imperva

Can We Save You Hours of Investigation & Still Improve Your Security?

Attack Analytics – Community Webinar
July 2020

Uzi Galili

Product Manager
uzi.galili@imperva.com

Michael Wright

Product Marketing Manager
michael.wright@imperva.com

Agenda

- Agenda | Intro
- Today’s Challenges
- Attack Analytics Functionality
- Demo
- Q & A
- Way Forward

Attack Analytics helps you **Focus** on what's **Important** and **Saves you Time**

Smartly cluster events to Incidents

Actionable Insights

Extended Visibility

Improves your security

Today’s Challenges

Alert Overload

27%
of organizations encounter 1M+ alerts daily[1]

80%
of alerts are often false positives [2]

Lack of Context

Millions
of stand alone security events from multiple sensors

Limited Workforce

1
AppSec-Focused SOC analyst

SIEM Complexity

Not
customized to your organization

[1] Bricata Poll [2] DarkReading

Today’s Challenges

Alert Overload

Alert Fatigue
Overlooked Events

Lack of Context

Not enough information

Longer time to resolve

Limited Workforce

Divided Responsibilities

Limited Coverage

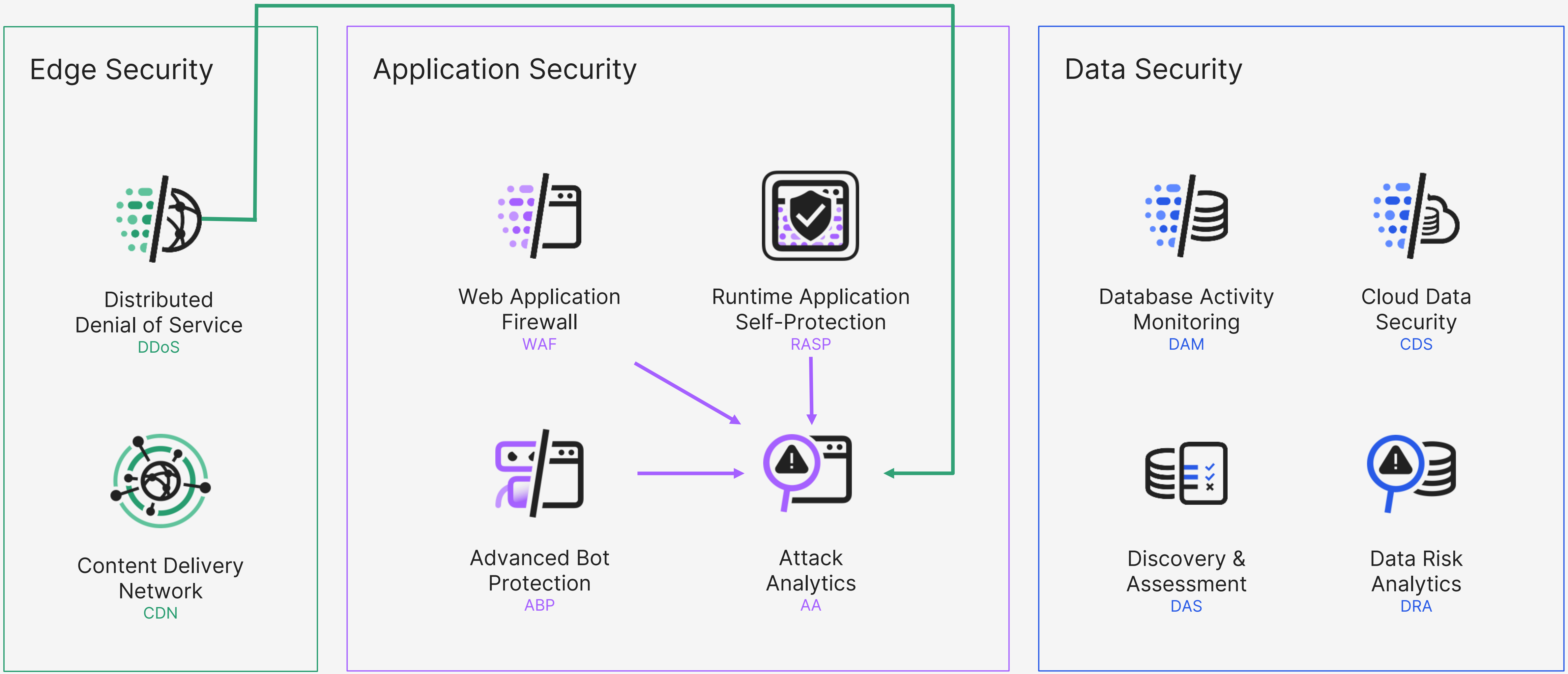
SIEM Complexity

Requires SMEs

Different User Groups

1. Bricata Poll 2. DarkReading

imperva Edge to End Protection



Edge Security

Distributed Denial of Service
DDoS

Content Delivery Network
CDN

Application Security

Web Application Firewall
WAF

Runtime Application Self-Protection
RASP

Advanced Bot Protection
ABP

Attack Analytics
AA

Data Security

Database Activity Monitoring
DAM

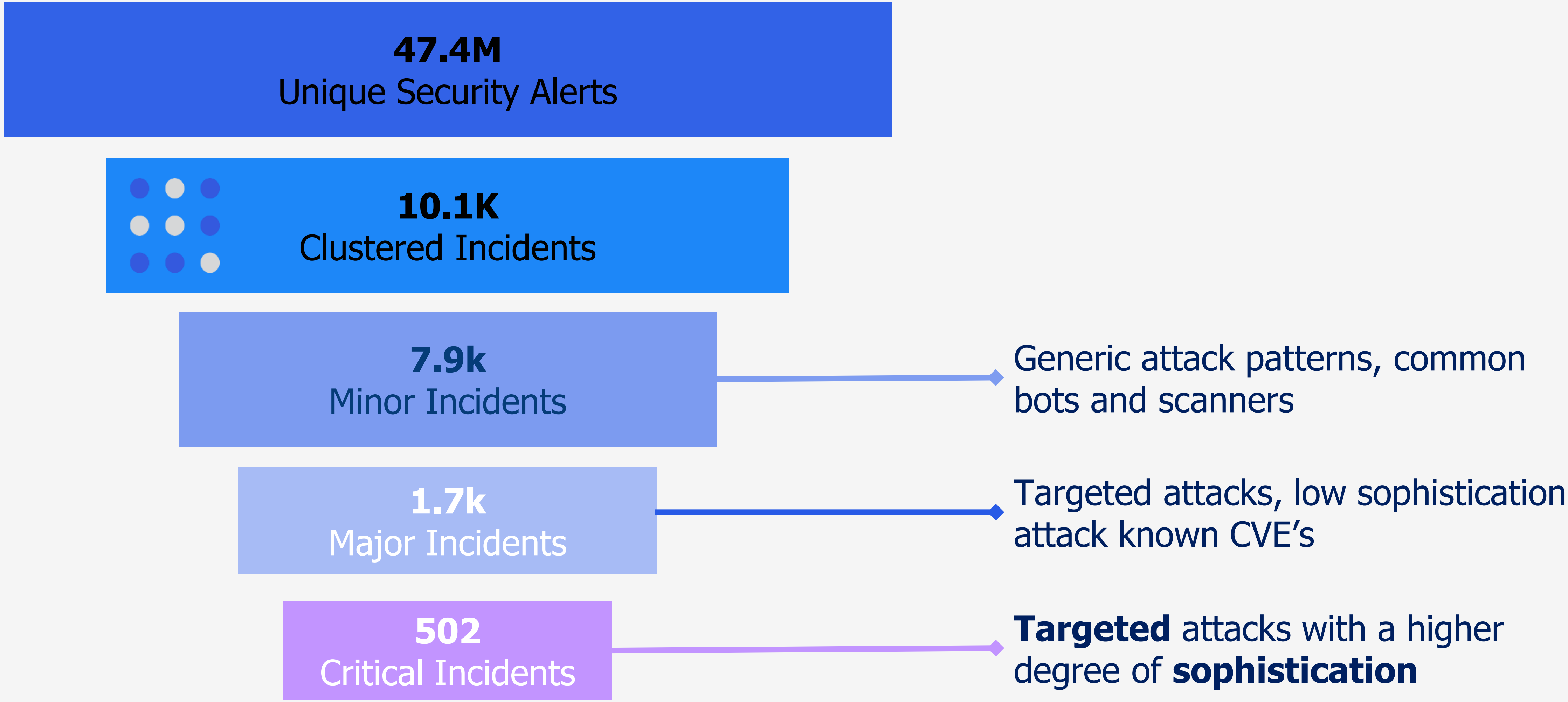
Cloud Data Security
CDS

Discovery & Assessment
DAS

Data Risk Analytics
DRA

Attack Analytics in Action – Use Case

90 Days of Attack Traffic



47.4M
Unique Security Alerts

10.1K
Clustered Incidents

7.9k
Minor Incidents

1.7k
Major Incidents

502
Critical Incidents

Generic attack patterns, common bots and scanners

Targeted attacks, low sophistication attack known CVE’s

Targeted attacks with a higher degree of **sophistication**

imperva

Attacking the Problem – Attack Narratives

Machine Learning and Domain Expertise

Raw Event

Contains properties like method, URL, HTTP version, attack payload, etc.

Event Enrichment

Add context to the event like ASN, IP reputation, attack sophistication, etc.

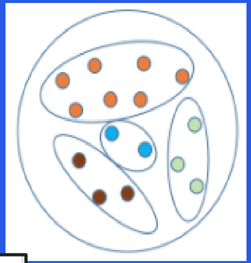
Feature Extraction

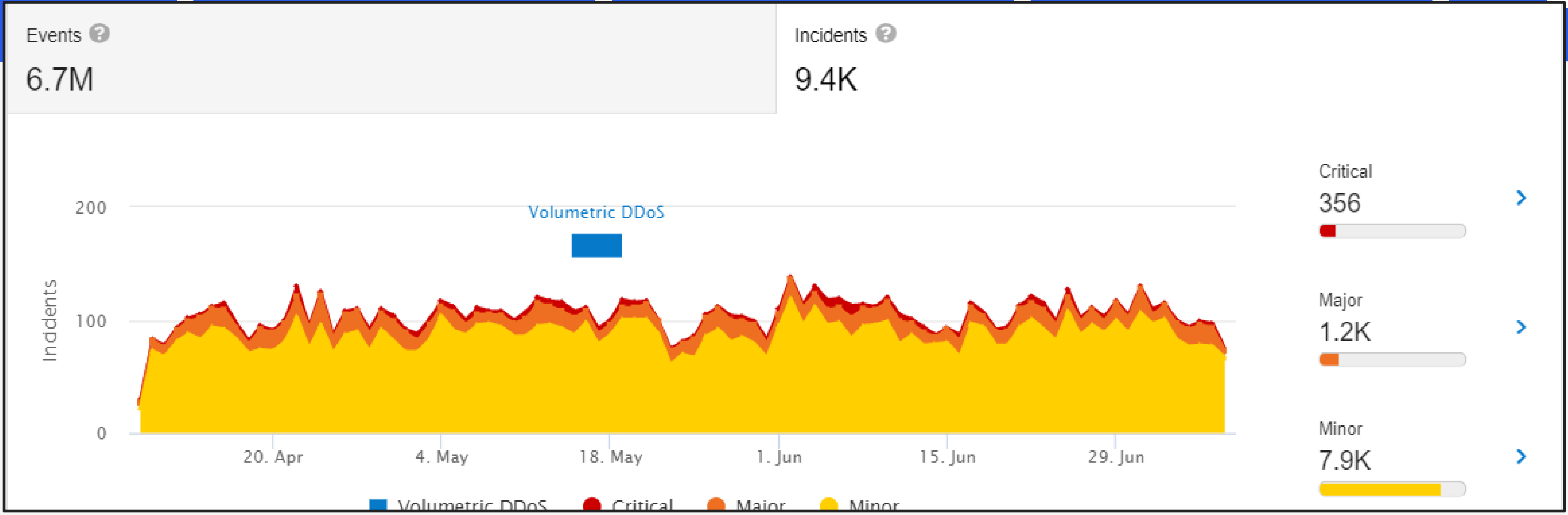
Derive numeric vectors from key properties.

Distance Calculations

Calculate distance between incoming events

Cluster Events by Distance





Events 6.7M

Incidents 9.4K

Critical 356

Major 1.2K

Minor 7.9K

Attacking the Problem – Actionable Insights

Improve your Security Posture

Attack Patterns

Analyze attacks in your environment

Sensor configurations

Cross reference your configuration with attacks and vulnerabilities

Global intelligence

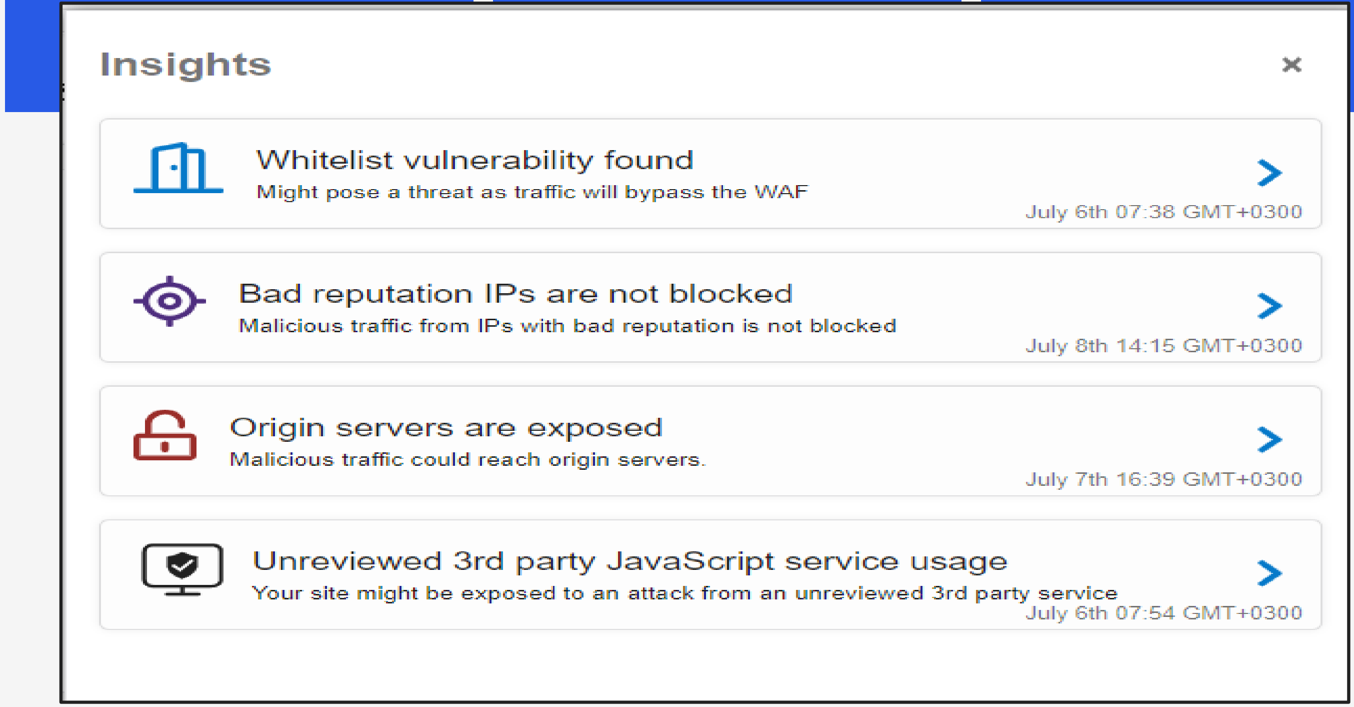
Correlate with the entire Imperva cloud community

Pin-Point config issues

Identify areas that might require your review

Get actionable recommendations

Recommend actions to take based on our expertise and threat research knowledge



Insights ×

Whitelist vulnerability found
Might pose a threat as traffic will bypass the WAF
July 6th 07:38 GMT+0300 >

Bad reputation IPs are not blocked
Malicious traffic from IPs with bad reputation is not blocked
July 8th 14:15 GMT+0300 >

Origin servers are exposed
Malicious traffic could reach origin servers.
July 7th 16:39 GMT+0300 >

Unreviewed 3rd party JavaScript service usage
Your site might be exposed to an attack from an unreviewed 3rd party service
July 6th 07:54 GMT+0300 >

Actionable Insights - Straight to the point

Misconfiguration of WAF Settings

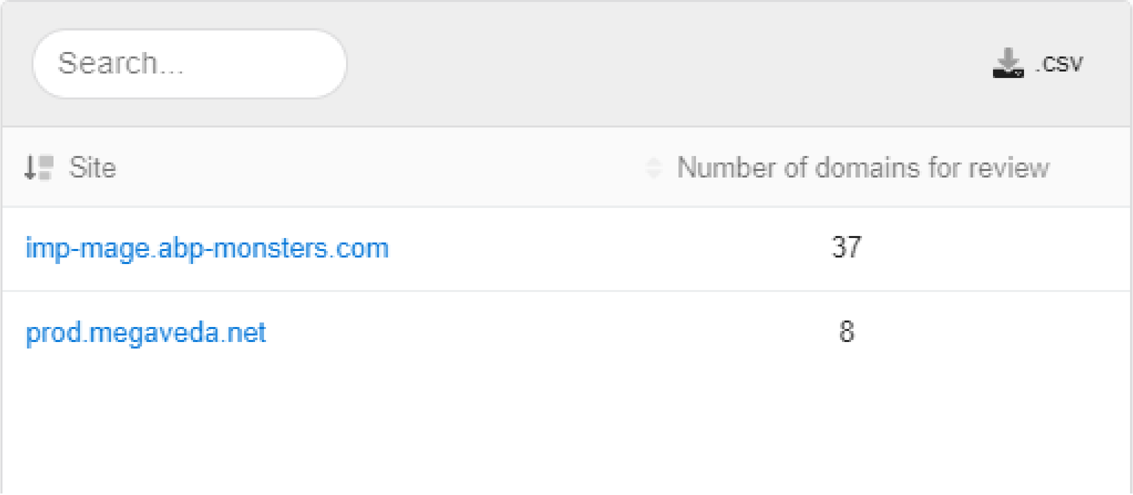
Whitelisted Malicious IP

Bad Reputation IPs

Exposed Origin Server

3rd Party CSP Javascript Service

Your site might be exposed to an attack from an unreviewed 3rd party service



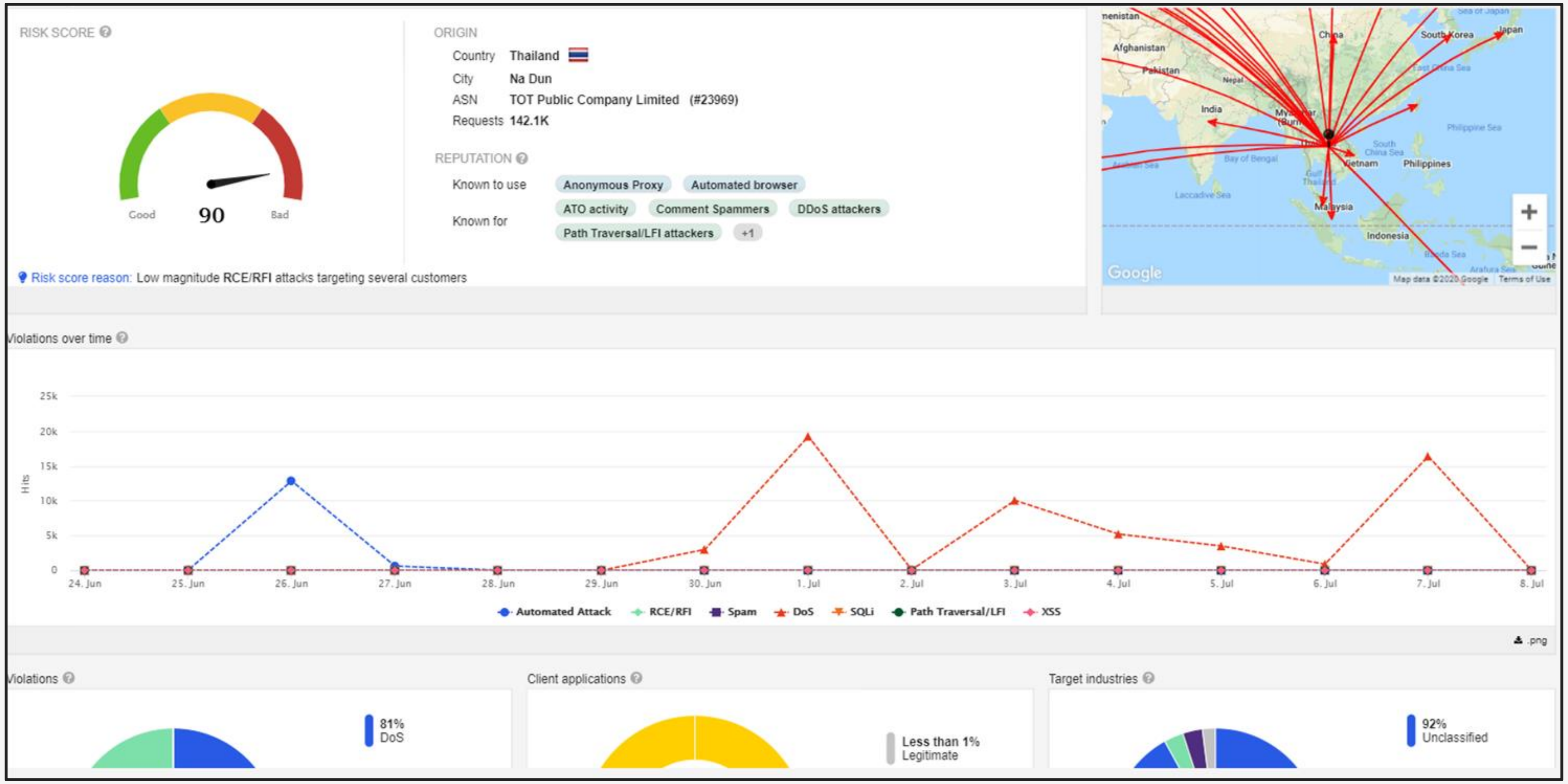
Site	Number of domains for review
imp-mage.abp-monsters.com	37
prod.megaveda.net	8

Attacking the Problem – Reputation Intelligence

Make Informed Decisions

IP Intelligence

See how IPs that are attacking you are ranked by Imperva based on Imperva's cloud community and Threat Research Labs



RISK SCORE

ORIGIN

Country Thailand
City Na Dun
ASN TOT Public Company Limited (#23969)
Requests 142.1K

REPUTATION

Known to use: Anonymous Proxy, Automated browser

Known for: ATO activity, Comment Spammers, DDoS attackers, Path Traversal/LFI attackers, +1

Risk score reason: Low magnitude RCE/RFI attacks targeting several customers

Violations over time

Violations

81% DoS

Client applications

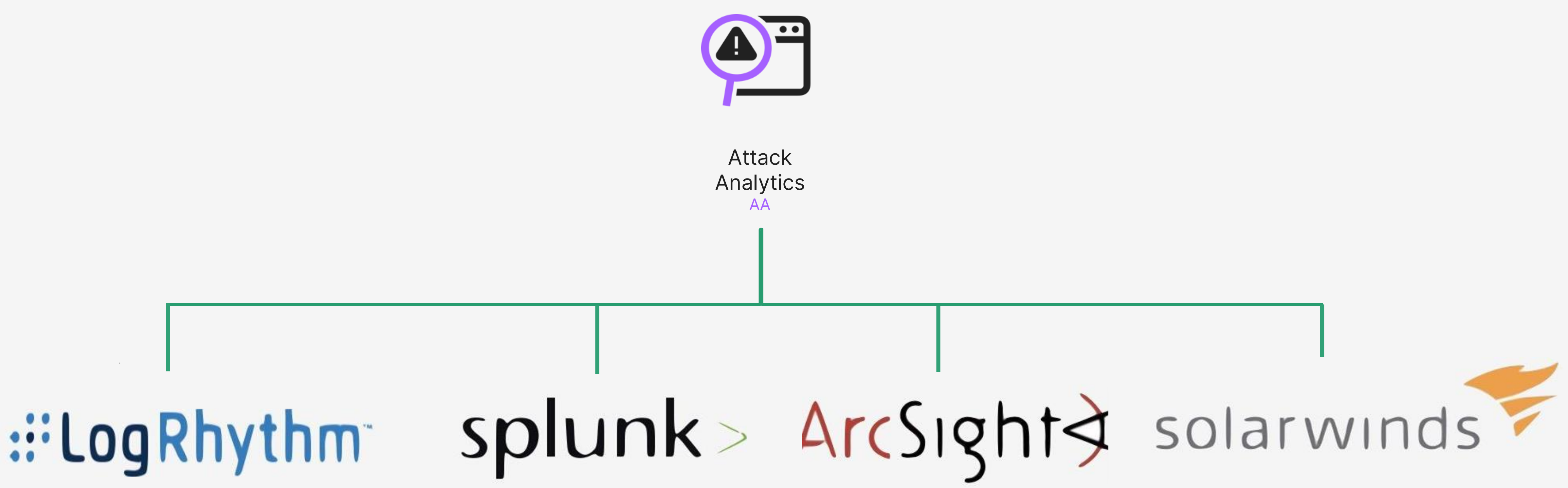
Less than 1% Legitimate

Target industries

92% Unclassified

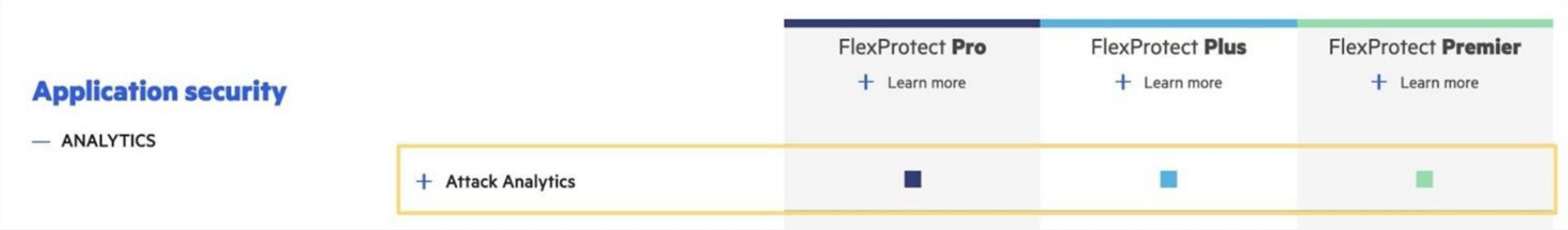
Demo

Leading SIEM Integration



Attack Analytics
AA

FlexProtect Inclusivity & Ad Hoc Add-ons



Application security

— ANALYTICS

	FlexProtect **Pro**	FlexProtect **Plus**	FlexProtect **Premier**
	+ Learn more	+ Learn more	+ Learn more
+ Attack Analytics	■	■	■

- Attack Analytics for 20 Mbps
- Attack Analytics for 50 Mbps
- Attack Analytics for 100 Mbps
- Attack Analytics for 250 Mbps
- Attack Analytics for 500 Mbps
- Attack Analytics for 1 Gbps
- Attack Analytics for 5 Gbps
- Attack Analytics for 10 Gbps

Attack Analytics Looking Forward

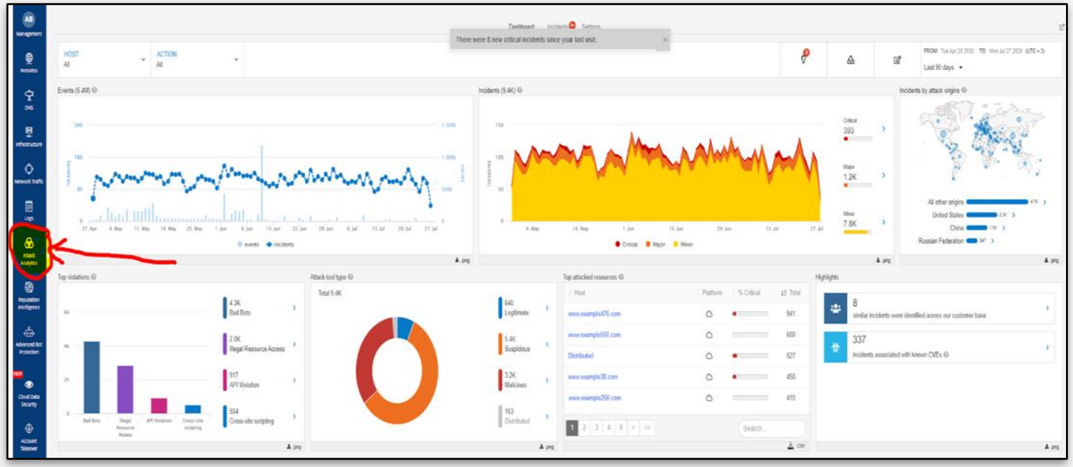
Extended Visibility	**Improved Actionable Insights look & feel**	**IncapRules Coverage**	**RASP coverage**	**ABP “distil” coverage**
Faster Discovery and Resolution	**Review 3rd pty domain (CSP)**	**Origin server exposed**	**“One-Click” insight mitigation**	**Extended Reputation Intelligence**
	Unprotected API Hosts	**“Snooze” Insights**	**Block by Geo- Location**	
	Q3		**Q4**	

imperva

Take Action

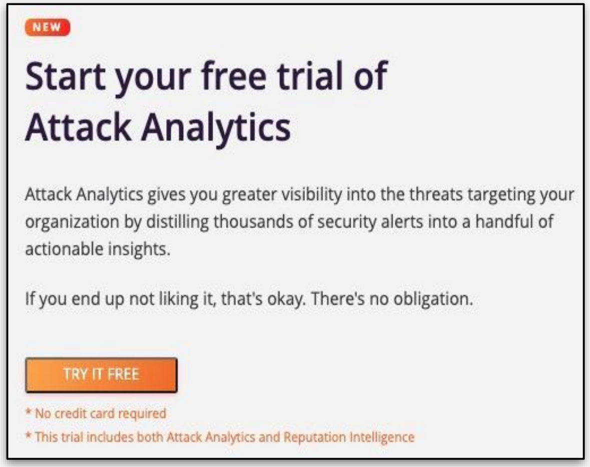
Licensed?

Use It



Not Licensed?

Start a Free Trial



NEW

Start your free trial of Attack Analytics

Attack Analytics gives you greater visibility into the threats targeting your organization by distilling thousands of security alerts into a handful of actionable insights.

If you end up not liking it, that's okay. There's no obligation.

TRY IT FREE

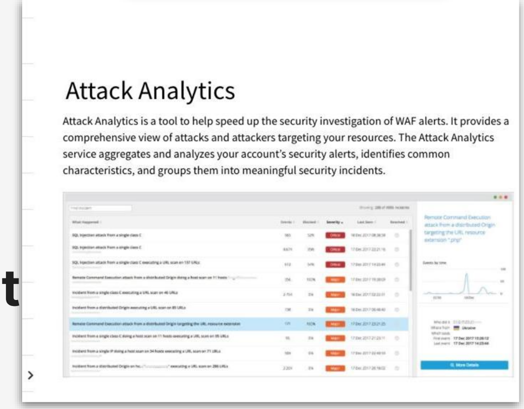
* No credit card required

* This trial includes both Attack Analytics and Reputation Intelligence

Additional Resources

-Community
-Imperva.com
-Customer Support

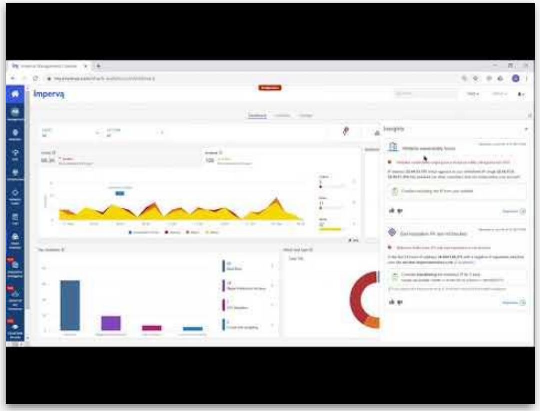
Documentation



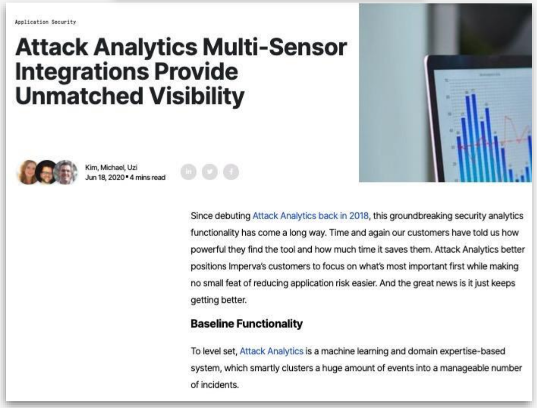
Attack Analytics

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.

Youtube Demos



Imperva Blogs



Application Security

Attack Analytics Multi-Sensor Integrations Provide Unmatched Visibility

Kim, Michael, Uzi
Jun 18, 2020 • 4 mins read

Since debuting Attack Analytics back in 2018, this groundbreaking security analytics functionality has come a long way. Time and again our customers have told us how powerful they find the tool and how much time it saves them. Attack Analytics better positions Imperva's customers to focus on what's most important first while making no small feat of reducing application risk easier. And the great news is it just keeps getting better.

Baseline Functionality

To level set, Attack Analytics is a machine learning and domain expertise-based system, which smartly clusters a huge amount of events into a manageable number of incidents.

imperva

Thank You!

Uzi Galili

Product Manager
uzi.galili@imperva.com

Michael Wright

Product Marketing Manager
michael.wright@imperva.com