CASE STUDY

mondoo

Emnify erzielt mit Mondoo ein einheitliches, risikobasiertes Schwachstellenmanagement

Über emnify

Emnify ist ein führender Anbieter von Mobilfunk-Kommunikation im IoT-Stack, der weltweit Millionen von IoT-Geräten (wie Sensoren, Tracker und intelligente Geräte) verbindet. Die emnify-Plattform bietet Funktionen wie Echtzeit-Monitoring, Provisionierung sowie Management-Tools über eine einzige API, die alle auf einer Cloud-nativen Architektur namens „SuperNetwork“ basieren.

Standorte: Deutschland, USA, Philippinen, Brasilien

 # Mitarbeiter: 200

Cloud: Große AWS Präsenz

Cloud-native Entwicklung: IaC, Kubernetes

Compliance: SOC 2

> **Mondoo hilft uns nicht nur maß-geblich dabei, Schwachstellen in unseren Anlagen zu identifizieren, sondern spielt auch eine Schlüssel-rolle bei der Ticket-Erstellung.”**
>
> **Nader Erian**, Staff Security Engineer bei emnify

Große AWS Präsenz

Mit seiner auf AWS aufgebauten Infrastruktur umfasst emnify Hunderte von EC2-Instanzen und Dutzende von AWS-Konten.

Security Anforderungen

Nader Erian, Staff Security Engineer bei emnify, ist Teil des Security Operations Teams, das von Benoit Flippen, CISO bei emnify, geleitet wird. Das Team ist für die Sicherheit der emnify Plattform verantwortlich und sorgt dafür, dass diese den höchsten Sicherheits- und Compliance-Standards entspricht.

Emnify suchte eine Schwachstellenmanagement-Lösung, die es dem Unternehmen ermöglicht:

- den Risikograd jeder identifizierten Schwachstelle über verschiedene Infrastrukturebenen hinweg zu verstehen
- automatisiert Informationen über die AWS-Infrastruktur und die damit verbundenen Schwachstellen zu sammeln, um den gesamten Vulnerability-Management-Prozess zu verbessern und Audits wie SOC 2 zu unterstützen

Das emnify Team begann, mögliche Lösungen zu testen. Mehrere Optionen wurden auf Basis von Anforderungen und Kostenüberlegungen evaluiert.

Die Lösung: Mondoo

Nach der Evaluierung verschiedener Lösungen entschied sich emnify für Mondoo. Nader Erian sagt: "Mit Mondoo können wir Schwachstellendaten einsehen und Abfragen von einer einzigen Plattform aus durchführen. Dadurch können wir bessere und schnellere Entscheidungen treffen. Außerdem erhalten wir einen Überblick über die Kritikalität fehlender Patches, sodass wir wissen, welche zuerst behoben werden müssen.

- **DATENTIEFE:** Die Datentiefe von Mondoo ist für emnify sehr hilfreich. So zeigt Mondoo zum Beispiel alle potenziellen Angriffsvektoren, entsprechende Hinweise und wie das Problem gepatcht werden muss. Es zeigt auch das Risiko der Schwachstelle, basierend auf Faktoren wie Verwundbarkeit, Netzwerk-Exposition, Einfachheit der Ausnutzung und kompensierende Kontrollen. Diese Informationen sind für emnify entscheidend, um die Gesamt-Kritikalität zu bewerten.

- **ANLEITUNG ZUR BEHEBUNG:** Ein weiterer wichtiger Aspekt ist, dass Mondoo genau anzeigt, welche Pakete betroffen sind und welches Update oder welcher Patch das Problem beheben würde. Dies reduziert den Rechercheaufwand zur Behebung des Problems und führt zu einer schnelleren MTTR (Mean Time To Resolution).

> **Mit Mondoo können wir von einer einzigen Plattform aus Schwachstellendaten einsehen und abfragen, was uns hilft, bessere und schnellere Entscheidungen zu treffen.".**
>
> Nader Erian, Staff Security Engineer, emnify

- **WORKSPACES:** Auch Mondoo Workspaces haben sich für emnify als nützlich erwiesen: "Die Möglichkeit für F&E-Ingenieure, sich mit zugewiesenen Rollen in die Plattform einzuloggen, war sehr wertvoll. So können sie ihre Assets einsehen, anfällige Pakete identifizieren, die aktualisiert werden müssen, und auf vorgeschlagene Patches für verschiedene Betriebssystemversionen zugreifen.

- **S3 EXPORTER:** Nader Erian fügt hinzu: "Die umfassenden Integrationen von Mondoo – insbesondere der AWS S3 Exporter – waren entscheidend für die Automatisierung der Ticket-Erstellung für die F&E-Teams. Sie haben die Geschwindigkeit, mit der emnify Schwachstellen beheben kann, deutlich erhöht.

Ergebnisse

Mit der Mondoo-Plattform hat emnify die folgenden Ergebnisse erzielt:

- **Erkenntnisse für die Priorisierung:** Entscheidend für die Bewertung der Gesamt-Kritikalität waren die von Mondoo zur Verfügung gestellten Informationen zu den entdeckten Schwachstellen – z.B. ob ein Exploit in freier Wildbahn existiert oder ob bekannt ist, dass eine Schwachstelle aktiv ausgenutzt wird.

- **Schnellere Entscheidungsfindung:** Mondoo hat emnify maßgeblich bei der Identifizierung von Schwachstellen in allen Assets unterstützt und spielt eine Schlüsselrolle bei der Erstellung von Schwachstellen-Tickets.

- **Schnellere Behebung:** Im Zusammenspiel mit dem zuvor Genannten und anderen wertvollen Erkenntnissen innerhalb der Plattform, hat emnify die Behebung von Schwachstellen erheblich beschleunigt und sichergestellt, dass die kritischsten Schwachstellen priorisiert werden.

> **Der Kundensupport, den wir von Mondoo erhalten, ist hervorragend ".**
>
> Nader Erian, Staff Security Engineer, emnify

Fazit

Dank Mondoos einheitlicher Sicht auf die Schwachstellen in der gesamten Infrastruktur ist es für emnify jetzt viel einfacher, den Risikograd jedes Problems schnell zu verstehen und sich auf die Behebung der kritischsten zu konzentrieren. Diese Einblicke waren auch eine wertvolle Unterstützung bei Audits, z.B. für SOC 2 Compliance.

„Neben dem Produkt selbst ist auch der Kundensupport, den wir von Mondoo erhalten, hervorragend", sagt Nader Erian. "Das Team ist sehr reaktionsschnell, engagiert und kooperativ, hat immer ein offenes Ohr für unser Feedback und verbessert kontinuierlich die Plattform. Ihre Bereitschaft, die von uns gewünschten Funktionen zu implementieren, wird sehr geschätzt und ist ein großer Pluspunkt für das Produkt. Wir setzen auf Mondoo als vertrauensvollen Partner in unserer Sicherheitsstrategie".