitsziele erreichen können. Mithilfe dieser Funktionen können Sie eine Sicherheitsgrundlage aufbauen, um die Ziele für Ihre Cloud-Anwendungen umzusetzen.

Bei Verstößen gegen Ihre Vorgaben (z. B. durch eine Fehlkonfiguration) müssen Sie möglicherweise reagieren und eine Untersuchung durchführen. Dazu müssen Sie die grundlegenden Konzepte der Reaktion auf Sicherheitsvorfälle in Ihrer AWS-Umgebung sowie die Probleme verstehen, die Sie berücksichtigen müssen, um Ihre Cloud-Teams vor dem Eintreten von Sicherheitsproblemen vorzubereiten, zu informieren und zu schulen. Sie müssen wissen, welche Kontrollen und Funktionen Sie verwenden können, um aktuelle Beispiele zur Lösung potenzieller Probleme zu überprüfen und Behebungsmethoden zu identifizieren, mit denen Sie Automatisierung nutzen und Ihre Reaktionsgeschwindigkeit verbessern können.

Da die Reaktion auf Sicherheitsvorfälle ein komplexes Thema sein kann, empfehlen wir, klein anzufangen, Runbooks zu entwickeln, grundlegende Funktionen zu nutzen und eine erste Bibliothek mit Vorfallreaktionsmechanismen zu erstellen, die Sie anwenden und verbessern können. Diese Vorarbeit sollte Ihre Rechtsabteilung sowie nicht mit Sicherheitsaufgaben betraute Teams umfassen, damit Sie die Auswirkungen Ihrer Vorfallreaktion (Incident Response; IR) und Ihrer getroffenen Entscheidungen auf Ihre Unternehmensziele nachvollziehen können.

Themen

Bevor Sie beginnen

Zusätzlich zu diesem Dokument empfehlen wir Ihnen die Bewährten Methoden für Sicherheit, Identität und Compliance sowie das Whitepaper Sicherheitsperspektive des AWS Cloud Adoption

Framework (CAF). Das AWS CAF bietet Anleitungen zur Unterstützung der Koordination unterschiedlicher Abteilungen von Organisationen, die in die Cloud migrieren. Die CAF-Anleitung ist in mehrere Schwerpunktbereiche unterteilt, die für die Implementierung von cloudbasierten IT-Systemen relevant sind, die wir als Perspektiven bezeichnen. Die Sicherheitsperspektive beschreibt, wie ein Sicherheitsprogramm in mehreren Workstreams implementiert wird, von denen sich einer mit der Vorfallreaktion befasst. Dieses Dokument beschreibt einige unserer Erfahrungen bei der Unterstützung von Kunden zur Bewertung und Implementierung erfolgreicher Mechanismen in diesen Workstream.

AWS CAF-Sicherheitsperspektive

Die Sicherheitsperspektive umfasst vier Komponenten:

- Leitende Kontrollen etablieren die Governance-, Risiko- und Compliance-Modelle, mit denen die Umgebung ausgeführt wird.
- Vorbeugende Kontrollen schützen Ihre Workloads und entschärfen Sicherheitsrisiken und Schwachstellen.
- Aufdeckende Kontrollen bieten volle Sichtbarkeit und Transparenz des Betriebs Ihrer Bereitstellungen in AWS.
- Reagierende Kontrollen korrigieren potenzielle Abweichungen von Ihren Sicherheitsvorgaben.

Obwohl IR im Allgemeinen unter der Komponente „Reagierende Kontrollen“ verzeichnet wird, werden auch sie von den anderen Komponenten bedingt und beeinflusst. Beispielsweise helfen leitende und vorbeugende Sicherheitskontrollen bei der Festlegung einer Grundlage, sodass Sie Abweichungen von Ihren Vorgaben überwachen und untersuchen können. Dieser Ansatz beseitigt nicht nur Störungen, sondern trägt auch zu einem defensiven Sicherheitsdesign bei.

Grundlage der Vorfallreaktion

Alle AWS-Benutzer innerhalb eines Unternehmens sollten ein grundlegendes Verständnis der Reaktionsprozesse bei Sicherheitsvorfällen besitzen. Zudem muss das Sicherheitspersonal genau wissen, wie es auf Sicherheitsprobleme reagieren muss. Entsprechende Erfahrung und Ausbildung sind für ein Vorfallreaktionsprogramm in der Cloud von entscheidender Bedeutung, bevor Sie ein Sicherheitsereignis handhaben. Die Grundlage für ein erfolgreiches Vorfallreaktionsprogramm in der Cloud bilden Ausbildung, Vorbereitung, Simulation und Iteration.

Lesen Sie die folgenden Beschreibungen, um die einzelnen Aspekte zu verstehen:

- Informieren Sie Ihr für Sicherheitsvorgänge und Vorfallreaktionen zuständiges über Cloud-Technologien und wie Ihre Organisation diese nutzen möchte.
- Bereiten Sie Ihr Vorfallreaktionsteam darauf vor, Vorfälle in der Cloud zu erkennen und darauf zu reagieren, indem Sie Erkennungsfunktionen aktivieren und einen angemessenen Zugriff auf die erforderlichen Tools und Cloud-Services gewährleisten. Bereiten Sie außerdem die erforderlichen Handlungsanweisungen vor, sowohl manuell als auch automatisiert, um zuverlässige und konsistente Reaktionen auf den Vorfall zu gewährleisten. Arbeiten Sie mit anderen Teams zusammen, um erwartete Basisoperationen festzulegen, und nutzen Sie dieses Wissen, um Abweichungen von diesen normalen Operationen zu identifizieren.
- Simulieren Sie sowohl erwartete als auch unerwartete Sicherheitsereignisse in Ihrer Cloud-Umgebung, um die Effektivität Ihrer Vorbereitung nachzuvollziehen.
- Iterieren Sie das Ergebnis Ihrer Simulationen, um das Ergebnis Ihrer Reaktion zu verbessern, die Zeit bis zur Bewertung zu verkürzen und das Risiko weiter zu reduzieren.

Informieren

Themen

Geteilte Verantwortung

Die Verantwortung für Sicherheit und Compliance liegen in der geteilten Verantwortung von AWS und Ihnen. Dieses gemeinsame Modell reduziert Ihre betriebliche Belastung, da AWS die Komponenten des Host-Betriebssystems und der Virtualisierungsebene betreibt, verwaltet und steuert und zudem für die physische Sicherheit der Standorte sorgt, an denen der Service betrieben wird.

Sie sind für die Verwaltung der Gastbetriebssysteme (einschließlich Updates und Sicherheitspatches) und der Anwendungssoftware verantwortlich sowie für die Konfiguration der von AWS bereitgestellten Sicherheitskontrollen wie Sicherheitsgruppen, Netzwerkzugriffskontrolllisten sowie Identity and Access Management. Sie sollten sich gut überlegen, welche Services Sie verwenden, da Ihre Zuständigkeiten von den ausgewählten Services, von deren Integration in Ihre IT-Umgebung sowie von den geltenden Gesetzen und Vorschriften abhängen. Abbildung 2 zeigt eine typische Darstellung des Modells der geteilten Verantwortung, das für Infrastruktur-Services wie Amazon Elastic Compute Cloud (Amazon EC2) gilt. Es unterteilt die meisten Verantwortlichkeiten in zwei Kategorien: Sicherheit der Cloud (von AWS verwaltet) und Sicherheit in der Cloud (vom Kunden verwaltet). Die Verantwortlichkeiten können variieren, je nachdem, welche Services Sie nutzen. Für davon abgeleitete Services wie Amazon S3 und Amazon DynamoDB betreibt AWS die Infrastrukturebene, das Betriebssystem und die Plattformen. Kunden greifen zum Speichern und Laden von Daten auf die Endpunkte zu. Die Kunden sind für die Verwaltung ihrer eigenen Daten (einschließlich Verschlüsselungsoptionen) und die Klassifizierung ihrer Assets verantwortlich. Mithilfe der IAM-Tools weisen sie geeignete Berechtigungen zu.

Das Modell der geteilten Verantwortung ändert sich jedoch, wenn Container und andere Services hinzugefügt werden, die das Betriebsmodell zum Dienstanbieter verschieben. Wenn wir uns links vom Betriebsmodell weg von IaaS und Rechenzentren hin zu PaaS bewegen, nimmt die Verantwortung des Dienstanbieters zu. Die Verantwortlichkeiten eines Kunden in der Cloud werden weniger

und seine Arbeit leichter, wenn er auf die linke Seite des Diagramms migriert. Beachten Sie die folgenden Zahlen und die Unterschiede in der Fähigkeit, in der Cloud zu arbeiten oder diese zu nutzen. Wenn sich Ihre geteilte Verantwortung in der Cloud ändert, ändern sich auch Ihre Optionen bzgl. Vorfallreaktion oder Forensik. Als Kunde müssen Sie bei der Planung Ihrer Vorfallreaktion außerdem die Fähigkeiten Ihres Betriebsmodells berücksichtigen und die möglichen Interaktionen vorwegnehmen, bevor sie in dem von Ihnen ausgewählten Modell auftreten. Die Planung und das Verständnis dieser Kompromisse und deren Anpassung an Ihre Governance-Anforderungen ist ein entscheidender Schritt bei der Vorfallreaktion.

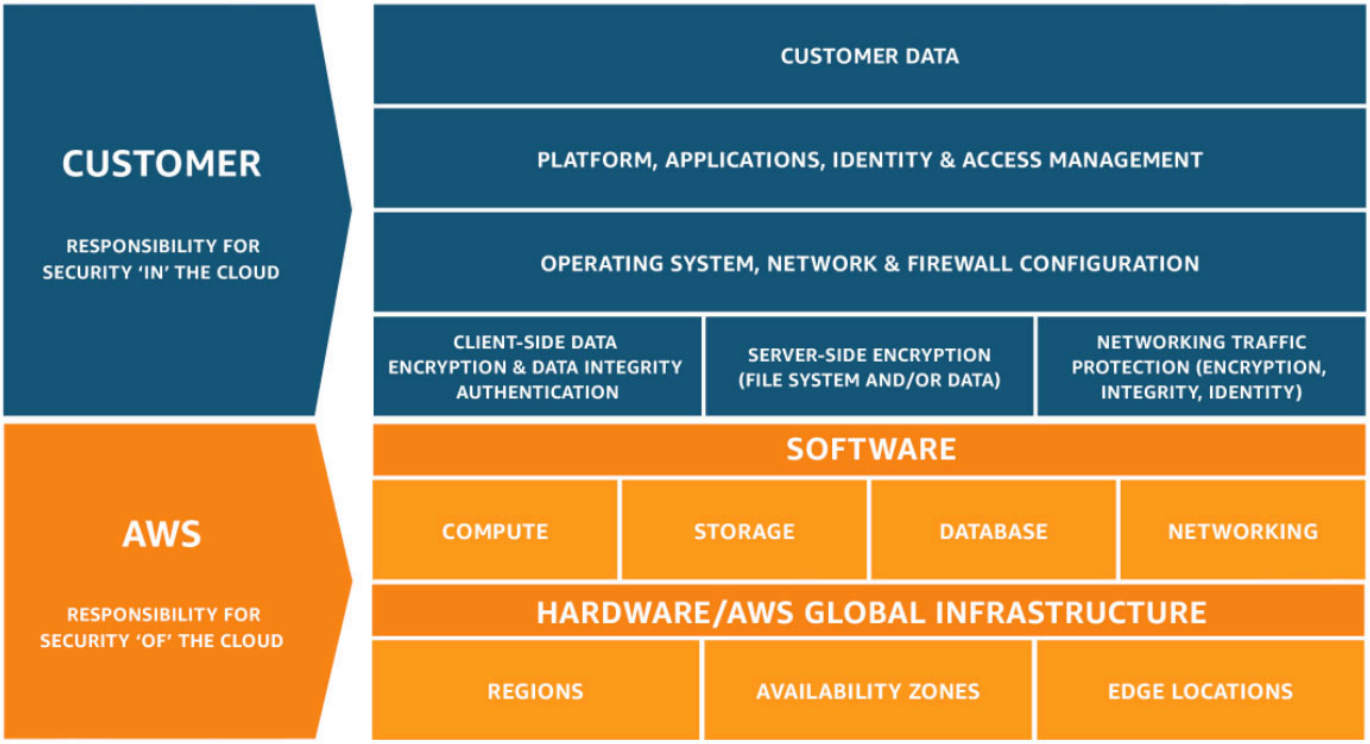

Abbildung 1: Modell der geteilten Verantwortung

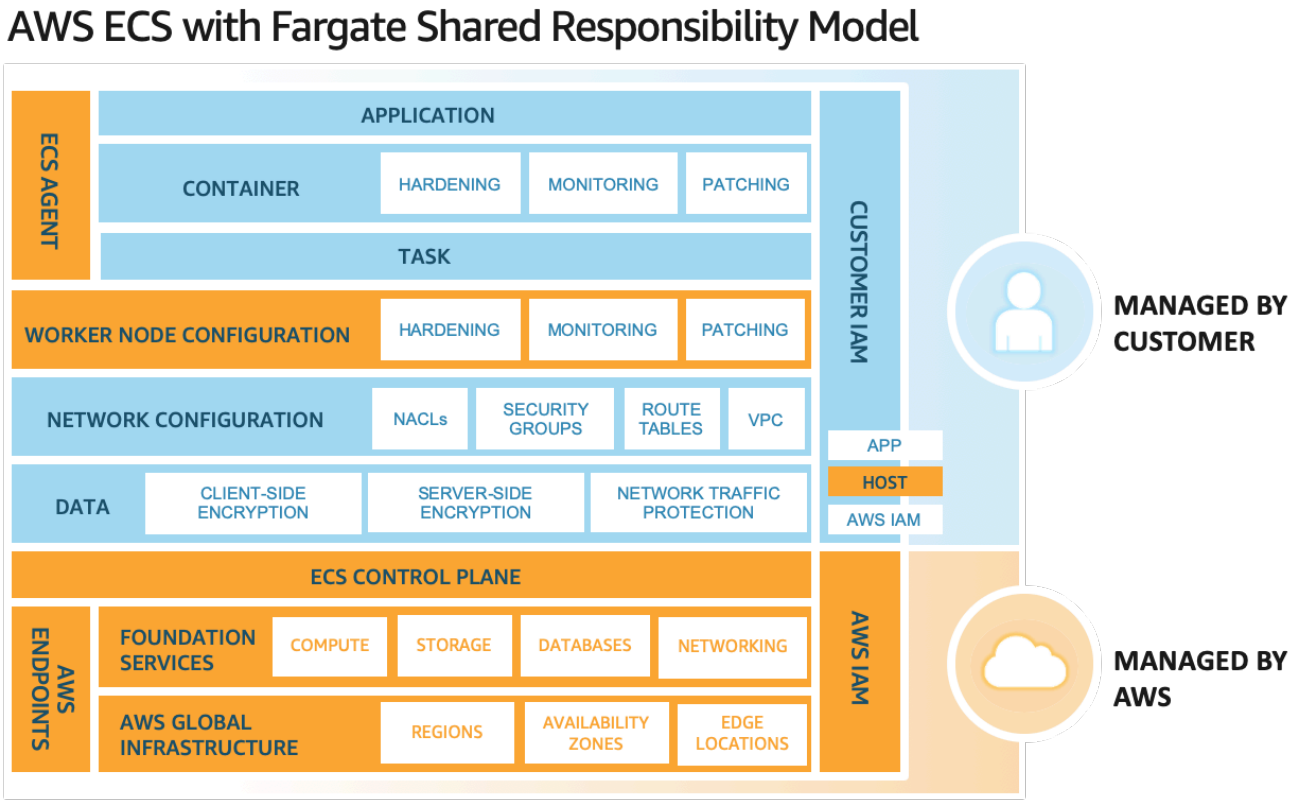

Abbildung 2: Amazon Elastic Container Service (Amazon ECS) mit AWS Fargate Modell der geteilten Verantwortung

Neben Ihrer direkten Beziehung zu AWS kann es andere Unternehmen geben, denen bei Ihrem speziellen Verantwortungsmodell Verantwortlichkeiten zukommen. Beispielsweise verfügen Sie eventuell über interne Organisationseinheiten, die die Verantwortung für einige Aspekte Ihres Betriebs übernehmen. Möglicherweise haben Sie auch Partner oder andere Dritte, die einen Teil Ihrer Cloud-Technologie entwickeln, verwalten oder betreiben.

Es ist äußerst wichtig, ein geeignetes Vorfallreaktions- und Forensik-Runbook zu erstellen, das Ihrem Betriebsmodell entspricht. Ihr Erfolg hängt von Ihrer Kenntnis der Tools ab, die Sie erstellen oder für das von Ihnen ausgewählte Betriebsmodell erwerben müssen. Je besser Ihr Unternehmen die verfügbaren Tools kennt, desto besser sind Sie darauf vorbereitet, die Anforderungen des Governance-, Risiko- und Compliance-Modells (GRC) Ihres Unternehmens zu erfüllen.

Reaktion auf einen Vorfall in der Cloud

Designziele für die Reaktion in der Cloud

Obwohl die allgemeinen Prozesse und Mechanismen zur Reaktion auf Vorfälle, wie sie im NIST SP 800 61 Computer Security Incident Handling Guide definiert sind, bestehen bleiben, empfehlen wir Ihnen, diese spezifischen Designziele zu bewerten, die für die Reaktion auf Sicherheitsvorfälle in einer Cloud-Umgebung relevant sind:

- Festlegen von Reaktionszielen: Arbeiten Sie mit Ihren Interessensvertretern, dem Rechtsbeistand und der Leitung der Organisation zusammen, um das Ziel der Reaktion auf einen Vorfall zu ermitteln. Einige gängige Ziele umfassen die Eindämmung und Behebung des Problems, die Wiederherstellung der betroffenen Ressourcen, die Aufbewahrung von Daten für die Forensik und die Zuordnung.
- Reagieren mit der Cloud: Implementieren Sie Ihre Handlungsempfehlung dort, wo das Ereignis und die Daten auftreten.
- Vorhandene und benötigte Informationen: Speichern Sie Protokolle, Snapshots und andere Beweise, indem Sie diese in ein zentralisiertes Sicherheits-Cloud-Konto kopieren. Verwenden Sie Tags, Metadaten und Mechanismen, die Aufbewahrungsrichtlinien erzwingen. Sie können beispielsweise den Linux-Befehl dd oder ein Windows-Äquivalent verwenden, um eine vollständige Kopie der Daten zu Untersuchungszwecken zu erstellen.
- Verwenden von Wiederbereitstellungsmechanismen: Wenn eine Sicherheitsanomalie auf eine falsche Konfiguration zurückzuführen ist, kann die Behebung so einfach sein wie das Entfernen der Abweichung durch die erneute Bereitstellung der Ressourcen mit der richtigen Konfiguration. Wenn möglich, sichern Sie Ihre Reaktionsmechanismen, damit sie mehr als einmal und mit einem unbekannten Status ausgeführt werden können.
- Automatisieren wo möglich: Wenn Sie feststellen, dass sich Probleme oder Vorfälle wiederholen, erstellen Sie Mechanismen, die programmgesteuert Tests durchführen und auf gängige Situationen reagieren. Reagieren Sie auf einzigartige, neue und sensible Vorfälle manuell.
- Auswahl skalierbarer Lösungen: Streben Sie nach der Skalierbarkeit des Cloud-Computing-Ansatzes Ihres Unternehmens und reduzieren Sie die Zeit zwischen Erkennung und Reaktion.
- Analysieren und Verbessern Ihres Prozesses: Wenn Sie Lücken in Ihrem Prozess, bei Ihren Tools oder Mitarbeitern identifizieren, planen Sie deren Behebung. Simulationen sind sichere Methoden, um Lücken aufzuspüren und Prozesse zu verbessern.

Die NIST-Designziele erinnern Sie daran, die Architektur auf ihre Fähigkeit zu überprüfen, sowohl auf Vorfälle zu reagieren als auch Bedrohungen zu erkennen. Berücksichtigen Sie bei der Planung Ihrer Cloud-Implementierung eine mögliche Reaktion auf einen Vorfall oder ein forensisches Ereignis. In einigen Fällen bedeutet dies, dass Sie speziell für diese Reaktionsaufgaben möglicherweise mehrere Organisationen, Konten und Tools einrichten. Diese Tools und Funktionen müssen dem Incident Responder über die Bereitstellungspipeline zur Verfügung gestellt werden und sie dürfen nicht statisch sein, da dies ein größeres Risiko darstellen würde.

Sicherheitsvorfälle in der Cloud

Themen

Domänen des Vorfalls

Es gibt drei Domänen im Verantwortungsbereich des Kunden, in denen Sicherheitsvorfälle auftreten können: Service, Infrastruktur und Anwendung. Der Unterschied zwischen den Domänen steht in Zusammenhang mit den Tools, die Sie bei Ihrer Vorfallreaktion einsetzen. Ziehen Sie die folgenden Domänen in Betracht:

- Servicedomäne: Vorfälle in der Servicedomäne betreffen das AWS-Konto eines Kunden, IAM-Berechtigungen, Ressourcen-Metadaten, Abrechnung und andere Bereiche. Auf ein Ereignis einer Servicedomäne reagieren Sie ausschließlich mit AWS-API-Mechanismen. Seine Root-Ursachen können mit Ihrer Konfiguration oder Ihren Ressourcenberechtigungen verknüpft sein und es kann möglicherweise über eine entsprechende serviceorientierte Protokollierung verfügen.
- Infrastrukturdomäne: Ereignisse in der Infrastrukturdomäne umfassen daten- oder netzwerkbezogene Aktivitäten, z. B. den Datenverkehr zu Ihren Amazon-EC2-Instances innerhalb der VPC, Prozesse und Daten auf Ihren Amazon Elastic Compute Cloud-Instances (Amazon EC2) und mehr. Ihre Reaktion auf Ereignisse in der Infrastrukturdomäne umfasst häufig das Abrufen, die Wiederherstellung oder die Erfassung von ereignisbezogenen Daten für die Forensik. Sie umfasst wahrscheinlich die Interaktion mit dem Betriebssystem einer Instance und kann in einigen Fällen auch AWS-API-Mechanismen beinhalten.
- Anwendungsdomäne: Vorfälle in der Anwendungsdomäne treten im Anwendungscode oder in der Software auf, die für die Services oder die Infrastruktur bereitgestellt wird. Diese Domäne sollte in Ihre Runbooks zur Erkennung von und Reaktion auf Cloud-Bedrohungen aufgenommen

werden und könnte ähnliche Reaktionen wie in der Infrastrukturdomäne beinhalten. Mit einer angemessenen und durchdachten Anwendungsarchitektur können Sie diese Domäne mit Cloud-Tools verwalten und dabei automatische Untersuchung, Wiederherstellung und Bereitstellung verwenden.

In diesen Domänen müssen Sie die Akteure berücksichtigen, die möglicherweise Ihr Konto, Ihre Ressourcen oder Daten angreifen. Verwenden Sie ein Risikokonzept, um die konkreten internen oder externen Risiken für Ihr Unternehmen zu ermitteln, und bereiten Sie sich entsprechend vor.

In der Servicedomäne verfolgen Sie Ihre Ziele ausschließlich mit AWS APIs. Die Behandlung eines Ereignisses, bei dem Daten aus einem Amazon S3-Bucket veröffentlicht wurden, umfasst beispielsweise API-Aufrufe zum Abrufen der Bucket-Richtlinie, die Analyse der S3-Zugriffsprotokolle und möglicherweise die Untersuchung der AWS CloudTrail-Protokolle. In diesem Beispiel werden Sie bei Ihrer Ermittlung wahrscheinlich keine Untersuchungstools oder Tools zur Netzwerkverkehrsanalyse einsetzen.

In der Infrastrukturdomäne können Sie eine Kombination aus AWS APIs und vertrauter Software für digitale Untersuchungen/Vorfallreaktion (DFIR) in dem Betriebssystem einer Workstation verwenden, z. B. eine Amazon-EC2-Instance, die Sie für die Vorfallreaktion vorbereitet haben. Ereignisse in der Infrastrukturdomäne können die Analyse von Netzwerkpaketen, Festplattenblöcken auf einem Amazon Elastic Block Store-Volume (Amazon EBS) oder flüchtigem Speicher von einer Instance erfordern.

Hinweise auf Sicherheitsereignisse in der Cloud

Es gibt viele Sicherheitsereignisse, die Sie möglicherweise nicht als Vorfälle einstufen, aber trotzdem untersucht werden sollten. Um sicherheitsrelevante Ereignisse in Ihrer AWS Cloud-Umgebung zu erkennen, können Sie folgende Mechanismen anwenden. Obwohl diese Liste nicht erschöpfend ist, sollten Sie die folgenden Beispiele für einige potenzielle Hinweise berücksichtigen:

- Protokolle und Überwachungssysteme: Überprüfen Sie AWS-Protokolle (wie Amazon CloudTrail, Amazon S3-Zugriffsprotokolle und VPC Flow Logs) und Sicherheitsüberwachungsservices (wie Amazon GuardDuty, Amazon Detective, AWS Security Hub und Amazon Macie). Verwenden Sie außerdem Überwachungssysteme wie Amazon Route 53-Zustandsprüfungen und Amazon CloudWatch-Alarme. Verwenden Sie darüber hinaus Windows Events, Linux-Syslog-Protokolle und andere anwendungsspezifische Protokolle, die Sie in Ihren Anwendungen generieren können, und melden Sie sich mit CloudWatch-Agenten bei Amazon CloudWatch an.

- Abrechnungsaktivität: Eine plötzliche Veränderung der Abrechnungsaktivität kann auf ein Sicherheitsereignis hinweisen.
- Bedrohungsinformationen: Wenn Sie einen Feed mit Bedrohungsinformationen von einem Drittanbieter abonnieren, können Sie diese Informationen mit anderen Protokollierungs- und Überwachungstools abgleichen, um potenzielle Hinweise auf Ereignisse zu erkennen.
- Partnertools: Partner im AWS-Partnernetzwerk (APN) bieten Hunderte von branchenführenden Produkten, mit denen Sie Ihre Sicherheitsziele erreichen können. Weitere Informationen finden Sie unter Sicherheits-Partnerlösungen und Sicherheitslösungen in AWS Marketplace.
- Kontakt durch AWS: AWS Support kontaktiert Sie möglicherweise, wenn wir missbräuchliche oder böswillige Aktivitäten feststellen. Weitere Informationen finden Sie im Abschnitt Reaktion von AWS auf Missbrauch und Sicherheitsverletzungen.
- Einmaliger Kontakt: Da auch Ihre Kunden, Entwickler oder andere Mitarbeiter in Ihrem Unternehmen Ungewöhnliches bemerken können, müssen Sie eine bekannte, öffentlichkeitswirksame Methode zur Kontaktaufnahme mit Ihrem Sicherheitsteam anbieten. Beliebte Optionen sind Ticketsysteme, E-Mail-Adressen und Onlineformulare zur Kontaktaufnahme. Wenn Ihre Organisation der Öffentlichkeit zugewandt ist, benötigen Sie möglicherweise auch einen öffentlich zugänglichen Mechanismus für sicherheitsrelevante Anfragen.

Eines der Tools, die AWS für die Automatisierung und Erkennung anbietet, ist AWS Security Hub. Security Hub bietet Ihnen einen umfassenden Überblick über Ihre Sicherheitswarnungen mit hoher Priorität und den Compliancestatus aller AWS-Konten an einem Ort für eine bessere Sichtbarkeit dieser Indikatoren. AWS Security Hub ist keine SIEM-Software (Security Information and Event Management) und speichert keine Protokolldaten, sondern aggregiert, organisiert und priorisiert Ihre Sicherheitswarnungen oder Ergebnisse aus mehreren AWS-Services. Mit Security Hub können Sie auch benutzerdefinierte Erkenntnisse erstellen, die aus mehreren Quellen stammen können. Dies liefert dem Security-Operations-Team bei einem Ereignis noch größeren Handlungsspielraum und Einblicke in weitere Informationen. Security Hub überwacht Ihre Umgebung kontinuierlich, indem es automatisierte Konformitätsprüfungen auf der Grundlage der bewährten Methoden von AWS und der von Ihrem Unternehmen eingehaltenen Industriestandards durchführt.

Sie können aufgrund dieser Sicherheits- und Compliance-Ergebnisse auch Maßnahmen ergreifen, indem Sie sie in Amazon Detective oder Amazon Athena untersuchen oder indem Sie Amazon CloudWatch Events oder Event Bus-Regeln anwenden, um die Ergebnisse an Ticketing-, Chat-, SIEM-, SOAR- (Security Orchestration Automation and Response) und Vorfallmanagementtools oder an benutzerdefinierte Playbooks mit Behebungsmaßnahmen zu schicken. Mit der ereignisbasierten

Automatisierung können Sie automatisch auf auftretende Vorfälle oder Ereignisse reagieren. Dieser Ansatz erhöht die Sicherheit und verbessert Ihren Umgang mit Ereignissen in der Cloud im Vergleich zu On-Premises-Umgebungen.

Cloud-Funktionen verstehen

AWS bietet eine Vielzahl von Sicherheitsfunktionen, mit denen Sie Sicherheitsereignisse in den Domänen untersuchen können. AWS bietet beispielsweise zahlreiche Protokollierungsmechanismen wie AWS CloudTrail-Protokolle, Amazon CloudWatch Logs, Amazon S3-Zugriffsprotokolle und mehr. Sie sollten die von Ihnen genutzten Services berücksichtigen und sicherstellen, dass Sie die Protokolle dieser Services aktiviert haben. AWS bietet auch eine zentrale Protokollierungslösung mit Informationen, wie Sie gängige Cloud-Protokolle zentralisieren und speichern können. Nachdem Sie diese Protokollierungsquellen aktiviert haben, müssen Sie entscheiden, wie Sie sie analysieren möchten, z. B. mit Amazon Athena, um Protokolle in Ihren Amazon S3-Buckets abzufragen.

Darüber hinaus gibt es zahlreiche APN-Partnerprodukte, die den Analyseprozess dieser Protokolle vereinfachen können, z. B. die im APN-Sicherheitskompetenzprogramm beschriebenen Produkte. Es gibt auch diverse AWS-Services, die Ihnen wertvolle Einblicke in diese Daten vermitteln, wie Amazon GuardDuty (ein Bedrohungserkennungsservice) und AWS Security Hub, die Ihnen einen umfassenden Überblick über Ihre Sicherheitswarnungen mit hoher Priorität und den Compliancestatus von AWS-Konten liefern können. Darüber hinaus sammelt Amazon Detective Protokolldaten aus Ihren AWS-Ressourcen und verwendet Machine Learning, statistische Analysen und Graphentheorie, um Sie bei der Ermittlung der Hauptursache potenzieller Sicherheitsprobleme oder verdächtiger Aktivitäten zu unterstützen. Weitere Informationen zu zusätzlichen Cloud-Funktionen, die Sie bei Ihren Untersuchungen nutzen können, finden Sie in Anhang A: Definitionen der Cloud-Funktionen.

Themen

Datenschutz

Uns ist bewusst, dass Kunden großen Wert auf ihre Privatsphäre und Datenschutz legen. Deswegen implementieren wir verantwortungsvolle und fortgeschrittene technische und physische Kontrollen, um den nicht autorisierten Zugriff auf Kundeninhalte oder deren Offenlegung zu verhindern. Unsere ständige Verpflichtung ist, das Vertrauen der Kunden aufrechtzuerhalten. Weitere Informationen zu

den Datenschutzverpflichtungen von AWS finden Sie auf unserer Seite mit Häufig gestellten Fragen zum Datenschutz.

Diese absichtlichen, selbst auferlegten Kontrollen schränken die Fähigkeit von AWS ein, die Vorfallreaktion in der Umgebung eines Kunden zu unterstützen. Aus diesem Grund müssen Sie sich unbedingt mit dem Modell der geteilten Verantwortung vertraut machen und entsprechende Fähigkeiten aufbauen, um in der AWS Cloud erfolgreich zu sein. Es ist zwar wichtig, Protokollierungs- und Überwachungsfunktionen in Ihren AWS-Konten zu aktivieren, bevor ein Vorfall eintritt, dennoch sind andere Aspekte der Vorfallreaktion ebenso unerlässlich für ein erfolgreiches Programm.

Datenschutz für Verbraucher in Kalifornien

Der California Consumer Privacy Act of 2018 (CCPA) gewährt „Verbrauchern verschiedene Rechte hinsichtlich personenbezogener Daten des Verbrauchers, die sich im Besitz eines Unternehmens befinden“, das dem CCPA unterliegt. Informationen zu den Datenschutz- und Datensicherheitsrichtlinien von AWS in Bezug auf Kunden, die dem CCPA unterliegen, finden Sie im Whitepaper Vorbereitung auf das kalifornische Datenschutzgesetz.

Die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO) ist ein europäisches Datenschutzgesetz (Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016), das am 25. Mai 2018 erlassen wurde. Die Datenschutz-Grundverordnung ersetzt die EU-Datenschutzrichtlinie (Richtlinie 95/46/EG). Ziel ist es, die Datenschutzgesetze innerhalb der Europäischen Union durch ein einziges Datenschutzgesetz zu vereinheitlichen, das für jeden Mitgliedsstaat verbindlich ist. Informationen zur Compliance von AWS mit der DSGVO finden Sie im Whitepaper Einhaltung der DSGVO in AWS.

Reaktion von AWS auf Missbrauch und Sicherheitsverletzungen

Missbrauchsaktivitäten sind beobachtete Verhaltensweisen von Instances oder anderen Ressourcen von AWS-Kunden, die böswillig, anstößig oder illegal sind oder andere Websites im Internet schädigen könnten. AWS arbeitet gemeinsam mit Ihnen daran, verdächtige und böswillige Aktivitäten auf Seiten Ihrer AWS-Ressourcen zu erkennen und zu behandeln. Unerwartete oder verdächtige Verhaltensweisen Ihrer Ressourcen können ein Hinweis darauf sein, dass die Sicherheit Ihrer AWS-Ressourcen nicht mehr gewährleistet ist, was potentielle Risiken für Ihr Unternehmen bergen kann. Denken Sie daran, dass Ihnen in Ihrem AWS-Konto alternative Kontaktmethoden zur Verfügung stehen. Befolgen Sie beim Hinzufügen von Kontakten bewährte Methoden hinsichtlich Sicherheit und

Abrechnung. Obwohl AWS zunächst die E-Mail-Adresse Ihres Root-Kontos anschreibt, teilt AWS Sicherheits- und Abrechnungsprobleme auch an sekundäre E-Mail-Adressen mit. Wenn Sie eine E-Mail-Adresse hinzufügen, die nur von einer Person überprüft wird, haben Sie Ihrem AWS-Konto einen SPOF hinzugefügt. Stellen Sie sicher, dass Sie Ihren Kontakten mindestens eine Verteilerliste hinzugefügt haben.

AWS erkennt Missbrauchsaktivitäten in Ihren Ressourcen mithilfe folgender Mechanismen:

- AWS-interne Ereignisüberwachung
- Externe Sicherheitslösungen für den AWS-Netzwerk-Adressbereich
- Missbrauchsvorwürfe im Internet gegen AWS-Ressourcen

Obwohl das Response Team von AWS gegen Missbrauch intensiv missbräuchliche oder betrügerische Aktivitäten auf AWS überwacht und beendet, bezieht sich ein Großteil der Beschwerden über Missbrauch jedoch auf Kunden, die rechtmäßig mit AWS zusammenarbeiten. Häufige Ursachen unabsichtlichen Missbrauchs sind unter anderem:

- Kompromittierte Ressource: Eine nicht gepatchte Amazon-EC2-Instance kann infiziert werden und als Botnet-Agent agieren.
- Unbeabsichtigter Missbrauch: Ein übermäßig aggressiver Webcrawler kann von einigen Internetseiten als Denial-of-Service-Angriff eingestuft werden.
- Untergeordneter Missbrauch: Ein Endbenutzer eines von einem AWS-Kunden bereitgestellten Services veröffentlicht schädliche Dateien in einem öffentlichen Amazon S3-Bucket.
- Unberechtigte Beschwerden: Manchmal melden Internetnutzer legitime Aktivitäten fälschlicherweise als Missbrauch.

AWS ist bestrebt, gemeinsam mit AWS-Kunden an der Vermeidung, Ermittlung und Minderung von Missbrauch zu arbeiten und ein erneutes Auftreten solcher Fälle in der Zukunft zu vermeiden. Wir empfehlen Ihnen, die Richtlinie zur zulässigen Nutzung von AWS zu lesen, in der die verbotene Nutzung der von Amazon Web Services und seinen verbundenen Unternehmen angebotenen Webservices beschrieben wird. Um eine zeitnahe Reaktion auf Missbrauchsbenachrichtigungen durch AWS zu unterstützen, vergewissern Sie sich, dass die Kontaktinformationen Ihres AWS-Kontos korrekt sind. Wenn Sie von AWS eine Missbrauchswarnung erhalten, sollten Ihre Sicherheitsexperten und Mitarbeiter im operativen Bereich die Angelegenheit sofort überprüfen. Verzögerungen können negative Auswirkungen auf den Ruf Ihres Unternehmens und rechtlichen Folgen für Sie und andere verlängern. Darüber hinaus können die betroffenen Missbrauchsressourcen von böswilligen

Benutzern beschädigt werden. Diese Gefährdung zu ignorieren, könnte Ihrem Unternehmen noch größeren Schaden zufügen.

Vorbereiten – Personal

Mit automatisierten Prozessen können sich Unternehmen verstärkt auf Maßnahmen konzentrieren, die die Sicherheit ihrer Cloud-Umgebungen und Anwendungen erhöhen. Die automatisierte Reaktion auf Vorfälle schafft Kapazitäten für Mitarbeiter, um Ereignisse zu korrelieren, Simulationen durchzuführen, neue Reaktionsverfahren zu entwickeln, zu forschen, neue Fähigkeiten zu entwickeln und neue Tools zu testen oder zu entwerfen. Trotz zunehmender Automatisierung haben Analysten und Responder in einer Sicherheitsorganisation noch immer alle Hände voll zu tun. Durch homogene Teams können Schwachstellen entstehen. Daher ist es wichtig, ein vielfältiges Team aufzubauen, das verschiedene Denkweisen, kulturelle Perspektiven sowie Arbeits- und Lebenserfahrung in komplexen Situationen einbringt. Bei der Planung von Veranstaltungen empfiehlt sich, auf vielfältige Teams und Reaktionspläne zu achten. Ein Team mit verschiedenen Perspektiven erkennt eher Schwachstellen, die andernfalls vielleicht nicht entdeckt worden wären, und kann Lösungen identifizieren, an die sonst möglicherweise niemand gedacht hätte.

Themen

Rollen und Zuständigkeiten definieren

Fähigkeiten und Mechanismen zur Reaktion auf Vorfälle sind besonders im Umgang mit neuen oder umfangreichen Ereignissen wichtig. Diese Ereignisse sind von den formulierten schriftlichen Standards und der Erfahrung Ihres Teams zum jeweiligen Zeitpunkt abhängig. Da wir nicht alle möglichen Ausgänge eines Ereignisses vorhersagen oder kodifizieren können, verlassen wir uns bei einfachen, sich wiederholenden Aufgaben wie das Sammeln von Instance-Speicher oder Diagnoseprotokollen auf die Automatisierung, und lassen Menschen schwierige Entscheidungen treffen. Der Umgang mit unklaren Sicherheitsvorfällen erfordert organisationsübergreifende Disziplin, entschlossenes Handeln und die Fähigkeit, Ergebnisse zu liefern. In Ihrer Organisationsstruktur sollten während eines Vorfalls mehrere Personen verantwortlich und rechenschaftspflichtig sein, konsultiert oder auf dem Laufenden gehalten werden, z. B. Vertreter der Personalabteilung (HR), Ihres Führungsteams und der Rechtsabteilung. Berücksichtigen Sie diese Rollen und Verantwortlichkeiten und überlegen Sie, ob Dritte hinzugezogen werden müssen. Beachten

Sie die lokalen Gesetze in verschiedenen Regionen, die Ihren Handlungsspielraum festlegen. Obwohl es verwaltungstechnisch aufwendig erscheinen mag, ein RACI-Diagramm (verantwortlich, rechenschaftspflichtig, konsultiert und informiert) für einen Vorfall zu erstellen, ermöglicht es eine schnelle und direkte Kommunikation und erläutert die Führung in verschiedenen Phasen des Ereignisses.

Vertrauenswürdige Partner können an der Untersuchung oder Vorfallreaktion beteiligt werden und zusätzliches Fachwissen sowie wertvolle Kontrollen einbringen. Wenn Sie diese Fähigkeiten in Ihrem eigenen Team nicht besitzen, können Sie eine externe Partei zur Unterstützung beauftragen. Wenn Sie einen externen Anbieter engagieren, stellen Sie sicher, dass er Ihre Teammitglieder schult. Wenn diese externen Parteien mit Ihren internen Entwicklern und Betreibern zusammenarbeiten, können sie die Fähigkeiten Ihrer Teammitglieder erweitern, und dieses neue Fachwissen kann Ihr IR-Programm in Zukunft bereichern.

Bei einem Vorfall ist es wichtig, die Besitzer und Entwickler der betroffenen Anwendungen und Ressourcen einzubeziehen, da sie als SME wichtige Informationen und Kontext liefern können. Üben Sie mit den Entwicklern und Anwendungsbesitzern und bauen Sie eine Beziehung zu ihnen auf, bevor Sie sich für eine Vorfallreaktion auf ihr Fachwissen verlassen. Anwendungsbesitzer oder SME müssen möglicherweise in Situationen einschreiten, in denen die Umgebung unbekannt ist, unvorhergesehene Komplexitäten vorliegen oder die Responder keinen Zugriff haben. Anwendungs-SMEs sollten sich dem IR-Team annähern und mit ihm üben.

Training anbieten

Um Abhängigkeiten zu reduzieren und die Reaktionszeit zu verkürzen, müssen Ihre Sicherheitsteams und Responder mit Cloud-Services vertraut sein und die Möglichkeit haben, Erfahrungen mit den spezifischen Cloud-Plattformen Ihres Unternehmens zu sammeln. Ein Teil dieser Trainings findet im Rahmen des Team Building und der Erstellung von Runbooks zu Beginn des Prozesses statt. Indem Sie möglichst viele Personen in den ersten Schritt der Erstellung von Runbooks einbeziehen, können Ihre internen Teams ihr Wissen erweitern. Das Training wird greifbarer, wenn die Teams beginnen, die Runbooks bei Tabletop-Übungen zu befolgen.

AWS und andere Dritte bieten auch Online-Sicherheitsworkshops (AWS Security Workshops) an, die Sie herunterladen und bearbeiten können. Ihr Unternehmen kann von zusätzlichen Trainings für Mitarbeiter profitieren, bei denen sie Programmierkenntnisse, Entwicklungsprozesse (einschließlich Versionskontrollsysteme und Bereitstellungspraktiken) und Infrastrukturautomatisierung erlernen.

AWS bietet verschiedene Trainingsoptionen und Lernpfade durch digitale Schulungen, Präsenzschulungen, APN-Partner und Zertifizierungen. Weitere Informationen finden Sie unter AWS Training und Zertifizierung.

Reaktionsmechanismen definieren

Ihr Reaktionsmechanismus ist von Ihrem Governance-, Risiko- und Compliance-Modell (GRC) abhängig. Im Idealfall wurde Ihr GRC-Modell erstellt, bevor Sie eine Vorfallreaktion planen. Wenn Sie mit Ihrem GRC-Modell noch nicht begonnen haben, ist dies ein notwendiger erster Schritt, um einen soliden Mechanismus zur Reaktion auf Vorfälle zu entwickeln. Wenn Sie gemeinsam mit anderen Teams (z. B. Ihrem Rechtsberater, Ihrer Geschäftsleitung, Stakeholdern usw.) einen Vorfallreaktionsansatz in der Cloud erwägen, müssen Sie sich Ihre Ressourcen und Bedürfnisse bewusst machen. Identifizieren Sie Stakeholder und relevante Kontakte und vergewissern Sie sich, dass Sie über entsprechenden Zugriff verfügen, um die erforderlichen Maßnahmen durchzuführen.

Zwar verfügen Sie in der Cloud dank der Service-APIs über mehr Transparenz und Funktionen, jedoch zeigt Ihnen erst Ihr GRC-Modell, wie Sie diese bei einer Vorfallreaktion nutzen können. Identifizieren Sie die AWS-Kontonummern Ihres Teams, die IP-Adressbereiche Ihrer Virtual Private Clouds (VPCs), die entsprechenden Netzwerkdiagramme, Protokolle, Datenpositionen und Datenklassifizierungen. Viele dieser technologischen Prozesse werden im Abschnitt Vorbereitung — Technologie beschrieben. Dokumentieren Sie anschließend Ihre Vorfallreaktionsverfahren, die häufig als Verfahren oder Runbooks bezeichnet werden und die Schritte zur Untersuchung und Behebung eines Vorfalls definieren.

Eine offene und anpassungsfähige Sicherheitskultur schaffen

AWS hat die Erkenntnis gewonnen, dass unsere Kunden und unsere internen Teams am erfolgreichsten sind, wenn Sicherheitsteams ihr Unternehmen und seine Entwickler unterstützen und eine Kultur fördern, in der alle Stakeholder zusammenarbeiten und eskalieren, um einen agilen, reaktionsschnellen Sicherheitsstatus aufrechtzuerhalten. Obwohl die Verbesserung der Sicherheitskultur Ihres Unternehmens nicht Gegenstand dieses Dokuments ist, können Sie relevante Informationen von nicht mit Sicherheitsaufgaben betrauten Mitarbeitern erhalten, wenn das Sicherheitsteam offen für Feedback ist. Wenn Ihr Sicherheitsteam offen und empfänglich ist und von der Führung unterstützt wird, stehen die Chancen für zusätzliche, zeitnahe Benachrichtigungen, Zusammenarbeit und Reaktionen auf Sicherheitsereignisse besser.

In einigen Organisationen müssen Mitarbeiter eventuell mit Maßregelung rechnen, wenn sie ein Sicherheitsproblem melden. Manchmal wissen sie einfach nicht, wie sie ein Problem melden

sollen. In anderen Fällen möchten sie möglicherweise keine Zeit verschwenden oder sie haben Angst, einen Sicherheitsvorfall zu melden, der sich später als unbedenklich herausstellt. Das Führungsteam muss eine Kultur der Anerkennung fördern und alle in die Sicherheit der Organisation einbinden. Stellen Sie klar, über welche Kanäle Tickets mit hohem Schweregrad eingereicht werden können, wenn der Verdacht auf ein potenzielles Risiko oder eine Bedrohung vorliegt. Begegnen Sie diesen Benachrichtigungen offen und unvoreingenommen und fordern Sie vor allem nicht mit Sicherheitsaufgaben betraute Mitarbeiter auf, derartige Benachrichtigungen zu begrüßen. Betonen Sie, dass Sie lieber massenweise über mögliche Probleme informiert werden, als überhaupt keine Benachrichtigungen zu erhalten. Für einen Entwickler ist es immer besser, eigene Fehler einzugestehen, als abzuwarten, bis Dritte in einem öffentlichen Artikel auf das Problem hinweisen.

Diese Meldungen sind eine wertvolle Gelegenheit, schnelle Untersuchungen unter Druck zu üben. Sie können als wichtige Feedback-Schleife bei der Entwicklung Ihrer Reaktionsverfahren dienen.

Reaktion vorhersagen

Da unmöglich alle potenziellen Ereignisse vorhergesagt werden können, müssen Sie sich weiterhin auf menschliche Analysen verlassen. Indem Sie sich die Zeit nehmen, Ihre Mitarbeiter sorgfältig zu schulen und Ihr Unternehmen vorzubereiten, können Sie unerwartete Situationen antizipieren. Ihre Organisation muss sich jedoch nicht im Alleingang vorbereiten. Die Zusammenarbeit mit vertrauenswürdigen Sicherheitspartnern zur Identifizierung unerwarteter Sicherheitsereignisse bietet Unternehmen zusätzliche Transparenz und Einblicke.

Partner und Reaktionsfenster

Für jedes Unternehmen sieht der Weg zur Cloud anders aus. Es gibt jedoch Muster und Praktiken, auf die andere Organisationen bereits gestoßen sind und auf die Sie ein vertrauenswürdiger Sicherheitspartner aufmerksam machen kann. Wir empfehlen, externe APN-Experten für AWS-Sicherheit zu beauftragen, die Ihnen externes Fachwissen und eine andere Perspektive bieten können, um Ihre Reaktionsfähigkeit zu verbessern. Ihre vertrauenswürdigen Sicherheitspartner können Ihnen dabei helfen, potenzielle Risiken oder Bedrohungen zu identifizieren, mit denen Sie möglicherweise nicht vertraut sind.

1955 entwarfen Joseph Luft und Harrington Ingham das Johari-Fenster, eine Übung, bei der Kategorien gewisse Eigenschaften zugeordnet werden müssen. Das Fenster wird als ein Raster dargestellt, das aus vier Quadranten besteht, ähnlich wie im folgenden Diagramm.

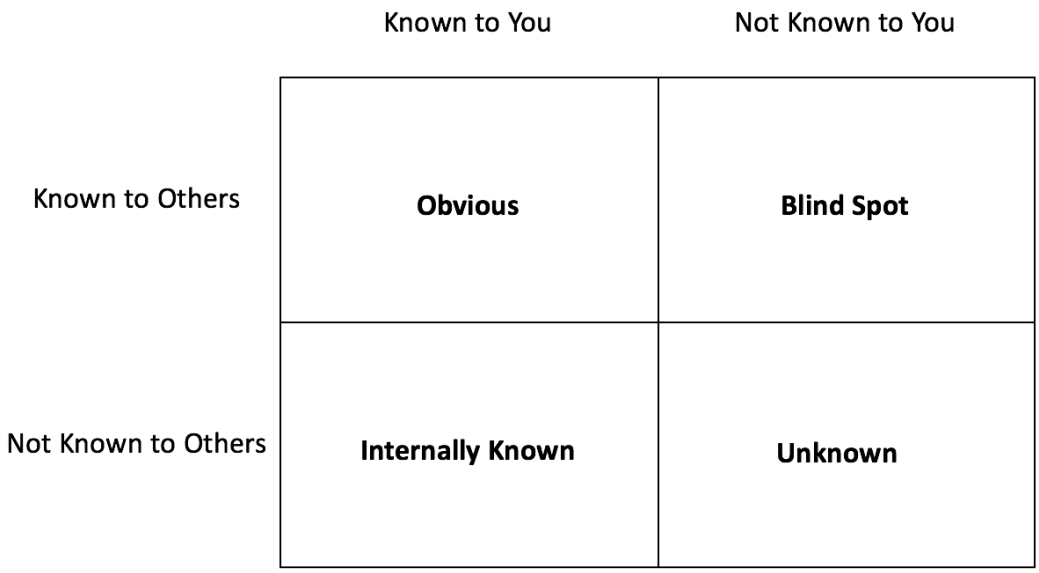

Abbildung 3: Angepasstes Johari-Fenster für Vorfallreaktionen

Obwohl das Johari-Fenster nicht mit Blick auf die Informationssicherheit entwickelt wurde, können wir das Konzept in ein einfaches mentales Modell verwandeln, das die Beurteilung der Bedrohungen einer Organisation erleichtert. Unser modifiziertes Konzept besteht aus folgenden vier Quadranten:

- Offensichtlich – Ein Risiko, das sowohl Ihr Team als auch Ihr APN-Partner kennen.
- Intern bekannt – Ein Risiko, das Ihr Team kennt, jedoch Ihrem APN-Partner unbekannt ist. Dies kann bedeuten, dass Sie über internes Fachwissen oder unternehmensspezifische Kenntnisse verfügen.
- Schwachstelle – Ein Risiko, das Ihr APN-Partner kennt, jedoch Ihrem Team unbekannt ist.
- Unbekannt – Ein Risiko, das weder Sie noch Ihr APN-Partner kennen.

Dieses zwar vereinfachte Diagramm bietet die Vorteile eines vertrauenswürdigen APN-Partners. Vor allem können Schwachstellen vorliegen, die Ihnen unbekannt sind, auf die Sie jedoch ein APN-Partner mit dem richtigen Fachwissen aufmerksam machen kann. Auch wenn Sie möglicherweise beide die Risiken im Quadranten Offensichtlich kennen, kann Ihr APN-Partner Ihnen Kontrollen und Lösungen vorschlagen, mit denen Sie noch nicht vertraut sind. Auch bei Risiken im Quadranten Intern bekannt, auf die Sie möglicherweise Ihren APN-Partner aufmerksam machen, kann er Ihnen eventuell optimierte Kontrollen zur Reduzierung dieses Risikos empfehlen. Wenden Sie sich an Ihren APN-Partner, wenn Sie Verbesserungen in Ihrem Unternehmen vornehmen möchten.

Unbekanntes Risiko

Wenn Sie sich damit befassen, Warnungen anzupassen, Ihre Verfahren der Vorfallreaktion durch Automatisierung und Ihre Sicherheitsmaßnahmen zu verbessern, fragen Sie sich möglicherweise, was Sie als Nächstes optimieren sollten. Möglicherweise würden Sie gern Ihre unbekannten Risiken kennen, wie in Abbildung 3 zur Kategorie „Unbekannt“ dargestellt. Sie können unbekannte Risiken mit folgenden Methoden reduzieren:

- Sicherheitsannahmen definieren – Welchen Fakten sind Sie sich sicher? Welche sicherheitsbezogenen Grundelemente sollten in Ihrer Umgebung unbedingt zutreffen? Indem Sie diese klar definieren, können Sie nach dem Gegenteil suchen. Dieser Schritt gestaltet sich leichter zu Beginn Ihres Wegs in die Cloud, anstatt später zu versuchen, Ihre Sicherheitsannahmen zurückzuentwickeln.
- Schulung, Kommunikation und Forschung – Schulen Sie unter Ihren Mitarbeitern Cloud-Sicherheitsexperten oder ziehen Sie externe Fachpersonen hinzu, die Sie bei der Überprüfung Ihrer Umgebung unterstützen. Stellen Sie Ihre Annahmen in Frage und achten Sie auf feinsinnige Überlegungen. Integrieren Sie Feedback-Schleifen in Ihre Prozesse und ermöglichen Sie Ihren Entwicklungsteams mit den Sicherheitsteams zu kommunizieren. Sie können auch Ihre Verfahren zur Überwachung relevanter Sicherheitsmailinglisten und Offenlegungen zur Informationssicherheit erweitern.
- Angriffsfläche reduzieren – Verbessern Sie Ihre Verteidigung, um Risiken zu vermeiden und um mehr Zeit bei unbekannten Angriffen zu haben. Legen Sie Ihren Angreifern Steine in den Weg und zwingen Sie sie, Spuren zu hinterlassen.
- Bedrohungsinformationen – Abonnieren Sie einen kontinuierlichen Feed mit aktuellen und relevanten Bedrohungen, Risiken und Indikatoren aus der ganzen Welt.
- Warnungen – Generieren Sie Benachrichtigungen, die Sie auf ungewöhnliche, schädliche oder kostspielige Aktivitäten aufmerksam machen. Sie können beispielsweise eine Benachrichtigung bei Aktivitäten erstellen, die in ungenutzten Regionen oder Services stattfinden.
- Machine Learning – Nutzen Sie Machine Learning, um für eine bestimmte Organisation oder einzelne Personen komplexe Anomalien zu identifizieren. Um ungewöhnliche Verhaltensweisen zu erkennen, können Sie auch ein Profil der normalen Eigenschaften Ihrer Netzwerke, Benutzer und Systeme erstellen.

Bedrohungsinformationen sind bei der Analyse von Schwachstellen und unbekannten Faktoren ausschlaggebend. Das Johari-Fenster veranschaulicht die Kategorisierung von bekannten und unbekannten Elementen. Bedrohungsinformationen hingegen zeigen, wie Sie noch unbekannte

Faktoren berücksichtigen können. Die Threat Intelligence ist eine Disziplin, mit der Unternehmen Bedrohungsmodelle durchschauen und Risiken identifizieren können, deren Existenz Ihrem Unternehmen möglicherweise nicht bewusst war.

Bedrohungsinformationen umfassen im Allgemeinen:

1. Identifizierung neuen Bedrohungen.
2. Definition neuer Muster.
3. Definition neuer automatisierter Erfassungstechniken.
4. Wiederholung dieser Prozesse.

Obwohl dieses Vorgehen hilfreich sein kann, kann die Aufstellung und Aufrechterhaltung eines Threat-Intelligence-Teams viele Organisationen, selbst große Unternehmen, überlasten. Letztlich läuft es darauf hinaus, ein Gleichgewicht zwischen Ihrem Bedrohungsmodell, der Größe Ihres Unternehmens und Ihrer Bedrohung zu finden. Berücksichtigen Sie folgende Fragen:

- Unterscheidet sich Ihr Bedrohungsmodell ausreichend von den Standards der Branche, in der Ihr Unternehmen tätig ist?
- Ist Ihre Risikobereitschaft so gering, dass ein solches Team benötigt wird?
- Ist es steuerlich sinnvoll, in Ihrem Unternehmen ein spezialisiertes Team zu beschäftigen?
- Ist Ihr Risikoprofil interessant genug, um entsprechende Talente für Ihr Projekt zu gewinnen?

Wenn Sie eine dieser Fragen mit Nein beantworten, sollten Sie eher einen externen Threat-Intelligence-Partner beauftragen. Dieser Service wird von vielen großen und renommierten Unternehmen preiswert angeboten.

AWS bietet Ihnen Tools und Services, mit denen Sie diese Probleme selbst handhaben können. Der Einsatz von Machine Learning zur Identifizierung schädlicher Muster ist ein gut erforschtes Studiengebiet. Muster können von Kunden, AWS Professional Services, APN-Partnern und über AWS-Services wie Amazon GuardDuty und Amazon Macie implementiert werden. Einige dieser Muster wurden bei den AWS re:Invent-Konferenzen erörtert. Weitere Informationen finden Sie in diesem Whitepaper im Abschnitt Medien.

Kunden erweitern auch ihre traditionell geschäftsorientierten Data Lakes, um ähnliche Architekturmuster bei der Entwicklung von sicherheitsbezogenen Data Lakes zu nutzen. Sicherheitsteams intensivieren auch ihre Verwendung traditioneller Protokollierungs- und

Überwachungstools wie Amazon OpenSearch Service und OpenSearch-Dashboards bis hin zu Big-Data-Architekturen.

Diese Kunden sammeln interne Daten aus AWS CloudTrail-Ereignisprotokollen, VPC-Flow-Protokollen, Amazon CloudFront-Zugriffsprotokollen, Datenbankprotokollen und Anwendungsprotokollen und kombinieren diese Daten anschließend mit öffentlichen Daten und Bedrohungsinformationen. Mit diesen wertvollen Daten haben die Sicherheitsteams von Kunden Fähigkeiten in Datenwissenschaft und Datentechnik erworben, um Tools wie Amazon EMR, Amazon Kinesis Data Analytics, Amazon Redshift, Amazon QuickSight, AWS Glue, Amazon SageMaker und Apache MXNet auf AWS zu nutzen und damit benutzerdefinierte Lösungen zur Identifizierung und Vorhersage von Anomalien zu entwickeln, die ausschließlich ihr Unternehmen betreffen.

Schließlich finden Sie unter Sicherheits-Partnerlösungen Hunderte von branchenführenden Produkten von APN-Partnern, die mit vorhandenen Kontrollen in Ihren On-Premises-Umgebungen gleichwertig, identisch oder in diese integriert sind. Diese Produkte ergänzen die vorhandenen AWS-Services, sodass Sie eine umfassende Sicherheitsarchitektur bereitstellen und eine nahtlosere Erfahrung in der Cloud und Ihren On-Premises-Umgebungen ermöglichen können.

Vorbereitung — Technologie

Themen

Zugriff auf AWS-Konten vorbereiten

Während eines Vorfalls müssen Ihre Notfallteams Zugriff auf die Umgebungen und Ressourcen haben, die an dem Vorfall beteiligt sind. Stellen Sie sicher, dass Ihre Teams über den entsprechenden Zugriff verfügen, um ihre Aufgaben auszuführen, bevor ein Ereignis eintritt. Dazu müssen Sie wissen, welche Zugriffsebene Ihre Teammitglieder benötigen (z. B. welche Aktionen sie wahrscheinlich durchführen werden). Der Zugriff muss vorher erstellt werden. Dieser Zugriff wird aus den Governance-, Risikomanagement- und Compliance-Richtlinien (GRC) Ihres Unternehmens abgeleitet. Die Authentifizierung und Autorisierung Ihrer Teammitglieder sollten lange vor dem Eintreten eines Ereignisses dokumentiert und getestet werden,damit sie rechtzeitig ohne Verzögerungen reagieren können. Um auf einen Vorfall richtig reagieren zu können, sollte ein Teil Ihrer Vorbereitung darin bestehen, zu überprüfen, wie die AWS-Konten angeordnet sind und wie die Genehmigung und Organisation von kontenübergreifenden Rollen aussieht.

In dieser Phase müssen Sie eng mit Ihren Entwicklern, Architekten, Partnern, Governance-Teams und Compliance-Teams zusammenarbeiten, um zu bestimmen, welche Zugriffsebene für die Responder erforderlich ist. Identifizieren und besprechen Sie die AWS-Kontostrategie und die Cloud-Identitätsstrategie mit den Cloud-Architekten Ihres Unternehmens, um zu verstehen, welche Authentifizierungs- und Autorisierungsmethoden konfiguriert sind, zum Beispiel:

- Verbund – Ein Benutzer übernimmt eine IAM-Rolle in einem AWS-Konto von einem Identitätsanbieter.
- Kontoübergreifender Zugriff – Ein Benutzer übernimmt eine IAM-Rolle in mehreren AWS-Konten.
- Authentifizierung – Ein Benutzer authentifiziert sich als AWS IAM-Benutzer, der in einem einzigen AWS-Konto erstellt wurde.

Diese Optionen legen die technischen Optionen für die Authentifizierung bei AWS fest und wie Sie bei einer Reaktion Zugriff erhalten können. Einige Organisationen verlassen sich jedoch

möglicherweise auf ein anderes Team oder einen anderen Partner, um seine Reaktion zu unterstützen. Benutzerkonten, die speziell für die Reaktion auf einen Sicherheitsvorfall erstellt wurden, verfügen oft über die entsprechende Privilegien, um einen ausreichenden Zugriff zu ermöglichen. Daher sollte die Verwendung dieser Benutzerkonten eingeschränkt sein und sie sollten nicht für tägliche Aktivitäten verwendet werden.

Bevor Sie neue Zugriffsmechanismen erstellen, sollten Sie mit Ihren Cloud-Teams herausfinden, wie Ihre AWS-Konten organisiert und verwaltet werden. Viele Kunden verwenden AWS Organizations, um die zentrale Verwaltung der Abrechnung zu unterstützen, Ressourcen über ihre AWS-Konten hinweg zu teilen und den Zugriff, die Compliance und die Sicherheit zu kontrollieren. Ein Kernmerkmal von Organisationen besteht darin, dass es genutzt werden kann, um Service-Kontrollrichtlinien auf Gruppen von Konten anzuwenden, um eine Richtlinienverwaltung in großem Maßstab durchzusetzen. Weitere Informationen zur allgemeinen Implementierung von Governance-Mechanismen finden Sie unter AWS-Governance nach Maß. Nachdem Sie verstanden haben, wie Ihr Unternehmen Ihre AWS-Konten organisiert und verwaltet hat, sollten Sie sich mit den folgenden allgemeinen Reaktionsmustern beschäftigen, um zu bestimmen, welche Ansätze für Ihr Unternehmen geeignet sind.

Themen

Indirekter Zugriff

Wenn Sie indirekten Zugriff verwenden, müssen Ihre Kontoinhaber oder Anwendungsteams autorisierte Abhilfemaßnahmen in ihren AWS-Konten mit taktischer Anleitung des Notfallteams durchführen, das aus Ihren Sicherheitsexperten besteht. Diese Methode zum Ausführen von Methoden ist langsamer und komplexer, kann jedoch erfolgreich sein, wenn die Responder mit dem Konto oder der Cloud-Umgebung nicht vertraut sind.

Direkter Zugriff

Um Incident Respondern direkten Zugriff zu gewähren, stellen Sie in den AWS-Konten eine AWS IAM-Rolle bereit, die Ihre Sicherheitstechniker oder Incident Responder bei einem Sicherheitsereignis

übernehmen können. Der Incident Responder authentifiziert sich entweder durch einen normalen Verbundprozess oder einen speziellen Notfallprozess, wenn Ihr normaler Authentifizierungsprozess von dem Vorfall betroffen ist. Die Berechtigungen, die Sie der IAM-Rolle für Vorfallreaktionen erteilen, sind von den Aktionen abhängig, die die Responder voraussichtlich ausführen werden.

Alternativer Zugriff

Wenn Sie glauben, dass ein Sicherheitsereignis Ihre Sicherheits-, Identitäts- oder Kommunikationssysteme beeinträchtigt, müssen Sie möglicherweise nach alternativen Mechanismen und Zugangsmethoden suchen, um die Auswirkungen zu untersuchen und zu beheben. Mit einem neuen, speziell entwickelten AWS-Konto können Ihre Responder über eine alternative, sichere Infrastruktur kooperieren und zusammenarbeiten.

Responder können beispielsweise neue Infrastrukturen nutzen, die in der Cloud eingeführt wurden, z. B. Remote-Workstations mit Amazon WorkSpaces und E-Mail-Services von Amazon WorkMail. Sie müssen den Zugriff mit geeigneten Zugriffskontrollen (mit IAM-Richtlinien) delegieren, damit Ihr sicheres, alternatives AWS-Konto Berechtigungen für das betroffene AWS-Konto übernehmen kann.

Nachdem Sie den entsprechenden Zugriff delegiert haben, können Sie die AWS APIs im betroffenen Konto verwenden, um relevante Daten wie Protokolle und Volume-Snapshots zu teilen und Untersuchungen in der isolierten Umgebung durchzuführen. Weitere Informationen zu diesem kontoübergreifenden Zugriff finden Sie im Tutorial: Zugriff auf mehreren AWS-Konten mittels IAM-Rollen übertragen.

Automatisierungszugriff

Bei der Migration zur automatisierten Reaktion auf Sicherheitsereignisse müssen Sie spezielle IAM-Rollen für Ihre Automatisierungsressourcen erstellen (z. B. Amazon-EC2-Instances oder AWS Lambda-Funktionen). Diese Ressourcen können dann die IAM-Rollen und die der Rolle zugewiesenen Berechtigungen übernehmen. Anstatt AWS-Anmeldeinformationen zu erstellen und zu verteilen, sollten Sie die Berechtigung für Ihre AWS Lambda-Funktion oder Amazon-EC2-Instance delegieren. Die AWS-Ressource erhält automatisch eine Reihe von temporären Anmeldeinformationen und verwendet sie zur Signierung von API-Anforderungen.

Sie können auch eine sichere Methode für Ihre Automatisierung oder Authentifizierungstools erwägen und sie im Betriebssystem Ihrer Amazon-EC2-Instance anwenden. Obwohl Sie diese Automatisierung mit diversen Tools durchführen können, sollten Sie den AWS Systems Manager Run Command verwenden, da Sie mit ihm Instances über einen auf Ihrem Amazon-EC2-Instance-Betriebssystem installierten Agenten remote und sicher verwalten können.

Der AWS Systems Manager Agent (SSM Agent) ist standardmäßig auf einigen Amazon EC2 Amazon Machine Images (AMIs) installiert, z. B. für Microsoft Windows Server und Amazon Linux. Möglicherweise müssen Sie den Agenten jedoch manuell auf anderen Versionen von Linux und Hybrid-Instances installieren. Unabhängig davon, ob Sie den Run Command oder ein anderes Tool verwenden, sollten Sie alle erforderlichen Einstellungen und Konfigurationen vornehmen, bevor Sie Ihre erste sicherheitsrelevante Warnung untersuchen.

Zugriff auf Managed Services

Ihr Unternehmen arbeitet möglicherweise bereits mit einem IT-Anbieter zusammen, der Ihre Services und Lösungen verwaltet. Diese Partner übernehmen geteilte Verantwortung für die Sicherheit Ihres Unternehmens und Sie sollten sich dieser Beziehung vor Eintreten einer Anomalie bewusst sein. Unabhängig davon, ob Sie bereits mit einem AWS MSP-Partner (Managed Service Provider), AWS Managed Services oder einem Managed Security Services-Partner zusammenarbeiten, müssen Sie sich bewusst werden, welche Verantwortlichkeiten jeder Partner in Bezug auf Ihre Cloud-Umgebungen hat, welche Zugriffsrechte die Anbieter bereits auf Ihre Cloud-Services haben, welche Zugriffsrechte sie benötigen und welche Anlaufstellen oder Eskalationspfade existieren, falls Sie deren Unterstützung benötigen. Schließlich sollten Sie dies mit Ihrem Partner üben, damit Ihre Reaktionspläne vorhersehbar und erfolgreich sind.

Prozesse vorbereiten

Sobald der entsprechende Zugriff bereitgestellt und getestet wurde, muss Ihr Notfallteam die zugehörigen Prozesse definieren und vorbereiten, die für die Untersuchung und Behebung des Problems erforderlich sind. Diese Phase ist aufwendig, da Sie die geeignete Reaktion auf Sicherheitsereignisse in Ihren Cloud-Umgebungen ausreichend planen müssen.

Arbeiten Sie eng mit Ihren internen Teams und Partnern der Cloud-Services zusammen, um die erforderlichen Aufgaben zu bestimmen, damit diese Prozesse möglich werden. Arbeiten Sie zusammen oder weisen Sie einander Reaktionsaufgaben zu und stellen Sie sicher, dass die erforderlichen Kontokonfigurationen vorhanden sind. Wir empfehlen, Prozesse und zwingende Konfigurationen im Voraus vorzubereiten, damit Ihr Unternehmen die folgenden Reaktionsmöglichkeiten hat.

Themen

- Daten anzeigen oder kopieren
- Amazon EBS Snapshots teilen
- Teilen von Amazon CloudWatch Logs
- Unveränderlichen Speicher verwenden
- Ressourcen in der Nähe des Ereignisses starten
- Ressourcen isolieren
- Forensische Workstations starten

Entscheidungsbäume

Manchmal können verschiedene Bedingungen unterschiedliche Aktionen oder Schritte erfordern. Beispielsweise können Sie je nach Art des AWS-Kontos (Entwicklung ggü. Produktion), der Tags der Ressourcen, des Konformitätsstatus dieser Ressourcen mit den AWS Config-Regeln oder anderer Informationen unterschiedliche Maßnahmen ergreifen.

Damit die Erstellung und Dokumentation dieser Entscheidungen einfacher fällt, empfehlen wir Ihnen, gemeinsam mit Ihren anderen Teams und Stakeholdern einen Entscheidungsbaum zu entwerfen. Ähnlich wie ein Flussdiagramm ist ein Entscheidungsbaum ein Tool, das als Hilfe bei der Entscheidungsfindung genutzt werden kann, um die optimalen Maßnahmen und Ergebnisse basierend auf potenziellen Bedingungen und Informationen, einschließlich Wahrscheinlichkeiten, zu ermitteln.

Alternative Konten verwenden

Obwohl es notwendig sein kann, auf ein Ereignis im betroffenen Konto zu reagieren, sollten auch Daten außerhalb dieses Kontos untersucht werden. Einige Kunden verfügen über Prozesse zur Erstellung separater, isolierter AWS-Kontoumgebungen mithilfe von Vorlagen, welche die bereitzustellenden Ressourcen vorkonfigurieren. Diese Vorlagen werden über einen Service wie AWS CloudFormation oder Terraform bereitgestellt. Dabei handelt es sich um eine einfache Methode, um eine Sammlung verwandter AWS-Ressourcen zu erstellen und sie auf geordnete und vorhersehbare Weise bereitzustellen.

Durch die Vorkonfiguration dieser Konten mit Vorlagen können menschliche Interaktionen in der Anfangsphase eines Vorfalls eliminiert und sichergestellt werden, dass die Umgebung und die Ressourcen auf wiederholbare und vorhersehbare Weise vorbereitet werden, was in einem Audit

überprüft werden kann. Darüber hinaus stärkt dieser Mechanismus auch die Fähigkeit, die Sicherheit und Eingrenzung von Daten in der forensischen Umgebung aufrechtzuerhalten.

Bei diesem Ansatz müssen Sie mit Ihren Cloud-Services und Architektenteams zusammenarbeiten, um einen für Untersuchungen geeigneten AWS-Kontoprozess zu ermitteln. Ihre Teams für Cloud-Services könnten beispielsweise AWS Organizations verwenden, um neue Konten zu generieren und Sie bei der Vorkonfiguration dieser Konten mit einer vorlagen- oder skriptbasierten Methode zu unterstützen.

Diese Segmentierungsmethode eignet sich am besten, wenn Sie eine größere Organisation vor einer potenziellen Bedrohung schützen müssen. Diese Segmentierung mit einem neuen und weitgehend nicht verbundenen AWS-Konto bedeutet, dass ein Benutzer aus der Organisation, der aus der Dokumentation mehrerer Konten als Sicherheitsorganisationseinheit (OU) hervorgeht, zu dem Konto wechseln, die erforderlichen forensischen Aktivitäten ausführen und das Konto als Ganzes möglicherweise an eine juristische Person übergeben kann. Diese Forensik- und Zuordnungsmethode erfordert eine umfassende Überprüfung und Planung und sollte mit den GRC-Richtlinien des Unternehmens übereinstimmen. Diese Arbeit ist zwar komplex, jedoch wesentlich einfacher vor dem Aufbau einer großen Kundenbasis.

Daten anzeigen oder kopieren

Responder benötigen Zugriff auf Protokolle oder andere Beweise zur Analyse und müssen Daten anzeigen oder kopieren können. Die Responder sollten in der IAM-Berechtigungsrichtlinie mindestens Lesezugriff haben, damit sie Nachforschungen anstellen können. Um den entsprechenden Zugriff zu ermöglichen, sollten Sie einige vorgefertigte AWS-verwaltete Richtlinien in Betracht ziehen, wie SecurityAudit oder ViewOnlyAccess.

Beispielsweise möchten Responder möglicherweise eine zeitpunktbezogene Kopie von Daten wie den AWS CloudTrail-Protokollen von einem Amazon S3-Bucket in einem Konto erstellen und in einem Amazon S3-Bucket in einem anderen Konto ablegen. Mit den Berechtigungen der verwalteten Richtlinie ReadOnlyAccess können Responder beispielsweise diese Aktionen durchführen. Informationen zur Verwendung der AWS Command Line Interface (CLI) finden Sie unter Wie werden Objekte von einem Amazon S3-Bucket in einen anderen Bucket kopiert?.

Amazon EBS Snapshots teilen

Viele Kunden verwenden Amazon EBS-Snapshots (Amazon Elastic Block Store) im Rahmen ihrer Untersuchung von Sicherheitsereignissen, die ihre Amazon-EC2-Instances betreffen. Snapshots

von Amazon EBS-Volumes sind inkrementelle Backups. Weitere Informationen zu inkrementellen Amazon EBS-Snapshots finden Sie unter Amazon EBS-Snapshots.

Um eine Untersuchung eines Amazon EBS-Volumes in einem separaten, isolierten Konto durchzuführen, müssen Sie die Berechtigungen des Snapshots ändern, um ihn mit den anderen angegebenen AWS-Konten zu teilen. Autorisierte Benutzer können Ihre freigegebenen Snapshots als Grundlage für ihre eigenen EBS-Volumes verwenden, während Ihr Original-Snapshot davon unberührt bleibt. Weitere Informationen finden Sie unter Teilen eines Amazon EBS-Snapshots.

Wenn Ihr Snapshot verschlüsselt ist, müssen Sie auch den benutzerdefinierten AWS Key Management Service (AWS KMS) Customer Managed Key (CMK) freigeben, mit dem der Snapshot verschlüsselt wird. Sie können kontoübergreifende Berechtigungen auf einen benutzerdefinierten CMK bei dessen Erstellung oder zu einem späteren Zeitpunkt anwenden. Snapshots sind auf die Region beschränkt, in der sie erstellt wurden, aber Sie können einen Snapshot mit einer anderen Region teilen, indem Sie den Snapshot in diese Region kopieren. Weitere Informationen finden Sie unter Kopieren eines Amazon EBS-Snapshots.

Teilen von Amazon CloudWatch Logs

In Amazon CloudWatch Logs aufgezeichnete Protokolle wie Amazon VPC-Flow-Protokolle können über ein CloudWatch Logs-Abonnement mit einem anderen Konto (z. B. Ihrem zentralen Sicherheitskonto) geteilt werden. Diese Protokollereignisdaten können dann von einem zentralisierten Amazon Kinesis Stream gelesen werden, und es können benutzerdefinierte Verarbeitungsvorgänge und Analysen durchgeführt werden. Die benutzerdefinierte Verarbeitung ist besonders nützlich, wenn Sie Protokolldaten aus mehreren Konten erfassen. Erstellen Sie diese Konfiguration frühzeitig auf Ihrem Weg in die Cloud, bevor ein sicherheitsrelevantes Ereignis eintritt. Weitere Informationen finden Sie unter Freigabe von kontoübergreifenden Protokolldaten mit Abonnements.

Unveränderlichen Speicher verwenden

Stellen Sie beim Kopieren von Protokollen und anderen Beweisen in ein alternatives Konto sicher, dass die replizierten Daten geschützt sind. Sie müssen nicht nur die sekundären Beweise schützen, sondern auch die Integrität der Daten an der Quelle. Diese als unveränderlicher Speicher bekannten Mechanismen schützen die Integrität Ihrer Daten, indem sie die Manipulation oder Löschung von Daten verhindern.

Mit den nativen Funktionen von Amazon S3 können Sie einen Amazon S3-Bucket konfigurieren, um die Integrität Ihrer Daten zu schützen. Mit der S3-Objektsperre können Sie für einen festen Zeitraum oder auf unbegrenzte Zeit beispielsweise verhindern, dass ein Objekt gelöscht oder überschrieben

wird. Die Verwaltung von Zugriffsberechtigungen mit S3-Bucket-Richtlinien, die Konfigurierung des S3-Versioning und die Aktivierung von MFA Delete sind weitere Möglichkeiten, um einzuschränken, wie Daten geschrieben oder gelesen werden können. Diese Art der Konfiguration eignet sich zum Speichern von Untersuchungsprotokollen und Beweisen und wird oft als Write Once, Read Many (WORM) bezeichnet. Sie können die Daten auch durch eine serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) schützen und sicherstellen, dass nur geeignete IAM-Prinzipale berechtigt sind, die Daten zu entschlüsseln.

Wenn Sie Daten nach Abschluss der Untersuchung sicher in einem Langzeitspeicher aufbewahren möchten, sollten Sie erwägen, die Daten mithilfe von Objektlebenszyklusrichtlinien von Amazon S3 zu Amazon S3 Glacier zu verschieben. Amazon S3 Glacier ist ein sicherer, dauerhafter und äußerst kostengünstiger Cloud-Speicherservice für die langfristige Sicherung und Archivierung von Daten. Amazon S3 Glacier wurde für eine Zuverlässigkeit von 99,999999999 % entwickelt und bietet umfassende Sicherheits- und Compliance-Funktionen.

Darüber hinaus können Sie die Daten in Amazon S3 Glacier mit Amazon S3 Glacier Vault Lock schützen, mit der Sie die Compliancekontrollen für einzelne Amazon S3 Glacier Vaults mit einer Vault Lock-Richtlinie einfach bereitstellen und durchsetzen können. Sie können in einer Vault Lock-Richtlinie Sicherheitskontrollen festlegen (z. B. WORM) und die Richtlinie vor zukünftigen Änderungen schützen. Nachdem Sie die Richtlinie geschützt haben, kann sie nicht mehr geändert werden. Amazon S3 Glacier erzwingt die in der Vault Lock-Richtlinie festgelegten Kontrollen, um Sie bei der Erfüllung Ihrer Compliance-Vorgaben, z. B. im Hinblick auf die Datenaufbewahrung, zu unterstützen. Sie können eine Vielzahl von Konformitätskontrollen in einer Vault Lock-Richtlinie mit der AWS Identity and Access Management-Richtliniensprache (IAM) bereitstellen.

Ressourcen in der Nähe des Ereignisses starten

Für Responder, die neu in der Cloud sind, kann es verlockend sein, Cloud-Untersuchungen an dem Ort durchzuführen, an dem sich Ihre Tools befinden. Unserer Erfahrung zufolge erzielen AWS-Kunden, die mit Cloud-Technologien auf Vorfälle reagieren, bessere Ergebnisse – Isolationen können automatisiert, Kopien leichter erstellt, Beweise früher analysiert und die Analyse kann schneller abgeschlossen werden.

Es empfiehlt sich, Untersuchungen und forensische Analysen in der Cloud durchzuführen, in der sich die Daten befinden, anstatt die Daten vor der Untersuchung an ein Rechenzentrum zu übertragen. Sie können die sicheren Computing- und Speicherfunktionen der Cloud praktisch überall auf der Welt nutzen, um sichere Reaktionsverfahren durchzuführen. Viele Kunden entscheiden sich dafür, vorab ein separates AWS-Konto für eine Untersuchung zu erstellen. In manchen Fällen können Sie Ihre

Analyse jedoch auch im selben AWS-Konto durchführen. Wenn Ihr Unternehmen voraussichtlich Aufzeichnungen zu Compliance- und rechtlichen Gründen aufbewahren wird, empfiehlt sich, separate Konten für die Langzeitspeicherung und rechtliche Aktivitäten zu führen.

Es ist ebenso ratsam, die Untersuchung in derselben AWS-Region durchzuführen, in der das Ereignis eingetreten ist, anstatt die Daten in eine andere Region zu replizieren. Wir empfehlen diese Vorgehensweise hauptsächlich aufgrund des Zeitaufwands, der durch die Übertragung der Daten zwischen Regionen entsteht. Vergewissern Sie sich in allen AWS-Regionen, in denen Sie tätig sind, dass sowohl Ihr Reaktionsverfahren als auch die Responder die einschlägigen Datenschutzgesetze einhalten. Wenn Sie Daten zwischen Regionen verschieben müssen, sollten Sie die rechtlichen Auswirkungen der Übertragung von Daten zwischen verschiedenen Gerichtsbarkeiten berücksichtigen. Allgemein hat sich die Speicherung der Daten in der nationalen Gerichtsbarkeit bewährt.

Wenn Sie glauben, dass ein Sicherheitsereignis Ihre Sicherheits-, Identitäts- oder Kommunikationssysteme beeinträchtigt, müssen Sie möglicherweise nach alternativen Mechanismen und Zugangsmethoden suchen, um die Auswirkungen zu untersuchen und zu beheben. Mit AWS können Sie schnell eine neue Infrastruktur einführen, die als eine sichere, alternative Arbeitsumgebung eingesetzt werden kann. Wenn Sie beispielsweise den potenziellen Schweregrad der Situation untersuchen, sollten Sie eventuell ein neues AWS-Konto mit den sicheren Tools erstellen, die Ihr Rechtsberater, die PR-Abteilung und Ihre Sicherheitsteams für die Kommunikation und weitere Arbeit benötigen. Services wie AWS WorkSpaces (für virtuelle Desktops), AWS WorkMail (für E-Mails) und Amazon Chime (zur Kommunikation) können Ihren Notfallteams, Führungskräften und anderen Beteiligten die nötigen Funktionen und die erforderliche Konnektivität bieten, um ein Problem zu kommunizieren, zu untersuchen und zu beheben.

Ressourcen isolieren

Im Laufe Ihrer Untersuchung müssen Sie möglicherweise Ressourcen isolieren, um auf eine sicherheitsrelevante Anomalie zu reagieren. Durch die Isolierung von Ressourcen sollen potenzielle Auswirkungen begrenzt, die weitere Ausbreitung der betroffenen Ressourcen verhindert, die unbeabsichtigte Offenlegung von Daten eingedämmt und weitere unbefugte Zugriffe vermieden werden.

Wie bei jeder Vorfallreaktion müssen eventuell geschäftliche, regulatorische, rechtliche oder andere Überlegungen angestellt werden. Geplante Maßnahmen sollten gegen erwartete und unerwartete Folgen abgewogen werden. Wenn Ihre Cloud-Teams Ressourcen-Tags verwenden, können Sie mit diesen Tags die Kritikalität der zu kontaktierenden Ressource oder des Besitzers ermitteln.

Forensische Workstations starten

Einige Ihrer Aktivitäten zur Reaktion auf Vorfälle umfassen die Analyse von Datenträgerabbildern, Dateisystemen, RAM-Abbildern oder anderen Artefakten, die an einem Vorfall beteiligt sind. Viele Kunden entwickeln eine maßgeschneiderte forensische Workstation, mit der sie Kopien aller betroffenen Datenvolumes bereitstellen können (bekannt als EBS-Snapshots). Befolgen Sie dazu die folgenden grundlegenden Schritte:

1. Wählen Sie ein Amazon Machine Image (AMI) (wie Linux oder Microsoft Windows), das als forensische Workstation verwendet werden kann.
2. Starten Sie eine Amazon-EC2-Instance über diese Basis-AMI.
3. Stärken Sie das Betriebssystem, entfernen Sie unnötige Softwarepakete und konfigurieren Sie relevante Überwachungs- und Protokollierungsmechanismen.
4. Installieren Sie Ihre bevorzugte Suite von Open Source- oder privaten Toolkits sowie jegliche Software und Pakete anderer Anbieter, die Sie benötigen.
5. Halten Sie die Amazon-EC2-Instance an und erstellen Sie ein neues AMI aus der angehaltenen Instance.
6. Führen Sie einen wöchentlichen oder monatlichen Prozess ein, um die AMI mit den neuesten Software-Patches zu aktualisieren und zu erneuern.

Nachdem das forensische System mit einem AMI bereitgestellt wurde, kann Ihr Notfallteam diese Vorlage zur Erstellung einer neuen AMI verwenden, um für jede Untersuchung eine neue forensische Workstation einzuführen. Der Prozess zur Einführung der AMI als Amazon-EC2-Instance kann vorkonfiguriert werden, um den Bereitstellungsprozess zu vereinfachen. Sie können beispielsweise eine Vorlage für die benötigten Ressourcen der forensischen Infrastruktur in einer Textdatei erstellen und sie mithilfe von AWS CloudFormation in Ihrem AWS-Konto bereitstellen.

Wenn Ihre Ressourcen mit einer Vorlage schnell bereitgestellt werden können, können Ihre erfahrenen forensischen Experten für jede Untersuchung neue forensische Workstations nutzen, anstatt die Infrastruktur wiederzuverwenden. Durch dieses Verfahren können Sie Kreuzkontamination durch andere forensische Untersuchungen ausschließen.

Instance-Typen und Standorte

Amazon EC2 bietet eine große Auswahl von Instance-Typen, die für unterschiedliche Anwendungsfälle optimiert sind. Instance-Typen unterstützen verschiedene Kombinationen

von CPU, Arbeitsspeicher, Speicher und Netzwerkkapazität. So können Sie flexibel die ideale Ressourcenzusammenstellung für Ihre Anwendungen auswählen. Viele Instance-Typen bieten mehrere Instance-Größen, sodass Sie Ihre Ressourcen den Anforderungen Ihrer Ziel-Workload entsprechend skalieren können. Befolgen Sie bezüglich Vorfallreaktions-Instances die GRC-Richtlinien Ihres Unternehmens für den Standort und die Segmentierung aus dem Netzwerk, das Produktions-Instances ausführt.

AWS Enhanced Networking verwendet Single Root I/O Virtualization (SR-IOV), um Hochleistungsnetzwerk-Funktionen in unterstützten Instance-Typen bereitzustellen. SR-IOV ist eine Methode zur Gerätevirtualisierung, die im Vergleich zu herkömmlichen virtualisierten Netzwerkschnittstellen eine höhere E/A-Leistung bei niedrigerer CPU-Auslastung bietet. Die optimierte Netzwerkleistung ermöglicht eine größere Bandbreite, mehr Pakete pro Sekunde (PPS) und konstant niedrigere Latenzzeiten zwischen Instances. Für die Nutzung von Enhanced Networking fallen keine zusätzlichen Gebühren an. Informationen über die Instance-Typen, die Netzwerkgeschwindigkeiten von 10 oder 25 Gbit/s unterstützen, und andere erweiterte Funktionen finden Sie unter Amazon-EC2-Instance-Typen.

Unterstützung des Cloud-Anbieters

Themen

- AWS Managed Services
- AWS Support
- Unterstützung der DDoS-Antwort

AWS Managed Services

AWS Managed Services (AWS) stellt die fortlaufende Verwaltung Ihrer AWS-Infrastruktur bereit, damit Sie sich auf Ihre Anwendungen konzentrieren können. Durch die Implementierung bewährter Methoden für die Verwaltung Ihrer Infrastruktur trägt AWS dazu bei, den Betriebsaufwand und das Risiko zu reduzieren. AWS automatisiert häufige Aktivitäten wie Änderungsanforderungen, Überwachung, Patch-Verwaltung, Sicherheit sowie Backup-Services und bietet während der gesamten Lebensdauer Services zum Bereitstellen, Ausführen und Unterstützen Ihrer Infrastruktur.

Als Infrastrukturbetreiber übernimmt AMS die Verantwortung für die Bereitstellung einer Reihe von Sicherheitskontrollen und stellt bei Warnungen rund um die Uhr eine erste Verteidigungslinie mithilfe eines Follow-the-Sun-Modells dar. Wenn eine Warnung ausgelöst wird, befolgt AMS eine

Reihe von automatisierten und manuellen Standard-Runbooks, um eine einheitliche Reaktion zu gewährleisten. Diese Runbooks werden AWS-Kunden während des Onboardings mitgeteilt, damit sie die Vorfallreaktion gemeinsam mit AMS entwickeln und koordinieren können. AMS animiert zur gemeinsamen Durchführung von Sicherheitssimulationen mit Kunden, um bei einem echten Vorfall angemessen vorbereitet zu sein.

AWS Support

AWS Support bietet eine Reihe von Plänen, die den Zugriff auf Tools und das Know-how für den Erfolg und den betriebsbereiten Zustand der AWS-Lösungen ermöglichen. Alle Supportpläne bieten Kundenservice rund um die Uhr und gewähren Ihnen Zugriff auf Dokumentationen, Whitepaper und Support-Foren von AWS. Wenn Sie den technischen Support und Zugriff auf zusätzliche Ressourcen benötigen, die Ihnen helfen, Ihre AWS-Umgebung zu planen, bereitzustellen und zu optimieren, können Sie einen Support-Plan auswählen, der auf Ihren AWS-Anwendungsfall zugeschnitten ist.

Betrachten Sie das Supportcenter im AWS Management Console als zentralen Ansprechpartner, um Unterstützung bei Problemen in Zusammenhang mit Ihren AWS-Ressourcen zu erhalten. Der Zugriff auf AWS Support wird von IAM gesteuert. Weitere Informationen über den Zugriff auf AWS-Supportfunktionen finden Sie unter Zugriff auf den Support.

Wenn Sie zudem einen Missbrauch von Amazon EC2 melden möchten, wenden Sie sich an das AWS-Abuse-Team.

Unterstützung der DDoS-Antwort

Bei einem DoS-Angriff (Denial of Service) ist Ihre Website oder Anwendung für Endbenutzer nicht mehr verfügbar. Angreifer bedienen sich verschiedener Techniken, die Netzwerkbandbreite oder andere Ressourcen belasten und den Zugriff durch rechtmäßige Endbenutzer unterbrechen. Im einfachsten Fall wird ein DoS-Angriff von einem einzelnen Angreifer von einer einzelnen Quelle aus gegen ein Ziel ausgeführt.

Bei einem DDoS-Angriff (Distributed Denial of Service) verwendet ein Angreifer mehrere Hosts, die durch mehrere Mithelfer gefährdet oder kontrolliert werden, um einen Angriff gegen ein Ziel durchzuführen. An dem Angriff nehmen alle Mithelfer oder gefährdeten Hosts teil, indem sie eine Unmenge an Paketen oder Anforderungen generieren, um das vorgesehene Ziel zu überlasten.

AWS bietet seinen Kunden AWS Shield. Dabei handelt es sich um einen verwalteten Service zum Schutz gegen DDoS-Angriffe, der Webanwendungen schützt, die auf AWS ausgeführt werden. AWS Shield bietet die ständige Erkennung und automatische Inline-Abhilfemaßnahmen, die Ausfallzeiten

und Latenzzeiten von Anwendungen minimieren, so dass für den Schutz gegen DDoS der AWS Support nicht erforderlich ist. Es gibt zwei Stufen von AWS Shield: Standard und Advanced.

Alle AWS-Kunden profitieren kostenfrei von den automatischen AWS Shield Standard-Schutzvorkehrungen. AWS Shield Standard schützt vor den häufigsten DDoS-Angriffen auf Netzwerk- und Transportebene, die auf Websites oder Anwendungen gerichtet sind. Wenn Sie AWS Shield Standard mit Amazon CloudFront und Amazon Route 53 verwenden, erhalten Sie einen umfassenden Verfügbarkeitsschutz vor allen bekannten Infrastruktur-Angriffen (Ebene 3 und 4).

Für einen größeren Schutz vor Angriffen auf Ihre Webanwendungen, die auf Ressourcen von Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), Amazon CloudFront und Amazon Route 53 ausgeführt werden, können Sie AWS Shield Advanced abonnieren. Darüber hinaus erhalten Sie mit AWS Shield Advanced rund um die Uhr Zugriff auf das AWS DDoS Response Team (DRT). Weitere Informationen zu AWS Shield Standard und AWS Shield Advanced erhalten Sie unter AWS Shield.

Simulieren

Themen

Sicherheitsvorfall-Reaktionssimulationen

Sicherheitsvorfall-Reaktionssimulationen (SIRS) sind interne Ereignisse mit der strukturierten Möglichkeit, Ihre Vorfallmanagementpläne und -verfahren in einem realistischen Szenario zu üben. Bei SIRS-Ereignissen geht es im Wesentlichen um die Vorbereitung und die schrittweise Verbesserung Ihrer Reaktionsfähigkeiten. Einige der Gründe, warum Kunden SIRS-Aktivitäten nützlich finden, sind:

- Bereitschaftsvalidierung.
- Vertrauensförderung durch neue Erkenntnisse aus Simulationen und Mitarbeiterschulungen.
- Einhaltung der Compliance oder vertraglicher Verpflichtungen.
- Generierung von Artefakten für die Akkreditierung.
- Agilität und schrittweise Verbesserungen durch Fokus.
- Verbesserung der Geschwindigkeit und der Tools.
- Präzision von Kommunikation und Eskalation.
- Einstellung auf seltene und unerwartete Vorfälle.

Diese Vorteile zeigen, weshalb die Teilnahme an einer SIRS-Aktivität die Effizienz des Unternehmens bei kritischen Ereignissen erhöht. Die Entwicklung einer realistischen und nützlichen SIRS-Aktivität kann schwierig sein. Obwohl das Testen Ihrer Verfahren oder der Automatisierung für bekannte Ereignisse gewisse Vorteile hat, ist es ebenso wertvoll, an kreativen SIRS-Aktivitäten teilzunehmen, um sich auf unerwartete Ereignisse vorzubereiten.

Schritte zur Simulation

Unabhängig davon, ob Sie Ihre eigene SIRS entwerfen oder einen vertrauenswürdigen Partner für die grundlegenden Aufgaben haben, durchlaufen Simulationen normalerweise diese Phasen:

1. Ein Problem identifizieren – Definieren Sie den Auslöser, der eine Reaktion hervorrufen soll.
2. Qualifizierte Sicherheitsingenieure bestimmen – Eine Simulation erfordert einen Entwickler und einen Tester.
3. Ein realistisches Modellsystem entwickeln – Die Simulation muss realistisch und angemessen sein. Wenn sie nicht realistisch ist, lehnen die Teilnehmer die Übung möglicherweise ab. Wenn sie zu reduziert ist, kann die Übung als trivial angesehen werden. Beginnen Sie mit einfachen Übungen und arbeiten Sie auf ein umfassendes Ereignis hin.
4. Elemente des Szenarios entwickeln und testen – Möglicherweise muss relevantes Simulationsmaterial erstellt werden, z. B. Protokollierungsartefakte, Benachrichtigungen und Warnungen per E-Mail sowie potenzielle Runbooks.
5. Andere Sicherheitsexperten und organisationsübergreifende Teilnehmer einladen – Laden Sie alle Personen ein, die teilnehmen und sich fortbilden sollten. Wenn Ihr allgemeiner Rechtsberater, Ihre Führungskräfte und die PR-Abteilung an der Simulation beteiligt sind, sollten Sie sie auch einladen.
6. Die Simulation durchführen – Wählen Sie aus, ob Ihre Mitarbeiter auf das SIRS-Ereignis hingewiesen werden sollen oder ob die Simulation nicht angekündigt werden soll.
7. Feiern, messen, verbessern und wiederholen – Die Simulation ist mit Stress verbunden, deswegen sollten Sie die Bemühungen Ihrer Teilnehmer fördern und feiern. Nach dem Lob können Sie Leistungen messen, verbessern und Vorgänge für die nächste Simulation wiederholen. AWS empfiehlt, diese Aktivitäten zur Gewohnheit zu machen.

> **Important**
>
> Wenn Sie eine Sicherheitsvorfall-Reaktionssimulation (SIRS) planen, lesen Sie Penetrationstests und den Abschnitt Andere simulierte Ereignisse, um aktuelle Informationen zum weiteren Vorgehen zu erhalten.

Beispiele für Simulationen

Sicherheitssimulationen müssen realistisch sein, um den erwarteten Nutzen zu liefern. Wenn Sie oder Ihre Partner an Ihren eigenen Simulationen arbeiten, sollten Sie vergangene, reale Ereignisse immer als wertvolle Quelle für potenzielle Simulationsübungen berücksichtigen. Im Folgenden finden Sie einige Beispiele, die AWS-Kunden für ihre ersten Simulationen nützlich fanden:

- Unautorisierte Änderungen an Netzwerkkonfiguration oder Ressourcen.
- Anmeldeinformationen, die durch eine Fehlkonfiguration des Entwicklers fälschlicherweise öffentlich zugänglich gemacht wurden.
- Vertrauliche Inhalte, die durch eine Fehlkonfiguration des Entwicklers fälschlicherweise öffentlich zugänglich gemacht wurden.
- Isolierung eines Webservers, der mit potenziell schädlichen IP-Adressen kommuniziert.

Neben wertvollem erfahrungsorientiertem Lernen generieren auch SIRS-Aktivitäten nützliche Informationen wie gewonnene Erkenntnisse, die Sie bei der nächsten Programmphase einsetzen können: der Iteration.

Wiederholen

Im vorherigen Abschnitt wurden einige der Vorteile von SIRS-Aktivitäten definiert. Einer der Vorteile ist die höhere Agilität durch schrittweise Verbesserungen. Simulationen sollen nützliche Ergebnisse liefern, mit denen Sie Ihre Sicherheitsreaktion verbessern können. Sie sind eine Feedback-Schleife für die Organisation, um zu sehen, was funktioniert und was nicht. Mit diesem Wissen können Sie schrittweise neue Verfahren entwerfen oder bestehende Verfahren aktualisieren, um Ihre Reaktion zu verbessern.

Themen

Runbooks

Wenn eine Sicherheitsanomalie erkannt wird, sind die Eindämmung des Ereignisses und die Wiederherstellung eines bewährten Zustands wichtige Elemente eines Reaktionsplans. Wenn die Anomalie beispielsweise aufgrund einer sicherheitsrelevanten Fehlkonfiguration auftrat, kann das Problem einfach durch Entfernen der Abweichung gelöst werden, indem die Ressourcen mit der richtigen Konfiguration erneut bereitgestellt werden. Dazu müssen Sie vorausschauend planen und Ihre eigenen Sicherheitsreaktionsverfahren definieren, die oft als Runbooks bezeichnet werden.

Ein Runbook ist die dokumentierte Version der Verfahren einer Organisation zur Durchführung einer oder mehrerer Aufgaben. Diese Dokumentation wird normalerweise entweder in einem internen digitalen System oder in Papierform gespeichert. Vielleicht verfügen Sie bereits über Runbooks zur Reaktion auf Vorfälle oder Sie müssen diese erst erstellen, um den Ansprüchen eines Sicherheitssystems zu genügen. Wenn Sie geschriebene Runbooks jedoch manuell befolgen, besteht ein höheres Fehlerrisiko. Stattdessen empfehlen wir Ihnen, alle Ihre wiederholbaren Aufgaben zu automatisieren. Die Automatisierung befreit Ihr Notfallteam von allgemeinen Aufgaben, damit es mehr Zeit für wichtige Tätigkeiten hat, z. B. Ereignisse korrelieren, bei Simulationen üben, neue Reaktionsverfahren entwickeln, Forschungsarbeiten durchführen, neue Fähigkeiten erwerben sowie neue Tools testen oder entwickeln. Bevor Sie die Aufgaben jedoch in eine programmierbare Logik zerlegen und zur Automatisierung iterieren können, müssen Sie zunächst ein Runbook schreiben.

Erstellen von Runbooks

Um Runbooks für die Cloud zu erstellen, sollten Sie sich zunächst auf die aktuell ausgegebenen Warnungen konzentrieren. Wenn eine Warnung ausgegeben wird, sollte Sie sie untersuchen. Beschreiben Sie zunächst die manuellen Prozesse, die Sie ausführen. Testen Sie anschließend die Prozesse und wiederholen Sie das „Runbook“-Muster, um die Kernlogik Ihrer Reaktion zu verbessern. Bestimmen Sie die Ausnahmen und welche alternativen Lösungen für diese Szenarien gelten. In einer Entwicklungsumgebung können Sie beispielsweise eine falsch konfigurierte Amazon EC2-Instance beenden. Wenn jedoch dasselbe Ereignis in einer Produktionsumgebung aufgetreten ist, können Sie die Instance, statt sie zu beenden, anhalten und mit den Stakeholdern sicherstellen, dass kritische Daten nicht verloren gehen und die Beendigung akzeptabel ist.

Sobald Sie die beste Lösung gefunden haben, können Sie die Logik in eine codebasierte Lösung zerlegen, die von vielen Respondern als Tool verwendet werden kann. Dadurch können die Reaktion automatisiert und Abweichungen oder Rätselraten bei der Arbeit Ihrer Responder beseitigt werden. Außerdem beschleunigt es die Reaktion auf einen Vorfall. Das nächste Ziel besteht darin, diesen Code vollständig zu automatisieren, damit er von den Warnungen oder Ereignissen anstelle eines Mitarbeiters des Notfallteams aufgerufen wird.

Erste Schritte

Wenn Sie sich nicht sicher sind, womit Sie anfangen müssen, sollten Sie mit den Warnungen beginnen, die von AWS Trusted Advisor generiert werden, den Allgemeinen bewährten Methoden für die Sicherheit des AWS Security Hub und AWS-Config-Regeln (einschließlich des AWS-Config-RegelnGithub-Repositorys). Konzentrieren Sie sich dann auf von Services generierte Ereignisse, die Systeme beschreiben, mit denen Sie sich befassen.

Amazon GuardDuty und Access Analyzer beschreiben viele der Domänen, die eine Anwendung in AWS verwenden, weshalb sie allgemein empfohlen werden. Amazon Inspector und Amazon Macie haben jedoch spezielle Anwendungen für Organisationen, die sich um ihre Daten und Endpunkte sorgen. Informationen zu den Ergebnissen von Amazon GuardDuty finden Sie im Amazon GuardDuty-Benutzerhandbuch. Die Ergebnisse des Access Analyzers finden Sie im Benutzerhandbuch des Amazon Access Analyzer. Die Ergebnisse von Macie finden Sie im Benutzerhandbuch von Amazon Macie. Die Ergebnisse von Amazon Inspector finden Sie im Benutzerhandbuch von Amazon Inspector. Mit dem Security Hub können Sie diese Ergebnisse an einem Ort vereinen und mit geringer Latenz darauf reagieren, weshalb er als zentraler Ort für die Abwehr vorgeschlagen wird.

Alle oben genannten Services senden Benachrichtigungen über Amazon CloudWatch Events, wenn sich die Ergebnisse oder Warnungen ändern, einschließlich neu generierter Warnungen und Aktualisierungen vorhandener Warnungen. Sie können die Regeln von Amazon CloudWatch Events einrichten, um AWS Lambda-Funktionen zur Ausführung einer ereignisgesteuerten Reaktion auszulösen. Die Möglichkeit, benutzerdefinierte Erkenntnisse zu gewinnen und eigene Ergebnisse aus der Anwendungsdomäne hinzuzufügen, spricht jedoch dafür, stattdessen Security Hub zu verwenden. Weitere Informationen finden Sie im Abschnitt Ereignisgesteuerte Reaktion.

Automatisierung

Automatisierung ist ein Kraftmultiplikator, d. h. die Anstrengungen Ihrer Responder werden skaliert, um sie der Geschwindigkeit des Unternehmens anzupassen. Dank des Wechsels von manuellen Prozessen zu automatisierten Prozessen können Sie mehr Zeit dafür aufwenden, die Sicherheit Ihrer AWS Cloud-Umgebung zu erhöhen.

Themen

Automatisierung der Vorfallreaktion

Zur Automatisierung von Sicherheitstechnik und Betriebsfunktionen können Sie eine umfassende Palette von APIs und Tools von AWS verwenden. Sie können Identitätsmanagement, Netzwerksicherheit, Datenschutz und Überwachungsfunktionen vollständig automatisieren. Wenn Sie die Sicherheit automatisieren, lassen Sie Ihr System eine Reaktion überwachen, prüfen und einleiten, statt nur Ihren Sicherheitsstatus zu überwachen und manuell auf Ereignisse zu reagieren.

Wenn Ihre Vorfallreaktionsteams auf Warnungen weiterhin auf die gleiche Weise reagieren, riskieren sie eine Abstumpfung der Warnung. Im Laufe der Zeit kann das Team für Warnungen desensibilisiert werden und entweder Fehler bei der Verarbeitung normaler Situationen machen oder außergewöhnliche Warnungen übersehen. Automatisierung hilft, eine Abstumpfung von Warnungen zu vermeiden, indem Funktionen verwendet werden, die sich wiederholende und gewöhnliche Warnungen verarbeiten, sodass Mitarbeiter die nötigen freien Kapazitäten haben, um sich um sensible und einzigartige Vorfälle zu kümmern.

Sie können manuelle Prozesse verbessern, indem Sie die Schritte im Prozess automatisieren. Nachdem Sie das Korrekturmuster für ein Ereignis definiert haben, können Sie dieses Muster in

umsetzbare Logik zerlegen und den Code schreiben, um die Logik auszuführen. Notfallteams können anschließend diesen Code ausführen, um das Problem zu beheben. Mit der Zeit können Sie immer mehr Schritte automatisieren und schließlich häufige Vorfälle automatisch verarbeiten.

Ihr Ziel sollte jedoch sein, die Zeit zwischen erkennenden Mechanismen und reagierenden Mechanismen weiter zu verkürzen. In der Vergangenheit konnte diese Zeitspanne Stunden, Tage oder sogar Monate betragen. Einer Umfrage zum Thema Vorfallreaktion von SANS im Jahr 2016 zufolge gaben 21 % der Befragten an, dass bei ihnen die Zeit bis zur Erkennung zwei bis sieben Tage beträgt, und nur 29 % der Befragten waren in der Lage, Vorfälle innerhalb desselben Zeitfensters zu beheben. In der Cloud können Sie diese Reaktionszeit auf Sekunden reduzieren, indem Sie ereignisgesteuerte Reaktionsfunktionen entwickeln.

Themen

Optionen zur Automatisierung der Reaktion

Sie müssen unbedingt die Unternehmensimplementierung und die Organisationsstruktur miteinander in Einklang bringen. Abbildung 4 veranschaulicht anhand eines Radardiagramms die unterschiedlichen technischen Attribute jeder automatisierten Reaktionsoption in Ihrer AWS-Implementierung. Das Diagramm zeigt die zunehmende Stärke dieses technischen Attributs für die entsprechende Automatisierungsreaktion, je weiter sich das technische Attribut von der Mitte des Diagramms entfernt. Zum Beispiel bietet AWS Lambda eine höhere Geschwindigkeit und erfordert weniger technische Fähigkeiten. AWS Fargate bietet mehr Flexibilität und erfordert weniger Wartung und technische Fähigkeiten. Tabelle 1 liefert einen Überblick über diese Automatisierungsoptionen und eine Zusammenfassung ihrer jeweiligen technischen Attribute.

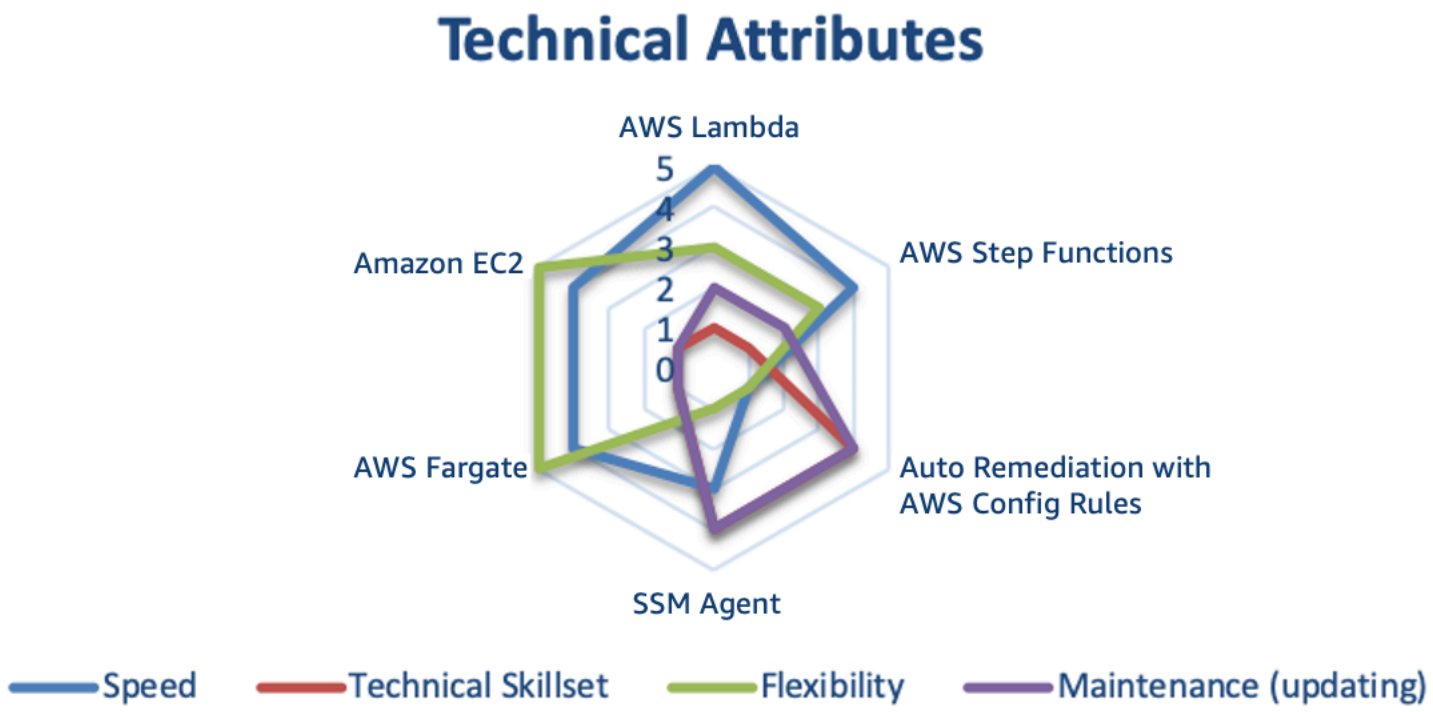

Abbildung 4: Unterschiede in den technischen Attributen von automatisierten Reaktionsansätzen

Tabelle 1: Optionen für automatisierte Reaktionsansätze

AWS-Service oder -Funktion	Beschreibung	Zusammenfassung der Attribute *
AWS Lambda	Das System verwendet nur AWS Lambda, wobei die Unternehmenssprache Ihres Unternehmens gebraucht wird.	Geschwindigkeit Flexibilität Wartung Fähigkeiten
AWS Step Functions	Das System verwendet AWS Step Functions, Lambda und SSM Agent.	Geschwindigkeit Flexibilität Wartung Fähigkeiten

AWS-Service oder -Funktion	Beschreibung	Zusammenfassung der Attribute *
Automatische Korrektur mit AWS-Config-Regeln	Eine Reihe von AWS-Config-Regeln und automatischen Korrekturen, die die Umgebung analysieren und in die genehmigte Spezifikation zurücksetzen.	Wartung und Fähigkeiten Geschwindigkeit und Flexibilität
SSM Agent	Eine Reihe von Automatisierungsregeln und -dokumenten, die viele Teile der Umgebungen und internen Systeme überprüfen und Korrekturen vornehmen.	Wartung und Fähigkeiten Geschwindigkeit Flexibilität
AWS Fargate	Das AWS Fargate-System verwendet den Open Source Step Function Code und die Ereignisse von Amazon CloudWatch. Andere Systeme übernehmen die Erkennung und Abwehr.	Flexibilität Geschwindigkeit Wartung und Fähigkeiten
Amazon EC2	Ein System, das auf einer vollständigen Instance ausgeführt wird, ähnlich der Option AWS Fargate.	Flexibilität Geschwindigkeit Wartung Fähigkeiten

* Die Attribute werden für jeden Service bzw. jede Funktion in absteigender Reihenfolge aufgeführt. Zum Beispiel bietet AWS Lambda mehr Geschwindigkeit und erfordert weniger technische Fähigkeiten. AWS Fargate bietet mehr Flexibilität und erfordert weniger Wartung und technische Fähigkeiten.

Wenn Sie diese Automatisierungsoptionen in Ihrer AWS-Umgebung in Betracht ziehen, müssen Sie auch die Zentralisierung und den Scanzeitraum (Ereignisse pro Sekunde [EPS]) berücksichtigen.

Zentralisierung bezieht sich auf ein zentrales Konto, in dem die gesamte Erkennungs- und Abwehrtätigkeit einer Organisation stattfindet. Dieser Ansatz scheint die beste sofort einsatzbereite Option zu sein und gilt als derzeit bewährte Methode. Unter bestimmten Umständen müssen Sie jedoch von diesem Ansatz abweichen. Zu wissen wann, ist davon abhängig, wie Sie mit Ihren untergeordneten Konten umgehen. Wir empfehlen, zunächst den Ansatz des Security Tooling-Kontos im Multi-Account-Framework in AWS Organizations oder AWS Control Tower anzuwenden.

Tabelle 2: Vor- und Nachteile der Zentralisierung

	Zentralisierung	Dezentralisierung
Vorteile	Einfache Konfigurationsverwaltung Reaktionen können nicht abgebrochen oder geändert werden	Einfache Architektur Schnellere Ersteinrichtung
Nachteile	Komplexere Architektur Onboarding/Offboarding von Konten und Ressourcen	Mehr zu verwaltende Ressourcen Komplizierte Aufrechterhaltung einer Software-Baseline

Ein Kostenvergleich dieser Implementierungen kann Ihrem Unternehmen helfen, sich für die beste Option zu entscheiden. Die Kosten lassen sich am besten anhand der Ereignisse pro Sekunde (EPS) abschätzen. Letztendlich kann es viel einfacher und preiswerter sein, zentralisierte oder dezentrale Ansätze zu verfolgen, aber wir können unmöglich nachvollziehen, wie Sie diese Kosten in ihrem Konto bewerten werden. Denken Sie daran, die EPS zu berücksichtigen, wenn Sie diese Ereignisse für eine Reaktion an ein zentrales Konto senden. Je mehr EPS, desto höher sind die Kosten, um diese Ereignisse an ein zentrales Konto zu senden.

Kostenvergleiche von Scanmethoden

Die Kosten werden darüber hinaus durch das Scanverfahren, mit dem eine Anomalie erkannt wird, und den Zeitrahmen zwischen den Validierungen bestimmt. Bei den Scanmethoden können Sie

zwischen der ereignisbasierten oder periodischen Überprüfung wählen. Tabelle 3 zeigt die Vor- und Nachteile beider Ansätze.

Tabelle 3: Vor- und Nachteile verschiedener Scanmethoden

	Ereignisbasiert	Periodischer Scan
Vorteile	Weniger Zeit vom Ereignis bis zur Reaktion Begrenzte Notwendigkeit, zusätzliche API-Aufrufe abzufragen	Umfassendes Bild zu einem bestimmten Zeitpunkt
Nachteile	Begrenzter Kontext zum Status der Ressource Ausgelöste Ereignisse können eine Ressource erfordern, die nicht unmittelbar verfügbar ist	Service-Limits bei großen Konten Kann aufgrund des hohen Volumens von API-Aufrufen gedrosselt werden

In einem gereiften Unternehmen ist eine Kombination beider Scanansätze in vielen Fällen wahrscheinlich die beste Wahl. AWS Security Hub und der AWS Foundational Security Best Practices-Standard bieten eine Kombination aus beiden Scanmethoden.

Abbildung 5 zeigt ein Radardiagramm mit einem Kostenvergleich von Ereignissen pro Sekunde (EPS) für jeden der Automatisierungsansätze. Zum Beispiel weisen Amazon EC2 und AWS Fargate die höchsten Kosten für 0–10 EPS auf, während mit AWS Lambda und AWS Step Functions die höchsten Kosten für die Ausführung von mehr als 76 EPS anfallen.

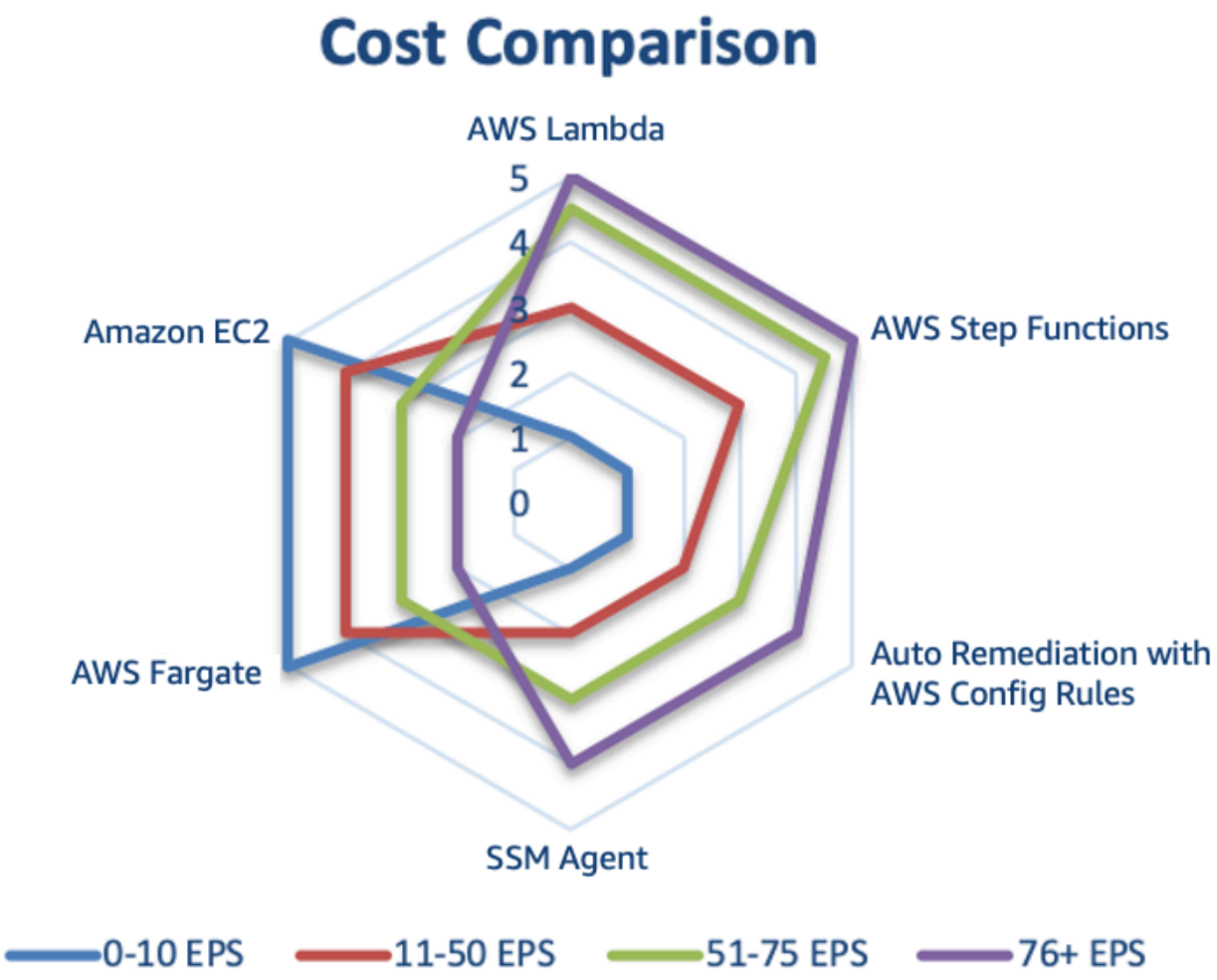

Abbildung 5: Kostenvergleich der Scanmethoden für Automatisierungsoptionen (Ereignisse pro Sekunde [EPS])

Ereignisgesteuerte Reaktion

Bei einem ereignisgesteuerten Antwortsystem löst ein Mechanismus zur Aufdeckung eine Reaktion aus, um das Ereignis automatisch zu beheben. Sie können ereignisgesteuerte Antwortfunktionen verwenden, um die Wertschöpfung zwischen Aufdeckung und Reaktion zu beschleunigen. Zur Erstellung dieser ereignisgesteuerten Architektur können Sie AWS Lambda verwenden. Dabei handelt es sich um einen serverlosen Computing-Service, der Ihren Code als Reaktion auf Ereignisse ausführt und automatisch die zugrunde liegenden Datenverarbeitungsressourcen für Sie verwaltet.

Angenommen, Sie haben ein AWS-Konto mit aktiviertem AWS CloudTrail-Service. Wenn AWS CloudTrail jemals deaktiviert wird (über die `cloudtrail:StopLogging`-API), besteht die Reaktion darin, den Service erneut zu aktivieren und zu bestimmen, welcher Benutzer die AWS

CloudTrail-Protokollierung deaktiviert hat. Anstatt diese Schritte manuell in AWS Management Console auszuführen, können Sie die Protokollierung programmgesteuert erneut aktivieren (über die `cloudtrail:StartLogging`-API). Wenn Sie dies mit Code implementieren, muss das Ziel Ihrer Reaktion sein, diese Aufgabe so schnell wie möglich auszuführen und danach die Responder darüber zu informieren.

Sie können die Logik in einfachen Code zerlegen, der in einer AWS Lambda-Funktion zur Durchführung dieser Aufgaben ausgeführt wird. Sie können dann Amazon CloudWatch Events verwenden, um das jeweilige `cloudtrail:StopLogging`-Ereignis zu überwachen, und bei Bedarf die Funktion aufrufen. Wenn diese AWS Lambda-Responderfunktion von Amazon CloudWatch Events aufgerufen wird, können Sie der Anwendung die Details des jeweiligen Ereignisses mit den Informationen des Prinzipals übermitteln, der AWS CloudTrail deaktiviert hat, wann es deaktiviert wurde, welche Ressource betroffen war sowie andere relevante Informationen. Sie können diese Informationen verwenden, um die Erkenntnisse aus Protokollen zu bereichern und dann eine Benachrichtigung oder Warnung ausschließlich mit den spezifischen Werten zu generieren, die ein Reaktionsanalyst benötigen würde.

Im Idealfall besteht das Ziel der ereignisgesteuerten Reaktion darin, dass die Lambda-Responderfunktion die Reaktionsaufgaben ausführt und dann den Responder mit allen relevanten Hintergrundinformationen darüber informiert, dass die Anomalie erfolgreich behoben wurde. Es obliegt dann dem menschlichen Responder, zu entscheiden, wie die Ursache des Ereignisses festgestellt und Wiederholungen in der Zukunft verhindert werden könnten. Diese Feedback-Schleife ermöglicht weitere Verbesserungen der Sicherheit Ihrer Cloud-Umgebungen. Um dieses Ziel zu erreichen, benötigen Sie eine Kultur, in der Ihr Sicherheitsteam eng mit Ihren Entwicklungs- und Betriebsteams zusammenarbeiten kann.

Beispiele für Vorfallreaktionen

Themen

Vorfälle der Servicedomäne

Vorfälle der Servicedomäne werden normalerweise ausschließlich mit AWS APIs gehandhabt.

Identitäten

AWS stellt APIs für unsere Cloud-Services bereit, die von Millionen von Kunden verwendet werden, um neue Anwendungen zu entwickeln und Geschäftsergebnisse zu verbessern. Diese APIs können auf verschiedene Weise aufgerufen werden, z. B. mit Software Development Kits (SDKs), die AWS CLI und AWS Management Console. Der IAM Service unterstützt Sie bei der Interaktion mit AWS über diese Methoden, indem er einen sicheren Zugriff auf AWS-Ressourcen gewährleistet. Sie können IAM verwenden, um zu kontrollieren, wer authentifiziert (angemeldet) und autorisiert (berechtigt) ist, Ressourcen auf Kontoebene zu nutzen. Unter AWS-Services, die mit IAM funktionieren finden Sie eine Liste der AWS-Services, die Sie mit IAM nutzen können.

Wenn Sie ein AWS-Konto erstellen, enthält es zunächst eine Single Sign-On-Identität (SSO), die über Vollzugriff auf sämtliche AWS-Services und -Ressourcen in dem Konto verfügt. Diese Identität wird als Root-Benutzer des AWS-Kontos bezeichnet. Um auf den Root-Benutzer zuzugreifen, müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir empfehlen dringend, den Root-Benutzer nicht für Ihre täglichen Aufgaben und insbesondere nicht für administrative Aufgaben zu verwenden. Stattdessen empfehlen wir, die bewährten Methoden zur Verwendung des Root-Benutzers ausschließlich zum Erstellen des ersten IAM-Benutzers befolgen und die Anmeldeinformationen des Root-Benutzers dann an einem sicheren Ort aufzubewahren. Der Root-Benutzer sollte nur für einige wenige Aufgaben zur Konto- und Serviceverwaltung verwendet werden. Weitere Informationen finden Sie unter Erstellen individueller IAM-Benutzer.

Diese APIs bieten Millionen von Kunden einen Mehrwert. Dennoch können einige von ihnen missbraucht werden, wenn die falschen Personen Zugriff auf Ihr IAM-Konto oder Ihre Root-Anmeldeinformationen erhalten. Sie können beispielsweise die APIs verwenden, um die

Protokollierung in Ihrem Konto zu ermöglichen, z. B. AWS CloudTrail. Wenn Angreifer jedoch in den Besitz Ihrer Anmeldeinformationen gelangen, können sie diese Protokolle auch über die API deaktivieren. Sie können diese Art von Missbrauch verhindern, indem Sie geeignete IAM-Berechtigungen nach einem Modell mit den geringsten Berechtigungen konfigurieren, und indem Sie Ihre IAM-Anmeldeinformationen angemessen schützen. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im AWS Identity and Access Management-Benutzerhandbuch. Wenn ein solches Ereignis eintritt, gibt es verschiedene Erkennungskontrollen, um festzustellen, ob Ihre AWS CloudTrail-Protokollierung deaktiviert wurde, darunter AWS CloudTrail, AWS Config, AWS Trusted Advisor, Amazon GuardDuty und AWS CloudWatch Events.

Ressourcen

Abhängig von der Organisation können auch andere Funktionen missbraucht oder falsch konfiguriert werden, je nachdem, wie jeder Kunde in der Cloud arbeitet. Einige Organisationen machen beispielsweise bestimmte Daten oder Anwendungen öffentlich zugänglich, während andere ihre Anwendungen und Daten intern und vertraulich behandeln. Nicht alle Sicherheitsereignisse sind schädlich, manche Ereignisse können auf unbeabsichtigte oder falsche Konfigurationen zurückzuführen sein. Überlegen Sie, welche APIs oder Funktionen für Ihr Unternehmen wichtig sind und ob Sie sie häufig oder eher selten verwenden.

Sie können viele sicherheitsrelevante Fehlkonfigurationen mithilfe von Tools und Services erkennen. AWS Trusted Advisor bietet beispielsweise diverse Mechanismen zur Prüfung der Befolgung von bewährten Methoden. APN-Partner bieten Hunderte von branchenführenden Produkten, die mit vorhandenen Kontrollen in Ihren On-Premises-Umgebungen gleichwertig oder identisch sind oder sich in diese integrieren lassen. Viele dieser Produkte und Lösungen wurden vom AWS-Partnerkompetenzprogramm vorqualifiziert. Wir empfehlen Ihnen, den Abschnitt Konfiguration und Schwachstellenanalyse des APN-Sicherheitskompetenzprogramms zu besuchen, um sich über diese Lösungen zu informieren und zu überlegen, ob sie Ihren Anforderungen entsprechen.

Vorfälle der Infrastrukturdomäne

Die Infrastrukturdomäne umfasst in der Regel die Daten oder netzwerkbezogenen Aktivitäten Ihrer Anwendung, z. B. den Datenverkehr zu Ihren Amazon-EC2-Instances innerhalb der VPC und die in den Betriebssystemen Ihrer Amazon-EC2-Instance ausgeführten Prozesse.

Angenommen, Ihre Überwachungslösung hat Sie über eine potenzielle Sicherheitsanomalie in Ihrer Amazon-EC2-Instance informiert. Mit folgenden Aktionen kann dieses Problem in der Regel behoben werden:

1. Erfassen Sie die Metadaten aus der Amazon-EC2-Instance, bevor Sie Änderungen an Ihrer Umgebung vornehmen.
2. Schützen Sie die Amazon-EC2-Instance vor einer versehentlichen Beendigung, indem Sie den Beendigungsschutz für die Instance aktivieren.
3. Isolieren Sie die Amazon-EC2-Instance, indem Sie die VPC-Sicherheitsgruppe wechseln. Machen Sie sich jedoch mit VPC-Verbindungsverfolgungs- und anderen Abwehrtechniken vertraut.
4. Trennen Sie die Amazon-EC2-Instance von sämtlichen AWS Auto Scaling-Gruppen.
5. Melden Sie die Amazon-EC2-Instance von verwandten Elastic Load Balancing-Services ab.
6. Erstellen Sie einen Snapshot der Amazon EBS-Daten-Volumes, die zu Archivierungszwecken und für Folgeuntersuchungen der EC2-Instance angehängt werden.
7. Markieren Sie die Amazon-EC2-Instance als zur Untersuchung unter Quarantäne gestellt, und fügen Sie alle relevanten Metadaten hinzu, z. B. das mit der Untersuchung verknüpfte Trouble-Ticket.

Sie können alle vorherigen Schritte mit den AWS-APIs, AWS SDKs, AWS CLI und AWS Management Console ausführen. Der IAM Service unterstützt bei der Interaktion mit AWS über diese Methoden, indem er einen sicheren Zugriff auf AWS-Ressourcen gewährleistet. Sie verwenden IAM, um zu kontrollieren, wer authentifiziert und autorisiert ist, Ressourcen auf Kontoebene zu nutzen. Der IAM-Service authentifiziert und autorisiert Sie, diese Aktionen vorzunehmen und mit der Servicedomäne zu interagieren.

Ein Snapshot eines Amazon EBS-Volumes ist eine zeitpunktbezogene Kopie eines EBS-Datenvolumes auf Blockebene. Sie wird asynchron erstellt und nimmt möglicherweise einige Zeit in Anspruch, stellt in Zukunft aber ein Delta-Kodierung dieser Daten dar. Sie können aus diesen Kopien neue EBS-Volumes erstellen und sie für eine gründliche Offline-Analyse durch forensische Experten in die forensische EC2-Instance mounten. Das folgende Diagramm zeigt eine vereinfachte Darstellung des Ergebnisses und beschreibt nicht alle Netzwerkkomponenten (wie Subnetze, Routing-Tabellen und Netzwerk-Zugriffskontrolllisten).

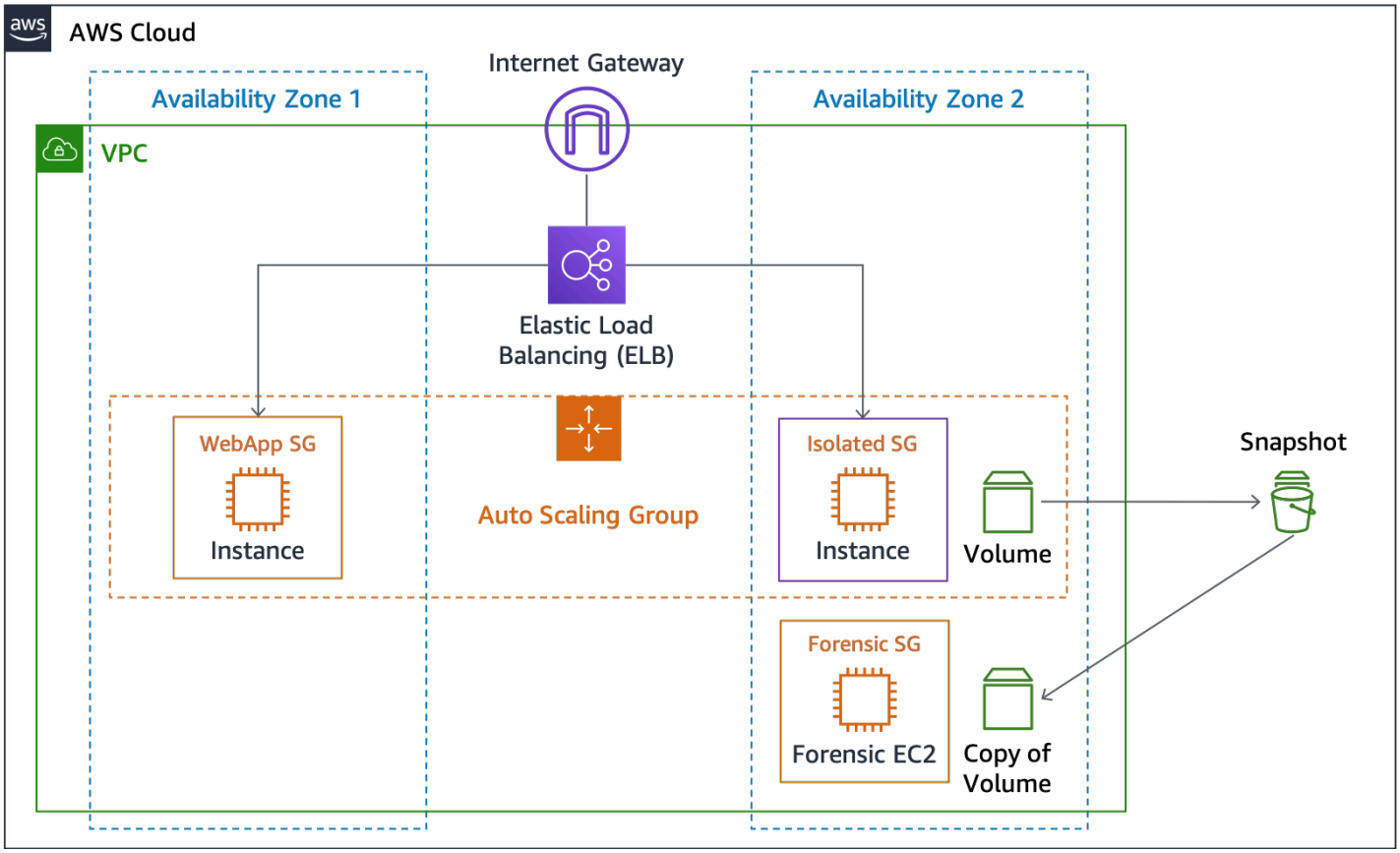

Abbildung 6: Isolierung der EC2-Instance und Snapshots

Themen

- Untersuchungsentscheidungen
- Erfassung flüchtiger Daten
- Verwenden des AWS Systems Manager
- Automatisierte Erfassung

Untersuchungsentscheidungen

An dieser Stelle können Sie zwischen einer Offline-Untersuchung (sofortiges Herunterfahren der Instance) oder einer Online-Untersuchung (Fortsetzen der Instance) wählen. Ein Vorteil der Offline-Untersuchung besteht darin, dass sich die Instance nach dem Herunterfahren nicht mehr auf die vorhandene Umgebung auswirkt. Darüber hinaus können Sie mit den EBS-Snapshots eine Kopie der betroffenen Instance erstellen und sie in einem isolierten AWS-Konto mit einer isolierten Umgebung überprüfen, die speziell für Ihre Untersuchung eingerichtet wurde. Optional können Sie die Instance

auch später herunterfahren, wenn Sie möglicherweise bei einer Online-Untersuchung flüchtige Beweise im Host-Betriebssystem wie Arbeitsspeicher oder Netzwerkverkehr erfassen können.

Erfassung flüchtiger Daten

Auch wenn Sie sich gegen eine Online-Untersuchung entscheiden, ist es wichtig, die Mechanismen zu kennen, um flüchtige Daten aus einer Instance zu erfassen. Bei einer Online-Untersuchung muss mit dem Betriebssystem interagiert werden, das auf der Amazon-EC2-Instance ausgeführt wird. In diesem Fall benötigen Sie mehr als den AWS IAM-Service, um Aufgaben auf einer Amazon-EC2-Instance auszuführen. Obwohl Sie sich mit Standardmethoden (wie Linux Secure Shell (SSH) oder Microsoft Windows Remote Desktop (RDP)) direkt beim Computer anmelden können, wird von einer manuellen Interaktion mit dem Betriebssystem abgeraten. Wir empfehlen die programmgesteuerte Verwendung eines Automatisierungstools, um Aufgaben auf einem Host auszuführen.

Verwenden des AWS Systems Manager

Der AWS Systems Manager Run Command unterstützt Sie bei der entfernten und sicheren Durchführung von On-Demand-Änderungen, indem Sie Linux-Shell-Skripts und Windows PowerShell-Befehle auf einer Ziel-Instance durchführen. Sie können „Run Command“ mit Berechtigungen im AWS IAM-Service aufrufen, allerdings müssen Sie zunächst Ihre Amazon-EC2-Instances als verwaltete Instances aktivieren, den SSM Agenten auf Ihren Maschinen installieren (falls nicht standardmäßig installiert) und die AWS IAM-Berechtigungen konfigurieren. Wenn Sie „Run Command“ für Automatisierungs- oder Vorfallreaktionszwecke verwenden möchten, müssen Sie vor einer Untersuchung zunächst die erforderlichen Aktivitäten durchführen.

AWS Systems Manager, der auch „Run Command“ beinhaltet, ist in AWS CloudTrail integriert. Dieser Service erfasst API-Aufrufe, die von oder im Auftrag eines Systems Managers getätigt wurden, und übermittelt die Protokolldateien an einen festgelegten Amazon S3-Bucket. Anhand der von AWS CloudTrail erfassten Informationen können Sie bestimmen, welche Art von Anforderung gestellt wurde, von welcher Quell-IP-Adresse und welchem Benutzer sie ausging, wann die Anforderung erstellt wurde usw. CloudTrail erstellt Protokolle aller API-Aktionen des Systems Managers, einschließlich API-Anforderungen zur Ausführung von Befehlen mit Run Command oder zur Erstellung von Systems Manager-Dokumenten.

Mit dem Run Command des AWS Systems Managers können Sie den SSM Agenten aufrufen, der Linux-Shell-Skripts und Windows PowerShell-Befehle ausführt. Diese Skripts können bestimmte Tools laden und ausführen, um zusätzliche Daten vom Host zu erfassen, z. B. das LimE-Kernelmodul (Linux Memory Extractor). Anschließend können Sie den erfassten Speicher an Ihre forensische

Amazon-EC2-Instance im VPC-Netzwerk oder an einen Amazon S3-Bucket zur dauerhaften Archivierung übertragen.

Automatisierte Erfassung

Der SSM Agent kann unter anderem mit dem Run Command über Amazon CloudWatch Events aufgerufen werden, wenn die Instance mit einem bestimmten Tag markiert ist. Wenn Sie zum Beispiel eine betroffene Instance mit dem `Response=Isolate+MemoryCapture`-Tag markieren, können Sie Amazon CloudWatch Events so konfigurieren, dass zwei Aktionen ausgelöst werden:

- Eine Lambda-Funktion, die die Isolationsaktivitäten ausführt
- Ein Run Command, der einen Shell-Befehl ausführt, um den Linux-Speicher über den SSM Agenten zu exportieren

Diese taggesteuerte Antwort ist eine weitere Methode für eine ereignisgesteuerte Reaktion.

Fazit

Während Sie Ihren Weg in die Cloud fortsetzen, sollten Sie die oben genannten grundlegenden Konzepte zur Reaktion auf Sicherheitsvorfälle in Ihrer AWS-Umgebung berücksichtigen. Sie können die verfügbaren Steuerelemente, Cloud-Funktionen und Abwehroptionen kombinieren, um die Sicherheit Ihrer Cloud-Umgebung zu verbessern. Sie können auch klein anfangen und den Vorgang wiederholen, während Sie Automatisierungsfunktionen zur Erhöhung Ihrer Reaktionsgeschwindigkeit einsetzen, damit Sie besser auf Sicherheitsereignisse vorbereitet sind.

Weitere Ressourcen

Weitere Informationen finden Sie unter:

- AWS Well-Architected
- Seite AWS Cloud Adoption Framework
- AWS Centralized Logging Solution
- Visualisierung von AWS CloudTrail-Protokollen mit AWS Glue und Amazon QuickSight
- Überwachen von Warnungen hostbasierter Eindringungserkennungssysteme auf Amazon-EC2-Instances
- Speichern und Überwachen von Anwendungs- und BS-Protokolldateien mit Amazon CloudWatch
- Identity and Access Management in Amazon S3
- Verwenden von Versioning (Amazon S3)
- Löschen mit MFA Delete
- Schutz von Daten durch serverseitige Verschlüsselung mit verwalteten AWS KMS-Schlüsseln (SSE-KMS)
- Vorfallreaktion mit AWS-Konsole und CLI
- Vorbereitung auf das kalifornische Datenschutzgesetz (California Consumer Privacy Act, CCPA)

Medien

- AWS re:Invent 2014 (SEC402): Eindringungserkennung in der Cloud
- AWS re:Invent 2014 (SEC404): Vorfallreaktion in der Cloud
- AWS re:Invent 2015 (SEC308): Umgang mit Sicherheitsereignissen in der Cloud
- AWS re:Invent 2015 (SEC316): Verbessern Sie Ihre Architektur mit Simulationen von Reaktionen auf Sicherheitsvorfälle
- AWS re:Invent 2016: Automatisierung der Reaktion auf Sicherheitsereignisse, von der Idee über die Programmierung bis zur Ausführung (SEC313)
- AWS re:Invent 2017 (SID302): Stärken Sie Ihr Sicherheitsteam durch Automatisierung und mit Alexa
- AWS re:Invent 2016 (SAC316): Sicherheitsautomatisierung: Schnellere Sicherung Ihrer Anwendungen

- AWS re:Invent 2016 (SAC304): Vorausschauende Sicherheit: Big Data zur Stärkung Ihrer Schutzmaßnahmen
- AWS re:Invent 2017 (SID325): Amazon Macie: Datentransparenz durch Maschine Learning für Sicherheits- und Compliance-Workloads
- AWS London Summit 2018: Automatisierte Vorfallreaktion und Forensik in AWS

Tools von Drittanbietern

Die folgenden Links zu Tools von Drittanbietern sind externe Links und werden von AWS nicht unterstützt. AWS erteilt keinerlei Garantien oder Zusicherungen bzgl. dieser Tools oder Seiten.

- AWS_IR – Unter Python installierbares Befehlszeilen-Dienstprogramm zur Abwehr von Sicherheitsverletzungen von Hosts und anderen wichtigen Systemen.
- MargaritaShotgun – Tool zur Remote-Speichererfassung.
- ThreatPrep – Python-Modul zur Bewertung von bewährten Methoden für AWS-Konten bzgl. der Bereitschaft für den Umgang mit Vorfällen
- ThreatResponse Web – Webbasierte Analyseplattform zur Verwendung mit dem Befehlszeilen-Tool AWS_IR.
- GRR Rapid Response – Remote-Live-Forensik zur Reaktion auf Vorfälle.
- Linux-Schreibblocker – Kernel-Patch und Userspace-Tools zum Blockieren des Schreibens von Linux-Software.

Branchen-Referenzen

- NIST SP 800-61R2: Leitfaden zum Umgang mit Computersicherheitsvorfällen

Dokumentversionen

Abonnieren Sie den RSS-Feed, um über Aktualisierungen des Whitepapers benachrichtigt zu werden.

Update-Historie-Änderung	Update-Historie-Beschreibung	Update-Historie-Datum
Geringfügige Aktualisierungen	Bugfixes und zahlreiche geringfügige Änderungen des gesamten Systems.	2. Juni 2021
Geringfügige Aktualisierung	Defekte Links wurden korrigiert.	5. März 2021
Whitepaper aktualisiert	Defekte Links wurden korrigiert und zahlreiche Textänderungen vorgenommen, um die Lesbarkeit zu verbessern.	23. November 2020
Geringfügige Aktualisierung	Link zu „Vorfallreaktion mit AWS-Konsole und CLI“ korrigiert	30. Juni 2020
Whitepaper aktualisiert	Aktualisierung zur Integration neuer Sicherheitsservices, Bedrohungsinformationen, geteilter Verantwortung für Container, Automatisierung und CCPA. Anhänge mit Beispielentscheidungsbaum und Runbook hinzugefügt.	11. Juni 2020
Erste Veröffentlichung	Erstveröffentlichung des Whitepapers	1. Juni 2019

Anhang A: Definitionen der Cloud-Funktionen

AWS bietet über 150 Cloud-Services und Tausende von Funktionen. Viele bieten native Erkennungs-, Präventions- und Reaktionsfunktionen, andere können hingegen zur Entwicklung kundenspezifischer Sicherheitslösungen verwendet werden. In diesem Abschnitt werden einige dieser Services beschrieben, die für die Reaktion auf Vorfälle in der Cloud besonders wichtig sind.

Themen

Protokollierung und Ereignisse

AWS CloudTrail – Mit dem Service AWS CloudTrail können Sie Governance-, Compliance-, Betriebs- und Risikoprüfungen für Ihr AWS-Konto durchführen. Mit CloudTrail können Sie Kontoaktivitäten in Ihrer AWS-Infrastruktur protokollieren, fortlaufend überwachen und speichern. CloudTrail bietet einen Ereignisverlauf Ihrer AWS-Kontoaktivität. Dieser umfasst auch über die AWS Management Console, AWS SDKs, Befehlszeilen-Tools und andere AWS-Services ausgeführte Aktionen. Der Ereignisverlauf vereinfacht Sicherheitsanalysen, das Nachverfolgen von Ressourcenänderungen sowie die Problembehebung.

Validierte Protokolldateien sind bei Sicherheits- und kriminaltechnischen Ermittlungen unersetzlich. Wenn Sie feststellen möchten, ob eine Protokolldatei geändert, gelöscht oder nicht verändert wurde, nachdem sie von CloudTrail übermittelt wurde, verwenden Sie die Integritätsvalidierung für CloudTrail-Protokolldateien. Diese Funktion wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hash-Funktion und SHA-256 mit RSA für digitale Signaturen. Dadurch ist es computertechnisch nicht möglich, CloudTrail-Protokolldateien unerkannt zu ändern, zu löschen oder zu fälschen.

Die von CloudTrail an Ihren Bucket gelieferten Protokolldateien werden standardmäßig mit der serverseitigen Amazon-Verschlüsselung verschlüsselt. Optional können Sie die AWS Key Management Service (AWS KMS) verwalteten Schlüssel (SSE-KMS) für Ihre CloudTrail-Protokolldateien verwenden.

Amazon CloudWatch Events – Amazon CloudWatch Events liefert einen Stream von Systemereignissen in nahezu Echtzeit, der Änderungen an AWS-Ressourcen beschreibt oder wenn API-Aufrufe von AWS CloudTrail veröffentlicht werden. Mit einfachen Regeln, die sich schnell einrichten lassen, können Sie Ereignisse ordnen und sie zu einer oder mehreren Zielfunktionen oder Streams umleiten. CloudWatch Events erkennt betriebsbezogene Veränderungen, sobald diese auftreten. CloudWatch Events kann auf diese betriebsbezogenen Veränderungen reagieren und bei Bedarf Korrekturmaßnahmen durchführen, indem es Nachrichten an die Umgebung versendet, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst. Einige Sicherheitsdienste wie Amazon GuardDuty erzeugen eine Ausgabe in Form von CloudWatch Events.

AWS Config – Mit dem ServiceAWS Config können Sie die Konfigurationen Ihrer AWS-Ressourcen beurteilen, prüfen und evaluieren. Config überwacht kontinuierlich die Konfigurationen Ihrer AWS-Ressourcen und zeichnet diese auf. Sie erhalten die Möglichkeit, die Beurteilung der aufgezeichneten Konfigurationen im Hinblick auf gewünschte Konfigurationen zu automatisieren. Mit Config können Sie Änderungen an Konfigurationen und Beziehungen zwischen AWS-Ressourcen manuell oder automatisch überprüfen. Sie können detaillierte Ressourcenkonfigurationshistorien und Ihre allgemeine Compliance mit den in Ihren internen Richtlinien angegebenen Konfigurationen überprüfen. Dies ermöglicht Ihnen, Compliance-Prüfungen, Sicherheitsanalysen, das Änderungsmanagement sowie die betriebliche Fehlerbehebung zu vereinfachen.

Amazon S3-Zugriffsprotokolle – Wenn Sie vertrauliche Informationen in einem Amazon S3-Bucket speichern, können Sie S3-Zugriffsprotokolle aktivieren, um alle Uploads, Downloads und Änderungen dieser Daten aufzuzeichnen. Dieses Protokoll wird getrennt von und zusätzlich zu den CloudTrail-Protokollen erstellt, die Änderungen am Bucket selbst aufzeichnen (z. B. Änderungen der Zugriffsrichtlinien und Lebenszyklusrichtlinien).

Amazon CloudWatch Logs – Sie können Amazon CloudWatch Logs verwenden, um Ihre Protokolldateien (wie Ihr Betriebssystem, Ihre Anwendung und benutzerdefinierte Protokolldateien) über Ihre Amazon Elastic Compute Cloud-Instances (Amazon EC2) mithilfe des CloudWatch Logs-Agenten zu überwachen, zu speichern und darauf zuzugreifen. Darüber hinaus kann Amazon CloudWatch Logs Protokolle von AWS CloudTrail, Amazon Route 53 DNS-Abfragen, VPC-Flow-Protokolle, Lambda-Funktionen und andere Quellen erfassen. Anschließend können Sie die zugehörigen Protokolldaten aus CloudWatch Logs abrufen.

Amazon VPC Flow Logs – Mit VPC Flow Logs können Sie Informationen über den IP-Datenverkehr erfassen, der über die Netzwerkschnittstellen in Ihrer VPC ein- und ausgeht. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die darin enthaltenen Daten in Amazon CloudWatch Logs anzeigen und abrufen. Mit VPC Flow Logs können Sie diverse Aufgaben ausführen.

Sie können beispielsweise Flow-Protokolle verwenden, um das Problem zu lösen, aus dem bestimmter Datenverkehr eine Instance nicht erreicht, wodurch Sie übermäßig restriktive Sicherheitsgruppenregeln erkennen können. Außerdem lassen sich Flow-Protokolle als Sicherheitstool zur Überwachung des Datenverkehrs zu Ihrer Instance einsetzen.

AWS WAF-Protokolle – AWS WAF unterstützt jetzt die vollständige Protokollierung aller Webanfragen, die vom Service geprüft werden. Diese Protokolle können zu Compliance- und Prüfungszwecken in Amazon S3 gespeichert und zu Debugging- und zusätzlichen Forensik-Zwecken verwendet werden. Die Protokolle vermitteln Ihnen ein besseres Verständnis dafür, weshalb bestimmte Regeln ausgelöst und bestimmte Webanfragen blockiert werden. Sie können die Protokolle auch in Ihr SIEM- und Ihre Protokollanalysetools integrieren.

Andere AWS-Protokolle – Dank unserer Innovationsgeschwindigkeit stellen wir unseren Kunden praktisch jeden Tag neue Funktionen und Funktionen zur Verfügung, d. h. es gibt Dutzende von AWS-Services, die Protokollierungs- und Überwachungsfunktionen bieten. Informationen zu den Funktionen der einzelnen AWS-Services finden Sie in der AWS-Dokumentation zu diesem Service.

Sichtbarkeit und Warnfunktion

AWS Security Hub – AWS Security Hub gibt Ihnen einen umfassenden Überblick über die Sicherheitswarnungen mit hoher Priorität und den Konformitätsstatus für alle AWS-Konten. Mit Security Hub können Sie Ihre Sicherheitsmeldungen und Ergebnisse aus mehreren AWS-Services wie Amazon GuardDuty, Amazon Inspector und Amazon Macie sowie von AWS-Partner-Lösungen an einem zentralen Ort aggregieren, organisieren und priorisieren. Ihre Ergebnisse werden visuell auf integrierten Dashboards mit aussagekräftigen Grafiken und Tabellen zusammengefasst. Sie können Ihre Umgebung auch kontinuierlich überwachen, indem Sie automatisierte Compliance-Prüfungen auf der Grundlage der bewährten Methoden von AWS und der Industriestandards, die Ihr Unternehmen einhält, durchführen.

Amazon GuardDuty – Amazon GuardDuty ist ein verwalteter Service zur Bedrohungserkennung, der Ihre AWS-Konten und -Workloads zu deren Schutz fortlaufend auf böswillige oder unbefugte Verhaltensweisen überwacht. Der Service überwacht Ihre Konten und Instances auf Aktivitäten wie ungewöhnliche API-Aufrufe oder potenziell unbefugte Bereitstellungen, die auf eine mögliche Sicherheitsverletzung hindeuten. GuardDuty erkennt außerdem Instances mit potenziellen Sicherheitsverletzungen oder Informationsbeschaffungsaktivitäten durch Angreifer.

GuardDuty erkennt verdächtige Angreifer mithilfe integrierter Feeds mit Bedrohungsinformationen und nutzt Machine Learning zur Erkennung von Anomalien bei Konto- und Workload-Aktivitäten. Wenn der Service eine potenzielle Bedrohung erkennt, wird eine ausführliche Sicherheitswarnung in

der GuardDuty-Konsole und in AWS CloudWatch Events bereitgestellt. Auf diese Weise können Sie sofort Maßnahmen ergreifen und die Warnungen mühelos in bestehende Ereignisverwaltungs- und Workflowsysteme integrieren.

Amazon Macie – Amazon Macie ist ein KI-gesteuerter Sicherheitsservice, der Ihnen dabei hilft, Datenverlust zu vermeiden, indem er sensible, in AWS gespeicherte Daten automatisch erkennt, klassifiziert und schützt. Amazon Macie verwendet Machine Learning zur Neuorganisation sensibler Daten wie persönliche identifizierbare Informationen (Personally Identifiable Information, PII) oder geistiges Eigentum. Es weist einen Geschäftswert zu und liefert Transparenz bezüglich des Speicherorts und der Verwendung dieser Daten in Ihrer Organisation. Amazon Macie überwacht fortlaufend Datenzugriffsaktivitäten auf Anomalien und gibt Warnungen aus, wenn ein Risiko durch einen nicht autorisierten Zugriff oder unbeabsichtigte Datenlecks erkannt wird.

AWS-Config-Regeln – Eine AWS Config-Regel enthält die gewünschten Konfigurationen für eine Ressource. Sie wird anhand von Konfigurationsänderungen an den relevanten Ressourcen gemäß Aufzeichnung in AWS Config ausgewertet. Sie können die Ergebnisse der Auswertung einer Regel anhand der Konfiguration einer Ressource auf einem Dashboard sehen. Mit Config Rules können Sie Ihren allgemeinen Einhaltungs- und Risikostatus aus der Konfigurationsperspektive beurteilen, Compliancetrends im zeitlichen Verlauf anzeigen und ermitteln, durch welche Konfigurationsänderung eine Ressource gegen eine Regel verstößt.

AWS Trusted Advisor – AWS Trusted Advisor ist eine Onlineressource zur Kostenreduzierung, Performancesteigerung und Verbesserung der Sicherheit, indem Ihre AWS-Umgebung optimiert wird. Trusted Advisor bietet Echtzeitunterstützung bei der Bereitstellung Ihrer Ressourcen nach bewährten Methoden von AWS. Für Kunden mit einem Business- oder Enterprise-Supportplan ist der vollständige Satz von Trusted Advisor-Prüfungen, einschließlich der Integration von CloudWatch Events, verfügbar.

Amazon CloudWatch – Amazon CloudWatch ist ein Überwachungsservice für AWS Cloud-Ressourcen und die über AWS ausgeführten Anwendungen. Sie können Amazon CloudWatch verwenden, um Metriken zu erfassen und nachzuverfolgen, Protokolldateien zu sammeln und zu überwachen, Alarme festzulegen und automatisch auf Änderungen Ihrer AWS-Ressourcen zu reagieren. Amazon CloudWatch kann AWS-Ressourcen, wie Amazon-EC2-Instances, Amazon DynamoDB-Tabellen und Amazon RDS DB-Instances sowie von Ihren Anwendungen und Services generierte Metriken und Protokolldateien überwachen. Amazon CloudWatch bietet Ihnen einen systemweiten Einblick in die Auslastung Ihrer Ressourcen, die Anwendungsleistung und die Integrität Ihrer Betriebsabläufe. Anhand dieser Informationen können Sie entsprechend reagieren und die kontinuierliche Verfügbarkeit Ihrer Anwendung sicherstellen.

Amazon Inspector – Amazon Inspector ist ein automatisierter Service zur Sicherheitsbewertung, mit dem die Sicherheit und die Compliance von Anwendungen in AWS erhöht werden können. Amazon Inspector bewertet Anwendungen automatisch hinsichtlich Schwachstellen oder Abweichungen von bewährten Methoden. Nach einer Bewertung erstellt Amazon Inspector eine nach Schweregrad geordnete detaillierte Liste der Sicherheitsergebnisse. Sie können diese Ergebnisse direkt oder im Rahmen detaillierter Berichte prüfen, die über die Amazon Inspector-Konsole oder die API verfügbar sind.

Amazon Detective – Amazon Detective erfasst automatisch Protokolldaten aus Ihren AWS-Ressourcen und erstellt mithilfe von Machine Learning, statistischer Analyse und Graphentheorie einen verknüpften Datensatz, mit dem Sie schnellere und effizientere Sicherheitsüberprüfungen durchführen können. Amazon Detective kann Billionen von Ereignissen aus mehreren Datenquellen analysieren, z. B. aus VPC-Flow-Protokollen (Virtual Private Cloud), AWS CloudTrail und Amazon GuardDuty. Außerdem erstellt er automatisch eine einheitliche, interaktive Ansicht Ihrer Ressourcen und Benutzer sowie der Interaktionen zwischen ihnen im Laufe der Zeit. In dieser konsolidierten Ansicht können Sie alle Details und den Kontext an einem Ort visualisieren, um die zugrunde liegenden Ursachen für die Befunde zu identifizieren, relevante historische Aktivitäten zu ermitteln und die Ursache schnell festzustellen.

Automatisierung

AWS Lambda – AWS Lambda ist ein serverloser Computing-Service, der Ihren Code beim Eintreten bestimmter Ereignisse ausführt und für Sie automatisch die zugrunde liegenden Computing-Ressourcen verwaltet. Sie können Lambda verwenden, um weitere AWS-Services mit benutzerdefinierter Logik bereitzustellen, oder einen eigenen Backend-Service erstellen, der mit der Größenordnung, Leistung und Sicherheit von AWS arbeitet. Lambda führt Ihren Code auf einer hochverfügbaren Computing-Infrastruktur aus und erledigt alle verwaltungstechnischen Aufgaben für Ihre Computing-Ressourcen. Dies umfasst die Wartung von Servern und Betriebssystemen, die Bereitstellung von Kapazitäten und die automatische Skalierung, die Bereitstellung von Code und Sicherheitspatches ebenso wie die Codeüberwachung und -protokollierung. Sie müssen lediglich den Code bereitstellen.

AWS Step Functions – AWS Step Functions erleichtert Ihnen die Koordination der Komponenten verteilter Anwendungen und Microservices mit visuellen Workflows. Step Functions bietet Ihnen eine grafische Konsole, auf der Sie die Komponenten Ihrer Anwendung als eine Reihe von Schritten anordnen und visualisieren können. Dies vereinfacht die Erstellung und Ausführung von mehrstufigen Anwendungen. Step Functions löst jeden Schritt automatisch aus und verfolgt ihn und führt bei

Fehlern Neuversuche aus, sodass Ihre Anwendung in der richtigen Reihenfolge und wie erwartet ausgeführt wird.

Step Functions protokolliert den Status von jedem Schritt, wenn also Probleme auftreten, können Sie Probleme schnell diagnostizieren und beheben. Sie können Schritte ändern und hinzufügen, ohne Code zu schreiben, damit Sie Ihre Anwendung problemlos weiterentwickeln und schneller Innovationen einführen können. AWS Step Functions ist Teil der AWS Serverless Platform und erleichtert die Orchestrierung vonAWS Lambda-Funktionen für Serverless-Anwendungen. Sie können Step Functions auch für die Orchestrierung von Mikroservices mittels Computing-Ressourcen wie Amazon EC2 und Amazon ECS nutzen.

AWS Systems Manager – AWS Systems Manager bietet Ihnen Transparenz und Kontrolle über Ihre Infrastruktur auf AWS. Systems Manager bietet eine einheitliche Benutzeroberfläche, damit Sie Betriebsdaten aus mehreren AWS-Services anzeigen und Betriebsaufgaben über Ihre AWS-Ressourcen hinweg automatisieren können. Mit Systems Manager können Sie Ressourcen nach Anwendungen gruppieren, Betriebsdaten zur Überwachung und Fehlerbehebung einsehen und Maßnahmen für die Ressourcengruppen ergreifen. Systems Manager kann Ihre Instances in ihrem definierten Zustand halten, On-Demand-Änderungen durchführen, z. B. die Aktualisierung von Anwendungen oder die Ausführung von Shell-Skripten, sowie weitere Automatisierungs- und Patching-Aufgaben durchführen.

Sichere Speicherung

Amazon S3 – Amazon S3 ist ein Objektspeicher zum Speichern und Abrufen beliebiger Datenmengen aus allen Speicherorten. Es ist auf eine 99,999999999%ige Haltbarkeit ausgelegt und speichert Daten für Millionen von Anwendungen, die von Marktführern aus allen Branchen verwendet werden. Amazon S3 bietet umfassende Sicherheit und wurde entwickelt, um Ihre regulatorischen Anforderungen zu erfüllen. Es bietet Kunden flexible Methoden bei der Verwaltung von Daten zur Kostenoptimierung, Zugriffssteuerung und Compliance. Amazon S3 bietet direkte Abfragefunktionen, mit denen Sie leistungsstarke Analysen Ihrer Data-at-Rest in Amazon S3 ausführen können. Amazon S3 ist der am meisten unterstützte Cloud-Speicherservice, der von der größten Gemeinschaft von Drittanbieterlösungen, Systemintegratoren und anderen AWS-Services integriert wird.

Amazon S3 Glacier – Amazon S3 Glacier ist ein sicherer, dauerhafter und äußerst kostengünstiger Cloud-Speicherservice für die langfristige Sicherung und Archivierung von Daten. Es wurde für eine 99,999999999%ige Zuverlässigkeit, umfassende Sicherheit und zur Erfüllung Ihrer regulatorischen Anforderungen entwickelt. Amazon S3 Glacier bietet direkte Abfragefunktionen, mit denen Sie leistungsstarke Analysen Ihrer archivierten Data-at-Rest ausführen können. Amazon S3 Glacier stellt

drei Optionen für den Zugriff auf Archive bereit, die von wenigen Minuten bis zu mehreren Stunden dauern können, um die Kosten niedrig zu halten und dennoch variierende Abrufanforderungen zu erfüllen.

Benutzerdefiniert

Die oben genannten Services und Funktionen erheben nicht den Anspruch auf Vollständigkeit. AWS fügt ständig neue Funktionen hinzu. Für weitere Informationen empfehlen wir Ihnen die Seiten Neuigkeiten bei AWS und AWS Cloud Security. Zusätzlich zu den Sicherheitsservices, die AWS als native Cloud-Services anbietet, könnten Sie daran interessiert sein, eigene Funktionen zusätzlich zu den AWS-Services zu entwickeln.

Obwohl wir empfehlen, eine Basisgruppe von Sicherheitsdiensten in Ihren Konten zu aktivieren, wie AWS CloudTrail, Amazon GuardDuty und Amazon Macie, möchten Sie diese Funktionen gegebenenfalls erweitern, um Ihre Protokollressourcen noch besser zu nutzen. Es gibt eine Reihe von Partnertools, z. B. die in unserem APN-Sicherheitskompetenzprogramm aufgeführten Tools. Möglicherweise möchten Sie auch Ihre eigenen Abfragen schreiben, um Ihre Protokolle zu durchsuchen. Dank der großen Zahl an verwalteten Services von AWS ist dies leichter denn je. Es gibt viele weitere AWS-Services, die bei Untersuchungen hilfreich sind, jedoch den Rahmen dieses Dokuments sprengen würden, wie Amazon Athena, Amazon OpenSearch Service, Amazon QuickSight, Amazon Machine Learning und Amazon EMR.

Anhang B: Beispiel-Code

Beispielereignis AWS CloudTrail

Das folgende Beispiel zeigt, dass ein IAM-Benutzer mit dem Namen `Alice` die AWS CLI verwendet hat, um Amazon EC2 `StopInstancesaction` mithilfe von `ec2-stop-instances` aufzurufen.

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
    }]}}
}]}
```

Beispiel eines AWS CloudWatch Event

Das folgende Beispiel für ein Amazon CloudWatch Event zeigt, dass ein AWS IAM-Benutzer mit dem Namen `jane-roe-test` auf `www.github.com` veröffentlicht wurde und von nicht autorisierten Benutzern missbraucht werden könnte.

```
{
  "check-name": "Exposed Access Keys",
  "check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
    "Fraud Type": "Exposed",
    "Location": "www.github.com"
  },
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

Beispiel für CLI-Aktivitäten von Infrastrukturdomänen

Die folgenden AWS CLI-Befehle zeigen ein Beispiel für die Reaktion auf ein Ereignis innerhalb der Infrastrukturdomäne. In diesem Beispiel werden die AWS-APIs verwendet, um viele der in diesem Dokument beschriebenen anfänglichen Vorfallreaktionsaktivitäten durchzuführen.

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
 disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name
 web-asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-
balancer-name web-load-balancer
```

```
# Create an EBS snapshot
> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-
REFERENCE-ID"
```

```
# Create a new EC2 instance from the Forensic Workstation AMI
> aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --
key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e
```

```
# Create a new EBS volume copy from the EBS snapshot
> aws ec2 create-volume --region us-east-1 --availability-zone us-east-1a --snapshot-id
 snap-abcd1234 --volume-type io1 --iops 10000
```

```
# Attach the volume to the forensic workstation
> aws ec2 attach-volume --volume-id vol-1234abcd --instance-id i-new4n6x --device /dev/
sdf
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to
 the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port
 0-65535 --source-group sg-1a2b3c4d
```

```
# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
 Key=Environment,Value=Quarantine:REFERENCE-ID
```

Anhang C: Beispiel-Runbook

Das folgende Beispiel eines Runbooks ist ein einzelner Eintrag eines größeren Runbooks. Dieses Runbook ist nicht offiziell und dient nur als Beispiel. Wenn Sie Ihre Runbooks erstellen, können sich Ihre Szenarien zu größeren Elementen mit unterschiedlichen Anfängen und Hinweisen auf Gefährdungen entwickeln, die aber alle ähnliche Ergebnisse oder zu ergreifende Maßnahmen haben. Die Erkenntnis dieser Änderung kann zudem neue Situationen mit besseren oder aufschlussreicheren Reaktionen eröffnen.

Runbook für Vorfallreaktionen – Root-Verwendung

Ziel

Das Ziel dieses Runbooks ist es, spezifische Anleitungen zur Nutzungsverwaltung des Root-AWS-Kontos zu liefern. Dieses Runbook ist kein Ersatz für eine umfangreiche Vorfallreaktionsstrategie. Dieses Runbook konzentriert sich auf den IR-Lebenszyklus:

- Kontrolle herstellen.
- Auswirkung bestimmen.
- Gegebenenfalls Wiederherstellung durchführen.
- Grundursache untersuchen.
- Verbessern.

Im Folgenden sind die Indikatoren für Gefährdungen (IOC), die ersten Schritte (Blutung stillen) und die detaillierten CLI-Befehle, die zur Ausführung dieser Schritte erforderlich sind, aufgeführt.

Annahmen

- CLI konfiguriert und installiert.
- Der Meldeprozess wurde bereits eingeführt.
- Trusted Advisor ist aktiv.
- Security Hub ist aktiv.

Indikatoren für Gefährdungen

- Für das Konto ungewöhnliche Aktivitäten.
  - Erstellung von IAM-Benutzern.
  - CloudTrail ist deaktiviert.
  - Cloudwatch ist deaktiviert.
  - SNS wurde angehalten.
  - Step Functions wurde angehalten.
- Einführung neuer oder unerwarteter AMIs.
- Änderungen der Kontakte im Konto.

Schritte zur Problembehebung – Kontrolle herstellen

In der AWS-Dokumentation für ein möglicherweise gefährdetes Konto werden die nachstehenden konkreten Aufgaben beschrieben. Die Dokumentation für ein möglicherweise gefährdetes Konto finden Sie unter: Was soll ich tun, wenn ich eine unbefugte Aktivität in meinem AWS-Konto feststelle?

1. Wenden Sie sich umgehend an AWS Support und TAM.
2. Ändern und rotieren Sie das Root-Passwort und fügen Sie ein mit Root verknüpftes MFA-Gerät hinzu.
3. Rotieren Sie Passwörter, Zugriffs-/geheime Schlüssel und CLI-Befehle, die für die Schritte zur Problembehebung relevant sind.
4. Überprüfen Sie die vom Root-Benutzer ergriffenen Aktionen.
5. Öffnen Sie die Runbooks für diese Aktionen.
6. Schließen Sie den Vorfall.
7. Überprüfen Sie den Vorfall und untersuchen Sie seine Ursache.
8. Beheben Sie die zugrunde liegenden Probleme, implementieren Sie Verbesserungen und aktualisieren Sie gegebenenfalls das Runbook.

Weitere Maßnahmen – Auswirkung ermitteln

Überprüfen Sie erstellte Elemente und mutierende Anrufe. Möglicherweise wurden Elemente erstellt, um in Zukunft den Zugriff zu ermöglichen. Achten Sie auf Folgendes:

- Kontoübergreifende IAM-Rollen
- IAM-Benutzer.
- S3-Buckets.
- EC2-Instances.
- [Ihre Anwendung und Infrastruktur werden diese Liste ergänzen.]

Hinweise

Kunden sind eigenverantwortlich für die unabhängige Bewertung der Informationen in diesem Dokument zuständig. Dieses Dokument: (a) dient rein zu Informationszwecken, (b) spiegelt die aktuellen Produktangebote und Verfahren von AWS wider, die sich ohne vorherige Mitteilung ändern können, und (c) impliziert keinerlei Verpflichtungen oder Zusicherungen seitens AWS und dessen Tochtergesellschaften, Lieferanten oder Lizenzgebern. AWS-Produkte oder -Services werden im vorliegenden Zustand und ohne ausdrückliche oder stillschweigende Gewährleistungen, Zusicherungen oder Bedingungen bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden wird durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen zwischen AWS und seinen Kunden und ändert diese Vereinbarungen auch nicht.