Cómo los pilares de Observabilidad de Datadog potencian DevSecOps

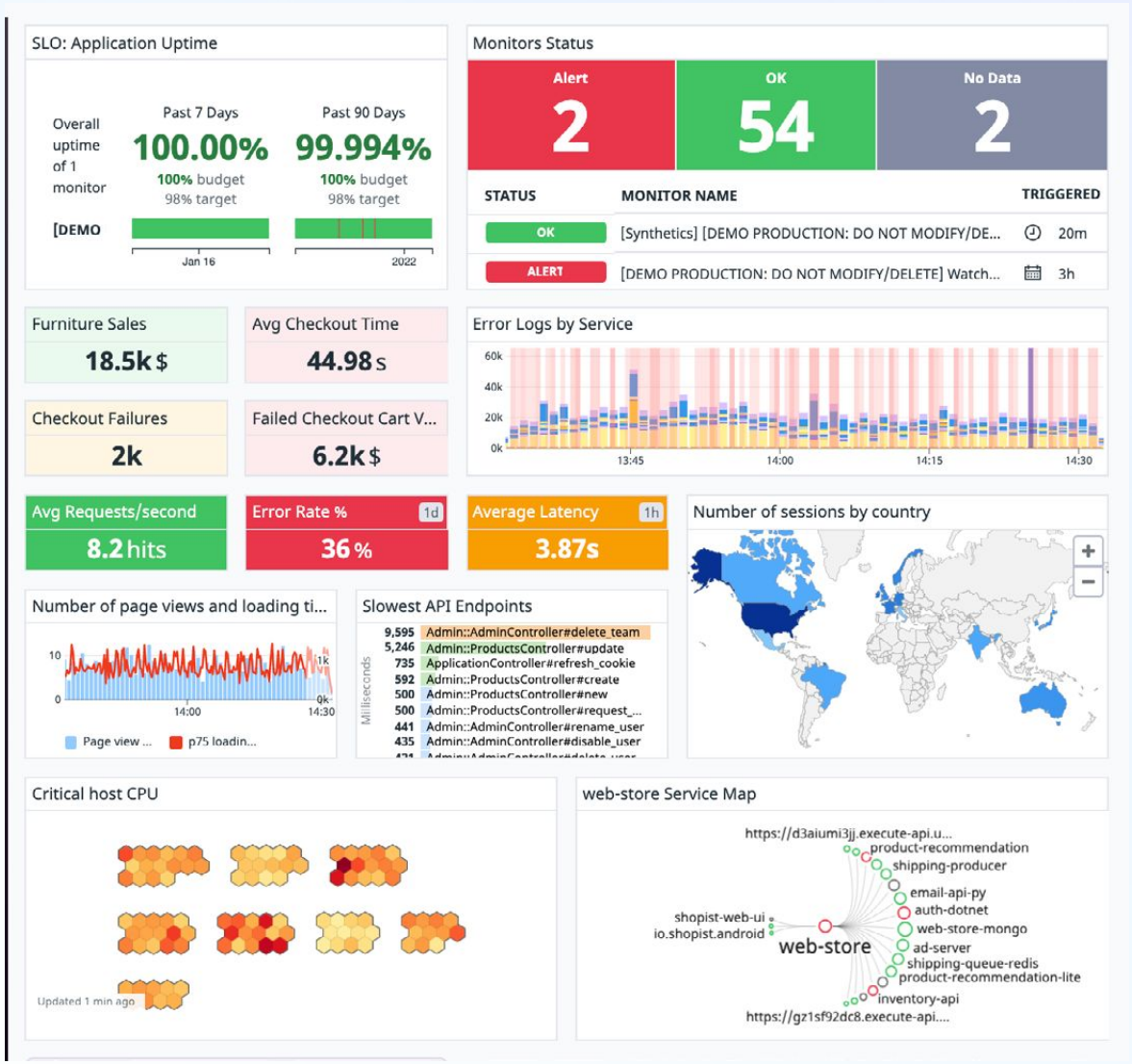
epidata
deploying ideas

Carlos Paz Soldán

GOLD DATADOG PARTNER

Tales Casagrande

DEFINICIÓN DE OBSERVABILIDAD



¿Qué es la Observabilidad?

Observabilidad es tener una visión completa del comportamiento de nuestros sistemas a través de métricas, registros, correlaciones y trazas. Permite comprender descriptivamente y predictivamente el funcionamiento interno y resolver problemas de manera más efectiva.

CARACTERÍSTICAS DE UNA PLATAFORMA DE OBSERVABILIDAD

epidata
deploying ideas

Fuente Única de Confianza

Recopilar y analizar múltiples tipos de datos de telemetría de diversas fuentes en un solo entorno

Escalabilidad

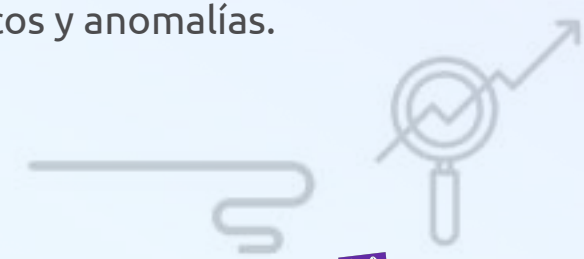
Adaptar el hecho de que los hosts, aplicaciones y dispositivos individuales escalan con expansión o contracción

Agregacíon Integrada

Etiquetas permiten a los ingenieros segmentar y agregar métricas a nivel de servicio

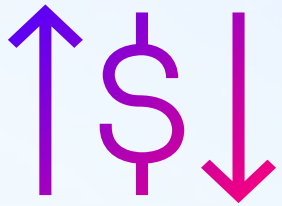
Colaboración y alertas

Descubrir y corregir el problema lo más rápido posible. Alertas de cambios relativos y automatizadas. Detección de valores atípicos y anomalías.

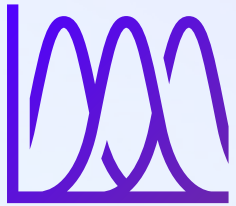


DATADOG

Beneficios

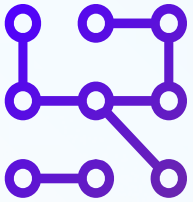


Operación y rentabilidad



Visibilidad de los problemas de rendimiento

Tiempo medio de detección y resolución más rápido



Más visibilidad del flujo de información.

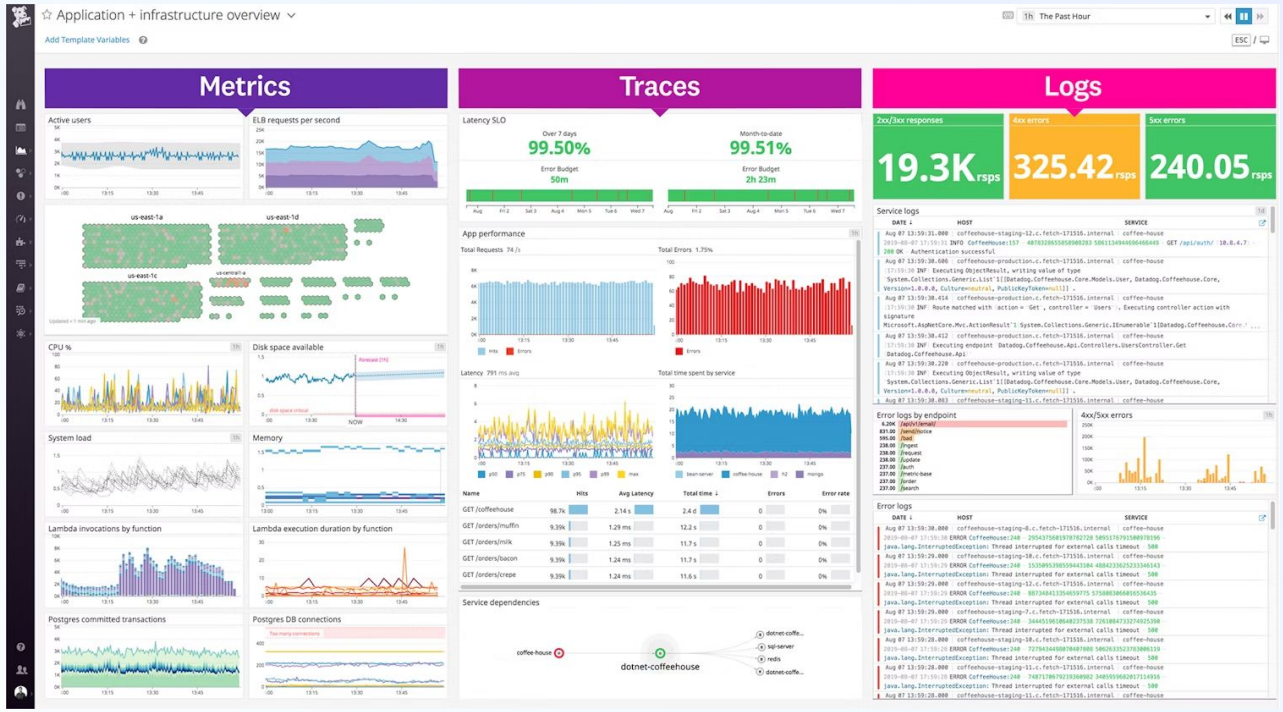
Extraiga más valor de una única plataforma correlacionada e integrada

Mayor cobertura ambiental para lograr observabilidad

DATADOG

DATADOG

PILARES DE LA OBSERVABILIDAD



Tras recopilar esta telemetría, la plataforma de observabilidad la correlaciona en tiempo real para proporcionar a los equipos de Ops, **DevOps**, Dev y al personal de TI información contextual y completa: el qué, el dónde y el porqué de los sucesos en ecosistemas de IT

Métricas

Las métricas, métricas de serie temporal, son medidas fundamentales de la salud del sistema y las aplicaciones durante un período de tiempo determinado, como por ejemplo la cantidad de capacidad de CPU, memoria que utiliza una aplicación durante un lapso de cinco minutos, o la latencia de uso de una aplicación durante un pico

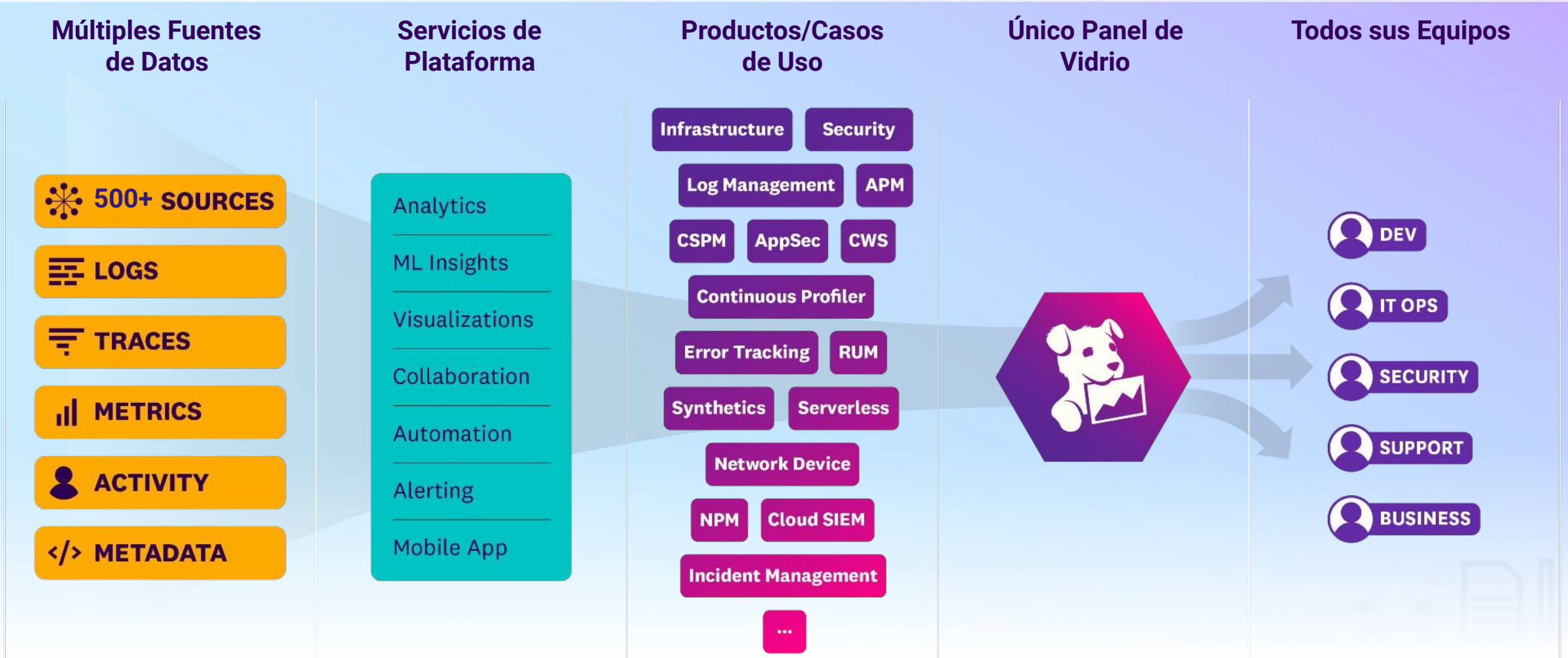
Registros

Los registros son granulares, con marca de tiempo, completos e inmutables de sucesos de aplicaciones. Los registros se pueden usar para crear una alta fidelidad, milisegundo por milisegundo, de cada suceso, y completarlo con el contexto circundante, que permite "reproducir" con fines de resolución de problemas y depuración.

Trazas

Las trazas siguen el recorrido de una solicitud a través de los diferentes componentes de nuestro sistema.
Registran el "trayecto" de cada solicitud de usuario de principio a fin, desde la IU o la aplicación móvil hasta que vuelve al usuario, pasando por toda la arquitectura distribuida.

Plataforma SaaS unificada de observabilidad y seguridad



DevSecOps Day

¡Protegiendo las aplicaciones que ya ves!

DATADOG

Tales Casagrande

Security Engineer, Datadog

DATADOG

Agenda

01 Quienes somos

02 Algunos conceptos

03 Problemas y desafíos

04 Protección en tiempo de ejecución

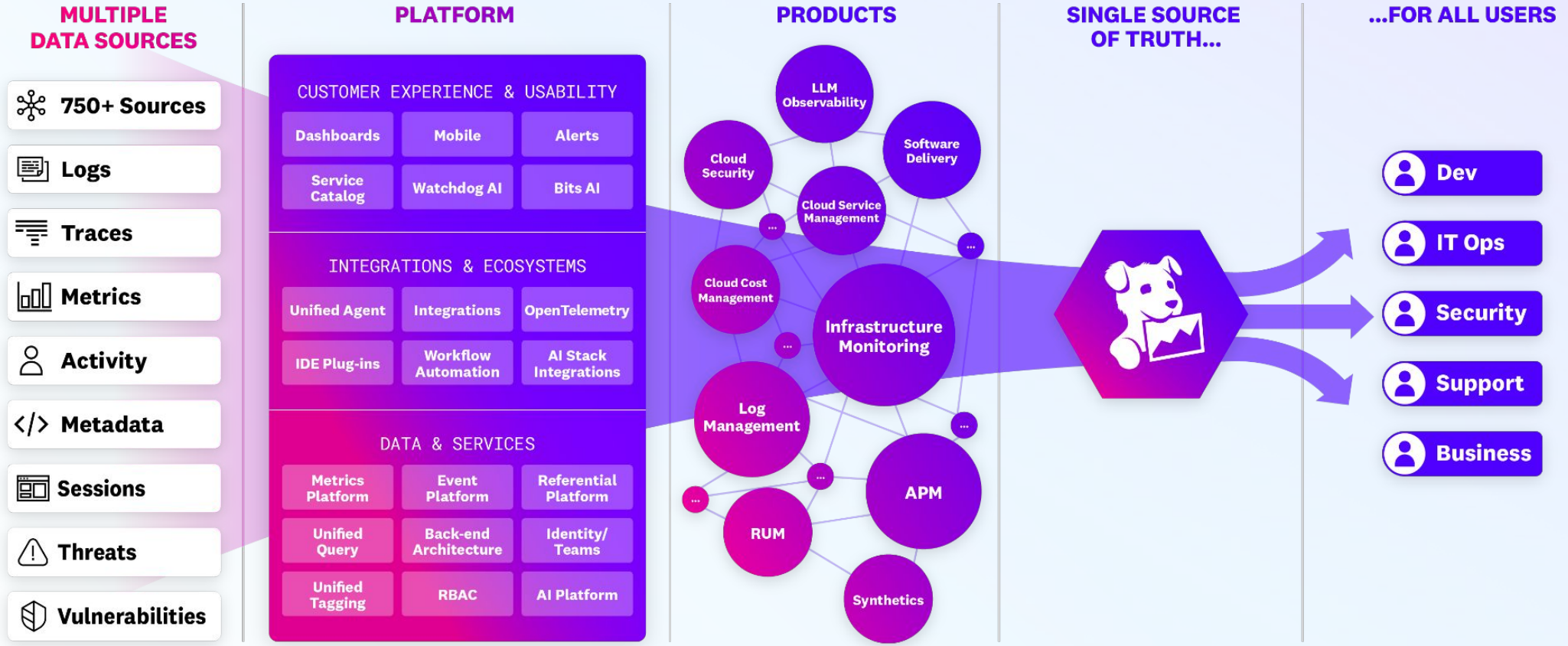
05 DEMO

06 Cierre

DATADOG

Quienes somos

Rompiendo silos con nuestra plataforma unificada



DATADOG

CNAPP + AppSec + SIEM en una sola plataforma

Application Security

- Software Composition Analysis — SCA
- Code Security — IAST
- Code Quality BETA — SAST
- Application and API Protection
  - Serverless Security
  - Account & Business Logic Protection — ATO
  - API Security

Cloud Security Management

- Cloud Security Posture Management — CSPM
- Cloud Infrastructure Entitlement Management — CIEM
- Kubernetes Security Posture Management — KSPM
- Container and Host Vulnerabilities — VM
- Agentless Scanning
- Cloud Workload Security — CWPP
- File Integrity Monitoring — FIM

Cloud SIEM

- Content Packs and 700+ Integrations
- Security Log Ingestion and Retention
- Real-time Threat Detection
- Historical Detection Engine
- Investigations with BitsAI
- Graph-based Investigator
- Historical Investigations
- Risk-Prioritized Entity Insights

Maturity DevSecOps self-assessment by Datadog

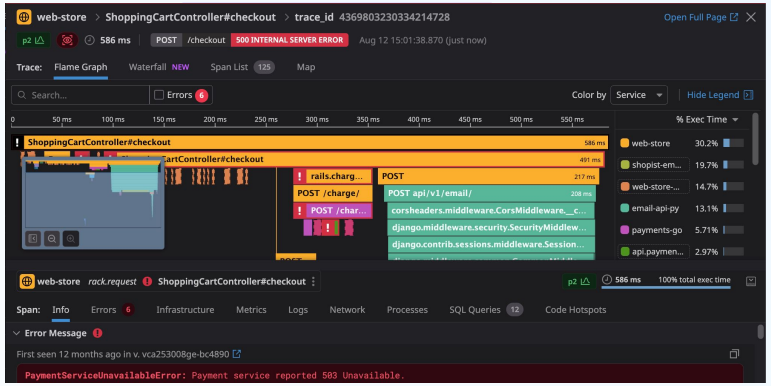
Shared Remediation, Investigation and Response Services
Integrations • Threat Intelligence • Security Labs • Case Management • Incident Management • Security Workflows

Collaboration with a Security Observability Platform
Correlations • Resource Catalog • Service Catalog • Dashboards • IDE Plugin

DATADOG

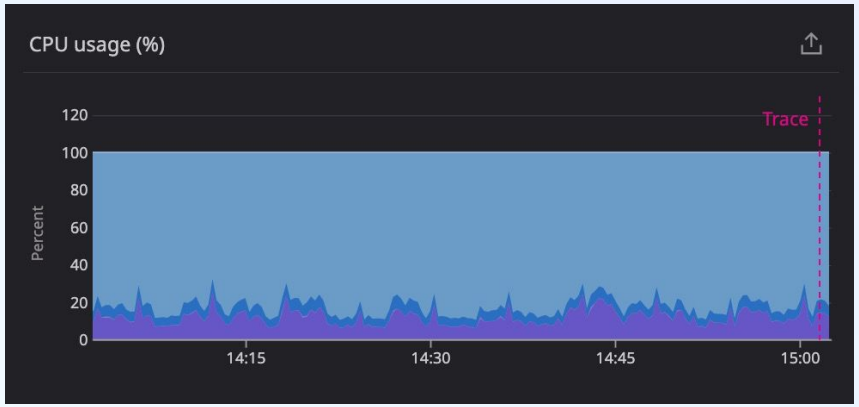
Cuando hablamos de Observabilidad pensamos en

Tracas



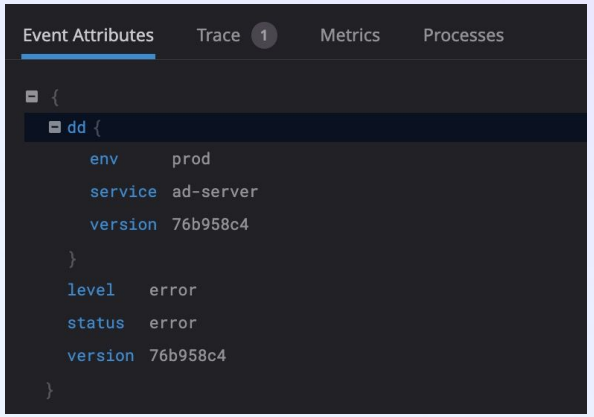
Vista continua del rendimiento de su aplicación y seguimiento de qué servicios se están ejecutando.

Metrica



Las métricas son valores numéricos que pueden rastrear cualquier cosa sobre su entorno.

Log

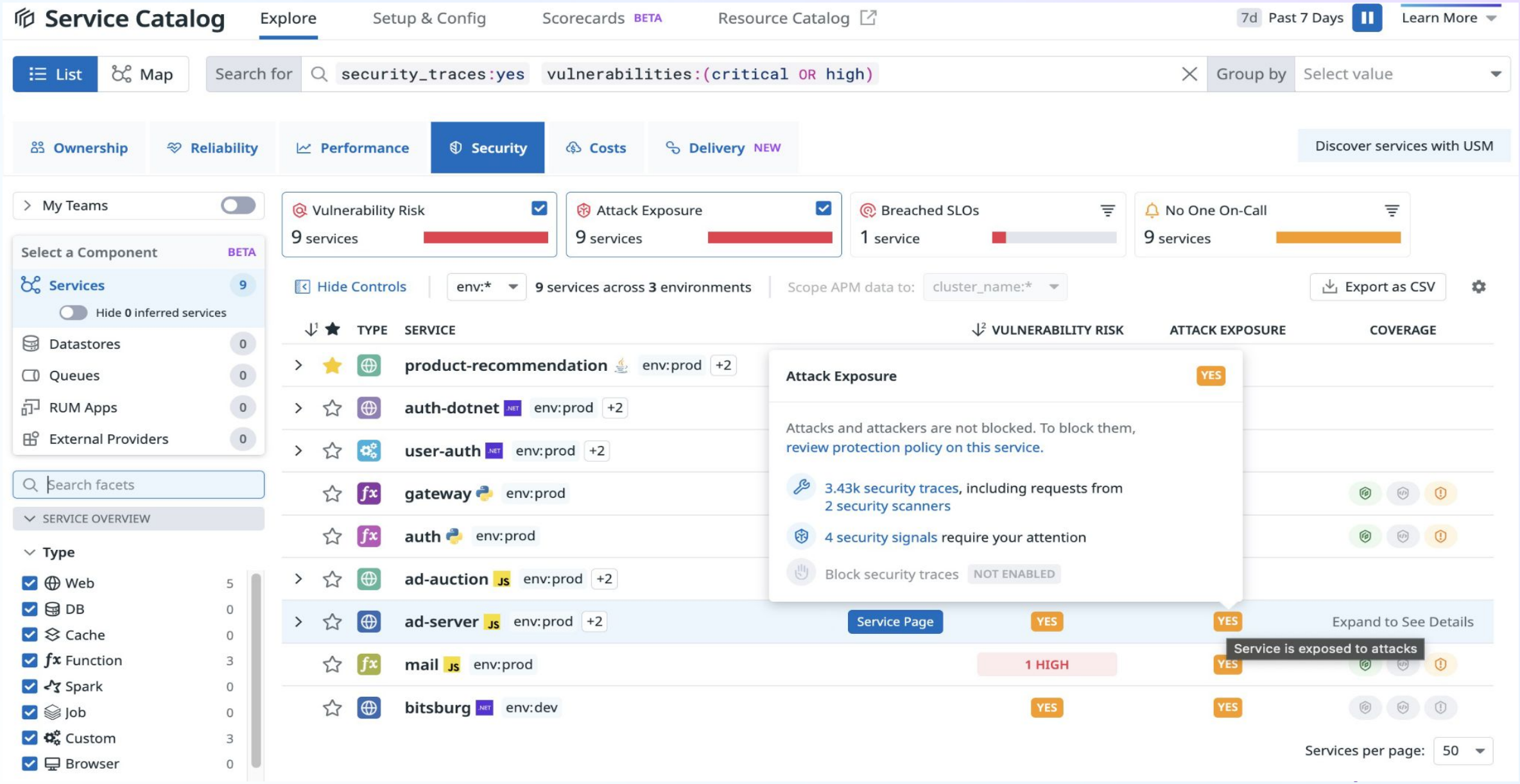


Estos son archivos generados por sistemas que almacenan información sobre todas las acciones.

Fonte: https://www.datadoghq.com/three-pillars-of-observability/

DATADOG

¿Dónde entra la seguridad?

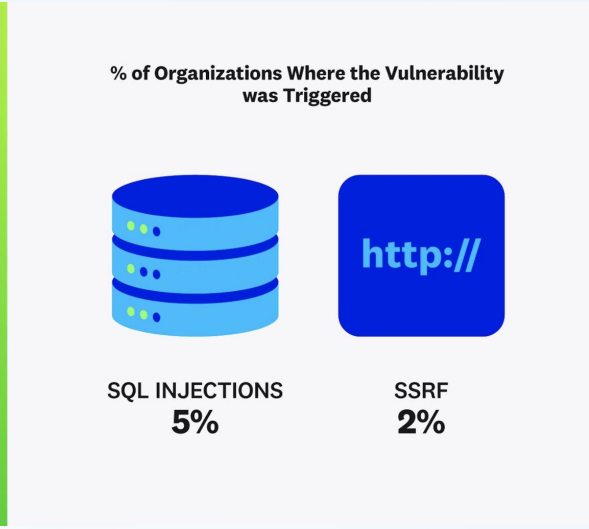


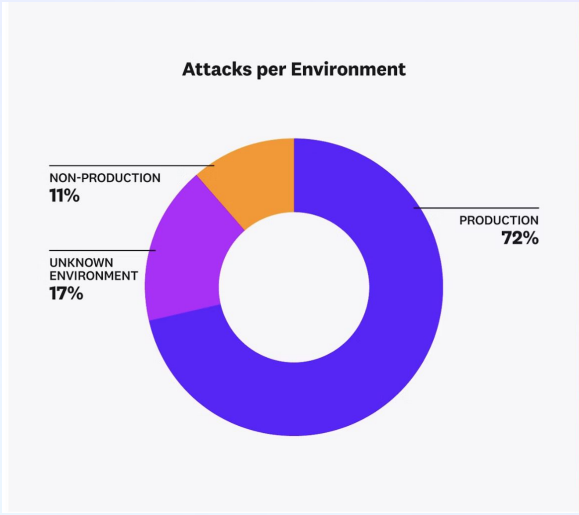
Problemas y desafíos

State of Application Security

ORGANIZATIONS STILL FACE VULNERABILITIES DISCOVERED IN THE '90S

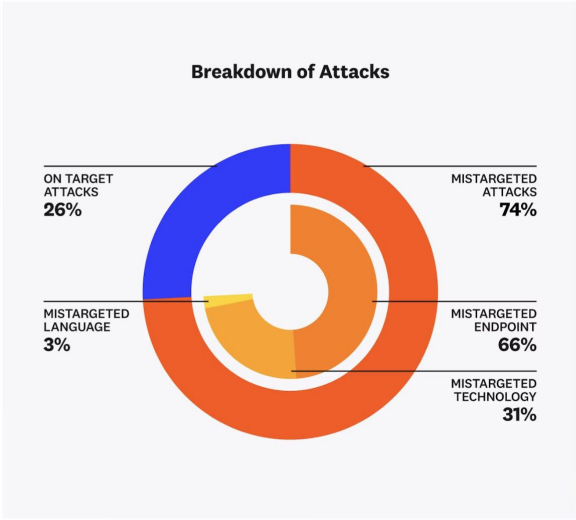
Source: Datadog





AT LEAST 11% OF ATTACKS TARGET NON-PRODUCTION ENVIRONMENTS, A POTENTIALLY NEGLECTED ATTACK SURFACE

Source: Datadog

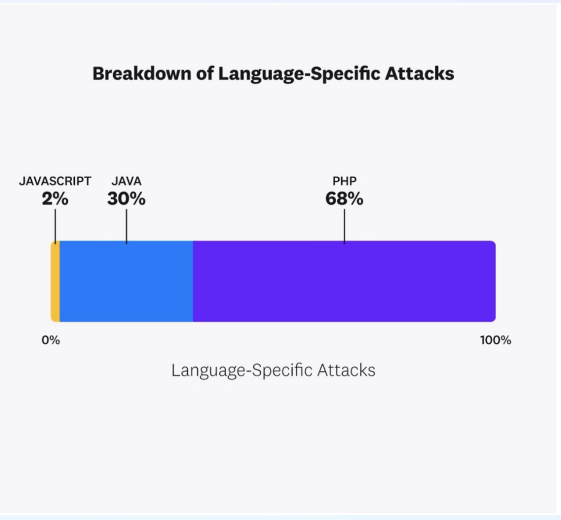


74% OF ATTACKS ARE MISTARGETED, FOR A HANDFUL OF REASONS

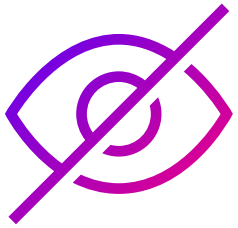
Source: Datadog

PHP IS THE TOP TARGET OF LANGUAGE-SPECIFIC ATTACKS

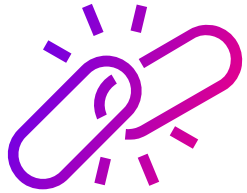
Source: Datadog



¿A qué desafíos se enfrentan las empresas?



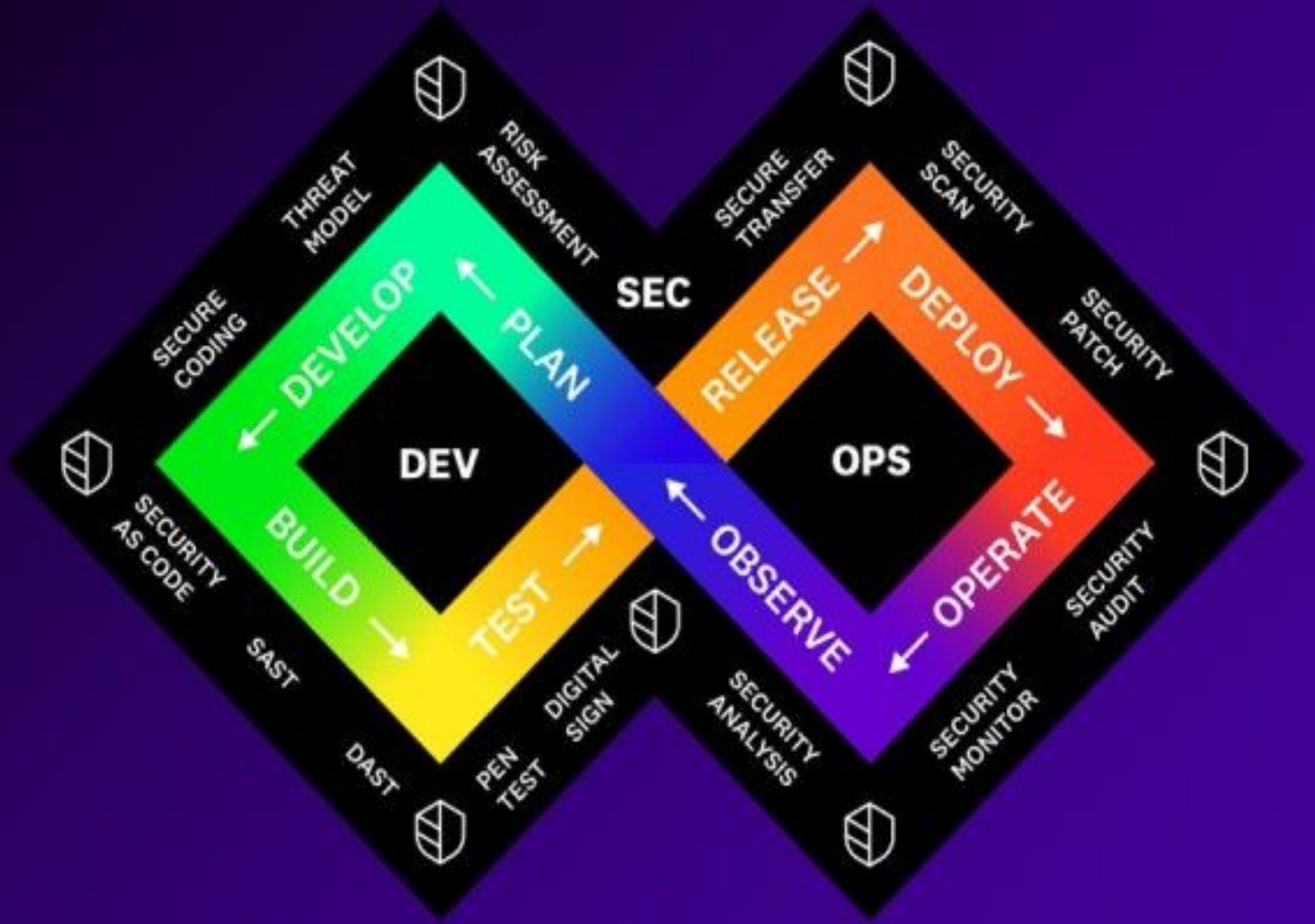
No hay visibilidad si la aplicación está bajo un ataque grave



No hay conexión entre el ataque y el código objetivo

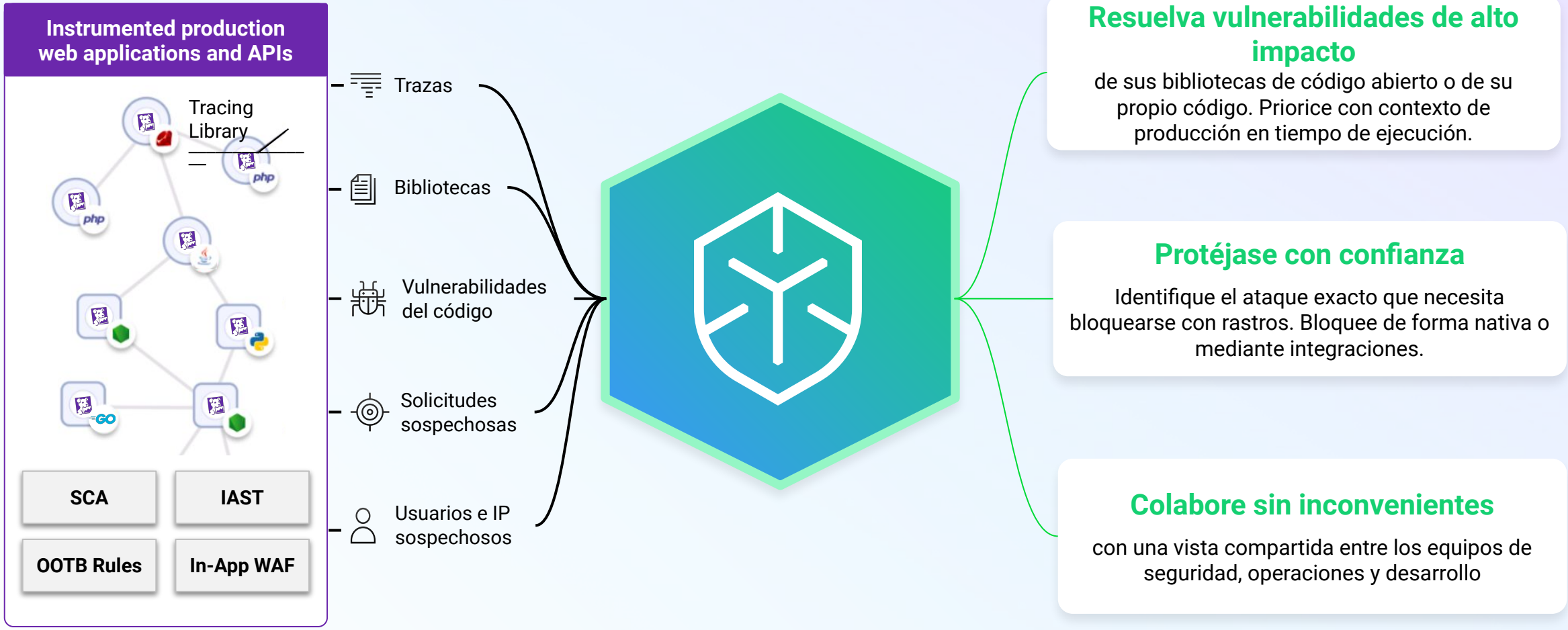
La respuesta y la remediación son lentas y costosas

cuando tenemos una aplicación sufriendo ataques y necesitamos protegerla


THREAT MODEL
RISK ASSESSMENT
SECURE CODING
SECURITY AS CODE
SAST
DAST
PEN TEST
DIGITAL SIGN
SECURITY ANALYSIS
SECURE TRANSFER
SECURITY SCAN
SECURITY PATCH
SECURITY AUDIT
SECURITY MONITOR
SEC
DEVELOP
PLAN
BUILD
TEST
RELEASE
DEPLOY
OPERATE
OBSERVE
DEV
OPS

¿Qué es Datadog ASM?

La autoprotección de aplicaciones en tiempo de ejecución es una tecnología vinculada a una aplicación (contenedor, sin servidor, monolítica) que ayuda a prevenir y detectar ataques en tiempo real.



Resuelva vulnerabilidades de alto impacto

de sus bibliotecas de código abierto o de su propio código. Priorice con contexto de producción en tiempo de ejecución.

Protéjase con confianza

Identifique el ataque exacto que necesita bloquearse con rastros. Bloquee de forma nativa o mediante integraciones.

Colabore sin inconvenientes

con una vista compartida entre los equipos de seguridad, operaciones y desarrollo

DATADOG

Solución de seguridad de aplicaciones todo en uno

Detección y protección de amenazas de aplicaciones y API

Detecta ataques OWASP en tiempo real contra tus aplicaciones

Responda a los ataques en tiempo real para proteger sus aplicaciones

+

Gestión de riesgos de aplicaciones

Detecta vulnerabilidades en tu aplicación (OSS, código personalizado)

Encuentre, priorice y solucione vulnerabilidades fácilmente

→

Application Security Management

Fomentar una cultura de propiedad de DevSecOps

Envíe y ejecute aplicaciones seguras

DATADOG

DEMO

Es eso...

Conclusiones …

Bloquear ataques y atacantes

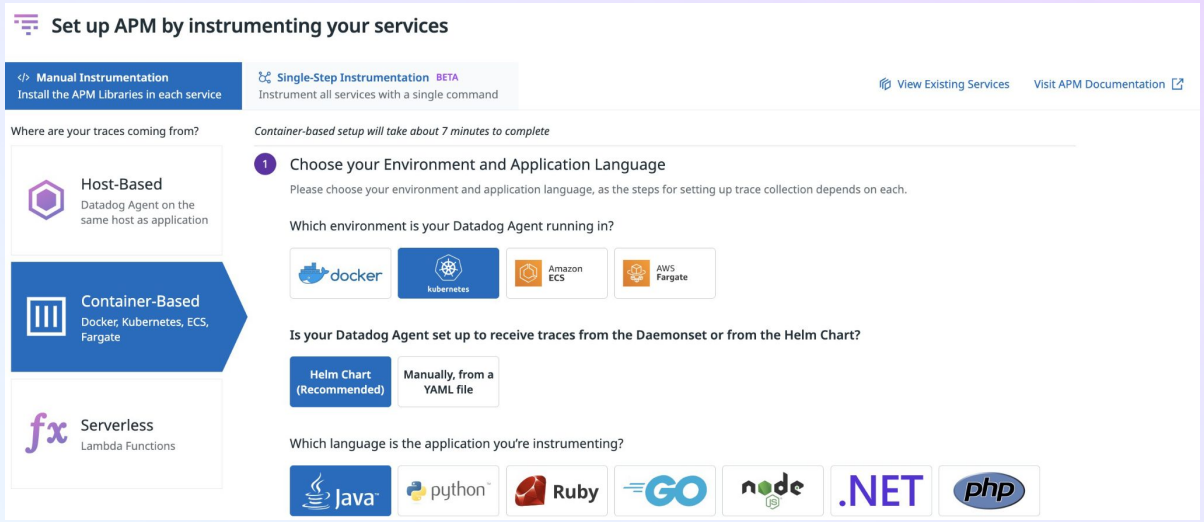
Obtenga visibilidad más allá de la IP para comprender quiénes son los actores autenticados que se dirigen a sus servicios y tomar medidas granulares

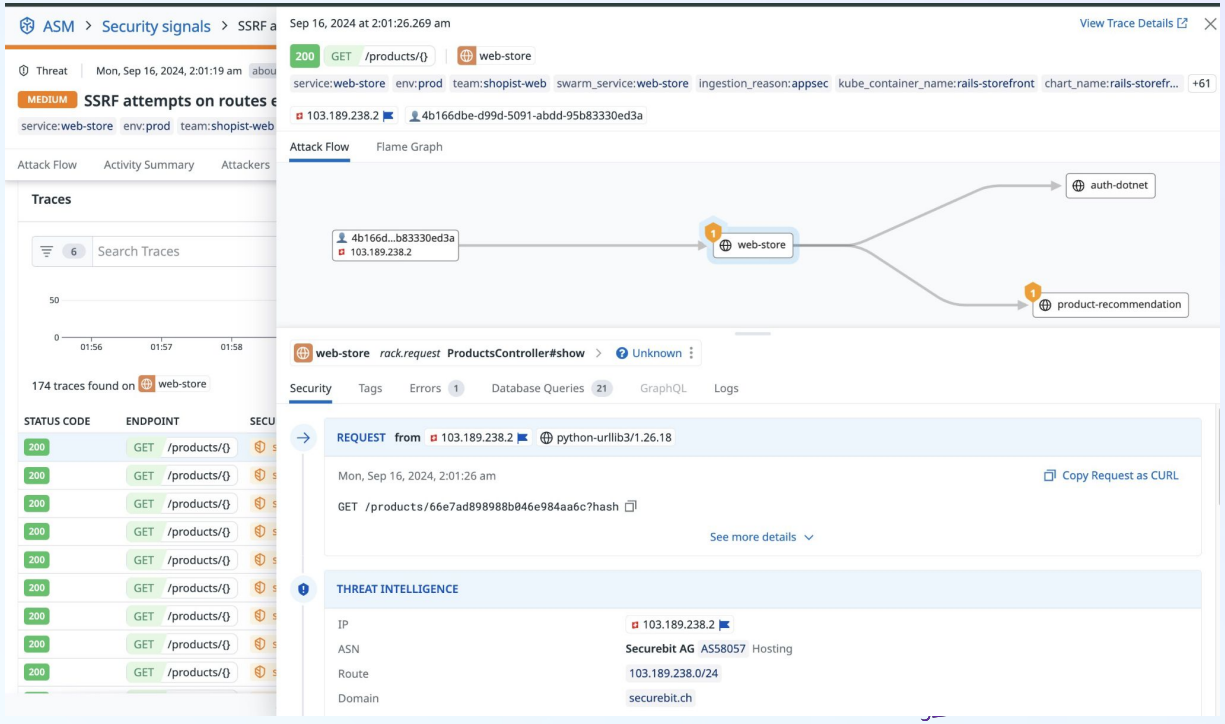
Rastrear la profundidad, impacto del ataque y reducir los riesgos

AppSec se superpone a Datadog Application Performance Monitoring (APM). Vincula la actividad de seguridad con los rastros de la aplicación para comprender si los ataques tuvieron impacto.

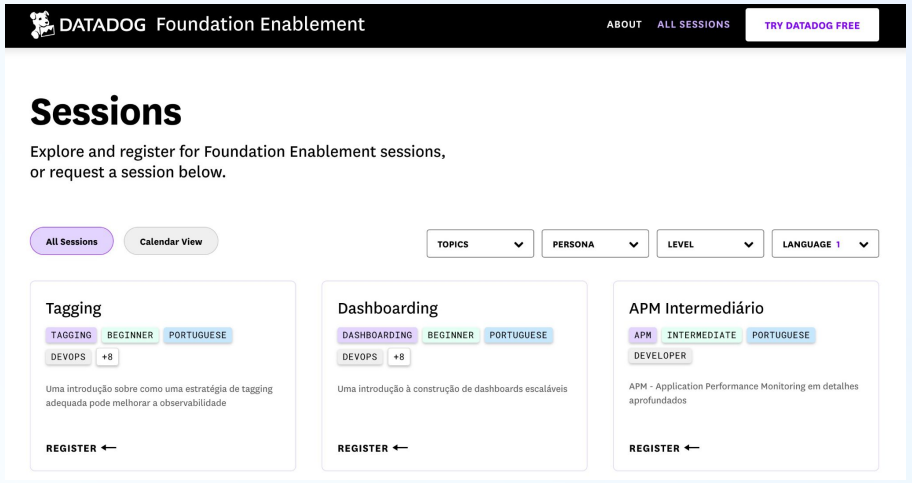
Habilite la colaboración en una plataforma unificada

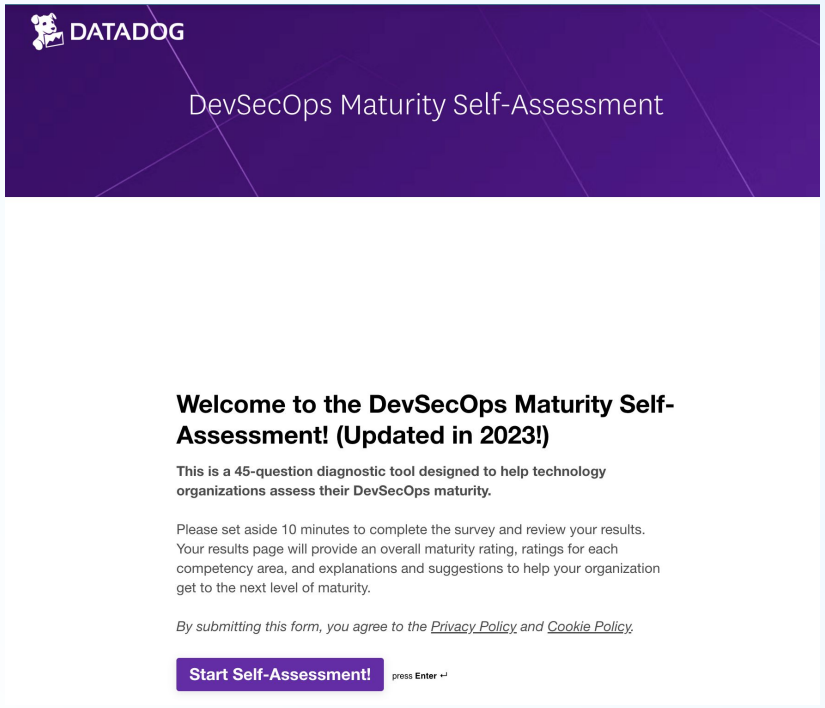
Los equipos de seguridad ahora pueden aprovechar la información a nivel de código para trabajar con los desarrolladores en función de información útil. Los ingenieros ven información de seguridad en la plataforma que ya utilizan.

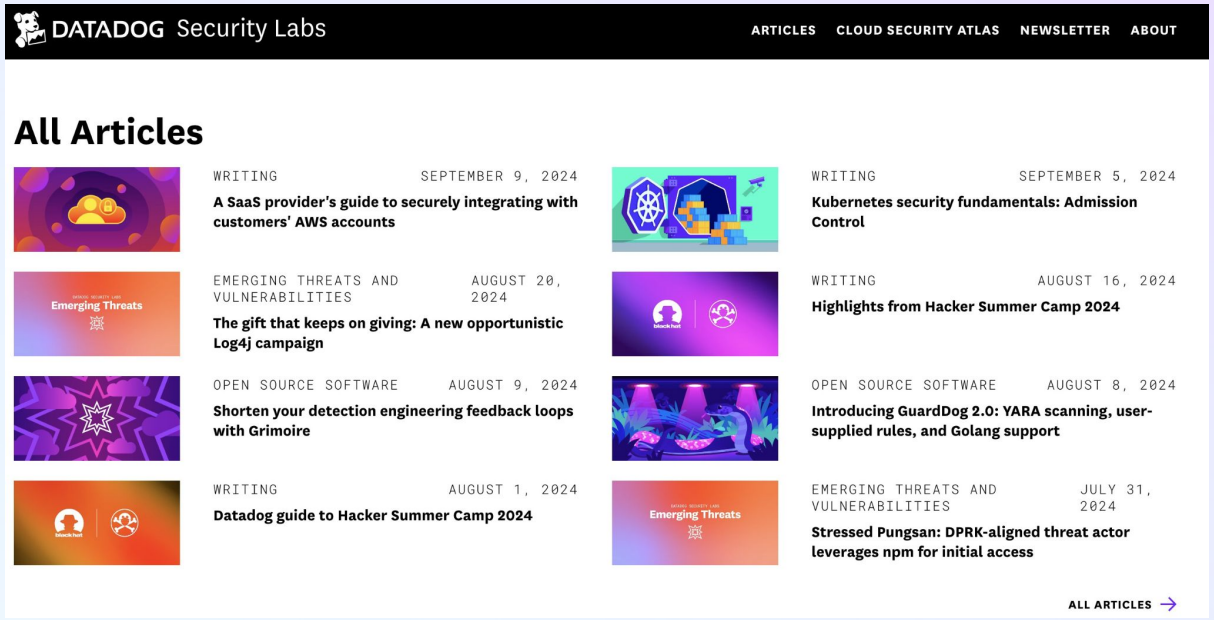


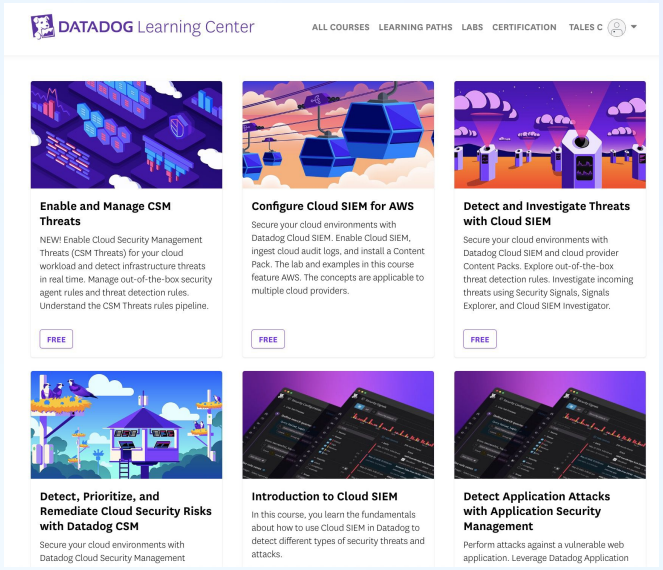


Contenido gratuito sobre Datadog









DATADOG


¡Muchas Gracias!