Datadog

Product Brochure

Datadog Cloud SIEM: Protect Your Modern Attack Surface **Gain unparalleled visibility and threat detection across your entire environment with Datadog Cloud SIEM.** In today's complex, distributed environments, traditional SIEM solutions struggle to keep pace. Datadog Cloud SIEM delivers a modern, cloud-native approach to security information and event management, providing real-time threat detection, investigation, and response capabilities without the operational overhead. **Key Features & Capabilities:** * **Unified Security Observability:** Consolidate logs, metrics, traces, security events, and cloud provider activity into a single, unified platform for comprehensive security insights. Built-in integrations with AWS, Azure, GCP, and common security tools like CrowdStrike and Palo Alto Networks accelerate onboarding and provide immediate value. * **Out-of-the-Box Detection Rules:** Leverage a rich library of pre-built detection rules, continuously updated by Datadog's security research team, to identify suspicious activity like lateral movement, credential stuffing, and data exfiltration. Customize rules with a powerful, intuitive query language (DDL) to tailor detection to your specific environment. * **Real-Time Correlation & Analysis:** Correlate events across your infrastructure in real-time to identify complex attack patterns and prioritize critical incidents. Datadog's AI-powered anomaly detection automatically flags unusual behavior, reducing alert fatigue and enabling faster response times. * **Interactive Investigation Workflows:** Streamline incident investigation with intuitive dashboards, timelines, and visualisations that provide context and accelerate root cause analysis. Collaboration features allow security teams to work together seamlessly, improving efficiency and reducing time to resolution. * **Compliance & Reporting:** Simplify compliance with built-in reports for industry standards like PCI DSS, SOC 2, and HIPAA. Automatically generate audit logs and demonstrate security posture to stakeholders. **Target Customers & Use Cases:** Datadog Cloud SIEM is ideal for security teams, security engineers, and SOC analysts in mid-sized to enterprise organizations who need a scalable, cloud-native solution for threat detection, investigation, and compliance. Use cases include: * Detecting and responding to security incidents in real-time * Automating security investigations and reducing alert fatigue * Improving security posture and compliance * Gaining visibility into cloud infrastructure security **Competitive Advantage:** Unlike traditional SIEMs, Datadog Cloud

SIEM leverages the power of a unified observability platform. This provides unparalleled context and visibility, enabling faster and more accurate threat detection. Its cloud-native architecture ensures scalability, reliability, and ease of deployment, while its intuitive interface and powerful detection rules make it easy to use and manage. Key metric: Milliseconds to ingest, process and correlate events from any source, at any scale. **Datadog Cloud SIEM empowers you to protect your most critical assets and stay ahead of evolving threats.**