

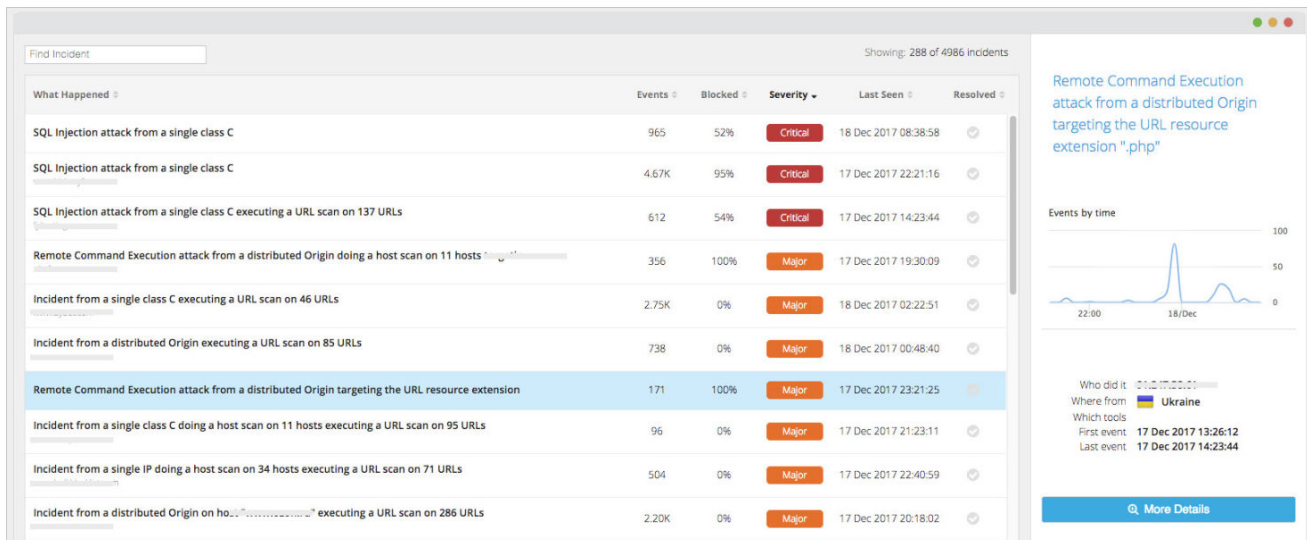


Attack Analytics

Contents

Attack Analytics. 3

Attack Analytics is a tool to help speed up the security investigation of WAF alerts. It provides a comprehensive view of attacks and attackers targeting your resources. The Attack Analytics service aggregates and analyzes your account's security alerts, identifies common characteristics, and groups them into meaningful security incidents.



In this topic:

- [Overview](#)
- [Availability](#)

Overview

The Imperva WAF blocks malicious web traffic. Attack Analytics provides you with the ability to analyze alert traffic. Attack Analytics is designed to deal with a large volume of WAF alerts, and with highly sophisticated and evolving attacks, and to meet the need to resolve security incidents quickly.

Attack Analytics takes events from both the On-Premises WAF (formerly SecureSphere) and the Cloud WAF (formerly Incapsula) and analyzes them to identify related events. A streamlined clustering algorithm factors in multiple attributes to find correlations between the events.

The sophisticated analysis can help you achieve the following objectives:

- Enhance security mechanisms.
- Enable fast response to emerging threats.
- Easily understand the security value provided by the On-Premises WAF and the Cloud WAF by seeing the volume and severity of attacks that are intercepted.

The analysis of attack patterns should answer the following questions:

- Is additional configuration tuning required?
- Do the findings of the analysis need to be passed on to other business units?

To achieve these objectives and answer the questions, Attack Analytics presents you with a display of **incidents**. Each incident is an aggregation of security events that share one or more significant common characteristics, and are thus likely to be linked. A review of an incident enables you to answer questions such as:

- Where did an attack originate?
- Which tools were used?
- Which resources were targeted?
- When did the attack occur?

Each incident is displayed along with its severity, timing, percentage of events that were blocked and alerted, and other data.

Availability

To purchase Attack Analytics, or to request more information or a demo, contact an Imperva sales representative.

See also:

- [Open Attack Analytics](#)
- [Attack Analytics Dashboard](#)
- [View Incidents](#)