

SimpleRose automatisiert mit Mondoo die Security über den gesamten Tech-Stack

Über SimpleRose

SimpleRose hilft Teams dabei, selbst die komplexesten Planungs- und Terminierungsprobleme schneller und detaillierter zu lösen. Ganz gleich, ob Unternehmen ihre bestehenden Optimierungsmodelle beschleunigen oder ein maßgeschneidertes System zur Entscheidungsunterstützung aufbauen möchten: SimpleRose hilft seinen Kunden, weniger Zeit mit der Vereinfachung und mehr Zeit mit Lösungen zu verbringen.

Standort: St. Louis, USA

Branche: Technologie

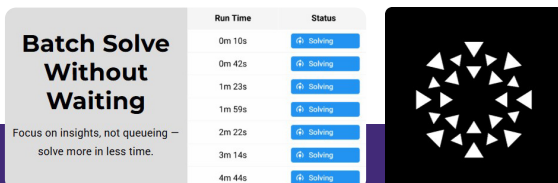
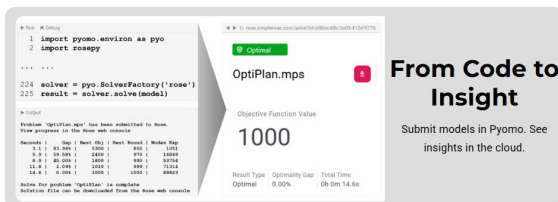
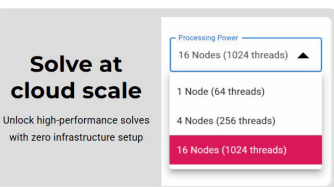
Cloud: AWS

ITSM: GitHub Issues

SaaS: Google Workspace

IaC: Terraform

Compliance: SOC 2, GDPR, CCPA, PCI DSS



“

Bevor wir Mondoo einsetzten, standen wir vor einem Meer aus roten Warnmeldungen, sahen aber keinen klaren Weg nach vorne. Durch die Einführung von Mondoo konnten wir die wichtigsten Themen identifizieren, sodass wir nach der vollständigen Implementierung nur noch eine leicht überschaubare Zahl von Themen hatten.”



Todd Bradfute

Senior Director of Security & Technology

Cloud-First IT infrastruktur

SimpleRose ist eine Cloud-First-Organisation, deren Infrastruktur hauptsächlich auf AWS basiert. Sie ist durch mehrere Unterkonten strukturiert, die unter einer AWS-Organisation verwaltet werden. Dabei werden bewährte Verfahren zur Trennung von Arbeitslasten und Sicherheit angewendet. SimpleRose setzt Cloud-native Entwicklungspraktiken ein und entwirft seine Applikationen für Skalierbarkeit, Ausfallsicherheit und Überprüfbarkeit. Dazu nutzt das Unternehmen Containerisierung und Infrastructure-as-Code in AWS.

Die Security ist in die breiteren IT- und Operation-Bereiche von SimpleRose eingebettet. Es handelt sich dabei nicht um eine eigenständige Abteilung, sondern um einen funktionsübergreifenden Teamansatz, an dem Sicherheitsbeauftragte aus den Bereichen Technik, Compliance und IT beteiligt sind. Diese werden von den „Rosarians“ koordiniert, dem Team für Security, Ops, IT und Compliance bei SimpleRose.

Security Herausforderungen

Eine der größten Herausforderungen für SimpleRose war es, in Echtzeit einen zentralen Überblick über die Compliance und die Konfiguration des vielfältigen und schnell wachsenden Tech-Stacks zu erhalten, einschließlich Cloud-Infrastruktur, Endpunkten, SaaS-Plattformen und Entwickler-Tools.

Todd Bradfute, Senior Director of Security & Technology bei SimpleRose, sagt: „Obwohl wir mit Tools wie CrowdStrike und Cloudflare über einen starken Perimeter- und Endpunktschutz verfügten und mit Vanta die Einhaltung grundlegender Workstation Compliances sicherstellen (z. B. Passwortsperrung, Verschlüsselung, Virenschutz, Bildschirmsperre [PEAS]), arbeiteten all diese Lösungen in Silos.“

SimpleRose fehlte eine einheitliche Plattform, die tiefe Einblicke in die breitere Compliance-Situation ihrer Systeme bieten konnte, wie z. B.:

- **PATCH STATUS UND SOFTWARE VERSIONEN**
- **DATEIBERECHTIGUNGEN UND SYSTEM-KONFIGURATION**
- **KONFIGURATION VON CLOUD-DIENSTEN UND CONTAINERSICHERHEIT**
- **SICHERHEITSSTATUS ON WEB-ASSETS (Z. B. FALSCH KONFIGURIERTE DOMÄNEN ODER CLOUD-DIENSTE)**

„Mit der Skalierung unserer Cloud-nativen Services und der Beschleunigung unserer CI/CD-Pipelines wurden diese Schwachstellen immer dringlicher“, ergänzt Todd. „Wir brauchten eine Möglichkeit, nicht nur Compliance-Anforderungen abzuholen, sondern den tatsächlichen Zustand der Systeme auf entwicklerfreundliche und erweiterbare Weise zu validieren – und Mondoo hat uns das ermöglicht.“



Mondoo gibt uns eine messerscharfe Antwort darauf, wie wir die festgestellten Probleme angehen können.“

Austin Palmer, Head of Cybersecurity and Compliance

Die Lösung: Mondoo

Als Todd auf den DevOpsDays von Mondoo's Policy as Code-Lösung hörte, war sein Interesse sofort geweckt. In Verbindung mit der Benutzerfreundlichkeit von Mondoo war SimpleRose schnell Feuer und Flamme.

Mit Mondoo kann SimpleRose seinen Compliance-Status für verschiedene Arten von Tools und Assets nun an einem Ort einsehen. Obwohl das Unternehmen bereits über andere Tools verfügte, die generelle Einblicke boten, geht Mondoo bei der Verifizierung auf Konfigurationsebene wesentlich weiter und bietet sowohl Breite als auch Tiefe.

Todd sagt: „Wir nutzten bereits Tools wie Vanta, um die grundlegende Konformität von Workstations zu validieren, aber wir mussten über die Kontrollen auf höchster Ebene hinausgehen und uns mit den Besonderheiten befassen – wie der Überprüfung, ob Dateiberechtigungen korrekt angewendet wurden, Patch-Versionen aktuell waren und Docker-Konfigurationen den Best Practices entsprachen.“

Dank Mondoo erhält SimpleRose jetzt:

- ✓ **Zentrale und anpassbare Transparenz:**
Konsolidierte Compliance-Einblicke aus verschiedenen Umgebungen (z. B. Laptops, AWS, DockerHub, interne Webservices) mit tiefgreifender Überprüfung auf Konfigurationsebene.
- ✓ **Anpassbare und skalierbare Richtlinien:**
SimpleRose kann Richtlinien als Code schreiben und anpassen, sodass sich Kontrollen an die spezifischen internen Standards einfach angleichen lassen
- ✓ **Automatisierte Security-Pipeline:**
Die reibungslose Integration in ihre CI/CD- und Infrastruktur-Pipelines ermöglicht Security als Code, ohne die Geschwindigkeit der Entwickler zu beeinträchtigen.



Mondoo verbessert unsere Fähigkeit, Sicherheitsrichtlinien über alle unsere IT-Oberflächen von einer einzigen Plattform aus zu überwachen, zu validieren und durchzusetzen, was uns sowohl Sichtbarkeit als auch Kontrolle ohne operativen Aufwand ermöglicht"

Todd Bradfute, Senior Director of Security & Technology

Umsetzung

„Mondoo war sehr einfach zu implementieren“, sagt Todd. „Ich hatte das Workstation-Scanning buchstäblich innerhalb einer Stunde nach der Mondoo-Präsentation auf den DevOpsDays am Laufen. Auch die Anbindung an unsere anderen Umgebungen war ziemlich mühelos.“

Ergebnisse

Mit Mondoo erreichte SimpleRose:

- ✓ **Verringerung der manuellen Arbeit:**
Was früher mehrstufige, manuelle und isolierte Arbeitsabläufe waren, sind jetzt klare, umsetzbare Wege zur Lösung mit automatisiertem Patching der betroffenen Systeme.
- ✓ **Deutlicher Rückgang der Anzahl an Schwachstellen:** Statt einer Flut roter Warnmeldungen ohne klaren Weg nach vorn gibt es nach der vollständigen Implementierung von Mondoo mit automatisierten Richtlinien nur noch eine leicht überschaubare Zahl an Themen.
- ✓ **Optimierter Aufmerksamkeitsfokus:**
SimpleRose kann sich jetzt auf das konzentrieren, was tatsächlich behoben werden muss, und die nötige Granularität anwenden, um benutzerdefinierte Richtlinien zu erstellen, die den Geschäftsanforderungen entsprechen.



Wiederholbarer und automatisierter

Behebungsprozess: SimpleRose profitiert jetzt von einem automatisierten und wiederholbaren Prozess (wie Todd es nennt: „spülen, schäumen und wiederholen“), um Schwachstellen und Fehlkonfigurationen im gesamten technischen Stack zu beheben:

1. Mondoo zeigt die gravierendsten Schwachstellen auf
2. SimpleRose wählt die wichtigsten aus, um sie zu beheben
3. SimpleRose verwendet RMM (für Workstations), IaC (für Workloads) und Terraform (für Cloud-Tools), um Korrekturen mit Mondoo's Code-Snippets bereitzustellen
4. Mondoo führt einen erneuten Scan durch und zeigt an, ob sich der Score verbessert hat.

Fazit

Die Hauptgründe für die Einführung von Mondoo bei SimpleRose waren die Notwendigkeit, Compliance und Konfigurationstransparenz in einem schnell wachsenden Tech-Stack zu vereinheitlichen und zu vertiefen.

Doch Mondoo konnte noch mehr leisten. Durch einen automatisierten, wiederholbaren Behebungsprozess konnte SimpleRose die manuelle Arbeit reduzieren, die Behebung beschleunigen und sicherstellen, dass die kritischsten Schwachstellen schnell behoben werden. Dank „Mondoo Policy as Code“ und der Integration in den SDLC konnte SimpleRose Sicherheit in den Entwicklungsprozess integrieren und Sicherheitsprobleme frühzeitig erkennen, ohne dabei Kompromisse bei der Geschwindigkeit einzugehen. Todd sagt: „Mondoo wurde zu unserer Brücke zwischen der technischen Konfiguration und den Richtlinienanforderungen. Das ist entscheidend für die Skalierung sicherer Abläufe ohne Reibungsverluste.“

Er sagt weiter: „Egal, wo Sie sich auf Ihrer Sicherheitsreise befinden, Mondoo unterstützt Sie dabei. Mondoo hatte für jedes Tool, das wir unterstützen mussten, eine Antwort parat. Für Organisationen, die wissen, dass sie viele verschiedene Frameworks unterstützen müssen, ist Mondoo ein großartiger Partner, mit dem man wachsen kann.“