Web Apps Vulnerability Management Circle How to make it simple with Imperva & Rapid 7 integration"

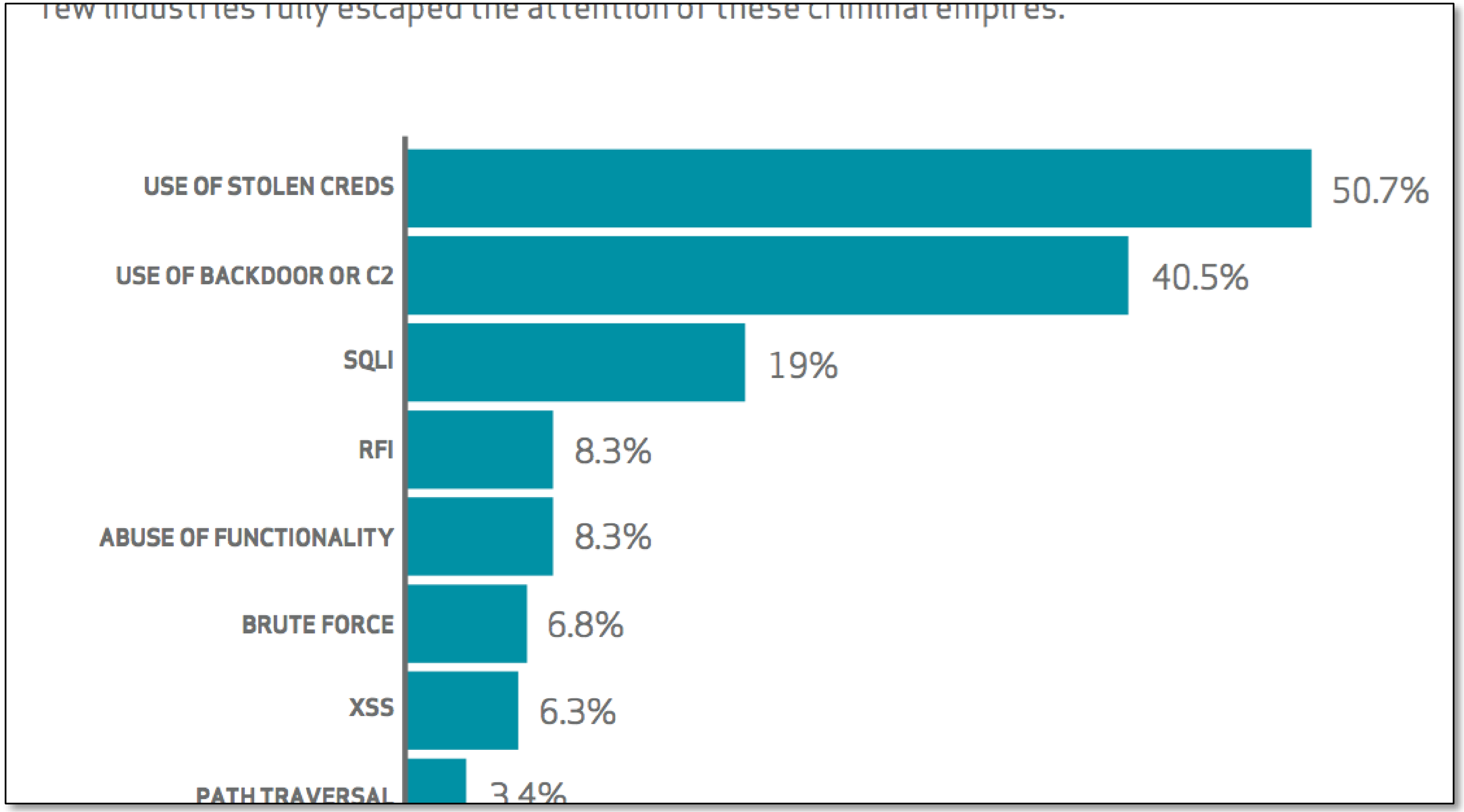
Bartosz Kryński, Senior Consultant, Clico

12.11.2015

Hackers Exploiting Same Old Vulnerabilities

“99.9%

OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.”



Source: Verizon 2015 Data Breach Investigation Report

96%

of applications have vulnerabilities

Source: Cenzic

90%

of security events
from known bad actors

Source: Imperva

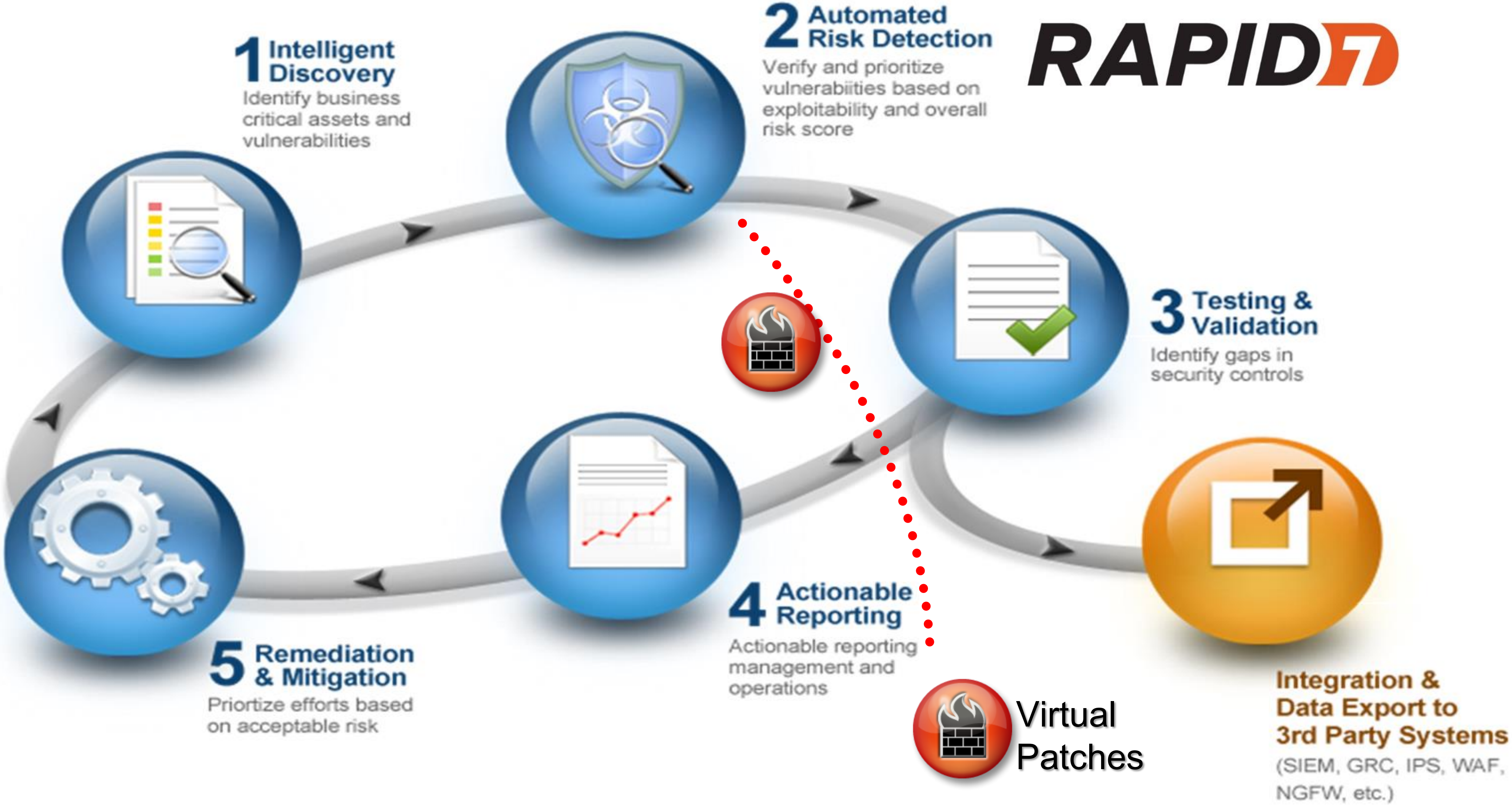
60%+

of website traffic
is non-human

Source: Imperva

What is the vulnerability management life cycle

IMPERVA®



RAPID7

1 Intelligent Discovery

Identify business critical assets and vulnerabilities

2 Automated Risk Detection

Verify and prioritize vulnerabiities based on exploitability and overall risk score

3 Testing & Validation

Identify gaps in security controls

4 Actionable Reporting

Actionable reporting management and operations

5 Remediation & Mitigation

Priortize efforts based on acceptable risk

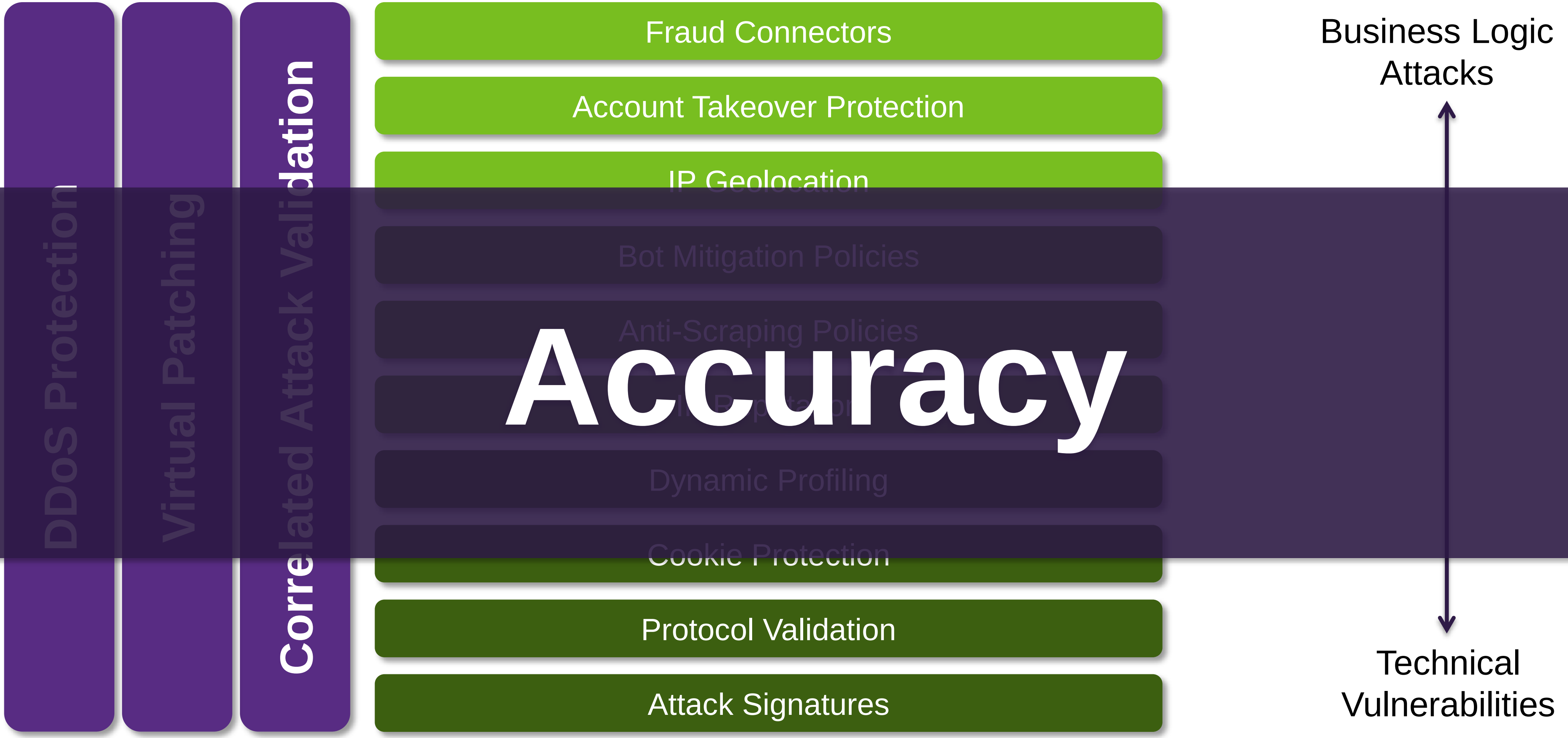
Integration & Data Export to 3rd Party Systems

(SIEM, GRC, IPS, WAF, NGFW, etc.)

Virtual Patches

… & about the mitigation…

Defenses Required to Protect Web Applications



DDoS Protection

Virtual Patching

Correlated Attack Validation

Fraud Connectors

Account Takeover Protection

IP Geolocation

Bot Mitigation Policies

Anti-Scraping Policies

IP Reputation

Dynamic Profiling

Cookie Protection

Protocol Validation

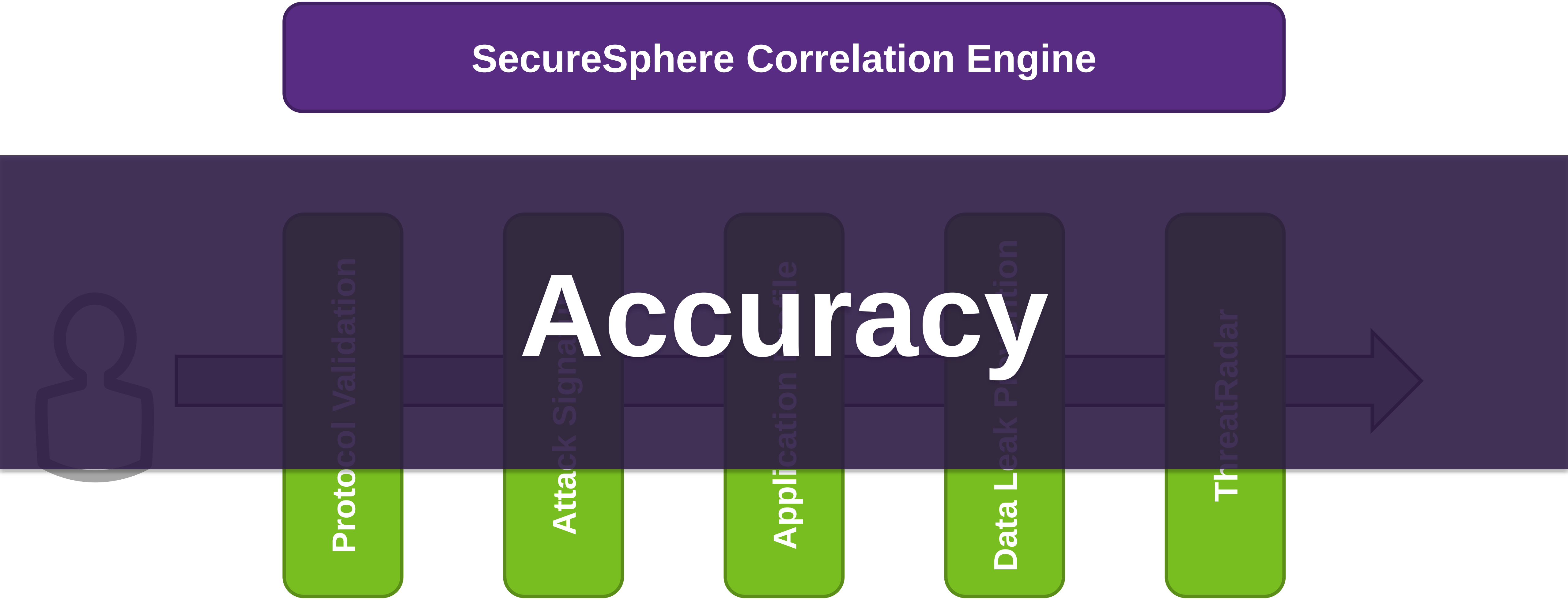
Attack Signatures

Business Logic Attacks

Technical Vulnerabilities

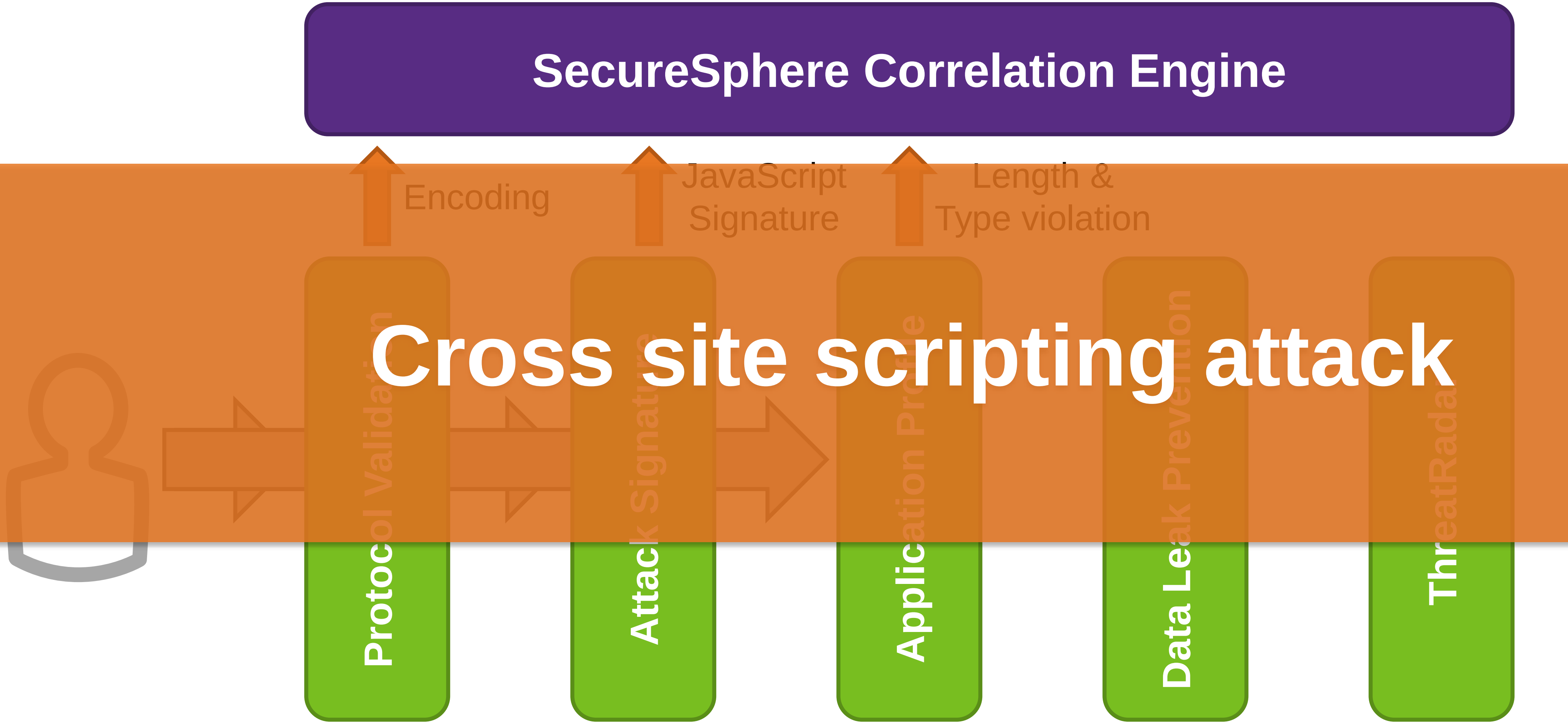
Accuracy

SecureSphere Correlation Engine



IMPERVA®

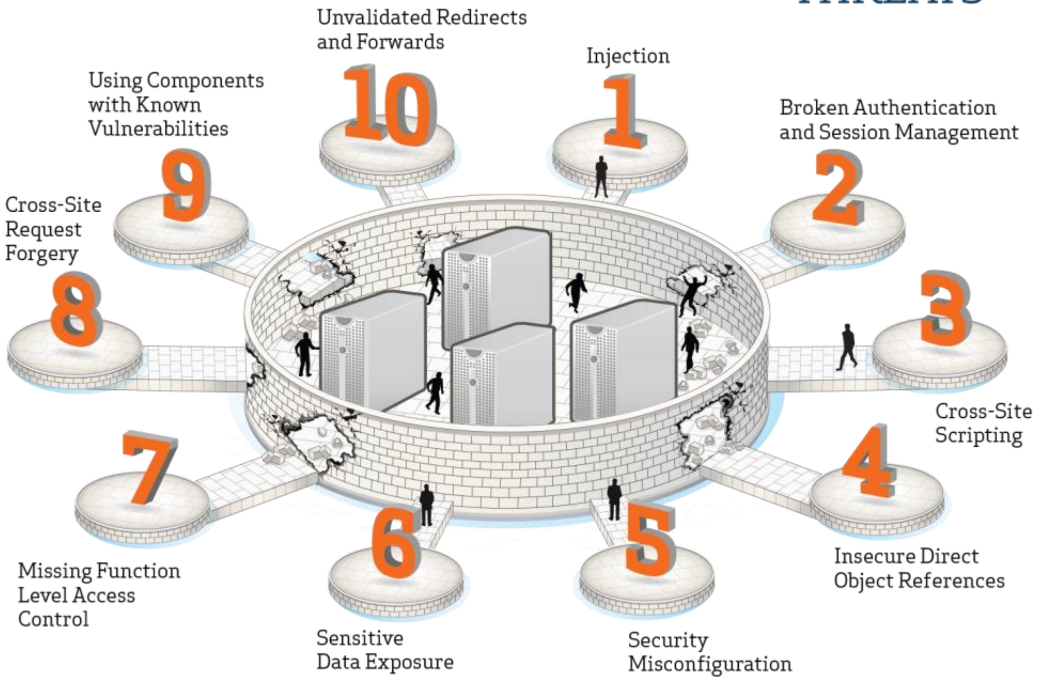
SecureSphere Correlation Engine



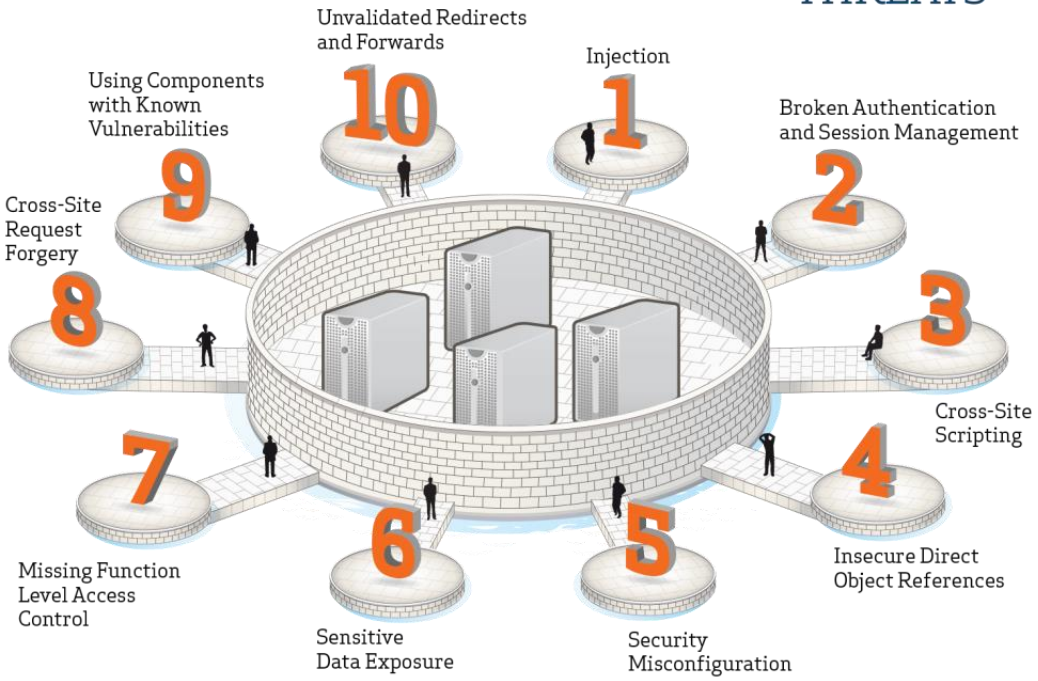
Cross site scripting attack

Superior Protection Versus Next-Generation Firewalls

NEXT GENERATION FIREWALLS → **BLOCK <40% OF THE OWASP TOP TEN THREATS**

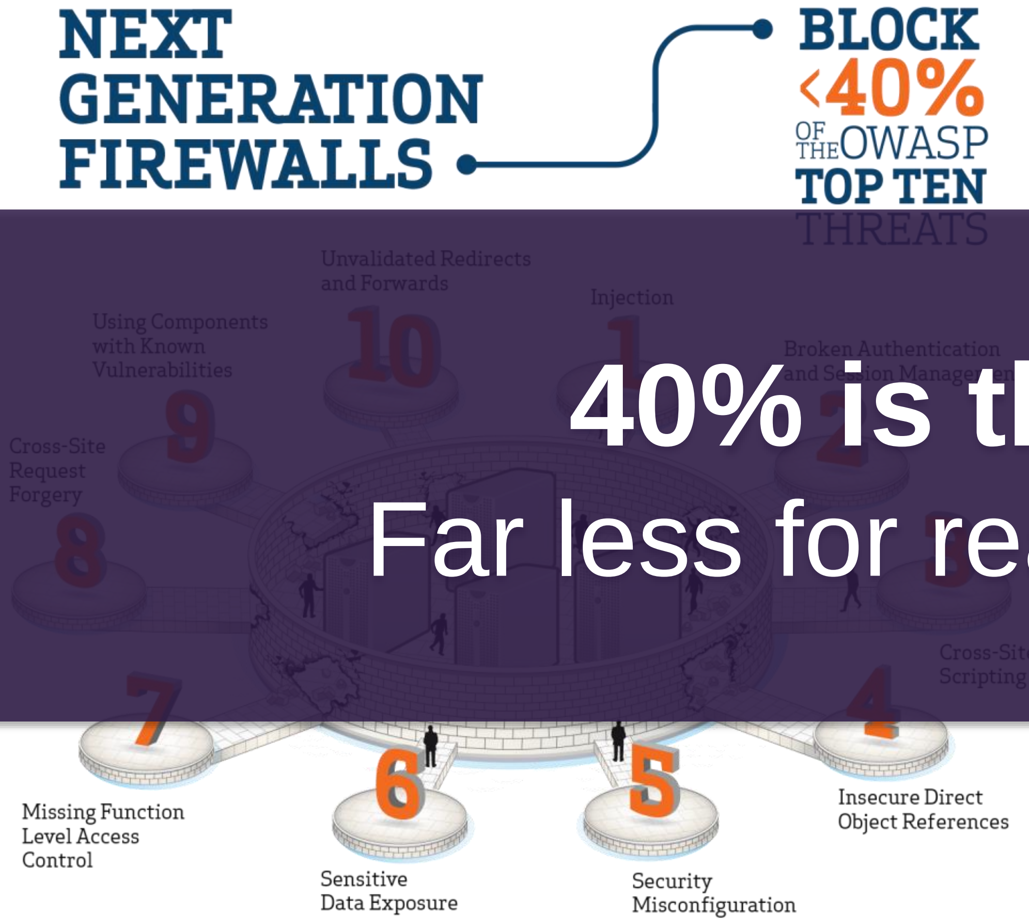

Unvalidated Redirects and Forwards
10
Injection
1
Using Components with Known Vulnerabilities
9
Broken Authentication and Session Management
2
Cross-Site Request Forgery
8
3
Cross-Site Scripting
7
4
Missing Function Level Access Control
6
5
Insecure Direct Object References
Sensitive Data Exposure
Security Misconfiguration

WEB APPLICATION FIREWALLS → **BLOCK 100% OF THE OWASP TOP TEN THREATS**

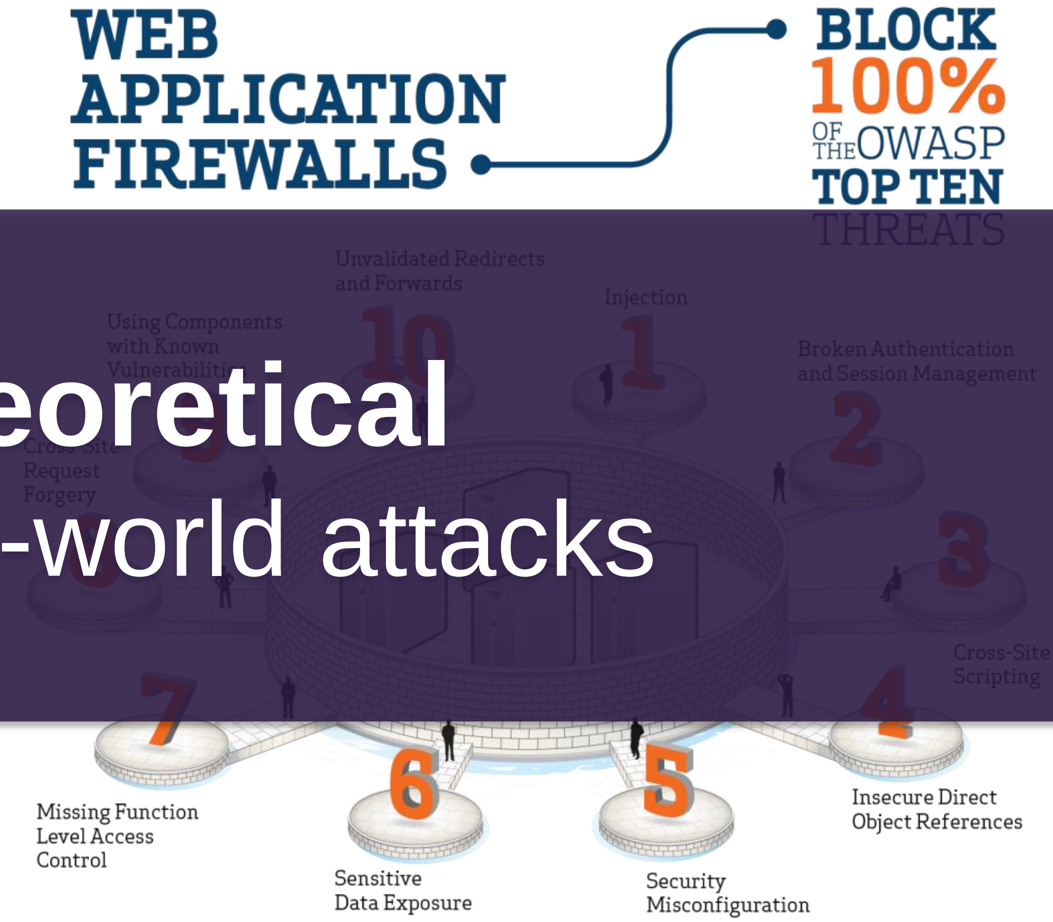

Unvalidated Redirects and Forwards
10
Injection
1
Using Components with Known Vulnerabilities
9
Broken Authentication and Session Management
2
Cross-Site Request Forgery
8
3
Cross-Site Scripting
7
4
Missing Function Level Access Control
6
5
Insecure Direct Object References
Sensitive Data Exposure
Security Misconfiguration

OWASP Top 10 (for 2013)

Superior Protection Versus Next-Generation Firewalls



NEXT GENERATION FIREWALLS
BLOCK <40% OF THE OWASP TOP TEN THREATS
Injection
1
Broken Authentication and Session Management
2
3
Cross-Site Scripting
4
Insecure Direct Object References
5
Security Misconfiguration
6
Sensitive Data Exposure
7
Missing Function Level Access Control
8
Cross-Site Request Forgery
9
Using Components with Known Vulnerabilities
10
Unvalidated Redirects and Forwards



WEB APPLICATION FIREWALLS
BLOCK 100% OF THE OWASP TOP TEN THREATS
Injection
1
Broken Authentication and Session Management
2
3
Cross-Site Scripting
4
Insecure Direct Object References
5
Security Misconfiguration
6
Sensitive Data Exposure
7
Missing Function Level Access Control
8
Cross-Site Request Forgery
9
Using Components with Known Vulnerabilities
10
Unvalidated Redirects and Forwards

40% is theoretical

Far less for real-world attacks

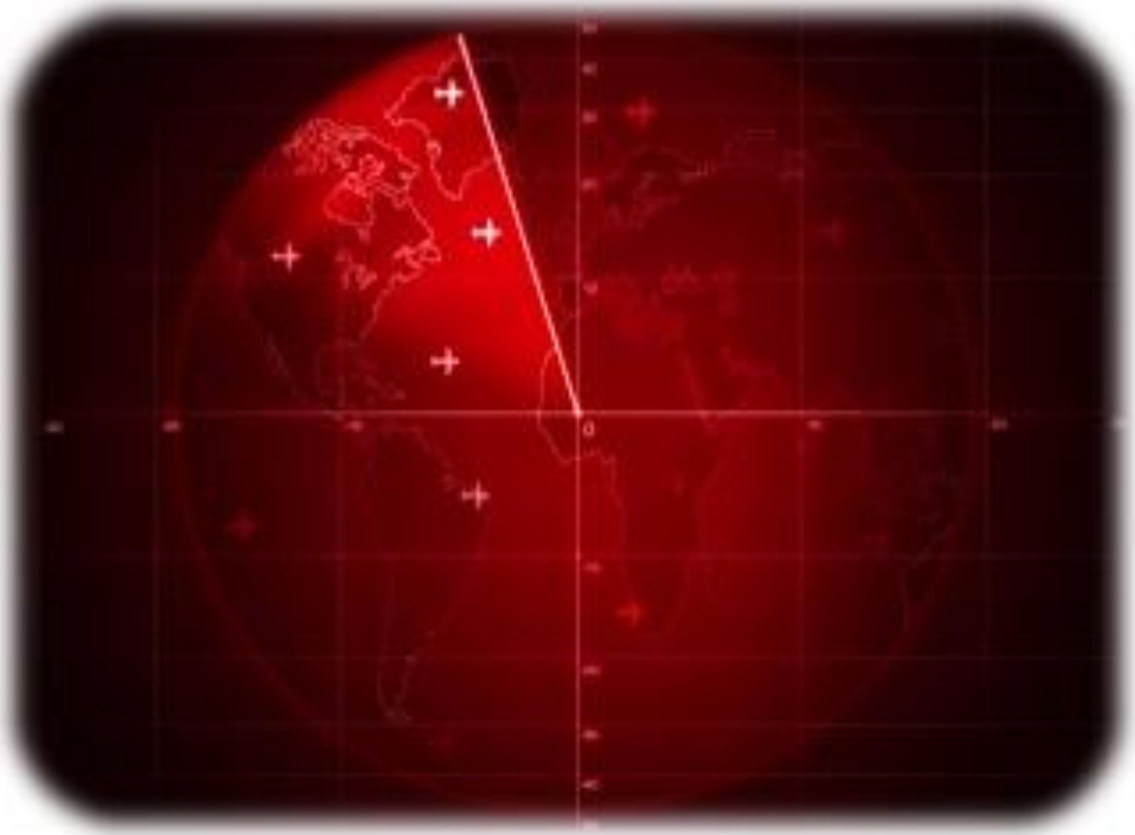
OWASP Top 10 (for 2013)

Industrialized Hacking

gives hackers extreme leverage

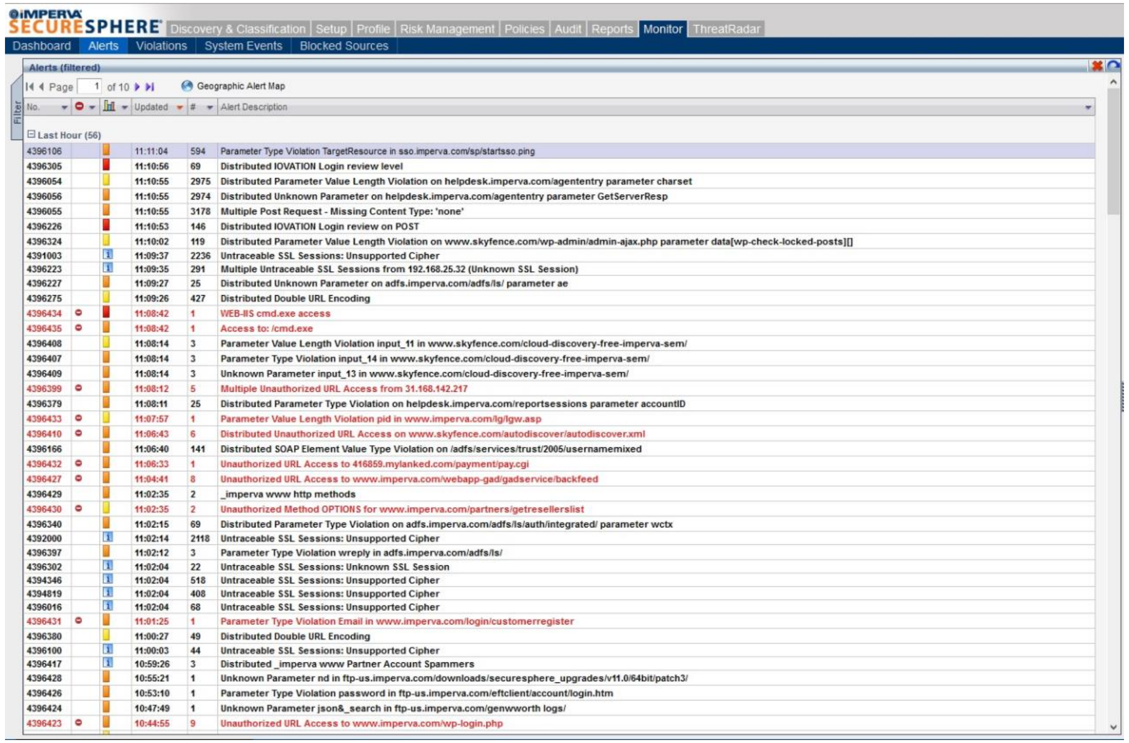
ThreatRadar Subscriptions

- ThreatRadar Reputation
- ThreatRadar Bot Protection
- ThreatRadar Account Takeover Protection



More Focused, More Productive Team

Eliminate the “noise” from known bad, and prioritize on truly worrisome



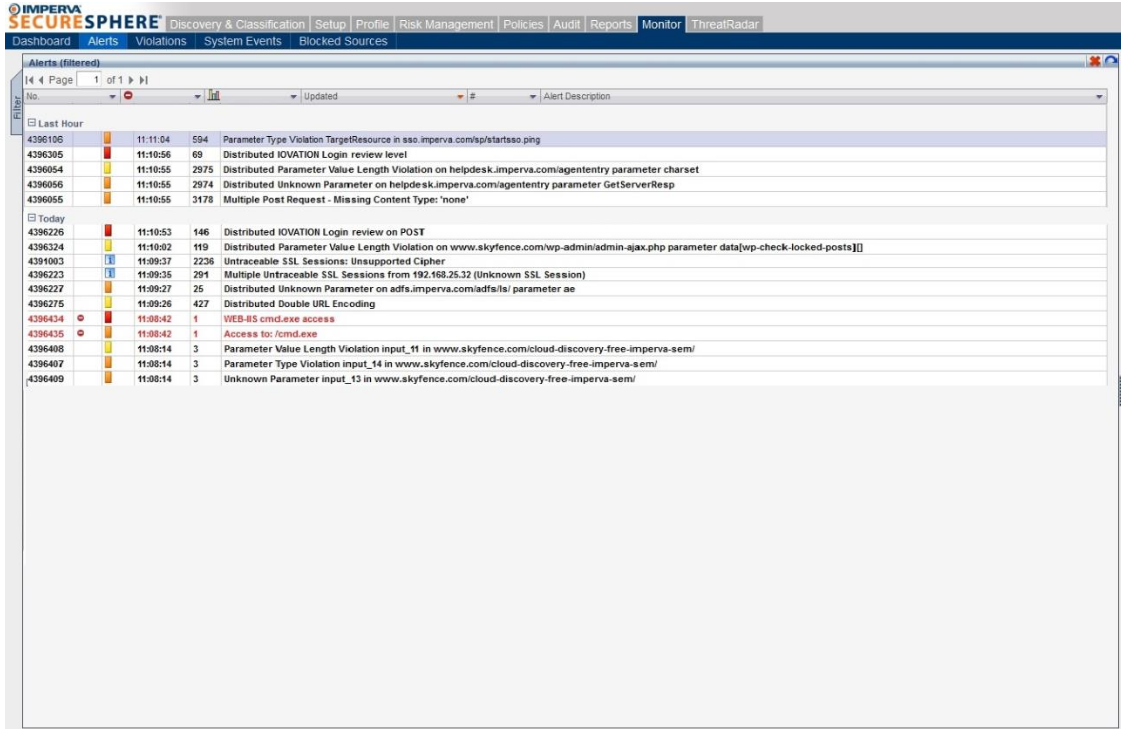
Alerts (filtered)

Page 1 of 10

⊟ Last Hour (56)

No.	⊖	📊	Updated	#	Alert Description
4396106		🟧	11:11:04	594	Parameter Type Violation TargetResource in sso.imperva.com/sp/startsso.ping
4396305		🟥	11:10:56	69	Distributed IOVATION Login review level
4396054		🟨	11:10:55	2975	Distributed Parameter Value Length Violation on helpdesk.imperva.com/agententry parameter charset
4396056		🟧	11:10:55	2974	Distributed Unknown Parameter on helpdesk.imperva.com/agententry parameter GetServerResp
4396055		🟧	11:10:55	3178	Multiple Post Request - Missing Content Type: 'none'
4396226		🟥	11:10:53	146	Distributed IOVATION Login review on POST
4396324		🟨	11:10:02	119	Distributed Parameter Value Length Violation on www.skyfence.com/wp-admin/admin-ajax.php parameter data[wp-check-locked-posts][]
4391003		i	11:09:37	2236	Untraceable SSL Sessions: Unsupported Cipher
4396223		i	11:09:35	291	Multiple Untraceable SSL Sessions from 192.168.25.32 (Unknown SSL Session)
4396227		🟧	11:09:27	25	Distributed Unknown Parameter on adfs.imperva.com/adfs/ls/ parameter ae
4396275		🟨	11:09:26	427	Distributed Double URL Encoding
4396434	⊖	🟥	11:08:42	1	WEB-IIS cmd.exe access
4396435	⊖	🟧	11:08:42	1	Access to: /cmd.exe
4396408		🟨	11:08:14	3	Parameter Value Length Violation input_11 in www.skyfence.com/cloud-discovery-free-imperva-sem/
4396407		🟧	11:08:14	3	Parameter Type Violation input_14 in www.skyfence.com/cloud-discovery-free-imperva-sem/
4396409		🟧	11:08:14	3	Unknown Parameter input_13 in www.skyfence.com/cloud-discovery-free-imperva-sem/
4396399	⊖	🟧	11:08:12	5	Multiple Unauthorized URL Access from 31.168.142.217
4396379		🟧	11:08:11	25	Distributed Parameter Type Violation on helpdesk.imperva.com/reportsessions parameter accountID
4396433	⊖	🟨	11:07:57	1	Parameter Value Length Violation pid in www.imperva.com/lg/lgw.asp
4396410	⊖	🟧	11:06:43	6	Distributed Unauthorized URL Access on www.skyfence.com/autodiscover/autodiscover.xml
4396166		🟧	11:06:40	141	Distributed SOAP Element Value Type Violation on /adfs/services/trust/2005/usernamemixed
4396432	⊖	🟧	11:06:33	1	Unauthorized URL Access to 416859.mylanked.com/payment/pay.cgi
4396427	⊖	🟧	11:04:41	8	Unauthorized URL Access to www.imperva.com/webapp-gad/gadservice/backfeed
4396429		🟧	11:02:35	2	_imperva www http methods
4396430	⊖	🟨	11:02:35	2	Unauthorized Method OPTIONS for www.imperva.com/partners/getresellerslist
4396340		🟧	11:02:15	69	Distributed Parameter Type Violation on adfs.imperva.com/adfs/ls/auth/integrated/ parameter wctx
4392000		i	11:02:14	2118	Untraceable SSL Sessions: Unsupported Cipher
4396397		🟧	11:02:12	3	Parameter Type Violation wreply in adfs.imperva.com/adfs/ls/
4396302		i	11:02:04	22	Untraceable SSL Sessions: Unknown SSL Session
4394346		i	11:02:04	518	Untraceable SSL Sessions: Unsupported Cipher
4394819		i	11:02:04	408	Untraceable SSL Sessions: Unsupported Cipher
4396016		i	11:02:04	68	Untraceable SSL Sessions: Unsupported Cipher
4396431	⊖	🟧	11:01:25	1	Parameter Type Violation Email in www.imperva.com/login/customerregister
4396380		🟨	11:00:27	49	Distributed Double URL Encoding
4396100		i	11:00:03	44	Untraceable SSL Sessions: Unsupported Cipher
4396417		i	10:59:26	3	Distributed _imperva www Partner Account Spammers
4396428		🟧	10:55:21	1	Unknown Parameter nd in ftp-us.imperva.com/downloads/securesphere_upgrades/v11.0/64bit/patch3/
4396426		🟧	10:53:10	1	Parameter Type Violation password in ftp-us.imperva.com/eftclient/account/login.htm
4396424		🟧	10:47:49	1	Unknown Parameter json&_search in ftp-us.imperva.com/genwworth logs/
4396423	⊖	🟧	10:44:55	9	Unauthorized URL Access to www.imperva.com/wp-login.php

Before



Alerts (filtered)

Page 1 of 1

⊟ Last Hour

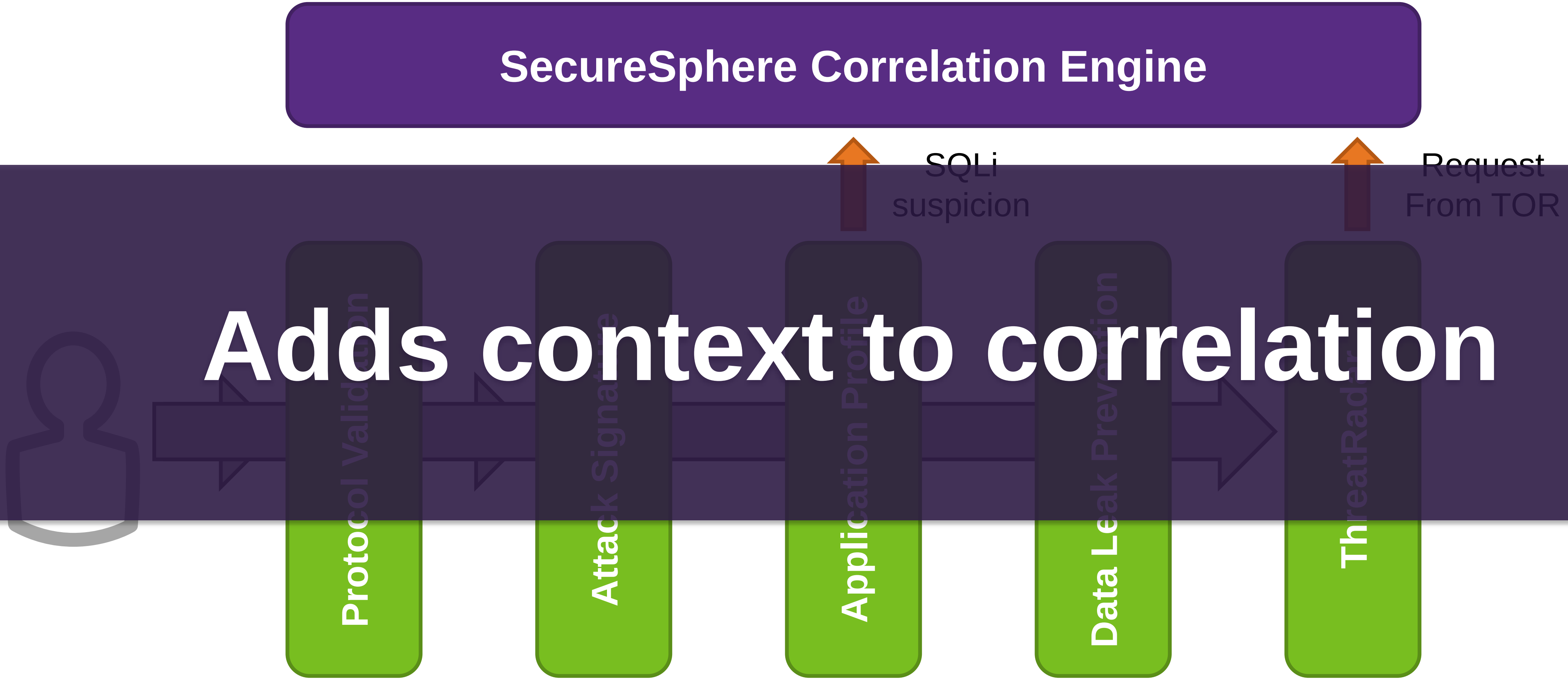
No.	⊖	📊	Updated	#	Alert Description
4396106		🟧	11:11:04	594	Parameter Type Violation TargetResource in sso.imperva.com/sp/startsso.ping
4396305		🟥	11:10:56	69	Distributed IOVATION Login review level
4396054		🟨	11:10:55	2975	Distributed Parameter Value Length Violation on helpdesk.imperva.com/agententry parameter charset
4396056		🟧	11:10:55	2974	Distributed Unknown Parameter on helpdesk.imperva.com/agententry parameter GetServerResp
4396055		🟧	11:10:55	3178	Multiple Post Request - Missing Content Type: 'none'

⊟ Today

No.	⊖	📊	Updated	#	Alert Description
4396226		🟥	11:10:53	146	Distributed IOVATION Login review on POST
4396324		🟨	11:10:02	119	Distributed Parameter Value Length Violation on www.skyfence.com/wp-admin/admin-ajax.php parameter data[wp-check-locked-posts][]
4391003		i	11:09:37	2236	Untraceable SSL Sessions: Unsupported Cipher
4396223		i	11:09:35	291	Multiple Untraceable SSL Sessions from 192.168.25.32 (Unknown SSL Session)
4396227		🟧	11:09:27	25	Distributed Unknown Parameter on adfs.imperva.com/adfs/ls/ parameter ae
4396275		🟨	11:09:26	427	Distributed Double URL Encoding
4396434	⊖	🟥	11:08:42	1	WEB-IIS cmd.exe access
4396435	⊖	🟧	11:08:42	1	Access to: /cmd.exe
4396408		🟨	11:08:14	3	Parameter Value Length Violation input_11 in www.skyfence.com/cloud-discovery-free-imperva-sem/
4396407		🟧	11:08:14	3	Parameter Type Violation input_14 in www.skyfence.com/cloud-discovery-free-imperva-sem/
4396409		🟧	11:08:14	3	Unknown Parameter input_13 in www.skyfence.com/cloud-discovery-free-imperva-sem/

After

More Focused, More Productive Team



SecureSphere Correlation Engine

SQLi suspicion

Request From TOR

Protocol Validation

Attack Signature

Application Profile

Data Leak Prevention

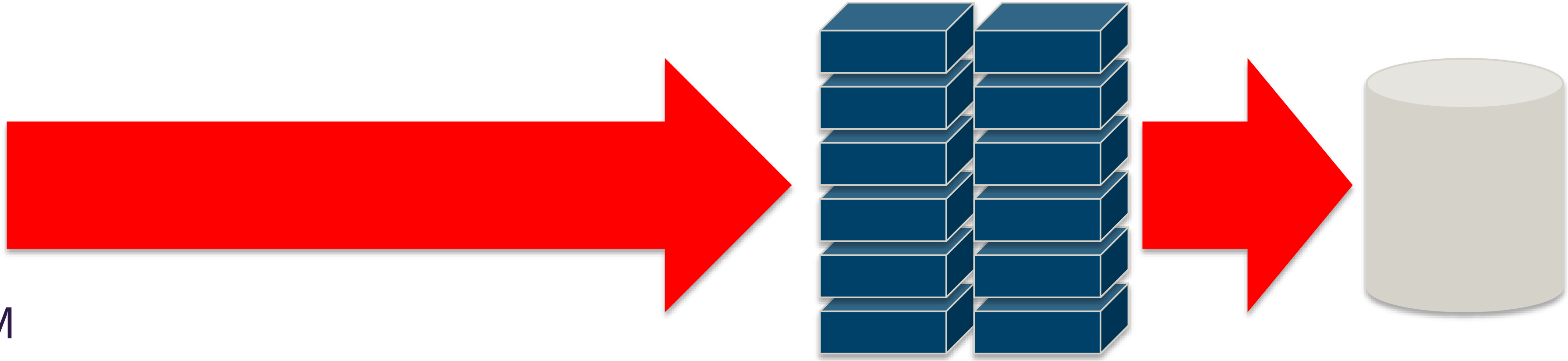
ThreatRadar

Adds context to correlation

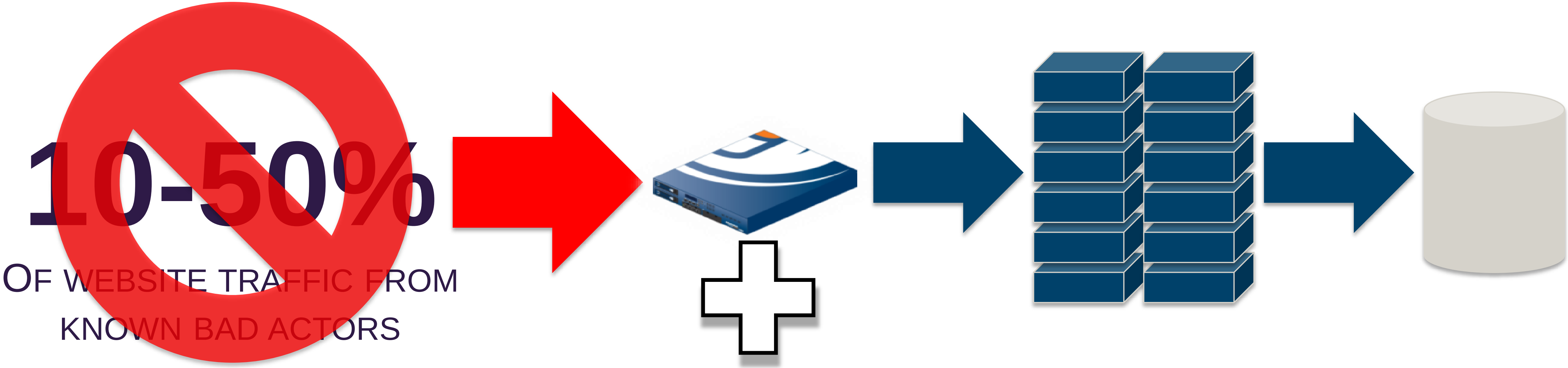
Reduce Infrastructure Costs

10-50%

OF WEBSITE TRAFFIC FROM KNOWN BAD ACTORS



Reduce Infrastructure Costs



10-50%

OF WEBSITE TRAFFIC FROM KNOWN BAD ACTORS

More efficient WAF

Fewer logs entries

Less disc needed

Fewer events to SIEM

Reduce Infrastructure Costs

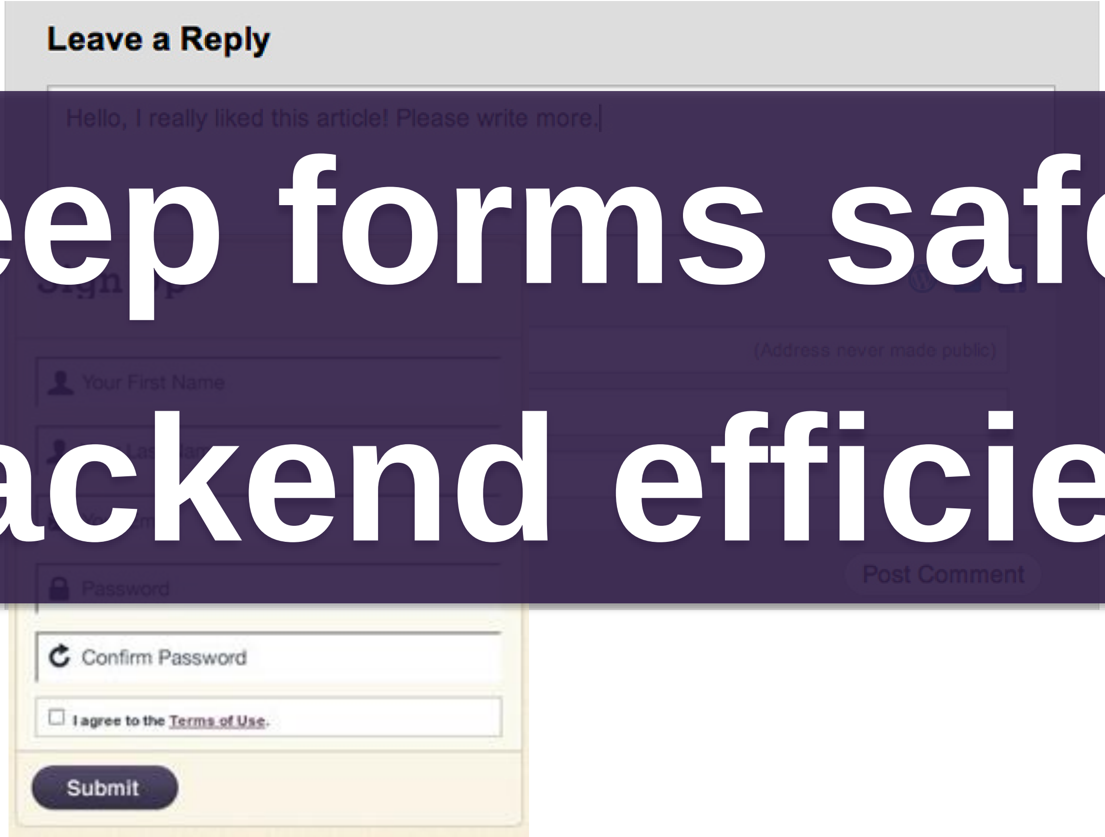
Spam Marketing

Spamdexing: Reputation Impact

Fraud

DDoS

Malicious Traffic



Leave a Reply

Hello, I really liked this article! Please write more.

Sign up

(Address never made public)

Your First Name

Password

Confirm Password

☐ I agree to the Terms of Use.

Submit

Post Comment

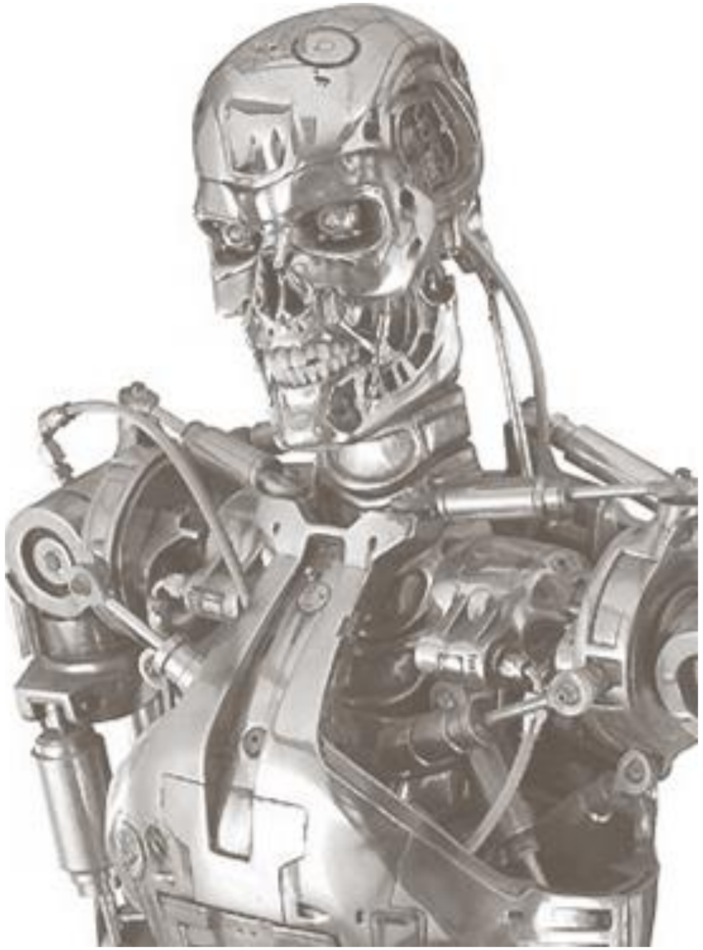
Manual Reviews

Keep forms safe

Gain backend efficiencies

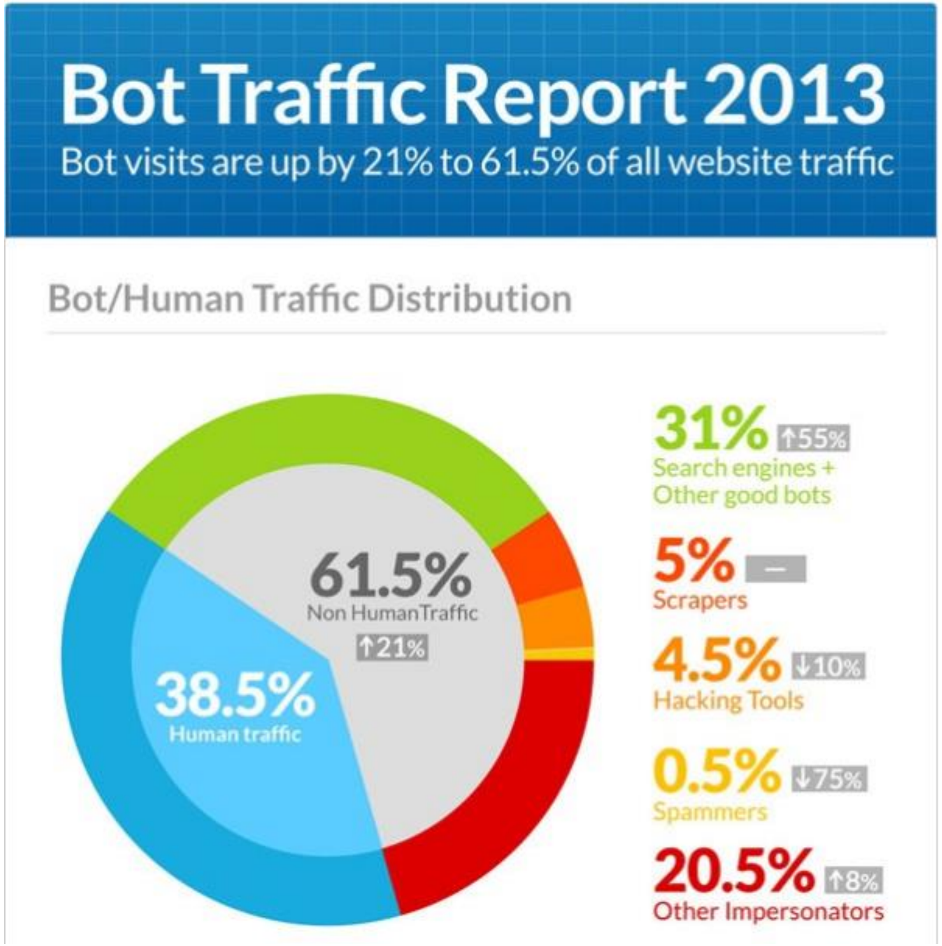
ThreatRadar Subscriptions

- ThreatRadar Reputation
- ThreatRadar Bot Protection
- ThreatRadar Account Takeover Protection



Majority of Website traffic from Bots

- Bots generate **>60%** of website traffic
- **Half** of this is malicious
- Bots are getting **harder to distinguish**



Identifying Bo

Inspect Client

1

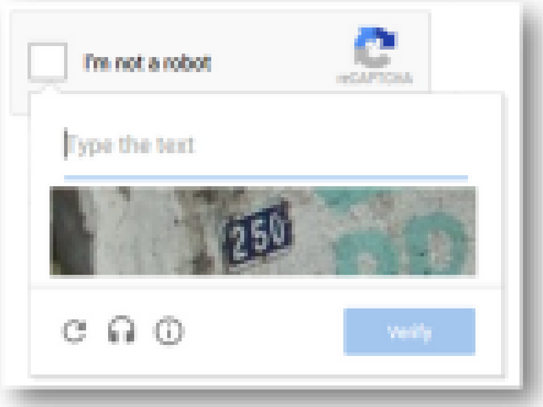
IP | Headers | User Agent

Known good bot
Known bad bot
Whitelisted bot

CAPTCHA: Further confidence it is a human

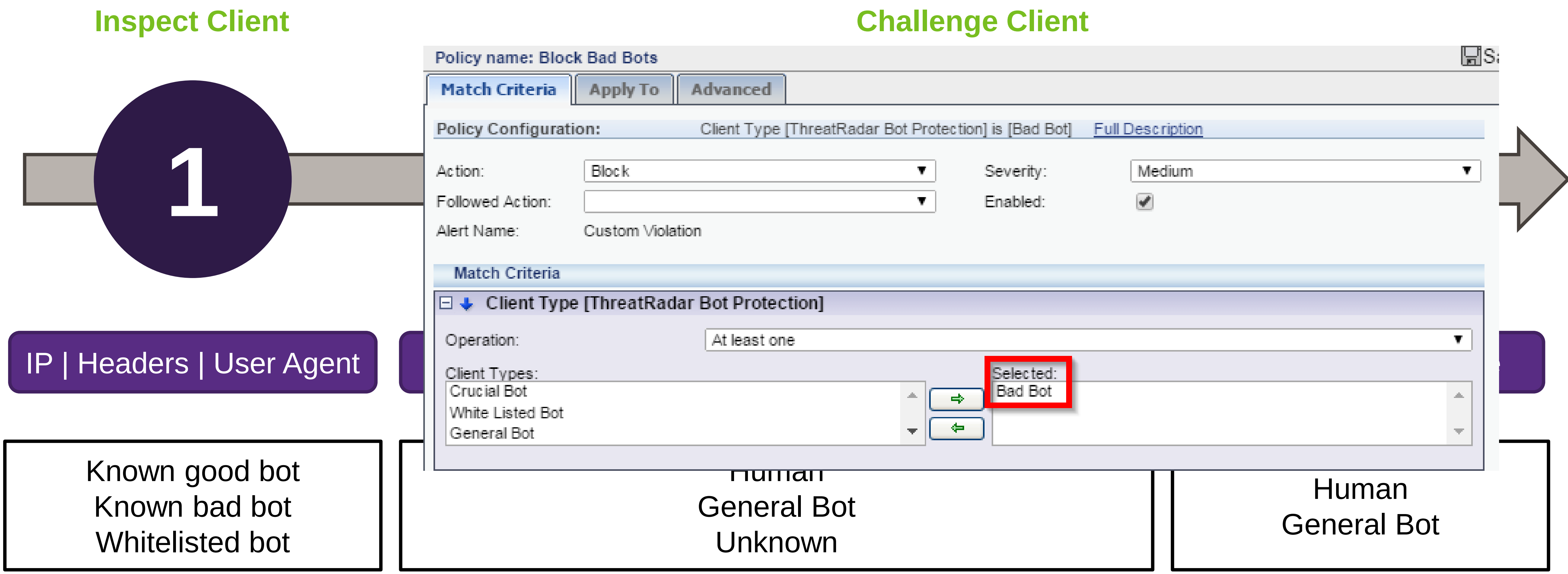
- CAPTCHA insertion options
  - Login event
  - Activity-based (controlled availability)

- Regular Web Custom Policy enforcement



IMPERVA®

Apply SecureSphere Policy Based Upon Classification



Inspect Client

1

IP | Headers | User Agent

Known good bot
Known bad bot
Whitelisted bot

Challenge Client

Human
General Bot
Unknown

Human
General Bot

Policy name: Block Bad Bots

Policy Configuration: Client Type [ThreatRadar Bot Protection] is [Bad Bot] Full Description

Action: Block
Severity: Medium
Followed Action:
Enabled: ☑
Alert Name: Custom Violation

Match Criteria

Client Type [ThreatRadar Bot Protection]

Operation: At least one

Client Types:
Crucial Bot
White Listed Bot
General Bot

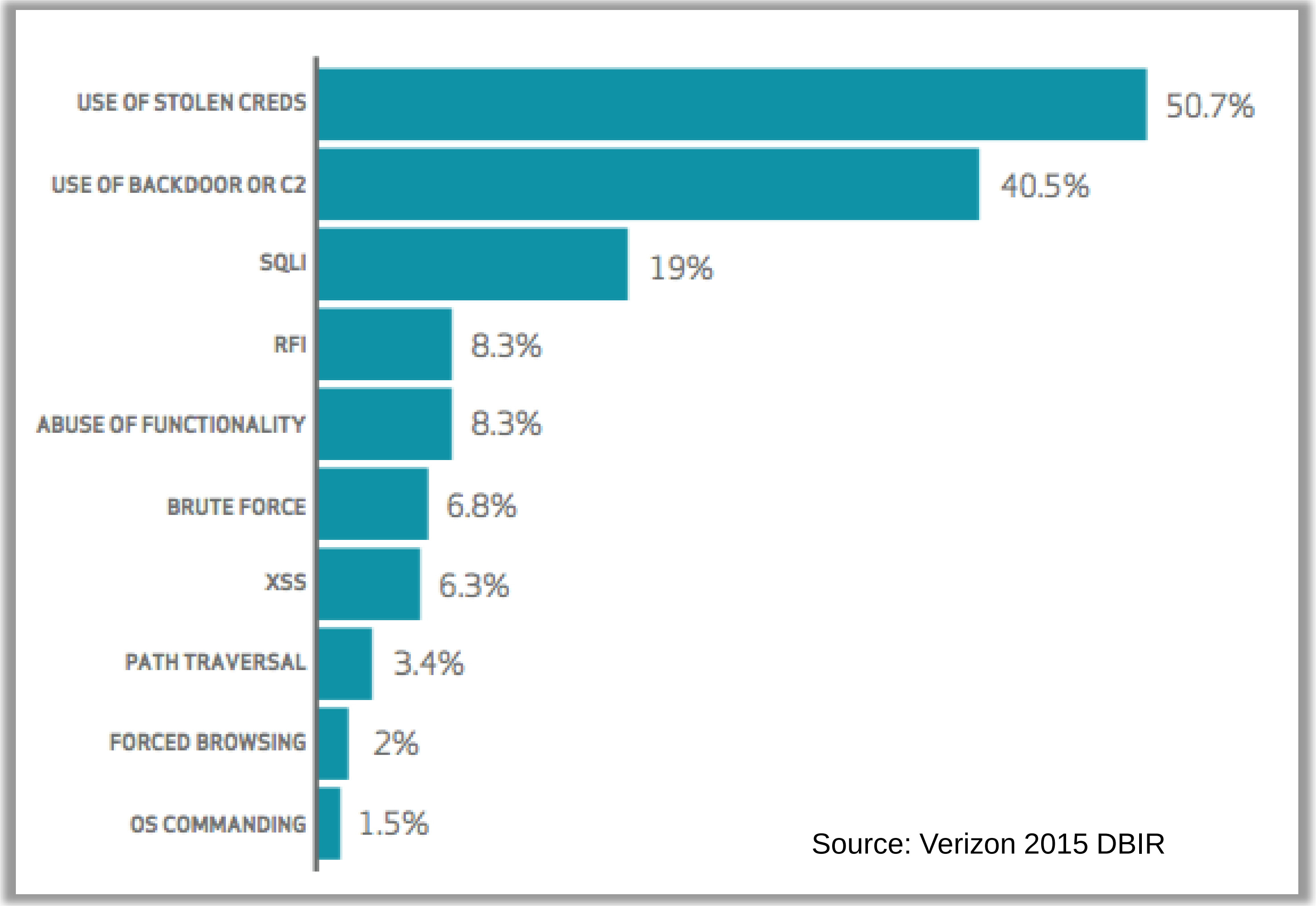
Selected:
Bad Bot

ThreatRadar Subscriptions

- ThreatRadar Reputation
- ThreatRadar Bot Protection
- ThreatRadar Account Takeover Protection

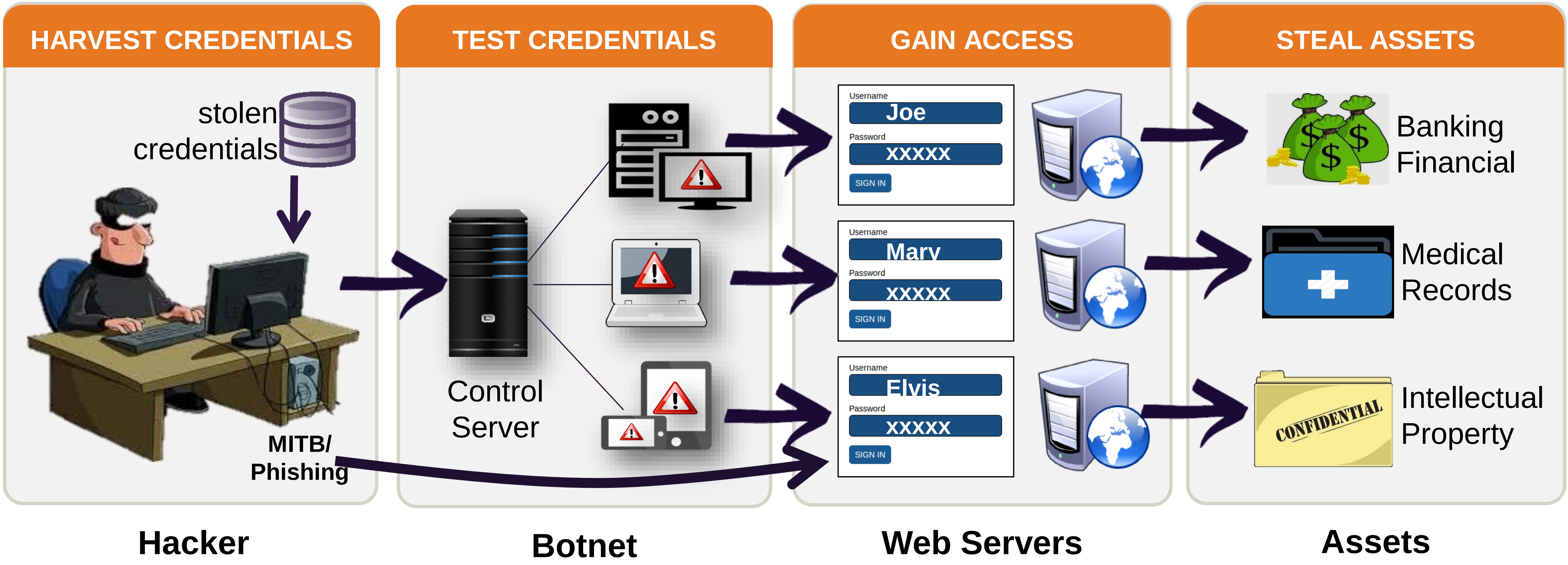
50%

Of successful web attacks involve stolen credentials



Source: Verizon 2015 DBIR

Anatomy of Account Takeover Attack



HARVEST CREDENTIALS

stolen credentials

MITB/ Phishing

Hacker

TEST CREDENTIALS

Control Server

Botnet

GAIN ACCESS

Username Joe
Password XXXXX
SIGN IN

Username Mary
Password XXXXX
SIGN IN

Username Elvis
Password XXXXX
SIGN IN

Web Servers

STEAL ASSETS

Banking Financial

Medical Records

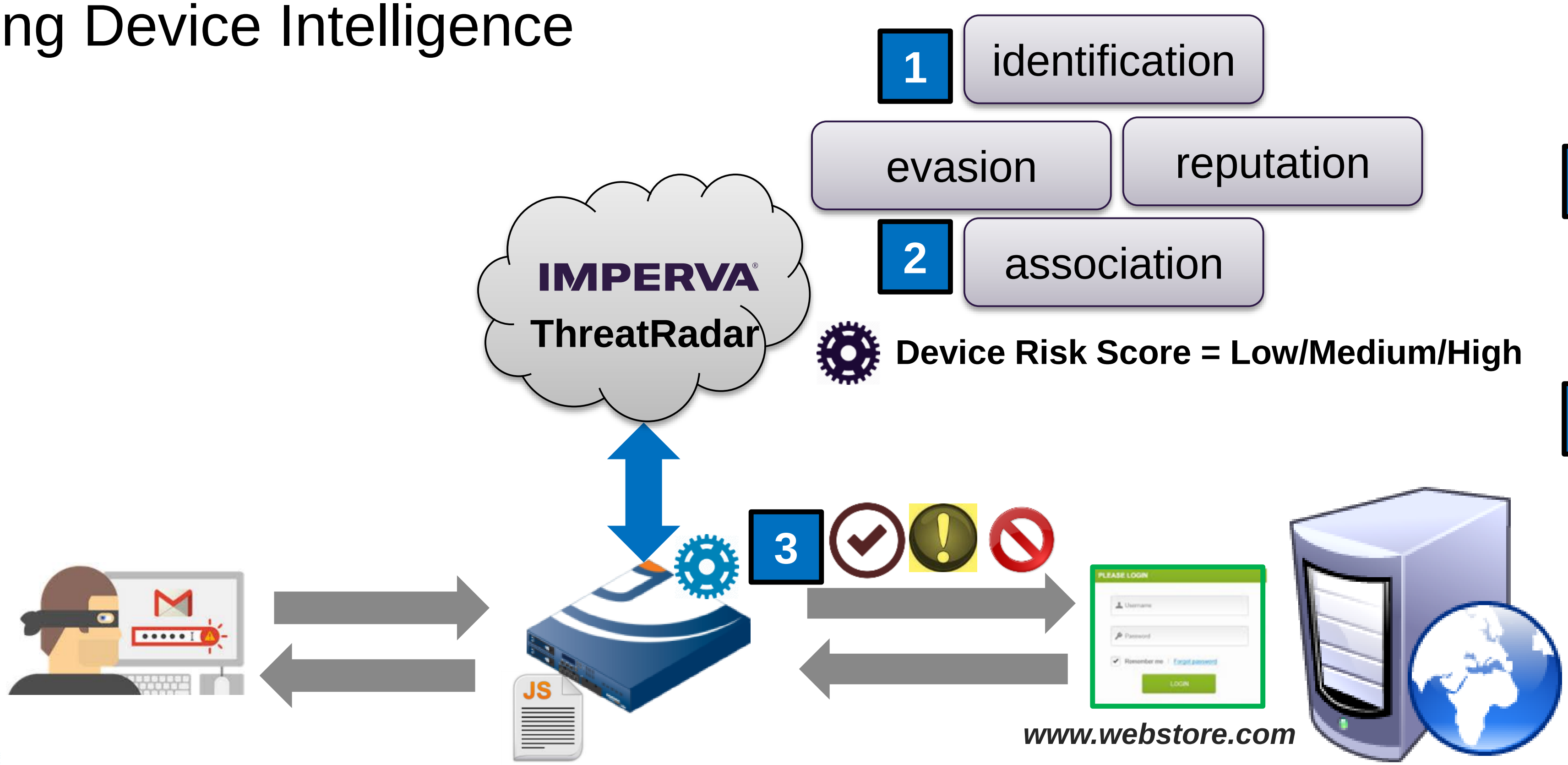
CONFIDENTIAL

Intellectual Property

Assets

Detecting Account Takeover

Using Device Intelligence



1 Device Profiling

2 Device Risk Evaluation

Returns device risk score

3 WAF Mitigation Rules

Correlates device
Risk-score with
other TR services
To audit/alert/block

WAF MITIGATION RULES:

Low-Risk (AUDIT) = Device (w/ prior fraud) attempts to login
Med-Risk (ALERT) = Device (w/ prior fraud) + Device (associated multiple accounts)
High-Risk (BLOCK) = Device (w/ prior fraud) + Device (associated w/ multiple accounts) + (TR known bot client)

Globally Crowd-sourced

Anonymous Proxy

Phishing URLs

ToR IPs

IP Forensics

Credit Card Cycling

Comment Spam IPs

Registration BOTS

Malicious IPs

SQLi IPs

RFI

Scanner IPs

Scraping BOTS

The Power of Community

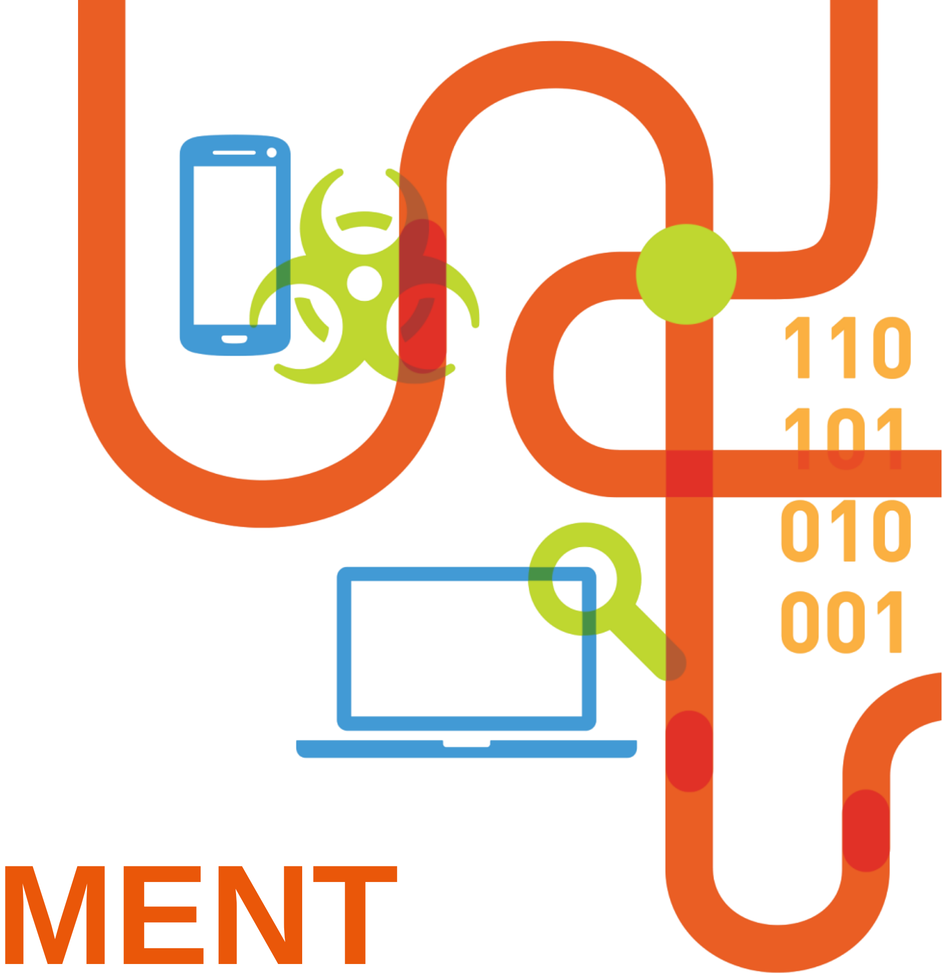
>75% of attacks come from same sources

99 little bugs in the code.
99 little bugs in the code.
Take one down, patch it around.

127 little bugs in the code...

RAPID7

appspider

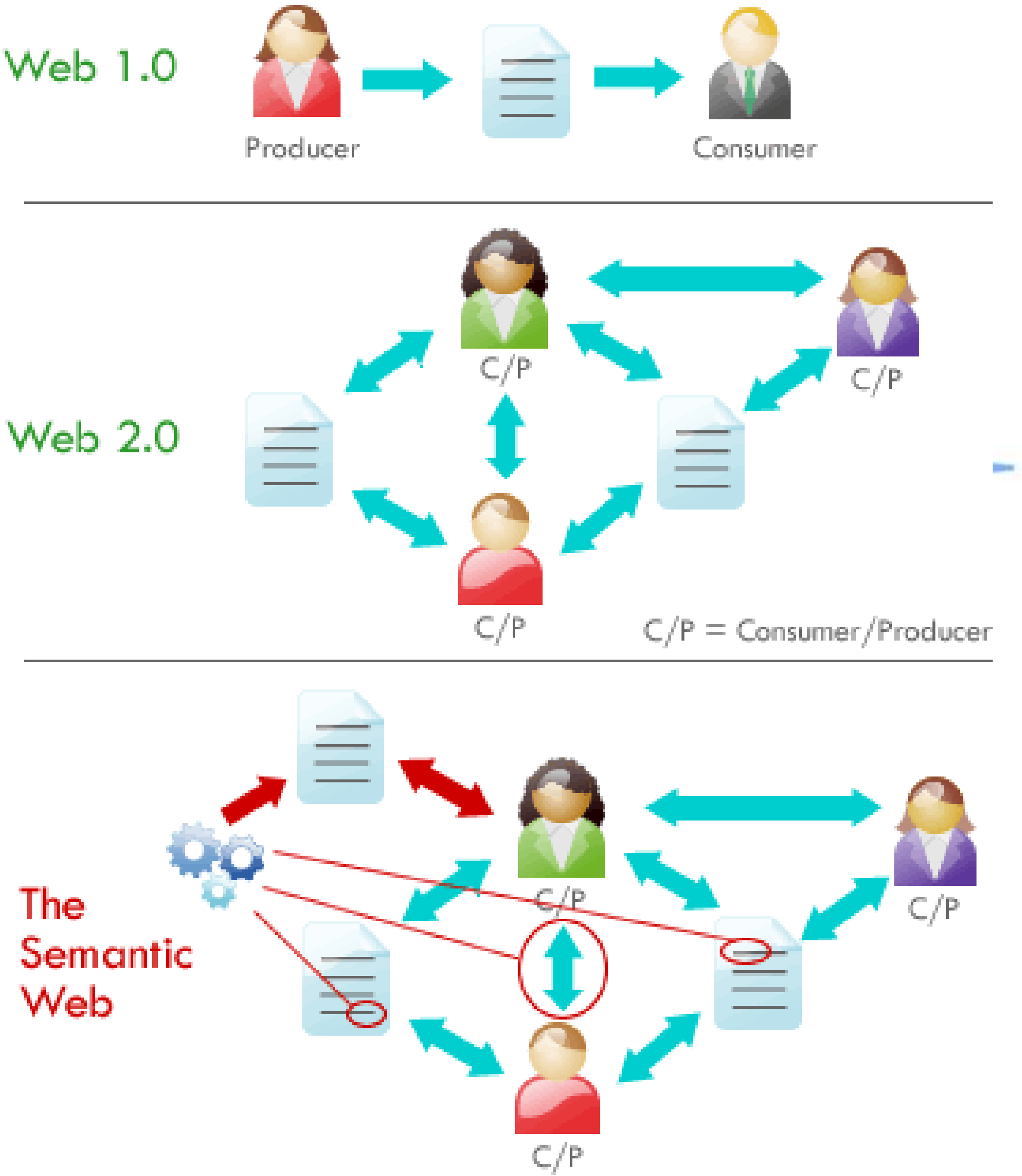


APPLICATION ASSESSMENT FOR THE MODERN WORLD

Know Your Weak Points

- Web Evolving Rapidly

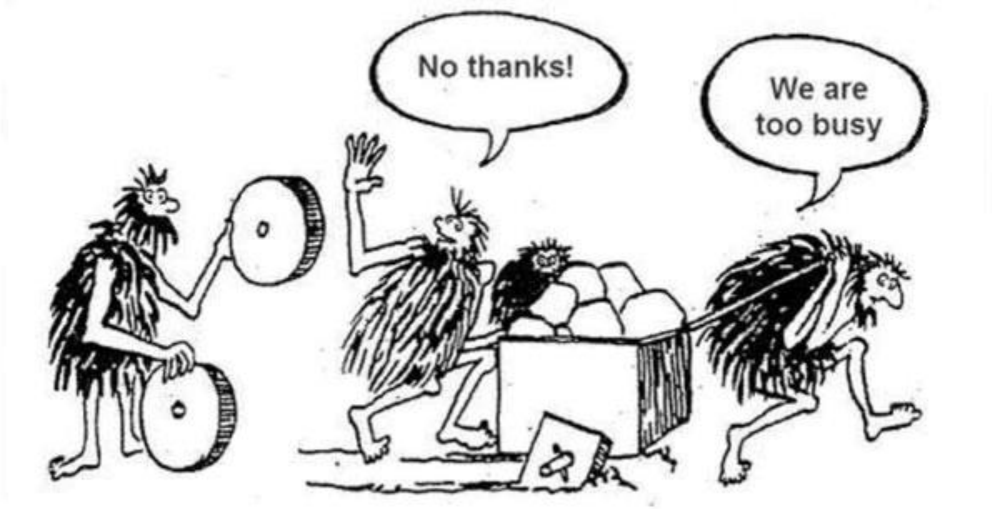
- Vulnerability responses are not consistent
  - Custom error pages can lead to false positives
- Requires advanced heuristics
  - Suppress false positives
  - Avoid false negatives
  - Difficult balance, made easier with better logic
- False Positive Costs
  - Time to investigate
  - Reputational impact to security team/MSSP
- False Negative Costs
  - Still exposed
  - Fewer findings reduces perception of value



Know Your Weak Points

- Dependence on Training: Failed Option

- Auditors rarely know the application very well
- Auditors have limited amount of time to spend training the scanners to each application
- Auditors time better spent on attacks only humans can do
- Dependence on Auditors to be able to train the scanner to every area of the application is a failed assumption



appspider

Application Assessment for the Modern World

Know your weak points

Prioritize what matters most

Improve your position

RAPID7

Know Your Weak Points

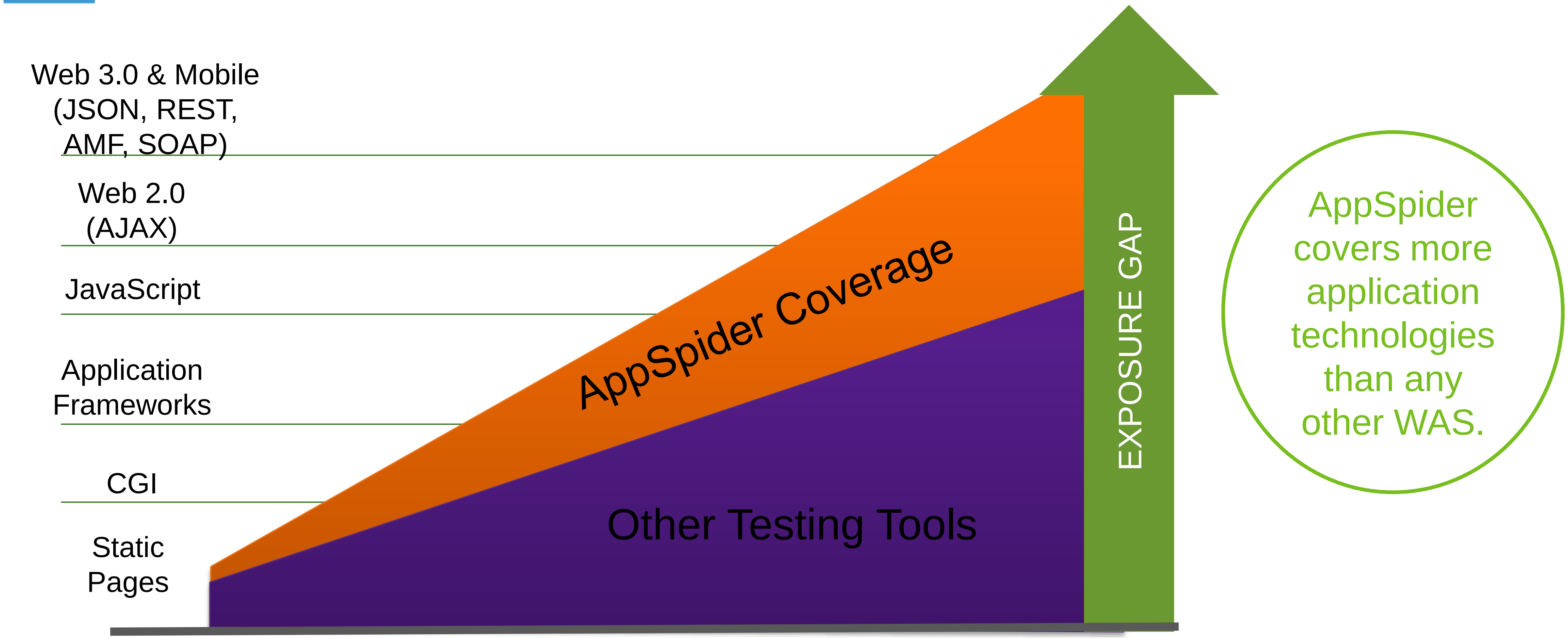
- The changing landscape

- Scanner paradigm shift
  - No longer just “HTML based” applications
  - Today’s applications are dynamic & complex
    - Rich clients – AJAX/Flash/Flex/Silverlight
    - Mobile clients - Communicate over HTTP to backend services
- Requires a paradigm shift in scanning technologies
  - Must handle Web 2.0, Mobile, and Web Services
  - Must evolve to test new formats and structures
  - JSON, REST, AMF, GWT-RPC, SOAP, XML-RPC, etc…

Flash Remoting (AMF) Flex SOAP
Flash CSRF tokens JQuery Flash shopping cart
Flex AJAX Flash Web Services JSON DOM REST DOM
GWT SOAP REST Flash Remoting (AMF) DOM SOAP XSD Flex SOAP
CSRF tokens Flash shopping cart JQuery XSD GWT Silverlight Flash
Flash JQuery REST GWT AJAX Web Services Flash Remoting (AMF) DOM AJAX JSON
Web Services Silverlight SOAP Silverlight
JSON SOAP XSD DOM Flash shopping cart JQuery GWT
SOAP GWT JQuery CSRF tokens XSD JSON
CSRF tokens AJAX REST Web Services Silverlight
Flash XSD Flash Remoting (AMF) JSON Flex
shopping cart SOAP

Know Your Weak Points

- The Widening Coverage Gap

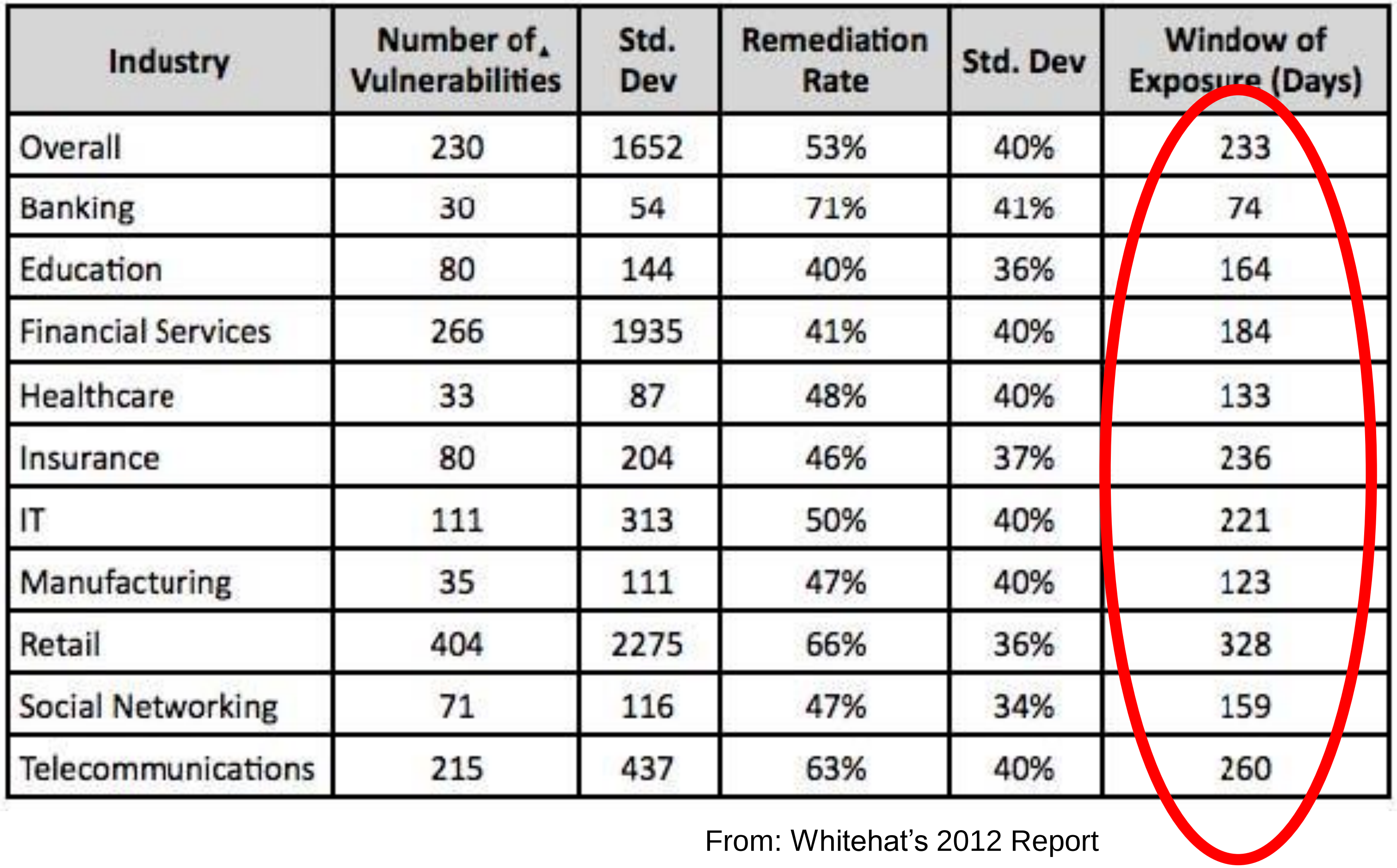


AppSpider covers more application technologies than any other WAS.

Improve Your Position

- Security Statistics Report Winter 2011

- How long does it take for website vulnerabilities to get fixed (Window of Exposure).



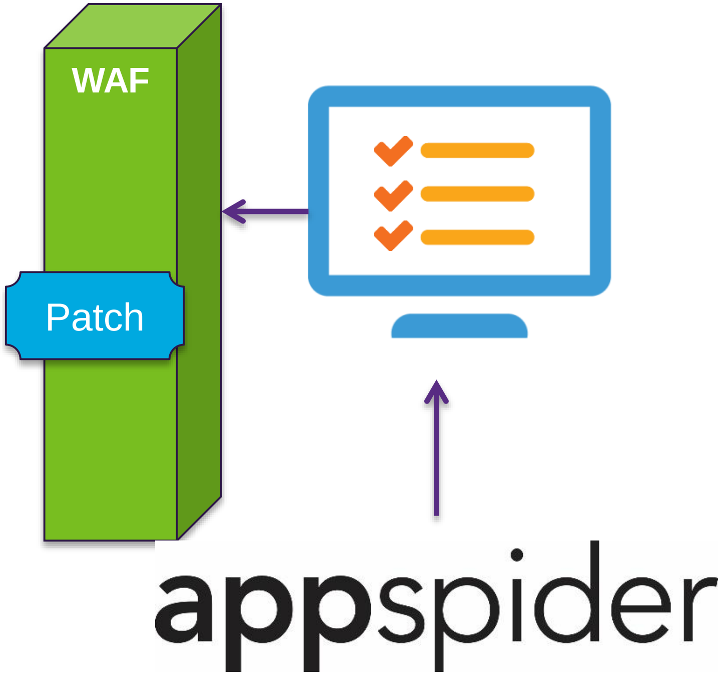
Industry	Number of Vulnerabilities	Std. Dev	Remediation Rate	Std. Dev	Window of Exposure (Days)
Overall	230	1652	53%	40%	233
Banking	30	54	71%	41%	74
Education	80	144	40%	36%	164
Financial Services	266	1935	41%	40%	184
Healthcare	33	87	48%	40%	133
Insurance	80	204	46%	37%	236
IT	111	313	50%	40%	221
Manufacturing	35	111	47%	40%	123
Retail	404	2275	66%	36%	328
Social Networking	71	116	47%	34%	159
Telecommunications	215	437	63%	40%	260

From: Whitehat's 2012 Report

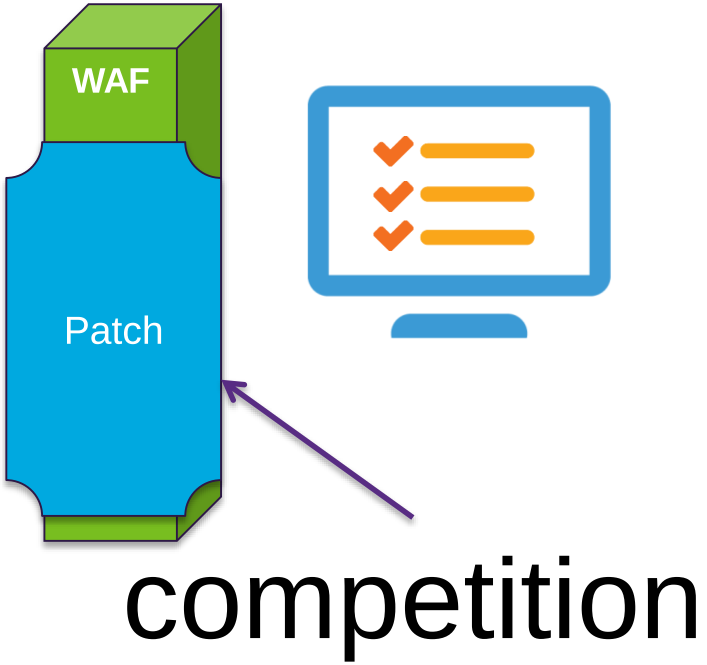
Improve Your Position

- Automate WAF/IPS Virtual Patching

Effective custom virtual patch
WAF knowledge + App knowledge



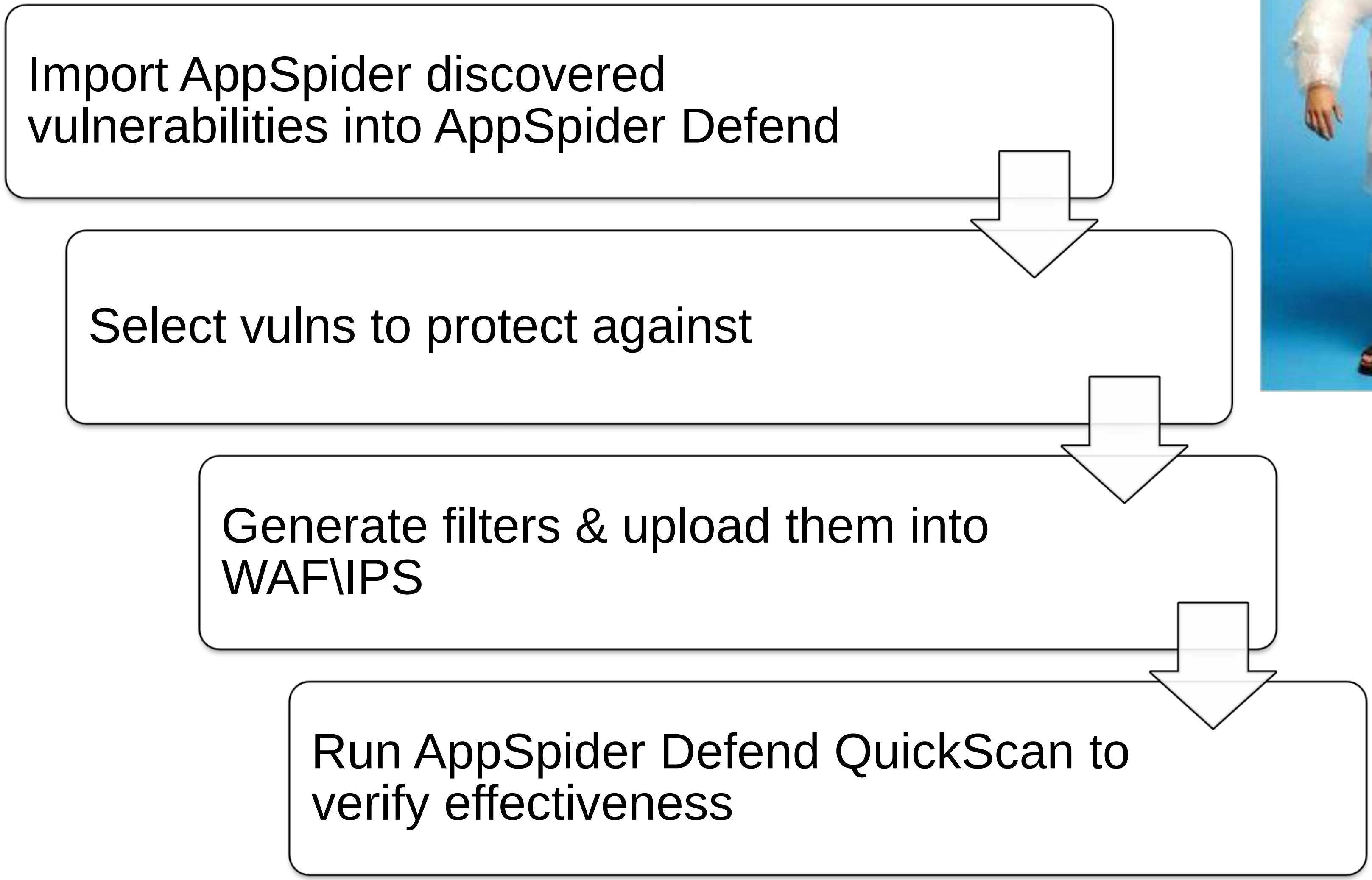
Ineffective virtual patch
Turn on default WAF rule



"[AppSpider's] generated rules are at least 39% more effective than the WAF/IPS default rules."
Application Security Consultant Larry Suto.

Improve Your Position

- Defensive Workflow



Import AppSpider discovered vulnerabilities into AppSpider Defend

Select vulns to protect against

Generate filters & upload them into WAF\IPS

Run AppSpider Defend QuickScan to verify effectiveness

CLICO

Summary

Improve Your Position

- Integration between R7 & Imperva SecureSphere WAF

- Generates rules/filters for Web Application Firewall (WAF)
- Improve effectiveness of Web Apps security tools
  - Rapid remediation of web vulnerability without modifying source code
  - Avoids tedious manual filter creation
  - Creates pinpoint specific rules/filters for your application
- Input from AppSpider saves time and effort
  - Rapid rule generation & easy installation
  - Security teams can handle installation
  - Gives developers time to update the code for the proper solution
  - Fast path to PCI compliance

Q&A ?

bartosz.krynski@clico.pl

+48 663 921 549