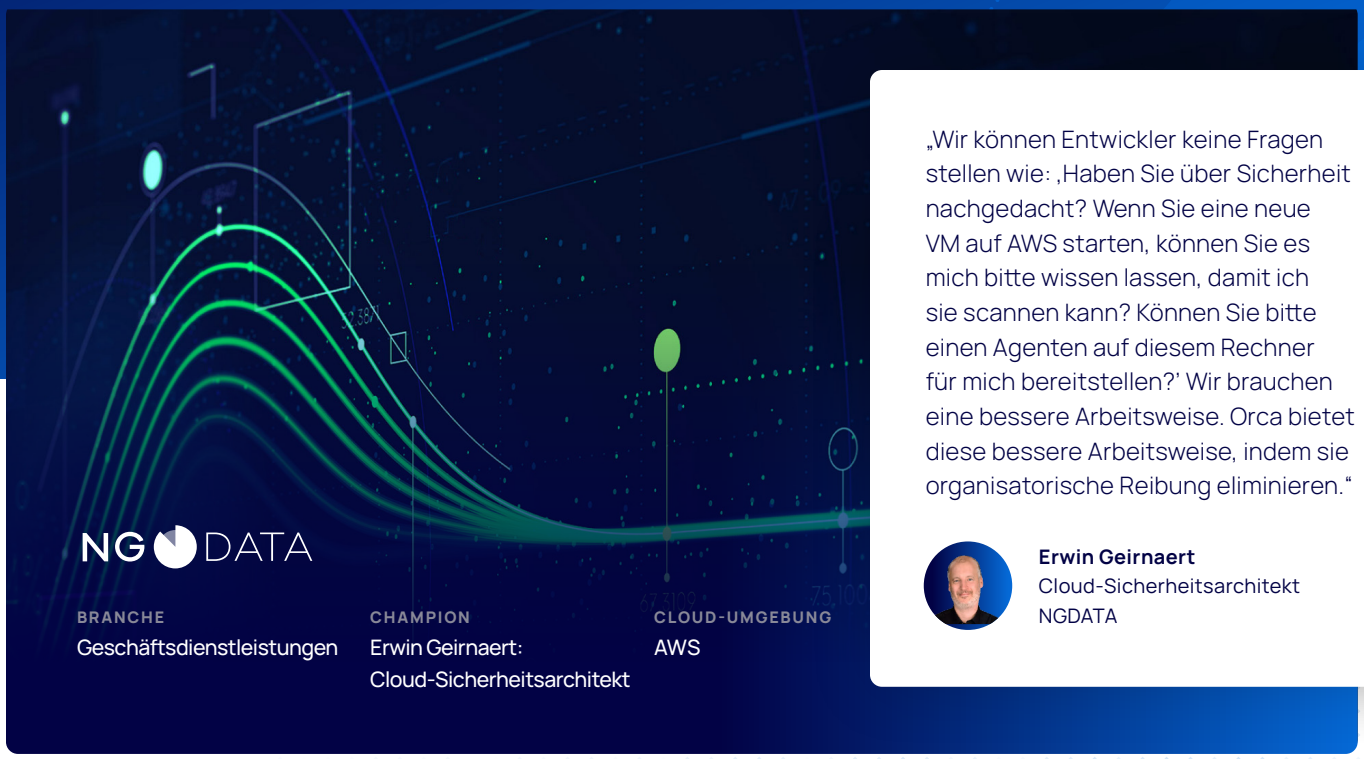
Orca Security bietet NGDATA ein Werkzeug für Sicherheit, DevOps und Compliance



BRANCHE
Geschäftsdienstleistungen

CHAMPION
Erwin Geirnaert: Cloud-Sicherheitsarchitekt

CLOUD-UMGEBUNG
AWS

„Wir können Entwickler keine Fragen stellen wie: ‚Haben Sie über Sicherheit nachgedacht? Wenn Sie eine neue VM auf AWS starten, können Sie es mich bitte wissen lassen, damit ich sie scannen kann? Können Sie bitte einen Agenten auf diesem Rechner für mich bereitstellen?' Wir brauchen eine bessere Arbeitsweise. Orca bietet diese bessere Arbeitsweise, indem sie organisatorische Reibung eliminieren."

Erwin Geirnaert
Cloud-Sicherheitsarchitekt
NGDATA

Herausforderungen der Cloud-Sicherheit

- Benötigt wird eine globale Echtzeitansicht von AWS-Assets für eine sich häufig ändernde Anlage, vorzugsweise ohne Einsatz von Agenten
- Sicherstellung des Schutzes der Vermögenswerte und des geistigen Eigentums von Unternehmen
- Benötigt werden Tools, die sich in die Arbeitsweise der Entwickler integrieren lassen

Ergebnisse der Cloud-Sicherheit

- Ermöglicht eine vollständige Übersicht über alle NGDATA in Echtzeit
- Integration in Jira zur Automatisierung des Prozesses zur Behebung von Schwachstellen
- Beseitigung der organisatorischen Reibung mit den Entwicklern bei der Umstellung zum DevSecOps-Ansatz

NGDATA hilft Unternehmen, durch Dateneinblicke persönlichere Kundenerlebnisse zu schaffen

NGDATA unterstützt Marken in datengesteuerten Branchen wie Finanzdienstleistungen, Telekommunikation, Versorgungsunternehmen und Gastgewerbe dabei, vernetzte Kundenerlebnisse zu schaffen. Ihre KI-gestützten CDP- und digitalen Transformationsdienste stellen den Menschen in den Mittelpunkt eines jeden Unternehmens durch die Kunden-DNA, die kontinuierlich aus dem Verhalten der Kunden lernt, um überzeugende Erlebnisse für Marken auf der ganzen Welt zu liefern. NGDATA hat seinen Hauptsitz in Gent, Belgien, und verfügt über Niederlassungen in den Vereinigten Staaten, Europa und im asiatisch-pazifischen Raum.

Die Softwareplattform kann vor Ort installiert oder in einer privaten Cloud bereitgestellt werden, während die gesamte Produktentwicklung in der Cloud erfolgt. NGDATA hat den Cloud-Sicherheitsarchitekten Erwin Geirnaert von Shift Left Security beauftragt, Ordnung in ihre Cloud-Umgebungen zu bringen, Schwachstellen zu identifizieren und systematisch zu beseitigen sowie Verfahren zur Aufrechterhaltung einer guten Sicherheitslage zu implementieren.

Orca Security ist erfolgreich, wo klassische Sicherheitsscans versagen

Als Erstes unternahm Geirnaert einen klassischen Penetrationstest, um so schnell wie möglich den Zustand der aktuellen Umgebung zu ermitteln. Der Scan war nur bedingt hilfreich, da es sich nur um eine Momentaufnahme eines sich ständig verändernden Cloud-Gebildes handelte. Aber selbst bei einem authentifizierten Scanner gibt es eine Lücke, wenn er nicht weiß, was zu scannen ist. „Es funktioniert einfach nicht in einem Cloud-nativen Ansatz“, sagt Geirnaert.

Er versuchte dann, Informationen über die IP-Bereiche zu erhalten, um aus den Amazon-Protokollen zu scannen, die er in ein Sumo Logic-Dashboard gezogen hatte. Dies führte zu beunruhigenden Ergebnissen.



> „Um Schwachstellen in einer Cloud-Infrastruktur zu finden, ist der klassische Penetrationstest zwecklos. Unser erster Scan mit Orca war ein echtes Aha-Erlebnis. Wir fanden Rechner, von deren Existenz wir bis dahin nicht wussten, die sensible Informationen enthielten, oder Dienste mit einer Anbindung an das Internet.“
>
> **Erwin Geirnaert**
> Cloud-Sicherheitsarchitekt
> NGDATA

Geirnaert erklärt, wie Orca die DevSecOps-Dynamik ermöglicht. „Ein Entwickler hat Zugriff auf die AWS-Konsole, sodass er ganz einfach Orca unter Verwendung einer schreibgeschützten Richtlinie anbringen kann. Er muss nichts bereitstellen, anwenden oder installieren, er konfiguriert AWS einfach und vertraut auf die Orca-Plattform, die das Scannen durchführt. Es dauert etwa fünf Minuten, eine schreibgeschützte Richtlinie zu erstellen und in Betrieb zu nehmen. Und er sieht sofort die Ergebnisse der Tiefenscans, die Orca durchführt."

„Mit einer vollständigen Compliance-Ansicht kann der Entwickler fragen: ‚Habe ich einige Sicherheitseinstellungen in Amazon verpasst, die sich auf meine Sicherheitslage auswirken können?' Er sieht sofort, dass er dies konfigurieren, das aktivieren, dies verwenden oder das tun muss. Orca aktualisiert auch die Compliance. Selbst wenn keine Schwachstelle gefunden wird, gibt uns das allein schon so viele Informationen, dass wir keine Sicherheitsfirma brauchen, die uns sagt, was zu tun ist. Orca sagt uns, was wir tun müssen und wie wir es tun sollen", sagt Geirnaert.

> „Orca ermöglicht es uns, unterschiedlichen Benutzern Zugang zu verschiedenen Rollen zu geben. Der CISO ist an Compliance interessiert. Der Sicherheitstechniker prüft Schwachstellen und Warnungen. Der Entwickler kann anhand des Dashboards erfahren, warum etwas ein Problem ist."
>
> **Erwin Geirnaert**
> Cloud-Sicherheitsarchitekt
> NGDATA

Dies führte zur Suche nach einem Tool, das sich mit der AWS-API verbinden und eine Echtzeitansicht aller NGDATA-Assets erhalten konnte. Ein solches Tool sollte kritische Schwachstellen offenlegen und zeigen, ob personenbezogene Daten oder geistiges Eigentum gefährdet sind. Auf dieser Suche fand Geirnaert Orca Security.

„Unser erster Scan mit Orca war ein echtes Aha-Erlebnis. Wir fanden Rechner, von derer Existenz wir bis dahin nicht wussten, die sensible Informationen enthielten, oder Services mit einer Anbindung an das Internet", sagt er. Mit den Erkenntnissen, die Orca liefert, richtete er tägliche Scans aller IP-Adressen und virtuellen Rechnern ein, auch wenn diese nicht mit dem Internet verbunden sind. „Wir müssen genau wissen, was wir haben, um sicherzustellen, dass die Vermögenswerte unserer Kunden – und auch das geistige Eigentum von NGDATA – geschützt sind."

Orca ist ein transformatives Tool für DevOps

Die Entwickler von NGDATA sind auf der ganzen Welt verbreitet. Geirnaert sagt: „Wir können sie nicht fragen: ‚Haben Sie über Sicherheit nachgedacht? Wenn Sie eine neue VM auf AWS starten, können Sie es mich bitte wissen lassen, damit ich sie scannen kann? Könnten Sie einen Agenten auf diesem Rechner für mich bereitstellen?' Wir brauchen eine bessere Arbeitsweise. Orca bietet diesen besseren Weg, indem diese organisatorische Reibung vollständig beseitigt wird.

„Ich glaube fest an einen DevOps-Ansatz und an eine Umstellung auf Cloud-Native und Serverless, da dies die Sicherheit erhöht, ohne dass die Entwickler zu Sicherheitsexperten ausgebildet werden müssen. Wir müssen sie mit Tools ausstatten, die sich in ihre bisherige Arbeitsweise integrieren lassen."

Vereinfachung der Einhaltung von Vorschriften und Sicherheits-Frameworks

Als Geirnaert bei NGDATA anfing, stellte er eine Liste von Best Practices zusammen, die auf dem Center for Internet Security Compliance Framework für AWS basierte. Er benutzte die 100-Punkte-Liste wie ein Projektmanagement-Tool, um Aufgaben zuzuweisen. Er braucht die Liste nicht mehr.

„Wenn wir Orca starten, prüft es dynamisch auf Compliance-Anforderungen. Vor Orca haben wir solche Kontrollen in Sumo Logic selbst geschrieben. Wenn wir uns die Ereignisse aus der AWS-CloudTrail-Protokollierung ansahen, konnten wir sie erfassen und in den Dashboards anzeigen. Jetzt sehen wir alles automatisch und sofort in einem einzigen Orca-Dashboard."

Die Einhaltung der DSGVO wird erleichtert, da Orca nach personenbezogenen Daten auf Servern und in Dateien sucht. Orca hilft dabei, versteckte personenbezogene Daten zu finden und zeigt Orte auf, an denen personenbezogene Daten erwartet werden. Als Sicherheitsexperte hat Geirnaert keinen Zugang zu Produktionsumgebungen, sodass er mit Orca einen Einblick erhält, den er normalerweise nicht hätte. In Bezug auf personenbezogene Daten hilft dies, Probleme zu beheben oder abzuschwächen.

Orca vereinfacht auch den Auditprozess. „Wir können ganz einfach filtern, um zu zeigen, wo personenbezogene Daten gespeichert sind. Da alles dokumentiert ist, können wir die von den Auditoren geforderten Nachweise problemlos vorlegen", sagt Geirnaert.



Über Orca Security

Mit seiner einzigartigen, zum Patent angemeldeten SideScanning™-Technologie bietet Orca Security cloudumfassende, workloadintensive Sicherheit und Compliance für AWS, Azure und GCP. Nach einer sofortigen, nur Lesegriff zulassenden und folgenlosen Integration in den Cloud-Provider erkennt es Schwachstellen, Malware, Fehlkonfigurationen, Risiken durch Seitwärtsbewegungen, Authentifizierungsrisiken und unsichere Daten mit hohem Risiko und priorisiert das Risiko auf der Grundlage des zugrunde liegenden Problems, seiner Zugänglichkeit und des Explosionsradius – ohne Einsatz von Agenten.

orca security

Verbinden Sie Ihr erstes Cloud-Konto in wenigen Minuten und überzeugen Sie sich selbst: Besuchen Sie orca.security

© Copyright Orca Security 2021. Alle in diesem Material genannten Marken, Dienstleistungsmarken und Handelsnamen sind Eigentum ihrer jeweiligen Inhaber.