CASE STUDY

Detecting Malicious Activity in Real Time with Datadog Security Monitoring

Delivery Hero - PedidosYa

Founded in 2009, PedidosYa is a member of the Delivery Hero group and the market leader for online food ordering in Latin America. With an innovative web and mobile app, PedidosYa gives users access to 12,000 restaurants across six countries in the region.

Challenges with scaling threat detection workflows

Identifying fraudulent and malicious activity is crucial when it comes to meeting service level objectives. At PedidosYa, the security team encountered a new challenge when the company introduced free food vouchers for new users. Users were creating several accounts from different IP addresses in order to receive multiple vouchers, but this behavior was difficult to pinpoint and prevent at scale. The team's threat detection workflow at the time involved manually creating firewall detection rules for every domain they operate, which was grueling, time-consuming, and required lots of maintenance. And as fraudulent activity increased, it became impossible to create individual rules for every IP address that needed to be blocked. This process led to a month-long delay in detection, which gave the malicious actors enough time to achieve their goal.

> *"In the last week we identified 37,000 unique users. We would not have been able to detect this fraudulent activity in real time in such an effective manner without Datadog Security Monitoring."*
>
> **SANTIAGO ROSENBLATT, HEAD OF INFORMATION SECURITY, PEDIDOSYA**

PedidosYa's requirements for a real-time security monitoring solution

The security team at PedidosYa realized they needed to speed up and automate security detection and analysis in order to prevent fraudulent activity. So, they started looking for a flexible security solution that detects outliers, automates detection rules, and gives quick visibility into the user's security posture.

PedidosYa ultimately selected Datadog because it offers customizable, out-of-the-box threat detection rules that facilitate comprehensive security analysis of malicious patterns across the entire tech stack. These flexible detection rules identify a wide range of attacker techniques in real time and are mapped to the MITRE ATT&CK framework. And because Datadog Security Monitoring is fully integrated with the rest of the Datadog platform, users can correlate a potential threat with relevant application and infrastructure monitoring data in order to quickly triage security alerts.

Additionally, Datadog's extensive tagging system allows users to group security signals in logical ways, such as by service, region, or IP address. For example, users can view high-level metric data for a particular security signal, and then use tags to zero in on a security group or region. These tags can also be used to create graphs based on filtered or aggregated metrics. This ability to group and visualize security data streamlines the threat detection process for complex systems, such as the one at PedidosYa.

Datadog Security Monitoring also comes equipped with expert-built, out-of-the-box dashboards that provide overviews of all security-related data. The IP address overview dashboard is particularly useful for troubleshooting malicious activity patterns like the one identified at PedidosYa, as it enables users to correlate IP addresses with security signals, events, and a variety of log types in a single pane of glass.

Security at PedidosYa today

Datadog played an important role in securing PedidosYa by detecting outliers and malicious patterns in real time. The security team was able to create customized rules in our simple rules editor—without using a query language. These rules require minimal setup and maintenance, and they also apply to all of PedidosYa's domains automatically, which has dramatically accelerated their workflow.

Datadog's tagging system has also enabled the PedidosYa team to filter and group security signals by specific attributes, such as a URL path. This ensures that PedidosYa is able to identify which user accounts could be connected to a brute force attack or fraudulent activity—and to block the associated IP addresses at the same time. They are then able to triage the security signal to the owner of the service, who can investigate further.

> *"Datadog's remediation includes blocking offensive IPs and fraudulent users at the edge, and with the help of Datadog Security Monitoring, we have been able to create more effective detection rules that automate the process and catch malicious activity."*

By using Datadog, PedidosYa eliminated the month-long detection delay that was hampering their efforts to curb fraudulent activity in their large-scale system. After implementing Datadog Security Monitoring, PedidosYa's Head of Information Security, Santiago Rosenblat, said, "Datadog was a complete upgrade from our previous security tools. We are able to work with DevOps now in a unified monitoring and security platform." Single users can no longer create multiple accounts in order to redeem multiple free food vouchers, and PedidosYa is able to focus on what matters most.