CEQUENCE

Solution Brief

Threat Insights and Automated Remediation with Datadog

DATADOG

The Challenge

To effectively respond to increasingly sophisticated attacks on your public facing APIs and web apps, your InfoSec, SecOps and Fraud teams need immediate access to threat details, often collected and stored in different network security solutions. Collecting data and coordinating the response burns precious and often limited resources, allowing the attack to continue, negatively impacting website performance, end-customer experience, and company bottom line. The Cequence Unified API Protection solution integration with Datadog solves the data access and collaboration challenge by feeding API and web application attack logs into a central Datadog repository. Using the power and flexibility of Datadog dashboards, threat response teams can collaborate, perform necessary analysis and respond in a timely manner.

The Solution

The integrated solution allows you to visualize anomalous or suspicious API or web application usage patterns detected by the Cequence Unified API Protection solution. Powerful, easy-to-configure dashboards allow your teams to quickly sift through Cequence-generated threat data, collaborating with other teams to confirm the attack validity and respond accordingly.

Key Benefits

- **Rapid discovery of malicious traffic patterns** improves response times and fosters team collaboration.
- **Correlate log data from multiple sources** to pinpoint and respond to threats resulting in a stronger security posture.
- **Generate automated security policy updates** based on Datadog findings for near real-time detection, analysis, and response.

Accelerate Threat Detection

Datadog's real-time log ingestion simplifies the threat analysis process by allowing you use dashboards to locate patterns, spikes in traffic and potential security gaps hiding in plain sight. Instantly uncover behaviors indicative of an account takeover or content scraping; find APIs exposing sensitive data or configured with weak authentication; and discover shadow, or non-conforming APIs. To further reduce your attack analysis and response time, you can configure Alert Monitors to send your alerts to Slack, Email, PagerDuty, and other collaboration tools to allow security or development teams to quickly take appropriate action. Site reliability engineering teams can use Datadog to correlate application performance monitoring and service health alerts with Cequence logs for a real-time view of the impact on site performance from attack identification to remediation.

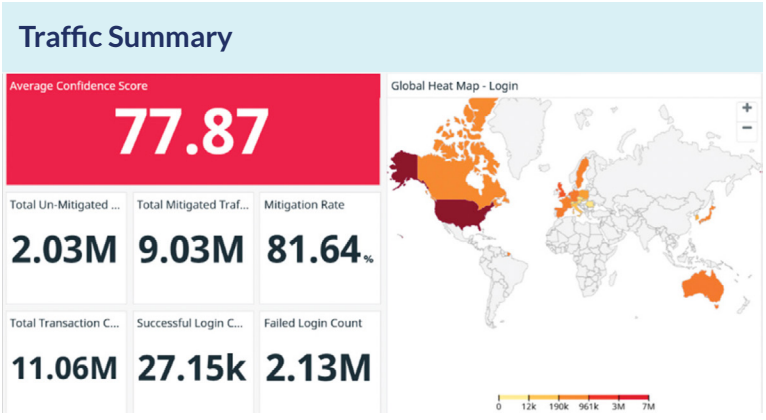

Image 1: Create high level dashboards to monitor traffic.

Account Takeover Behavior

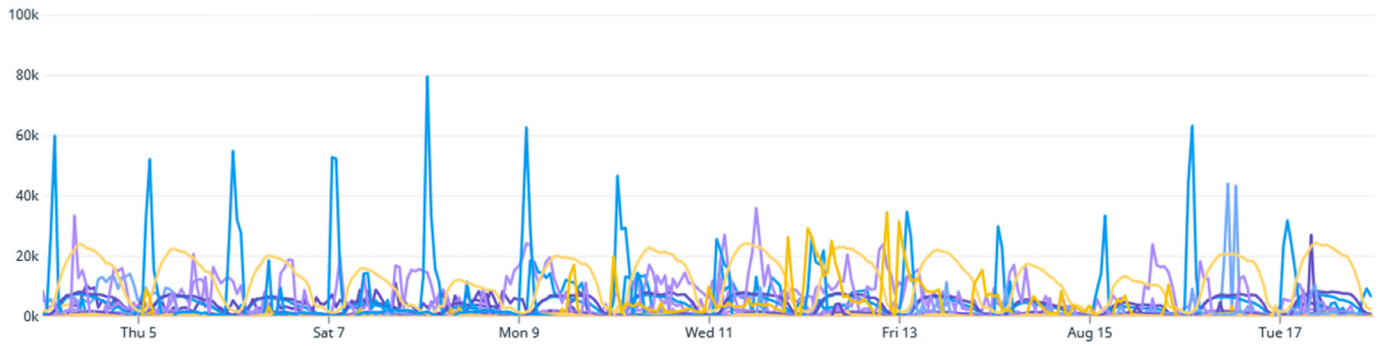

Image 2: Gain insights into attack behavior trends and patterns.

Automated Threat Remediation

Immediate access to the right types of data in Datadog can help security teams accelerate their threat response time. Findings discovered in Datadog can be used to generate a webhook that automatically creates or updates a mitigation policy in Cequence via the Policy-Engine API. Examples of policy-based actions you can initiate with the Datadog findings include:

- **Block a large bank of malicious IP addresses** discovered using Datadog by dynamically adding them to a policy. Mitigation actions include log, block, rate-limit, perform header-insertion, or deceive using HoneyTrap, a mechanism that allows you to send a deceptive response to the threat actor.
- **Block an attack based on behavioral fingerprint** to ensure the attack is blocked regardless of how the threat actors tries to retool and evade detection.

The Cequence-Datadog integration creates a near-real time feedback mechanism, allowing you to forward log data from Cequence to Datadog, perform threat analysis and then use the findings for mitigation. View the Datadog integration documentation here.

About Cequence

Cequence Security, the pioneer of Unified API Protection, is the only solution that unifies API discovery, inventory tracking, dynamic testing, risk analysis and native mitigation with proven, real-time threat protection against ever-evolving API attacks. Cequence Security secures more than 6 billion API calls a day and protects more than 2 billion user accounts across our Fortune 500 customers. Our customers trust us to protect their APIs and web applications with the most effective and adaptive defense against online fraud, business logic attacks, exploits and unintended data leakage, which enables them to remain resilient in today's ever-changing business and threat landscape. Learn more at **www.cequence.ai**.

About Datadog

Datadog is the essential monitoring and security platform for cloud applications. We bring together end-to-end traces, metrics, and logs to make your applications, infrastructure, and third-party services entirely observable. These capabilities help businesses secure their systems, avoid downtime, and ensure customers are getting the best user experience. Learn more at **www.datadog.com**.