

Cómo los pilares de Observabilidad de Datadog potencian DevSecOps



Carlos
Paz Soldán

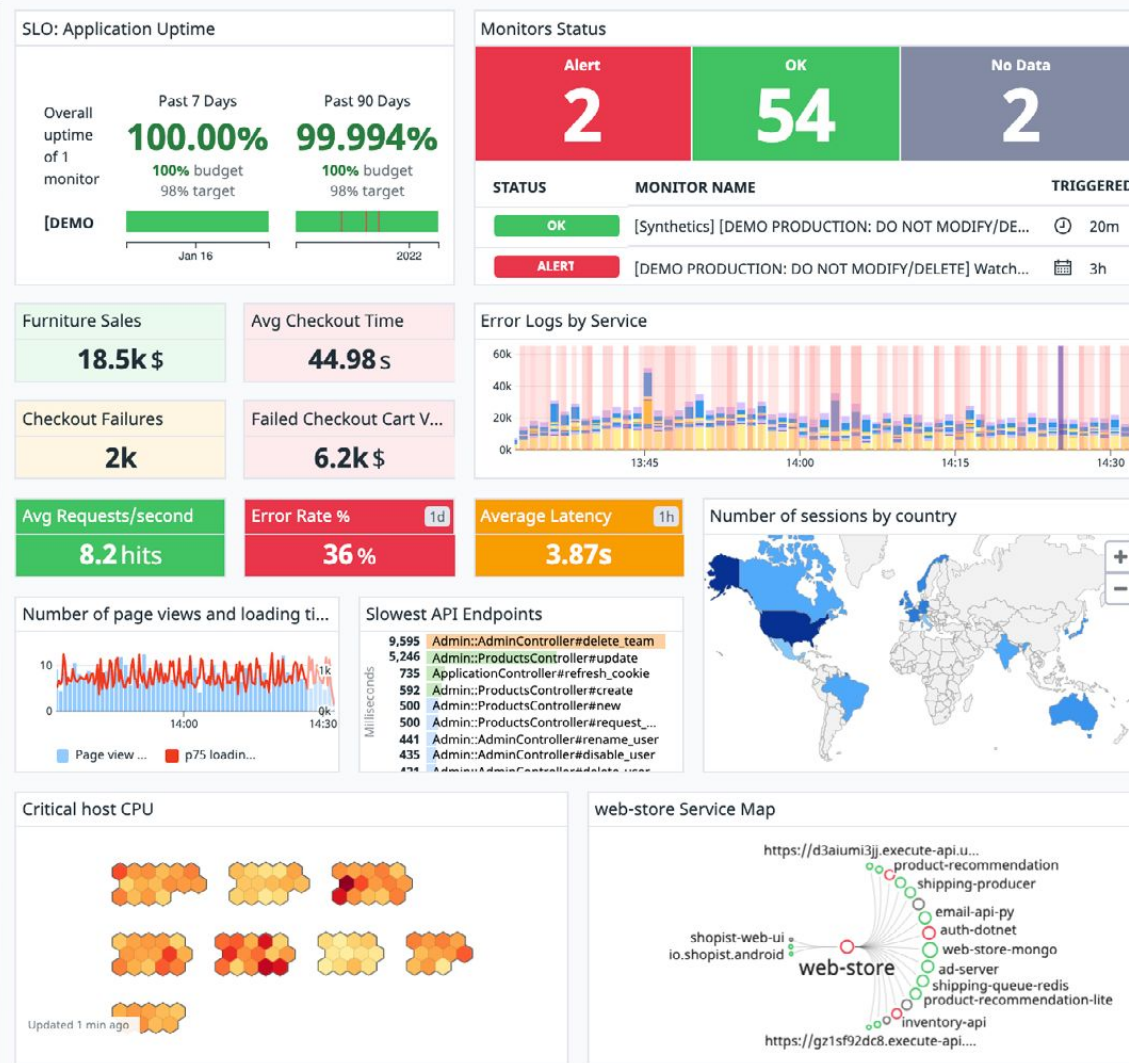


GOLD
DATADOG
PARTNER



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



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



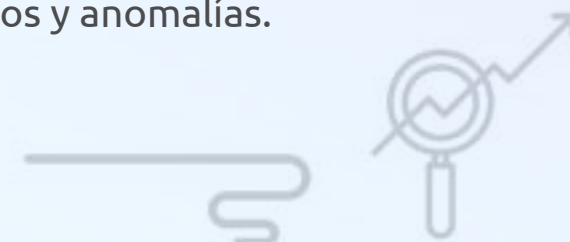
Agregación Integrada

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

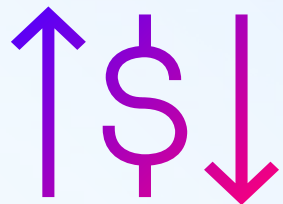


Colaboración y alertas

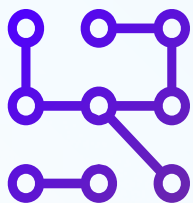
Descubrir y corregir el problema lo más rápido posible. Alertas de cambios relativos y automatizadas. Detección de valores atípicos y anomalías.



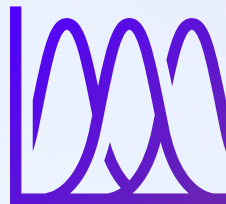
Beneficios



Operación y
rentabilidad



Más visibilidad del
flujo de
información.



Visibilidad de los
problemas de
rendimiento



Extraiga más valor de una
única plataforma
correlacionada e integrada

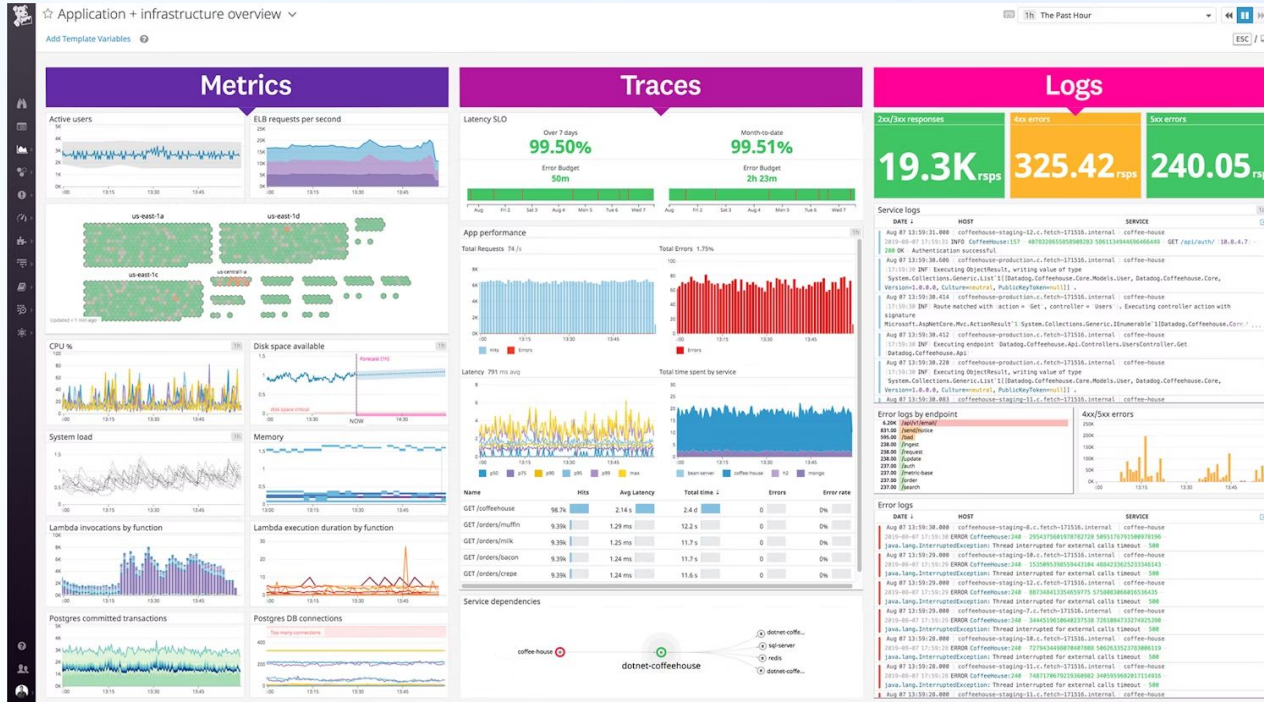


Tiempo medio de
detección y
resolución más
rápido



Mayor cobertura ambiental
para lograr observabilidad

PILARES DE LA OBSERVABILIDAD



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

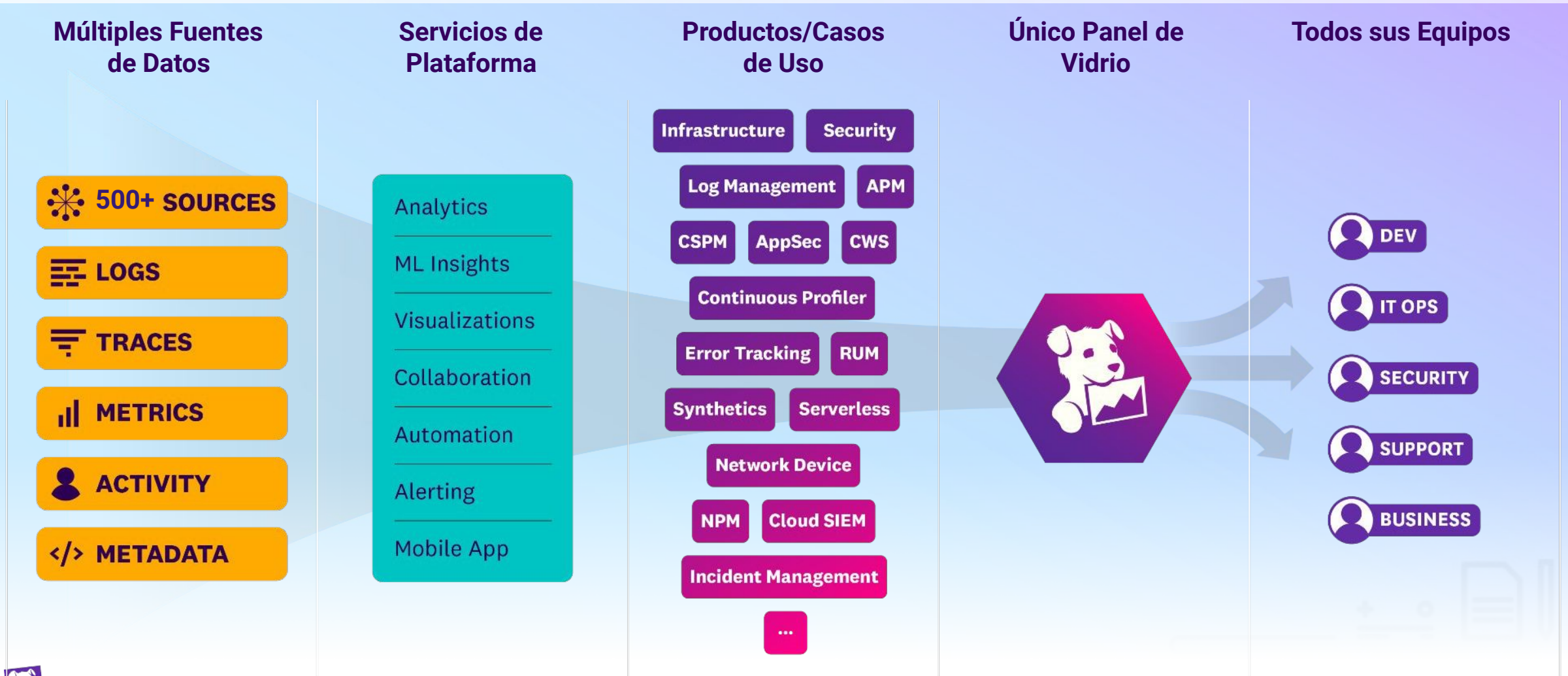
Los registros son granulares, con marca de tiempo, completos e inmutables de sucesos de aplicaciones. Los registros se pueden usar para crear una alta fidelidad, milisegundo por milisegundo, de cada suceso, y completarlo con el contexto circundante, que permite "reproducir" con fines de resolución de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

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

Plataforma SaaS unificada de observabilidad y seguridad



DevSecOps Day

¡Protegiendo las aplicaciones que ya ves!



DATADOG



Tales Casagrande

Security Engineer, Datadog



Agenda

01 Quienes somos

02 Algunos conceptos

03 Problemas y desafíos

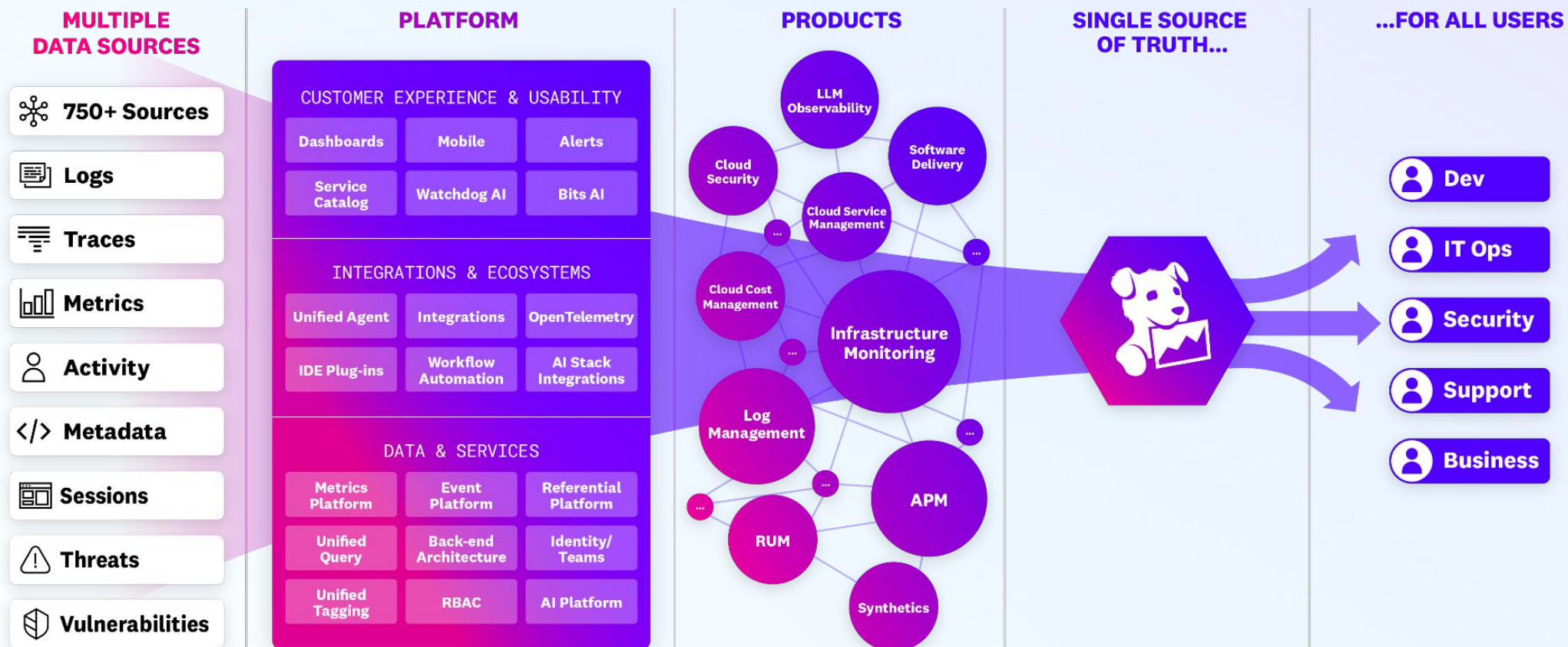
04 Protección en tiempo de ejecución

05 DEMO

06 Cierre

Quienes somos

Rompiendo silos con nuestra plataforma unificada



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

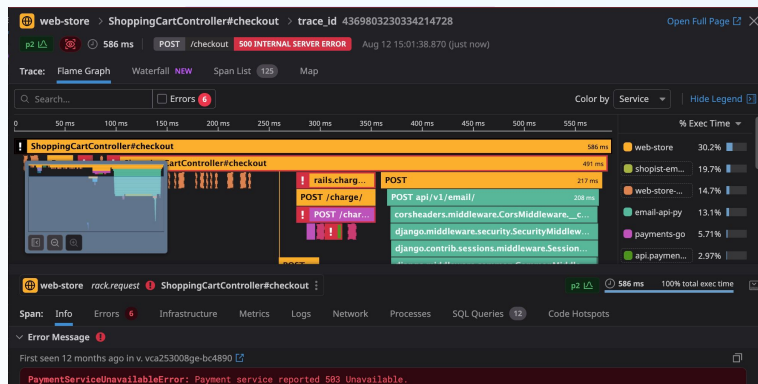
Integrations • Threat Intelligence • Security Labs • Case Management • Incident Management • Security Workflows

Collaboration with a Security Observability Platform

Correlations • Resource Catalog • Service Catalog • Dashboards • IDE Plugin

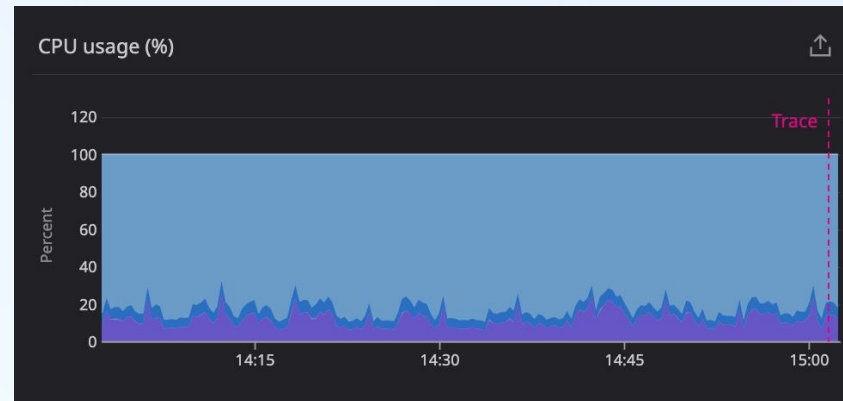
Cuando hablamos de Observabilidad pensamos en

Tracas



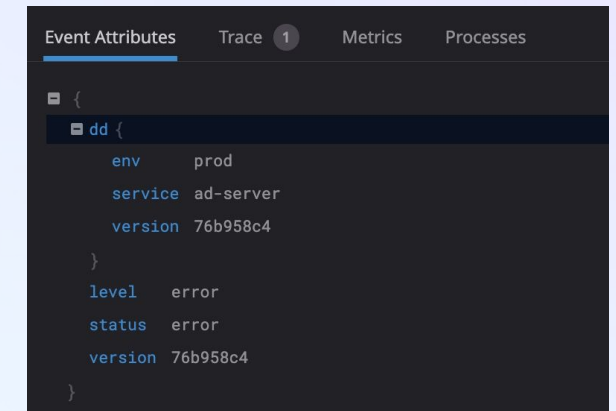
Vista continua del rendimiento de su aplicación y seguimiento de qué servicios se están ejecutando.

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.

¿Dónde entra la seguridad?

Service Catalog

[Explore](#)
[Setup & Config](#)
[Scorecards](#)
[Resource Catalog](#)

7d Past 7 Days

Learn More

List

Map

Search for

security_traces:yes vulnerabilities:(critical OR high)

Group by

Select value

Ownership

Reliability

Performance

Security

Costs

Delivery NEW

Discover services with USM

My Teams

Select a Component

Services

Hide 0 inferred services

Databases

Queues

RUM Apps

External Providers

Search facets

SERVICE OVERVIEW

Type

Web

DB

Cache

Function

Spark

Job

Custom

Browser

Vulnerability Risk

9 services

Attack Exposure

9 services

Breached SLOs

1 service

No One On-Call

9 services

Hide Controls

env:*

9 services across 3 environments

Scope APM data to:

cluster_name:*

Export as CSV

TYPE

SERVICE

VULNERABILITY RISK

ATTACK EXPOSURE

COVERAGE

product-recommendation

env:prod

+2

auth-dotnet

env:prod

+2

user-auth

env:prod

+2

gateway

env:prod

auth

env:prod

ad-auction

env:prod

+2

ad-server

env:prod

+2

mail

env:prod

bitsburg

env:dev

Attack Exposure

YES

Attacks and attackers are not blocked. To block them, review protection policy on this service.

3.43k security traces, including requests from 2 security scanners

4 security signals require your attention

Block security traces NOT ENABLED

Service Page

YES

YES

Expand to See Details

1 HIGH

YES

Service is exposed to attacks

YES

YES

Services per page:

50

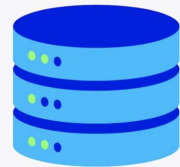
Problemas y desafíos

State of Application Security

**ORGANIZATIONS
STILL FACE
VULNERABILITIES
DISCOVERED
IN THE '90S**

Source: Datadog

% of Organizations Where the Vulnerability
was Triggered

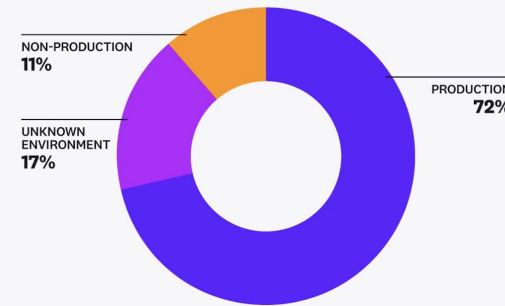


**SQL INJECTIONS
5%**



**SSRF
2%**

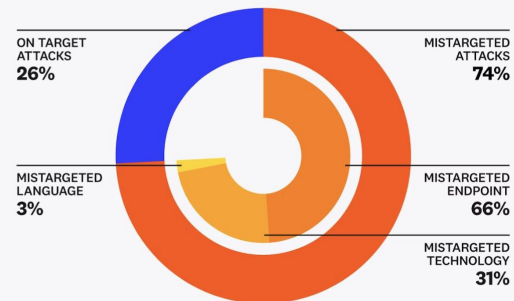
Attacks per Environment



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

Source: Datadog

Breakdown of Attacks



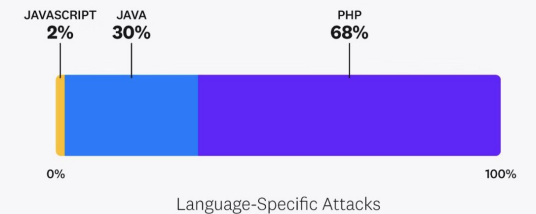
**74% OF
ATTACKS ARE
MISTARGETED,
FOR A HANDFUL
OF REASONS**

Source: Datadog

**PHP IS THE
TOP TARGET
OF LANGUAGE-
SPECIFIC
ATTACKS**

Source: Datadog

Breakdown of Language-Specific Attacks



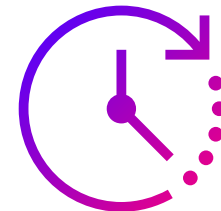
¿A qué desafíos se enfrentan las empresas?



No hay visibilidad si la aplicación está bajo un ataque grave



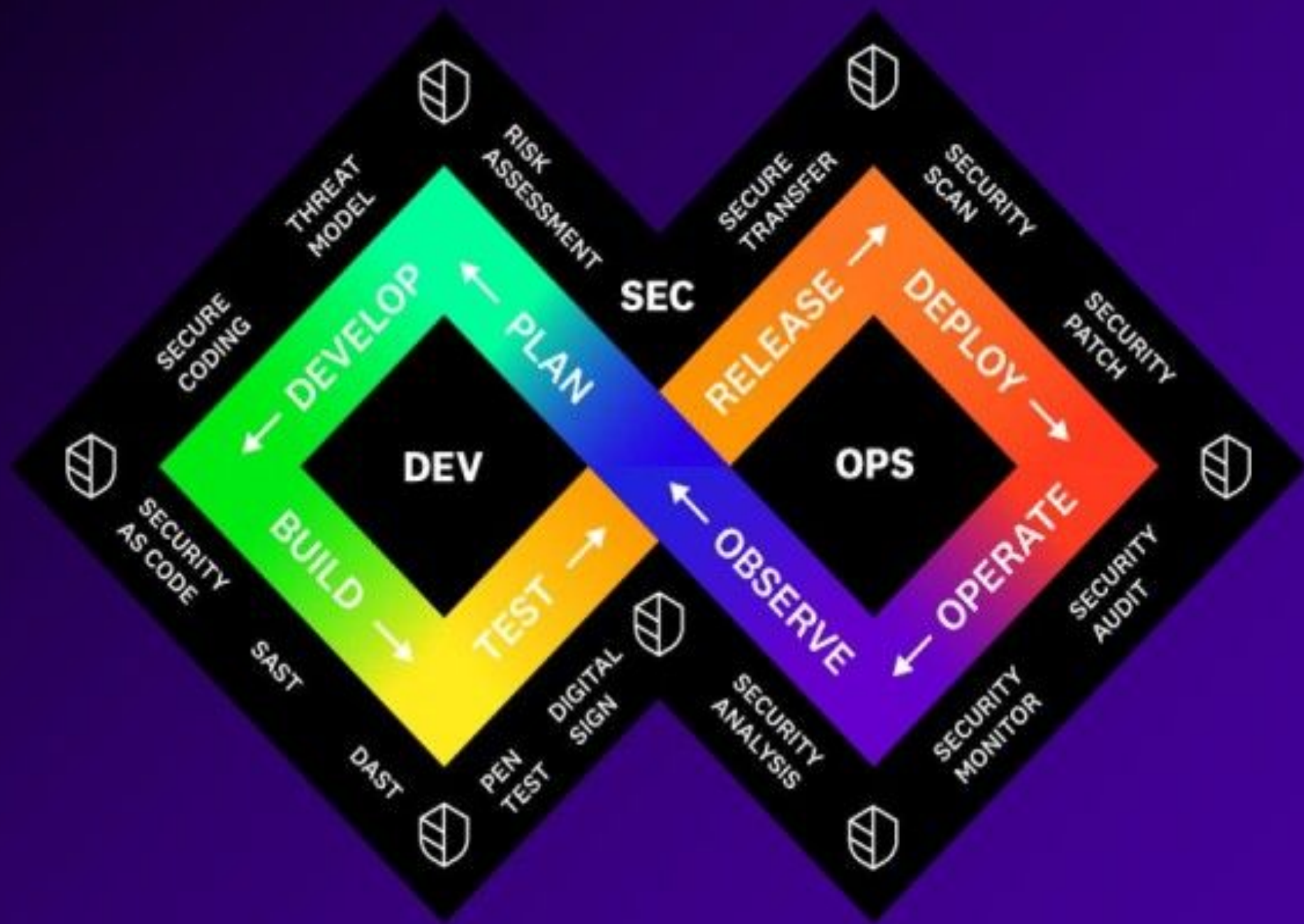
No hay conexión entre el ataque y el código objetivo



La respuesta y la remediación son lentas y costosas

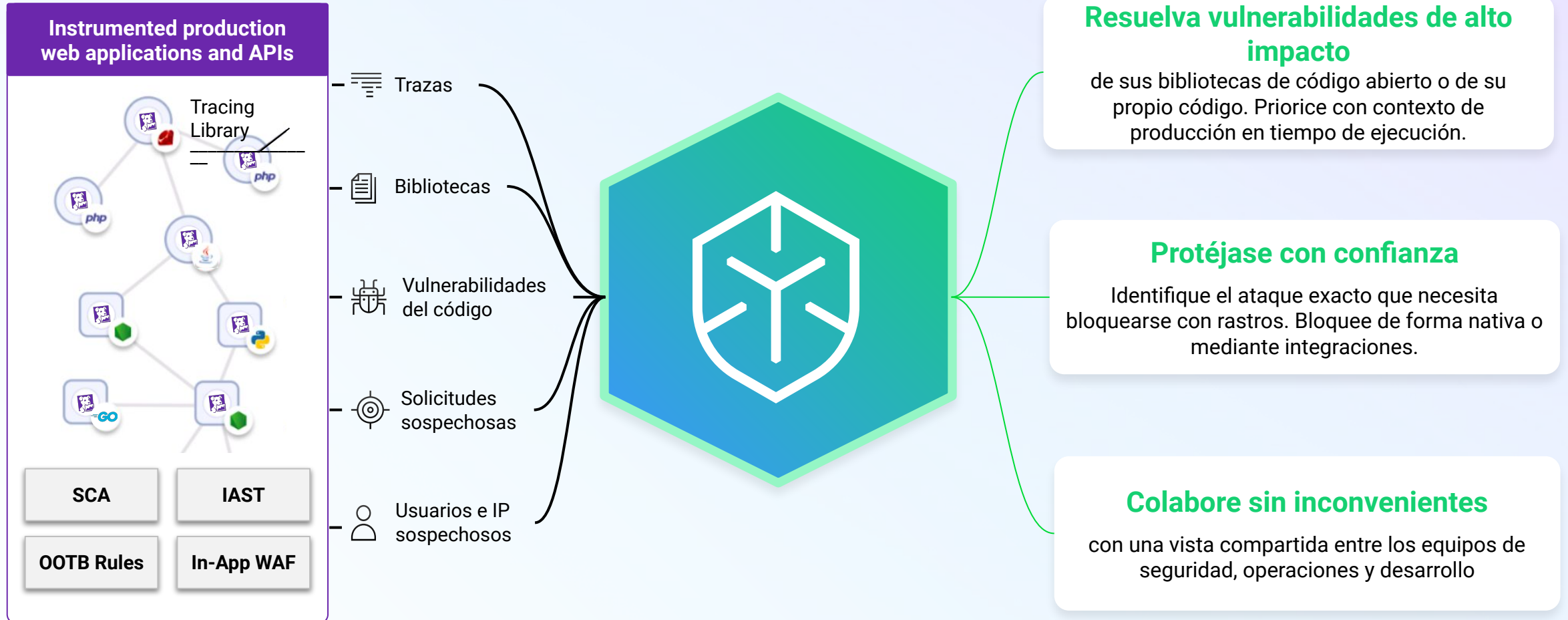


cuando tenemos una aplicación sufriendo ataques y necesitamos protegerla



¿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.



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

DEMO

Es eso...

Conclusiones ...

Bloquear ataques y atacantes

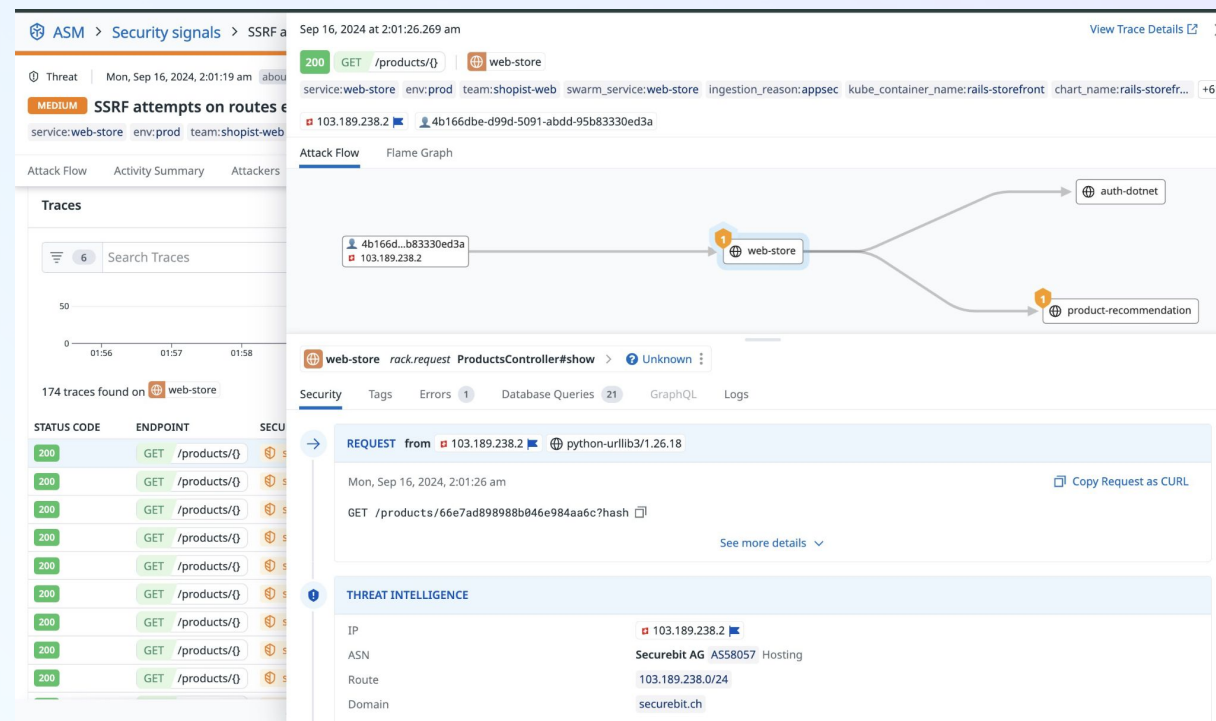
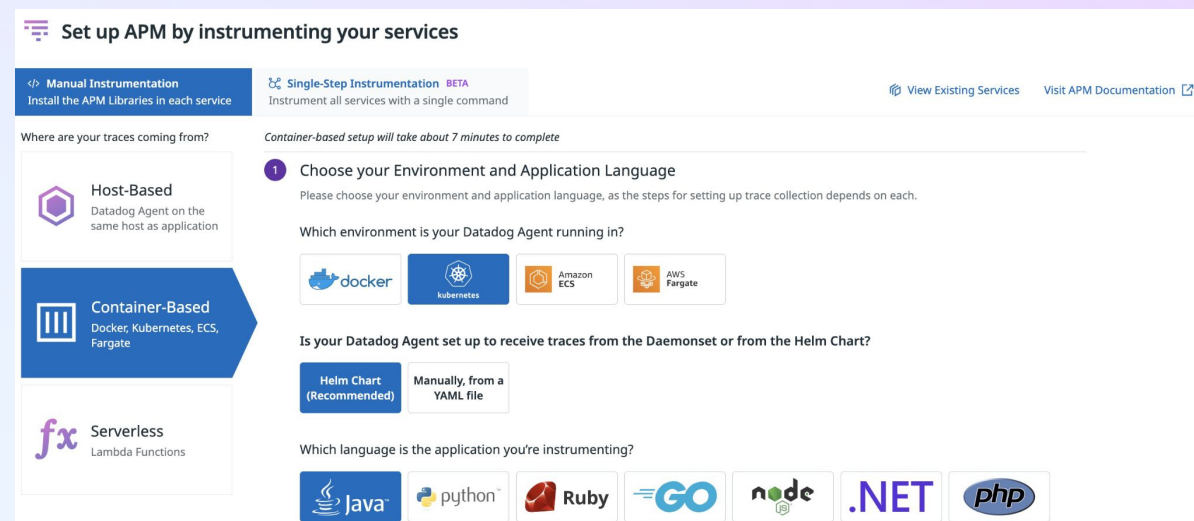
Obtenga visibilidad más allá de la IP para comprender quiénes son los actores autenticados que se dirigen a sus servicios y tomar medidas granulares

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

Sessions

Explore and register for Foundation Enablement sessions, or request a session below.

All Sessions

Calendar View

TOPICS

PERSONA

LEVEL

LANGUAGE 1

Tagging

[TAGGING](#) [BEGINNER](#) [PORTUGUESE](#)
[DEVOPS](#) +8

Uma introdução sobre como uma estratégia de tagging adequada pode melhorar a observabilidade

REGISTER

Dashboarding

[DASHBOARDING](#) [BEGINNER](#) [PORTUGUESE](#)
[DEVOPS](#) +8

Uma introdução à construção de dashboards escaláveis

REGISTER

APM Intermediário

[APM](#) [INTERMEDIATE](#) [PORTUGUESE](#)
[DEVELOPER](#)

APM - Application Performance Monitoring em detalhes aprofundados

REGISTER



DevSecOps Maturity Self-Assessment

Welcome to the DevSecOps Maturity Self-Assessment! (Updated in 2023!)

This is a 45-question diagnostic tool designed to help technology organizations assess their DevSecOps maturity.

Please set aside 10 minutes to complete the survey and review your results. Your results page will provide an overall maturity rating, ratings for each competency area, and explanations and suggestions to help your organization get to the next level of maturity.

By submitting this form, you agree to the [Privacy Policy](#) and [Cookie Policy](#).

Start Self-Assessment!

press Enter

All Articles



WRITING

SEPTEMBER 9, 2024

A SaaS provider's guide to securely integrating with customers' AWS accounts



WRITING

SEPTEMBER 5, 2024

Kubernetes security fundamentals: Admission Control



EMERGING THREATS AND VULNERABILITIES

AUGUST 20, 2024

The gift that keeps on giving: A new opportunistic Log4j campaign



WRITING

AUGUST 16, 2024

Highlights from Hacker Summer Camp 2024



OPEN SOURCE SOFTWARE

AUGUST 9, 2024

Shorten your detection engineering feedback loops with Grimoire



OPEN SOURCE SOFTWARE

AUGUST 8, 2024

Introducing GuardDog 2.0: YARA scanning, user-supplied rules, and Golang support



WRITING

AUGUST 1, 2024

Datadog guide to Hacker Summer Camp 2024



EMERGING THREATS AND VULNERABILITIES

JULY 31, 2024

Stressed Pungsan: DPRK-aligned threat actor leverages npm for initial access

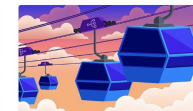
[ALL ARTICLES](#)



Enable and Manage CSM Threats

NEW! Enable Cloud Security Management Threats (CSM Threats) for your cloud workload and detect infrastructure threats in real time. Manage out-of-the-box security agent rules and threat detection rules. Understand the CSM Threats rules pipeline.

FREE



Configure Cloud SIEM for AWS

Secure your cloud environments with Datadog Cloud SIEM. Enable Cloud SIEM, ingest cloud audit logs, and install a Content Pack. The lab and examples in this course feature AWS. The concepts are applicable to multiple cloud providers.

FREE



Detect and Investigate Threats with Cloud SIEM

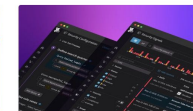
Secure your cloud environments with Datadog Cloud SIEM and cloud provider Content Packs. Explore out-of-the-box threat detection rules. Investigate incoming threats using Security Signals, Signals Explorer, and Cloud SIEM Investigator.

FREE

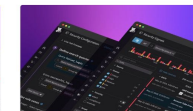


Detect, Prioritize, and Remediate Cloud Security Risks with Datadog CSM

Secure your cloud environments with Datadog Cloud Security Management



In this course, you learn the fundamentals about how to use Cloud SIEM in Datadog to detect different types of security threats and attacks.



Perform attacks against a vulnerable web application. Leverage Datadog Application



¡Muchas Gracias!