IMPERVA

Imperva Attack Analytics

DATASHEET

Some of the common challenges faced by security teams today are:

- Security systems are sending thousands of alerts every day
- Not humanly possible to analyze all the security events
- Hard to identify real attacks in a big heap of event clutter
- Lack a single, correlated view into all web app attacks in place

Uncover Attacks Hiding in an Avalanche of Security Events

Security-related investigations are becoming increasingly cumbersome and complex due to constant data breaches, sophisticated threats and massive overload of security events. As enterprises have initiatives to move applications gradually to the cloud, it is getting more complicated to secure applications on premises, in the cloud or in a hybrid environment.

IT organizations require proper information and analysis capabilities to decisively respond and resolve security events. The use of artificial intelligence and machine learning against large volumes of data is the only way to identify imminent threats.

Imperva Attack Analytics correlates and distills thousands of security events into a few distinct readable narratives. Attack Analytics employs artificial intelligence and machine learning to make the investigation of application security events easy, enabling IT organizations to mitigate and respond to real security threats quickly and decisively. Security events are sorted and grouped into clusters of narratives with associated severity level for quick investigation using machine learning technology. Powerful drill-down capabilities enables security teams for a focused analysis on targeted attacks.

Attack Analytics, part of the Imperva Application Security Solution, leverages security events delivered from the SecureSphere and Incapsula web application firewall solutions. It gathers events from web application firewall solutions across the enterprise delivering unified and contextual insights into security incidents. This allows enterprises to secure applications wherever they may reside – on premises, in the cloud or a hybrid environment.

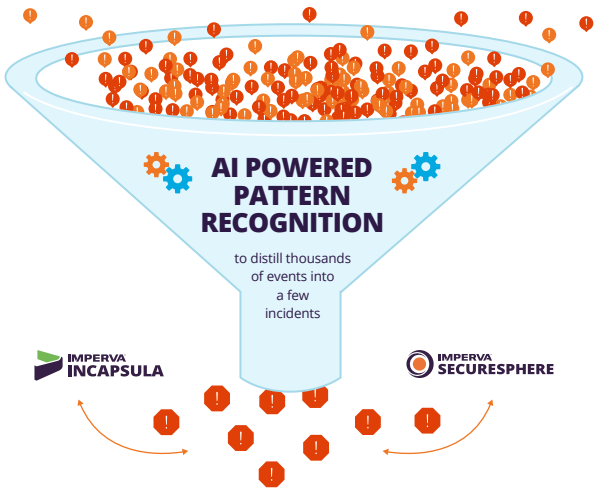

Figure 1: Attack Analytics distills thousands of security events into a few readable narratives

Separate The Wheat from The Chaff

Improved Operational Efficiency

Attack Analytics decreases security investigation time by distilling thousands of WAF events into a few distinct narratives. This significantly improves the efficiency of security operations centers by drastically cutting down the number of events to investigate.

Reduces Risk

By grouping many security events into narratives and prioritizing them, Attack Analytics removes the complexity associated with investigating security events. It makes it easy for security analysts to investigate and focus on a few security incidents that really matter, contrary to going through thousands of events to identify an attack. The use of artificial intelligence reduces the risk associated with missing attacks buried in a big heap of security events.

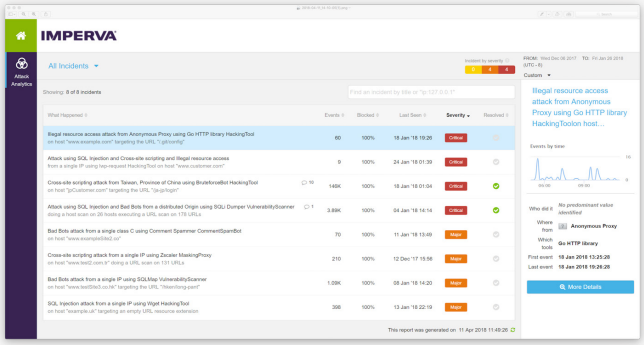

Figure 2: Unified and consolidated view of all WAF events

Unified Visibility

As companies start deploying security in the cloud to protect their cloud-based applications and APIs, it gets harder to monitor security events throughout the enterprise. Attack Analytics provides a unified view to monitor all the security events generated by Imperva cloud-based and on-premises web application firewall solutions. This enables complete visibility and helps in identifying enterprise-wide attack campaigns.

Global Insights

Using artificial intelligence, Attack Analytics clusters event data collected globally, on the customer's estate, to identify attack patterns. This information is of tremendous value to determine new or common attack campaigns that hackers are launching. The collective intelligence and insights will enable for quick attack identification.

Cloud Ready

Attack Analytics is a cloud- based solution and can be deployed with a click of the button. As it is cloud-based, there is no restriction on scalability, and it can accept as many events as an enterprise would like it to process.

Figure 3: Scalable, cloud-based solution

Imperva Application Security Solutions

Imperva application security solutions are available in a flexible, hybrid model that combines cloud-based services with virtual and physical appliances to deliver application security and DDoS defense. Imperva SecureSphere delivers physical and virtual appliances that can be deployed on-premises or in the cloud while Incapsula offers cloud-based services.

Attack Analytics collects event data from both SecureSphere and Incapsula web application firewalls. It collects data from physical, virtual and cloud-based deployments providing views into application security across the enterprise estate. Attack Analytics is supported on Incapsula and SecureSphere web application firewall products.