Mondoo vs. Tenable

mondoo

Aktionsfähige Security vs. Checkbox Security

Tenable basiert auf einer Kombination unabhängiger Module, die zum einen separat lizensiert werden müssen und zum anderen auch den Wechsel zwischen unterschiedlichen Konsolen erfordern. Höherer Aufwand bei geringerer Bildschärfe sind die Folge. Darüber hinaus basiert Tennables Lösung vor allen Dingen auf dem "Checkbox-Prinzip": Es werden eine begrenzte Anzahl an Überprüfungen vorgenommen und "abgehakt" ohne tatsächlich die Möglichkeit zu haben, aktiv einzugreifen oder gar in die "Remediation" einzusteigen.

Mondoo basiert hingegen auf einer zentralen Plattform names "ADA", die ihre komplette IT-Umgebung inkl. Software Development Lifecycle (SDLC) analysieren, bewerten und auch entsprechend agieren kann - eingebunden in die etablierten Prozesse Ihrer Organisation und immer mit dem Ziel, mögliche offene Flanken schnell zu entdecken, klug zu priorisieren und den Fehler unmittelbar aus einer zentralen Platform zu beheben.

Mondoo ist die richtige Lösung für Sie, wenn:

- Sie eine einheitliche Plattform statt isolierter Konsolen bevorzugen
- Sie Ihren SDLC mit mehr als nur IaC-Scanning sichern wollen
- Sie eine lückenlose Bestandsaufnahme Ihrer IT-Umgebung benötigen
- Sie ein durchgängiges Schwachstellen-management mit sofortigen Reaktions-möglichkeiten (Remediation) wünschen
- Sie Wert auf einfache und flexible Implementierung legen
- Sie die Risikopriorisierung an Ihre geschäftlichen Prioritäten anpassen möchten
- Sie unmittelbare Konformität mit den üblichen Branchenstandards, wie ISO, TISAX oder auch NIS2 wünschen

Funktionsvergleich

FUNKTION	MONDOO	TENABLE
Einfache Integration	**Ja**, einfache und flexible Implementierung - agentenbasiert sowie agentenlos. Cloud-Snapshot-Scanning für AWS, Azure und GCP - On-Premise, Linux, Windows und Mac. Mondoo-Agenten sind äußerst ressourcenschonend.	Das Onboarding einiger Cloud-Plattformen in Tenable Cloud Security kann manuellen Aufwand mit vielen Einzelschritten erfordern. Der Tenable-Agent ist zudem sehr ressourcenintensiv.
Full coverage	Mondoo deckt Ihre gesamte IT-Umgebung (Cloud, On-Premise, SaaS und Endpunkte) und den SDLC vom Code bis zur Laufzeit ab. In einer Lizenz.	Sie müssen viele verschiedene Module lizenzieren, wie Tenable Cloud Security, Tenable Vulnerability Management, Tenable Security Center, Tenable Nessus und andere. Tenable bietet keine SaaS-Sicherheitb.

Funktionsvergleich

FUNKTION	MONDOO	TENABLE
Regulatory compliance	Mondoo enthält mehr als 300 Vorlagen für Compliance-Frameworks (wie SOC2, PCI DSS, NIS2, HIPAA und NIST) und CIS-Benchmarks.	Lediglich Unterstützung für eine begrenzte Anzahl von Frameworks ohne umfassender Sichtbarkeit.
Automatische Ticketerstellung	**Ja,** Mondoo lässt sich direkt mit Jira, Zendesk, GitHub Issues, GitLab Issues, Microsoft Azure DevOps und anderen per E-Mail integrieren. Mondoo kann Tickets für einzelne oder mehrere Assets erstellen, Korrekturen automatisch validieren und Tickets je nach Bedarf schließen oder wieder öffnen.	Unterstützt nur Jira und ServiceNow. Liefert keine detaillierte Anleitung zur Remediation. Keine einfache Möglichkeit, Tickets zu erstellen, zu verfolgen und automatisch zu schließen.
Individuelle Risikopriorisierung	**Ja**, Mondoo ermöglicht die Anpassung von Risikofaktoren und aktualisiert die Werte bei Änderungen umgehend.	Erlaubt keine Feinabstimmung der Risikopriorisierung.
IaC Scanning ("Shift Left")	**Ja**, Mondoo bietet IaC-Scans für Terraform, Ansible, Kubernetes-Manifeste und Dockerdateien mit CI/CD-Integrationen. Mondoo deckt auch Code-Runtime wie Python und NodeJS ab.	Nur begrenzter Support für IaC Scanning.
Verwaltung von Ausnahmen	**Ja**, Richtlinien und Schwachstellen können für einzelne Anlagen oder Umgebungen pausiert, abgeschwächt, deaktiviert oder als Fehlalarme markiert werden.	**Begrenzt.** Die einzige Möglichkeit ist, Ressourcen von bestimmten Scans auszuschließen.
Security-Integration von Drittanbietern	**Ja**, Mondoo kann Daten von Microsoft Defender, SentinelOne und Crowdstrike einbeziehen.	Kein Einbezug von Drittanbieter Daten möglich**.**
Benutzer-definierte Arbeitsbereiche	**Ja**, Mondoo ermöglicht es Ihnen, Arbeitsbereiche auf der Grundlage von Attributen wie Asset-Name, Tag, Anmerkungen, Plattform, Plattformversion und Risikostufe zu erstellen. Die Arbeitsbereiche werden bei jeder Durchsuchung von Assets automatisch aktualisiert.	**Begrenzt.** Tenable kann zwar benutzerdefinierte Dashboards erstellen, aber die Daten in der Ansicht sind oft veraltet, da sie nur in unregelmäßigen Abständen aktualisiert werden.

Bereit für den Mondoo-Unterschied? Jetzt Demo anfordern: **mondoo.com/contact**

Was unsere Kunden sagen:

Einer der Hauptgründe, warum wir uns nicht für Tenable, Rapid7 und andere Tools dieser Art entschieden haben, ist, dass sie stark von Agenten abhängig sind. Doch je weniger Agenten ich auf meinen Boxen habe, desto besser."

Austin Palmer, Head of Cybersecurity and Compliance bei Campminder

campminder

emnify

Mondoo hilft uns nicht nur maßgeblich dabei, Schwachstellen in unseren Anlagen zu identifizieren, sondern spielt auch eine Schlüsselrolle bei der Ticket-Erstellung."

Nader Erian, Staff Security Engineer bei emnify

Dank Mondoo haben wir jetzt eine einheitliche Lösung für unseren Patch-, Sicherheits-, Risiko- und Compliance-Status sowie die Möglichkeit, in Zukunft auch andere Clouds, Container-Registries und On-Premise-Infrastrukturen zu sichern."

Head of Cloud & Information Security Solutions bei Universal Investment

Universal Investment

Sie möchten mehr erfahren?
Vereinbaren Sie jetzt einen Demo-Termin.

mondoo.com/contact

FOLGEN SIE UNS AUF: