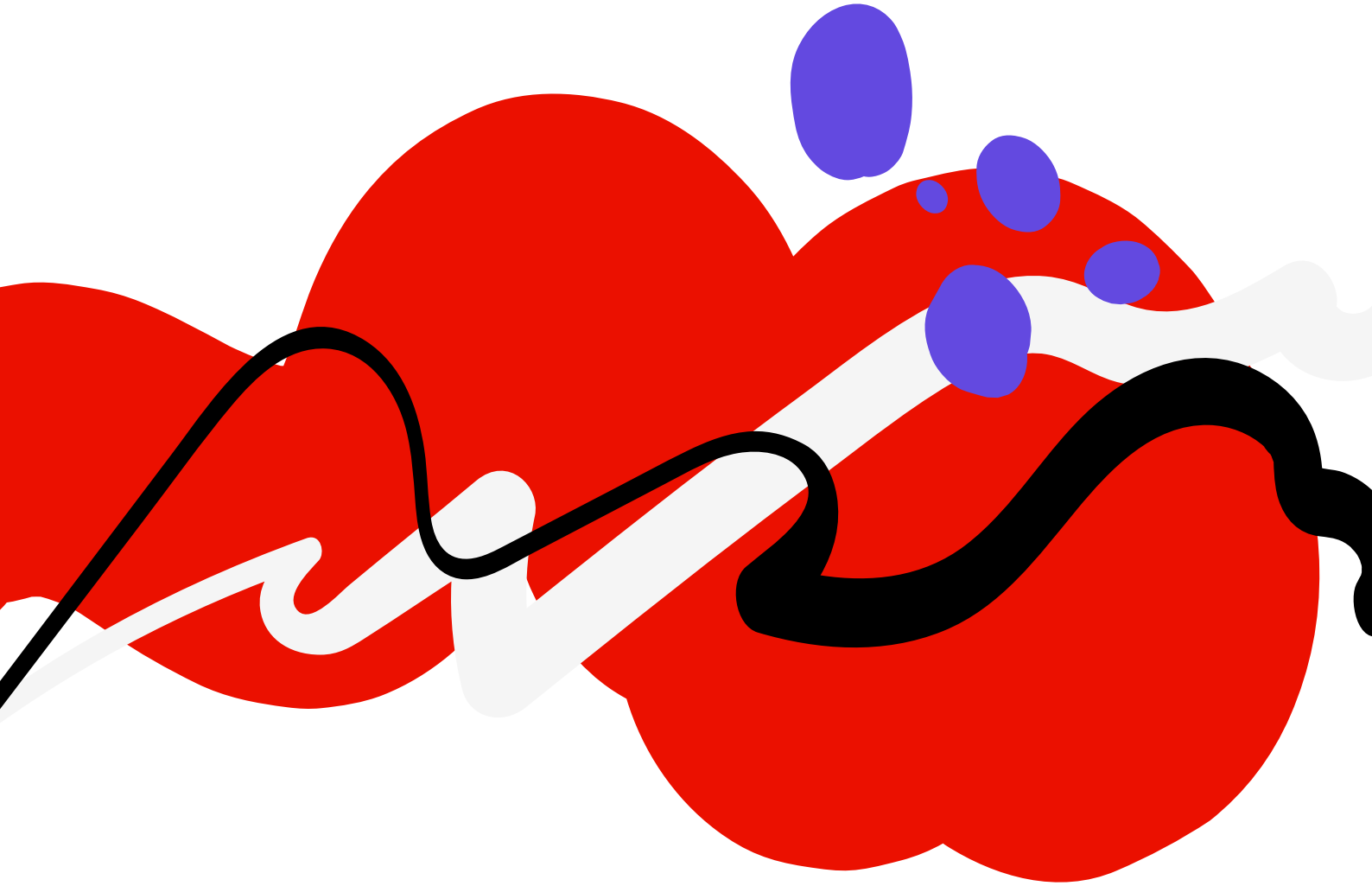
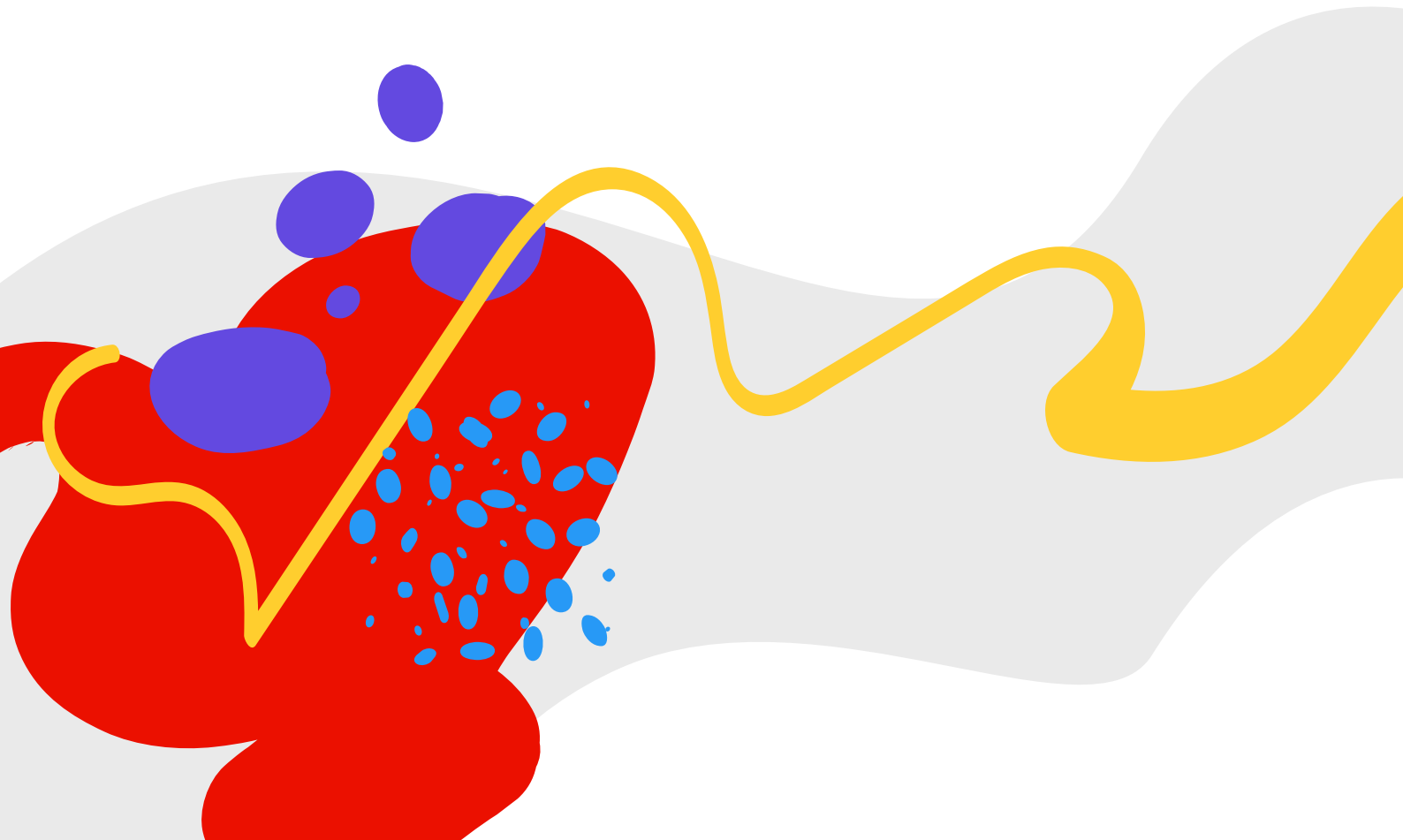
WHITEPAPER.

Überblick über die Betriebssicherheit bei Adobe.



Inhalt.



Einführung.

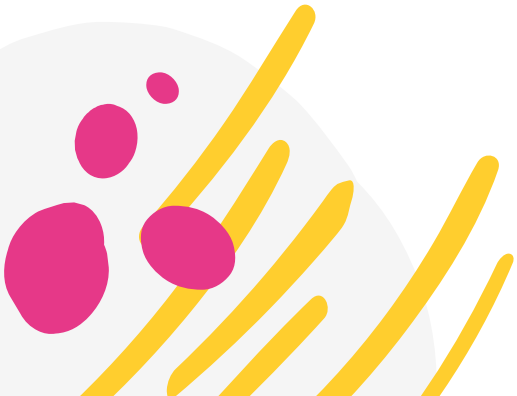
Die Multi-Cloud-Strategie von Adobe® mit öffentlichen und privaten Clouds verschiedener Provider basiert auf konsistenten, wiederholbaren Sicherungsmechanismen, die für unsere Produkt- und Serviceteams leicht zugänglich sind. Ein dediziertes Team für Betriebssicherheit (Operational Security, OpSec) ist dabei für den Schutz der Cloud-Ressourcen zuständig. Gleichzeitig trägt es zur Sicherheit der Kundenprogramme und -daten im Rahmen unseres laufend erweiterten Cloud-Infrastrukturbetriebs bei.

Dieses Whitepaper beschreibt Adobes Strategie für einen sicheren Cloud-Betrieb sowie die Prozesse und Tools, die unseren Mitarbeitenden in der Produkt- und Software-Entwicklung dabei helfen, die Sicherheit zu verbessern und Risiken auf Unternehmens- und Kundenseite zu minimieren, und die die Adobe-weite Einhaltung der Compliance- und Datenschutzvorgaben sowie anderer Governance-Auflagen fördern.

Adobes Strategie für sichere Cloud-Prozesse.

Fundament unserer Cloud-Prozesse sind die integrierten Sicherheitsmechanismen, mit denen wir potenziellen Problemen vorbeugen, die in diesem komplexen Sicherheitsumfeld auftreten können. Die kontinuierlich wachsende Cloud-Infrastruktur, die Multi-Cloud-Umgebungen und innovative Technologien wie Container und Orchestratror-Module umfasst, basiert auf Standardkonfigurationen und Richtlinien sowie Automatisierungs-Tools, die menschliche Fehler vermeiden helfen und unseren Kundinnen und Kunden die Sicherheit geben, dass die verschiedenen Ebenen der Infrastruktur vor potenziellen Schwachstellen geschützt sind. Die Skalierung von Sicherheit durch Automatisierung, ein regelmäßiges Monitoring unseres Sicherheitsstatus sowie vierteljährliche Compliance-Prüfungen ermöglichen die frühzeitige Erkennung von Abweichungen und anderen Sicherheitsproblemen, bevor diese kritisch werden.

Für jeden Service, den wir in der Cloud bereitstellen, haben wir Standardkonfigurationen und Sicherheitsrichtlinien entwickelt. So können sich unsere Entwicklungs-Teams auf ihre Schwerpunkte konzentrieren, und versehentliche Fehlentwicklungen zu Lasten der Sicherheit werden vermieden. Unsere Sicherheitskontrollen sind bereits in sehr frühen Entwicklungsphasen fest implementiert. Damit stärken wir die Sicherheit unserer Services von der Konzeption bis zur Bereitstellung und reduzieren gleichzeitig die Anzahl an Sicherheitslücken, die erst in einem späten Entwicklungsstadium erkannt werden, wenn sie sich nur unter großen Schwierigkeiten beheben lassen. Die automatisierte Umsetzung der Sicherheitskontrollen und Richtlinien für Cloud-Sicherheit trägt wesentlich zur Verbesserung der allgemeinen Sicherheit unseres Unternehmens und der unserer Kundinnen und Kunden bei – was für uns höchste Priorität hat.



Adobe Operational Security Stack.

Der Adobe Operational Security Stack (OSS) ist eine Entwicklung unseres OpSec-Teams. Er vereint eine Reihe von Tools, die dafür sorgen, dass alle Produkte und Services von Adobe von Grund auf unter Berücksichtigung sicherheitstechnischer Best Practices entwickelt werden. Der Adobe OSS basiert auf zwei Grundprinzipien, die den speziellen Anforderungen unserer Multi-Cloud-Infrastruktur Rechnung tragen: Standardisierung und Prävention. Er umfasst eine Reihe standardisierter Monitoring- und Workflow-Lösungen, auf die unsere Serviceteams bei der Entwicklung ihrer – von Grund auf sicheren – Private- und Public-Cloud-Umgebungen zurückgreifen können und die gleichzeitig zur proaktiven Risikoprävention beitragen.

Der Adobe OSS kommt bei zahlreichen Cloud-Ressourcen zum Einsatz. Er gewährleistet skalierbare Sicherheit mit standardisierten Sicherheitsfunktionen für das gesamte Unternehmen sowie transparenten Einblicken in die Betriebsumgebungen für die Sicherheits-, Audit- und Compliance-Teams von Adobe. Die Tools und Prozesse werden von den Produkt- und Serviceteams unseres Hauses gleichermaßen genutzt. So vermeiden wir Sicherheitsfehler und ermöglichen eine effizientere Implementierung von Sicherheitslösungen anhand bewährter Abläufe.

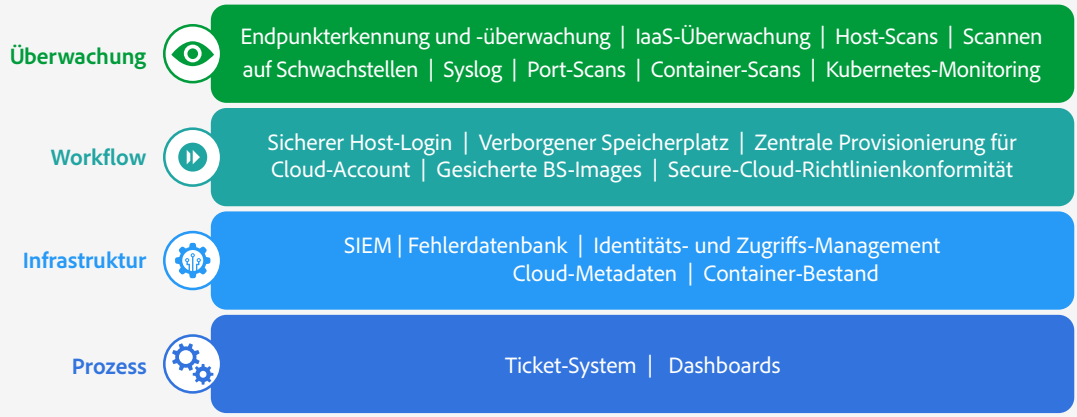


Abb. 1: Adobe Operational Security Stack

Der Adobe OSS besteht aus vier (4) Ebenen. Jede Ebene enthält eine umfassende Auswahl an Tools und Services, die allen Produkt-Teams zur Verfügung stehen und es ihnen ermöglichen, mit den neuesten Best Practices der schnelllebigen Sicherheitslandschaft zu arbeiten.

Überwachung.

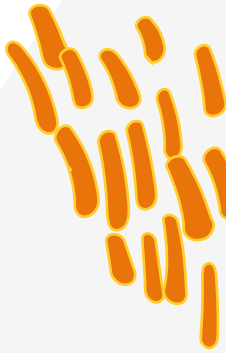
Die Überwachungsebene enthält Tools, mit denen die Log- und Konfigurationsdaten sämtlicher Adobe Cloud-Umgebungen in ein zentrales Data Warehouse eingespeist werden. Die gesammelten Daten werden durch die Adobe Sicherheits- und Compliance-Teams sowie das Adobe Security Operations Center (SOC) auf Sicherheitsabweichungen und -lücken geprüft. Die Prüfung kann sowohl manuell durch das Sicherheits-Team als auch mithilfe automatisierter Sicherheits-Tools erfolgen.

Zusätzlich führen unsere Sicherheits-Teams regelmäßige Scans der Hosts und Container der Programme und Netzwerke in unseren Cloud-Umgebungen durch. Die durch Scans und Penetrationstests aufgedeckten Schwachstellen werden bewertet, priorisiert und gegebenenfalls einem Plan zur Problembehebung zugewiesen.

Die Überwachungsebene des Adobe OSS enthält folgende Tools:

- **Endpoint Detection and Response (EDR)** – CrowdStrike Falcon ist ein schlanker EDR-Agent der nächsten Generation, der an allen Adobe-Endpunkten, einschließlich Servern, installiert ist. Die EDR-Lösung schützt Daten und Systeme durch kontinuierliche Echtzeit-Überwachung und -Erfassung, wodurch Gefahren schnell erkannt und behoben werden können.
- **IaaS-Überwachung** – MAVLink, ein von Adobe entwickeltes Tool zur Datenerfassung in Public Clouds, fragt Logging- und Umgebungskonfigurationsdaten von Amazon Web Services (AWS)- und Microsoft Azure-APIs ab und importiert diese Daten in ein Splunk-Data-Warehouse. Per MAVLink geben Entwickler den technischen Sicherheits-Teams von Adobe die Möglichkeit, den Sicherheitsstatus der Public Cloud zu einem bestimmten Zeitpunkt anzuzeigen. Auch die internen Audit- und Compliance-Teams von Adobe können diese Daten nutzen, um die Einhaltung verschiedener Elemente der AWS- und Azure-Sicherheitsstandards zu prüfen.
- **Scannen auf Schwachstellen** – Wir verwenden eine breite Palette an kommerziellen und selbst entwickelten Tools für regelmäßige Scans unserer Rechenzentren sowie unserer gesamten Cloud-Infrastruktur, um potenzielle Sicherheitsrisiken bereits im Vorfeld zu erkennen.
- **Host-Scans** – Mit Hubble, einem modularen Python-basierten Framework für Sicherheits-Compliance, das wir selbst entwickelt und als Open-Source für externe Parteien zur Verfügung stellen, führt Adobe folgende drei Aktivitäten aus:
  - Audit – Prüfung der Host-Systeme anhand von Richtliniendateien auf Basis von Center for Internet Security (CIS)-Standards
  - Abfrage – Erfassung von Systeminformationen mittels Osquery zur Erkennung von Angriffen
  - Dateiintegrität – Nachverfolgung von Dateiänderungen in Hauptverzeichnissen
- **Syslog** – Adobe erfasst System-Logs und Ereignismeldungen aus verschiedenen Rechnern und speichert sie zur Überwachung und Prüfung in Splunk.

- **Port-Scans** – Mit kontinuierlichen Scans vieler Hunderttausend Adobe IP-Adressen reduzieren wir die Reaktionszeit bei Gefährdungen. Mit dem Nmap-Portscanner führen wir schnelle Perimeter-Scans durch.
- **Container-Scans** – Adobe sammelt und scannt Containerimages auf häufige Schwachstellen und Sicherheitsrisiken sowohl bei Erstellung als auch zur Laufzeit. Die Scans werden in Splunk hochgeladen. Bei Problemen, die behoben werden müssen, erhalten die Teams ein Jira-Ticket.
- **Kubernetes-Monitoring** – Mithilfe eines internen Sicherheits-Tools zur Überwachung von Kubernetes-Clustern erstellen unsere technischen Sicherheits-Teams zu vordefinierten Zeitpunkten schreibgeschützte Konfigurations-Snapshots der Cluster und prüfen diese mit Eigenentwicklungen auf Sicherheitslücken. Die Resultate werden anschließend zur Analyse und Ticket-Erstellung an Splunk weitergeleitet.



Workflow.

Die Workflow-Ebene des Adobe OSS enthält Tools für die Produktentwicklungs-Teams von Adobe, die damit die End-to-End-Sicherheit der Adobe-Produkte sowie der Unternehmensinfrastruktur sicherstellen. Sie ermöglichen eine effiziente Implementierung der Sicherheitsrichtlinien für Vorgänge wie:

- **Sicherer Host-Login** – Die zentrale Zugangsdaten- und Zugriffsverwaltung mit Multi-Faktor-Authentifizierung (MFA) und dem Prinzip der geringstmöglichen Rechte ermöglicht eine strenge Kontrolle der virtuellen Cloud-Maschinen. Alle administrativen Sitzungen werden zudem zu Audit-Zwecken protokolliert.
- **Verborgener Speicherplatz** – Adobe verwendet ein Secure-Vault-Produkt eines führenden Drittanbieters zum Sichern, Speichern und Steuern des Zugriffs auf Token, Kennwörter, Zertifikate, API-Schlüssel und andere geheime Schlüssel.
- **Zentrale Provisionierung für Cloud-Account** – Die Produkt-Teams können die Cloud-Konten über einen zentralen Service erstellen und verwalten. Dies erleichtert die Verwaltung der Adobe Cloud-Infrastruktur sowie Einhaltung der Governance-Richtlinien, z. B. bei der Kontenabrechnung oder durchgängigen Anwendung von Betriebs- und Sicherheitsrichtlinien. Eine „Single Source of Truth“ für die Kontenmetadaten ist von zentraler Bedeutung für die Einschätzung von Umfang und Sicherheit unserer Cloud-Infrastruktur. Die zentrale Provisionierung ermöglicht eine exakte Bestimmung der Konteneigentümer und ihrer beabsichtigten Zwecke.
- **Gesicherte Betriebssystem-Images** – Durch die zentrale Bereitstellung von gehärteten Images gemäß CIS-Benchmarks (Center for Internet Security), Sicherheits-Updates mit CIS-Genehmigung und neuesten Sicherheits-Tools bietet Adobe seinen Produkt-Teams sichere, standardisierte Experiences. Die in der intern entwickelten Applikation „Image Factory“ gespeichertem Images werden durch unsere internen Sicherheits-Tools gescannt, bevor sie für den Einsatz in unseren Entwicklungs-Teams freigegeben werden. Darüber hinaus können die Produkt-Teams über das Image Factory-API das jeweils aktuelle Maschinen-Image direkt in ihre Build-Pipeline integrieren.

- **Secure-Cloud-Richtlinienkonformität** – Die meisten Cloud-Service-Provider bieten standardmäßige Sicherheitsrichtlinien. Adobe verwendet zusätzlich ein intern entwickeltes Tool zur Automatisierung der Richtliniendurchsetzung und Problembehebung. Es erweitert den Schutz gegen versehentliche Sicherheitsabweichungen und die Implementierung unsicherer Services in der Cloud. Unter Verwendung Cloud-nativer Services wie Azure Policy, AWS-Servicekontrollrichtlinien und AWS Config-Regeln gewährleistet das Tool die Durchsetzung der Anforderungen für Richtlinien- und Ressourcenkonformität in allen Public-Cloud-Konten von Adobe. Nicht konforme Ressourcen in einem Public-Cloud-Account lösen automatisch eine entsprechende Richtlinienaktion aus. Das Tool protokolliert diese Aktion und benachrichtigt die betreffenden Teams, damit sie die Ursache des Ereignisses ermitteln und beheben können.

Zur Vermeidung der gängigsten Konfigurationsfehler liegt der Schwerpunkt unserer Richtlinien auf vier Kategorien, die den häufigsten Einfallstoren von angreifenden Parteien entsprechen.

- Cloud-Identität und -Berechtigungen
- Datenschutz und Datenintegrität
- Exposition der Netzwerk-Endpunkte
- DNS-Integrität

Zudem schreiben unsere Richtlinien für Cloud-Betriebsmodelle vor, dass neue Konten bei der Provisionierung alle aktuell aktiven Richtlinien enthalten. Wenn Adobe eine neue Richtlinie veröffentlicht, wird diese durch einen automatisierten Prozess bei den vorhandenen Konten durchgesetzt. Als Beschleunigungsmaßnahme erfolgt diese automatische Durchsetzung innerhalb eines bestimmten Zeitraums – gewöhnlich ca. 30 Tage nach Freigabe. Bei nicht konformen Konten wird ein Ticket ausgegeben. Die Korrekturaufforderung enthält ein Fälligkeitsdatum, an dem das Konto den Richtlinien entsprechen muss.

Die automatische Durchsetzung ermöglicht es Entwicklerinnen und Entwicklern, sich auf übergeordnete Aufgaben im Rahmen der Richtlinienkonformität zu konzentrieren. Die Einhaltung wird durch den Prozess sichergestellt, der regelmäßig prüft, ob neue Konten vorhanden sind.

Infrastruktur.

Regelmäßig aktualisierte, umfangreiche Metadaten stellen eine Hauptkomponente der Infrastrukturebene im Adobe OSS dar, die das Fundament für die Überwachungs- und die Workflow-Ebene bildet. Anhand dieser Metadaten weist der Adobe OSS erkannte Sicherheitslücken dem Team zu, das für die betroffene Cloud-Ressource verantwortlich ist. Andere Tools der Infrastrukturebene umfassen:

- **Security Information and Event Management (SIEM)** – Mittels Splunk zur Suche, Überwachung, Visualisierung und Analyse der aggregierten Log-Daten in der Überwachungsebene kann das Adobe SOC eine tiefgreifendere Analyse der sicherheitsbezogenen Ereignisse und Vorfälle durchführen.

- **Fehlerdatenbank** – Adobe protokolliert Bugs mit automatisierter Ticket-Erstellung in Jira für eine optimierte zentralisierte Zuordnung und Nachvollziehbarkeit.
- **Identity and Access Management (IAM)** – Zur Authentifizierung verwendet Adobe Microsoft Active Directory in Kombination mit anderen Standard-Tools für das Authentifizierungs-Management.
- **Cloud-Metadaten** – Adobe verfolgt und prüft Metadaten für alle Public-Cloud-Konten. Zur Sicherung der Konten und Gewährleistung der Richtlinienkonformität wird ein vierteljährliches Audit dieser Daten durchgeführt. Das Cloud-Metadatenportal unterstützt Produkt- und Sicherheits-Teams beim Onboarding neuer Cloud-Konten gemäß den vorgegebenen Workflows. Darüber hinaus können die Teams im Data Warehouse auf die Metadaten zugreifen, um Datenrauschen und falsch positive Erkennungen zu eliminieren und kritische Bedrohungen zu priorisieren.
- **Container-Bestand** – Ein vielfältiges Set an Metadaten für das gesamte Container-Ökosystem von Adobe liefert unseren Produkt-Teams tiefe Einblicke in die Container-Orchestrierung. Sie verwenden sie auch zur Überwachung und Visualisierung von Kennzahlen sowie zur Darstellung von Kubernetes-Umgebungen.

Prozess.

Die Prozessebene dient der fortlaufenden Optimierung unserer Sicherheitsmechanismen sowie zur Implementierung von Best Practices. Daten aus den drei anderen Ebenen des Adobe OSS werden in einem zentralen Data Warehouse gespeichert und in Jira zur Behebung von Sicherheitslücken, in Dashboards zu Verwaltungszwecken sowie in andere interne Partnersysteme eingespeist.

Anhand von KPIs wird das Deployment des Adobe OSS im Unternehmen bewertet. KPIs dienen außerdem zur Identifizierung von Auffälligkeiten. Automatische Jira-Tickets informieren unsere Produkt-Teams im Falle der Abweichung eines Service von den festgelegten Sicherheitsstandards. Gleichzeitig finden sie in den Entwicklungs- und Betriebs-Teams für mehrere Kontrollbereiche im Adobe Common Controls Framework (CCF) Anwendung, u. a. beim Konfigurations- und Asset-Management.

Adobe Operational Security Stack in Aktion.

Ob Automatisierung, Kontrollen oder Standardisierung – das Zusammenspiel der einzelnen Ebenen des Adobe OSS fördert die Sicherheit unserer Cloud-Ressourcen.

Die Zugangsdaten- und Zugriffskontrollsysteme ermöglichen eine einheitliche Durchsetzung der Richtlinien für Identity and Access Management (IAM) in allen verwalteten Cloud-Services. Protokolle der Nutzungsaktivitäten liefern Erkenntnisse über Verbesserungs-möglichkeiten der Sicherheitsrichtlinien. Unter Verwendung gehärteter OS-Images aus unserer Image Factory-Infrastruktur erstellen, implementieren und verwalten unsere Entwicklungs-Teams dann Cloud-Services mit inhärenter Sicherheit.

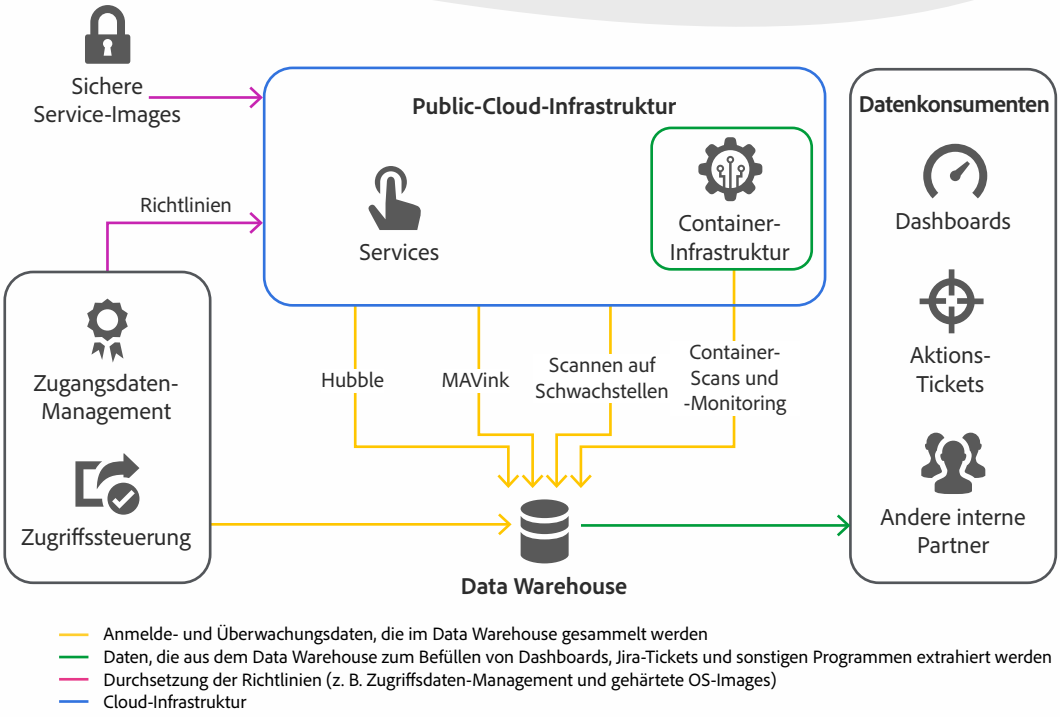


Abb. 2: Adobe OSS-Datenfluss

Unsere Monitoring-Lösungen überwachen fortlaufend die in der Cloud oder in unserer Container-Plattform bereitgestellten Services und senden Logs und andere relevante Informationen an ein zentrales Data Warehouse. Dashboards, Jira-Tickets und andere Applikationen im Unternehmen ziehen Daten aus diesem zentralen Warehouse für die nutzerseitigen Programme.

Fazit.

Unser OpSec-Konzept bietet unseren Produkt- und Serviceteams konsistente, wiederholbare Mechanismen, die eine sichere Bereitstellung der Adobe-Programme unter Berücksichtigung sämtlicher Compliance-, Datenschutz- und Governance-Auflagen gewährleisten. Durch automatisierte Prozesse und ein fortlaufendes Monitoring unserer Sicherheitsmechanismen mit Berichten, Dashboards und vierteljährlichen Compliance-Prüfungen können wir Sicherheitsrisiken proaktiv verhindern und End-to-End-Sicherheit für unsere Produkte und unsere Unternehmensinfrastruktur gewährleisten.

2/23