OWASP
The Open Web Application Security Project

Can Correlations Protect Web Applications?

Ofer Shezaf,
Product Manager, Security Solutions
HP ArcSight
ofr@hp.cm

About Myself

I live in Kibbutz Yiftah, Israel	
I create security products	Currently, Product Manager for Security Solutions at HP ArcSight
	Prior to that did security research and product management at Breach Security & at Fortify
I am an application security veteran	OWASP leader and founder of the OWASP Israeli chapter
	Leads the Web Application Firewall Evaluation Criteria project
	Wrote the ModSecurity Core Rule Set
I really try to learn what information security is	Read my blog at http://www.xiom.com
	Be ready to some philosophy of science and cognitive psychology

They Paid My Trip!

Agenda

OWASP
The Open Web Application Security Project

The Web Attacks You Haven’t Heard about and Really Matter

Correlations to the Rescue

Current WAF Implementations

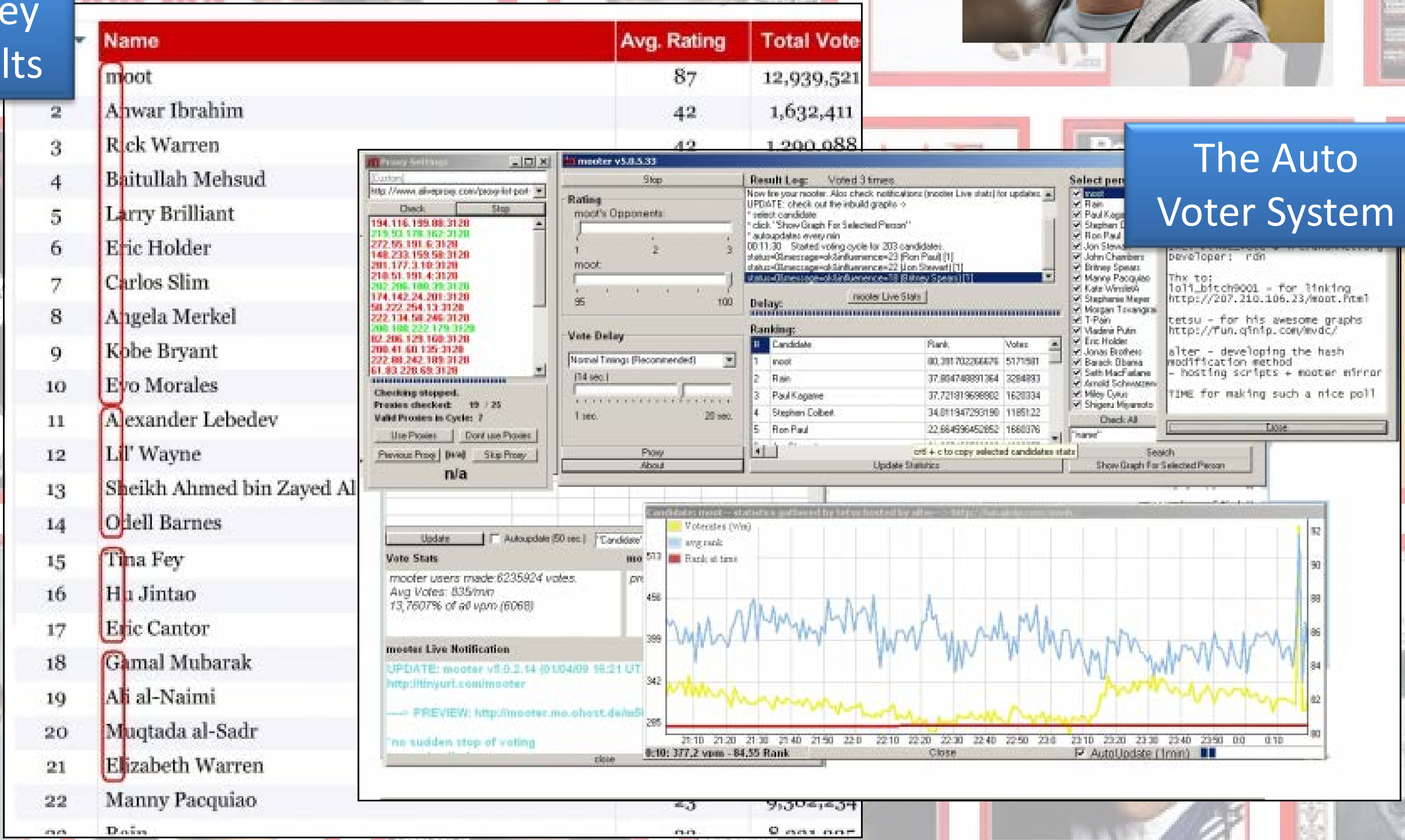
Using SIEM correlations

THE WEB ATTACKS YOU HAVEN’T HEARD ABOUT AND REALLY MATTERS

Meet the Time Magazine most influential person:

Survey Results

The Auto Voter System



	Name	Avg. Rating	Total Votes
	moot	87	12,939,521
2	Anwar Ibrahim	42	1,632,411
3	Rick Warren	42	1,290,988
4	Baitullah Mehsud		
5	Larry Brilliant		
6	Eric Holder		
7	Carlos Slim		
8	Angela Merkel		
9	Kobe Bryant		
10	Evo Morales		
11	Alexander Lebedev		
12	Lil' Wayne		
13	Sheikh Ahmed bin Zayed Al		
14	Odell Barnes		
15	Tina Fey		
16	Hu Jintao		
17	Eric Cantor		
18	Gamal Mubarak		
19	Ali al-Naimi		
20	Muqtada al-Sadr		
21	Elizabeth Warren		
22	Manny Pacquiao	43	9,302,434
	Rain		

Proxy Settings

Custom

http://www.aliveproxy.com/proxy-list-port

Check | Stop

```
194.116.199.88:3128
219.93.178.162:3128
272.55.191.6:3128
148.233.159.58:3128
201.177.3.10:3128
210.51.191.4:3128
202.206.180.39:3128
174.142.24.201:3128
58.222.254.13:3128
222.134.58.246:3128
200.188.222.179:3128
82.206.129.160:3128
200.41.60.135:3128
222.88.242.189:3128
61.83.228.69:3128
```

Checking stopped.
Proxies checked: 19 / 25
Valid Proxies in Cycle: 7

Use Proxies | Dont use Proxies
Previous Proxy | [n/a] | Skip Proxy

n/a

mooter v5.0.5.33

Stop

Rating
moot's Opponents: 1 2 3
moot: 95 100

Vote Delay
Normal Timing (Recommended)
(14 sec.)
1 sec. 20 sec.

Proxy
About

Result Log: Voted 3 times

```
Now fire your mooter. Also check notifications (mooter Live stats) for updates
UPDATE: check out the inbuild graphs ->
* select candidate
* click "Show Graph For Selected Person"
* autoupdates every min
00:11:30    Started voting cycle for 203 candidates
status=0&message=ok&influence=23 [Ron Paul] [1]
status=0&message=ok&influence=22 [Jon Stewart] [1]
status=0&message=ok&influence=18 [Britney Spears] [1]
```

mooter Live Stats

Delay:

Ranking:

#	Candidate	Rank	Votes
1	moot	80.3917022664 76	5171581
2	Rain	37.8047488891364	3284893
3	Paul Kagame	37.7218196988802	1620334
4	Stephen Colbert	34.0119472931 90	1185122
5	Ron Paul	22.8645964528 52	1660376

crtl + c to copy selected candidates stats

Update Statistics

Select person

☑ moot
☑ Rain
☑ Paul Kagame
☑ Stephen Colbert
☑ Ron Paul
☑ Jon Stewart
☑ John Chambers
☑ Britney Spears
☑ Manny Pacquiao
☑ Kate Winslet
☑ Stephenie Meyer
☑ Morgan Tsvangirai
☑ T-Pain
☑ Vladimir Putin
☑ Eric Holder
☑ Jonas Brothers
☑ Barack Obama
☑ Seth MacFarlane
☑ Arnold Schwarzen...
☑ Miley Cyrus
☑ Shigeru Miyamoto

Check All

"name"

Search
Show Graph For Selected Person

```
developer:  rdn

Thx to:
lol1_bitch9001 - for linking
http://207.210.106.23/moot.html

tetsu - for his awesome graphs
http://fun.qinip.com/mvdc/

alter - developing the hash
modification method
- hosting scripts + mooter mirror

TIME for making such a nice poll
```

Close

Update | ☐ Autoupdate (50 sec.) | "Candidate"

Vote Stats

mooter users made 6235924 votes.
Avg Votes: 835/min
13,7607% of all vpm (6068)

mooter Live Notification

UPDATE: mooter v5.0.2.14 (01/04/09 16:21 UT
http://tinyurl.com/mooter

---> PREVIEW: http://mooter.mo.ohost.de/a5

"no sudden stop of voting

close

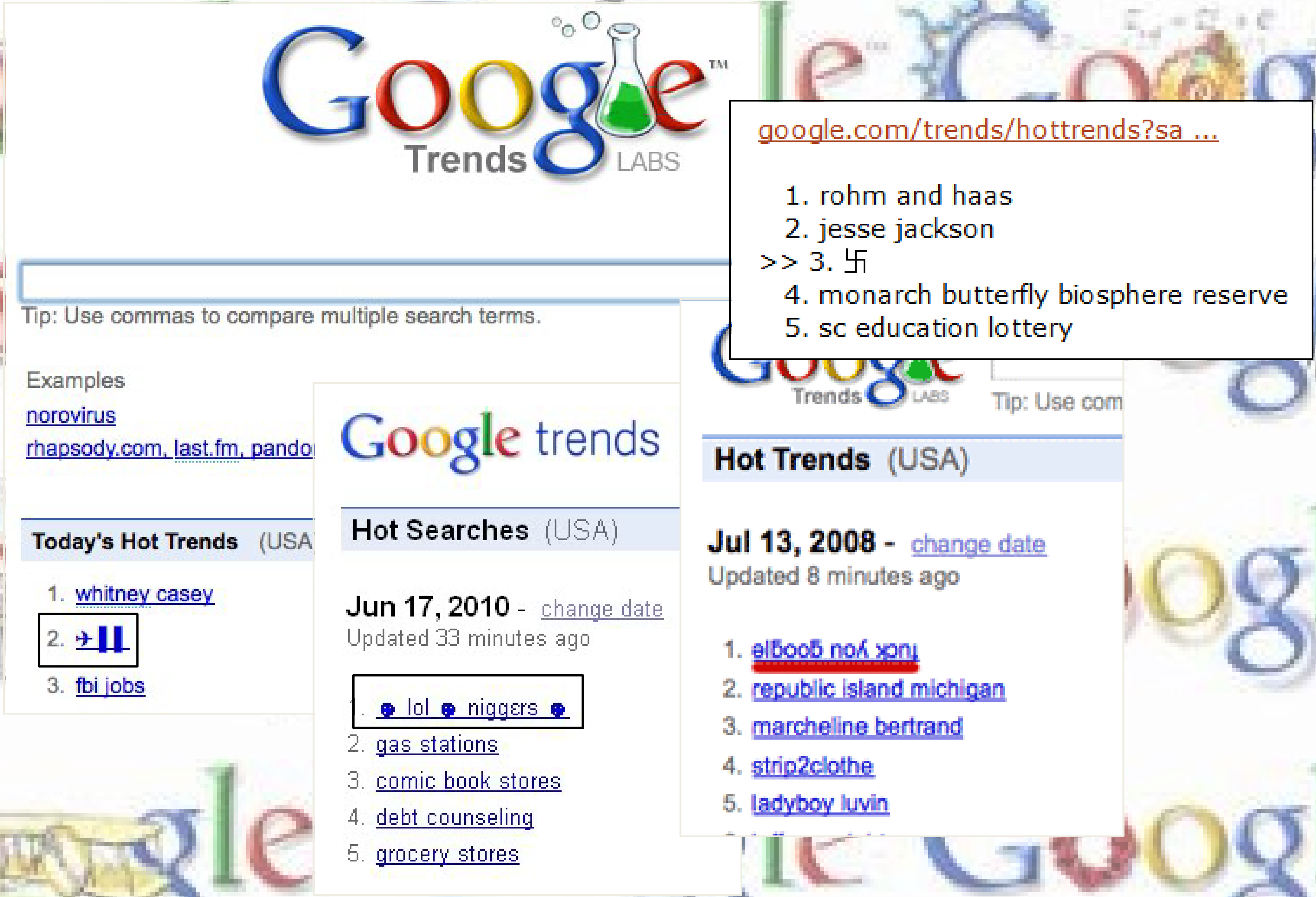
0:10: 377,2 vpm - 84,35 Rank

Close

☑ AutoUpdate (1min)

http://musicmachinery.com/2009/04/15/inside-the-precision-hack/

Found out Some of Google's Most Searched Keywords



Google Trends LABS

Tip: Use commas to compare multiple search terms.

Examples

norovirus

rhapsody.com, last.fm, pando

Today's Hot Trends (USA

1. whitney casey
2. ✈▌▌
3. fbi jobs

Google trends

Hot Searches (USA)

Jun 17, 2010 - change date

Updated 33 minutes ago

1. ☻ lol ☻ niggers ☻
2. gas stations
3. comic book stores
4. debt counseling
5. grocery stores

Google Trends LABS

Tip: Use com

Hot Trends (USA)

Jul 13, 2008 - change date

Updated 8 minutes ago

1. ǝlƃooƃ noʎ ʞɔnɟ
2. republic island michigan
3. marcheline bertrand
4. strip2clothe
5. ladyboy luvin

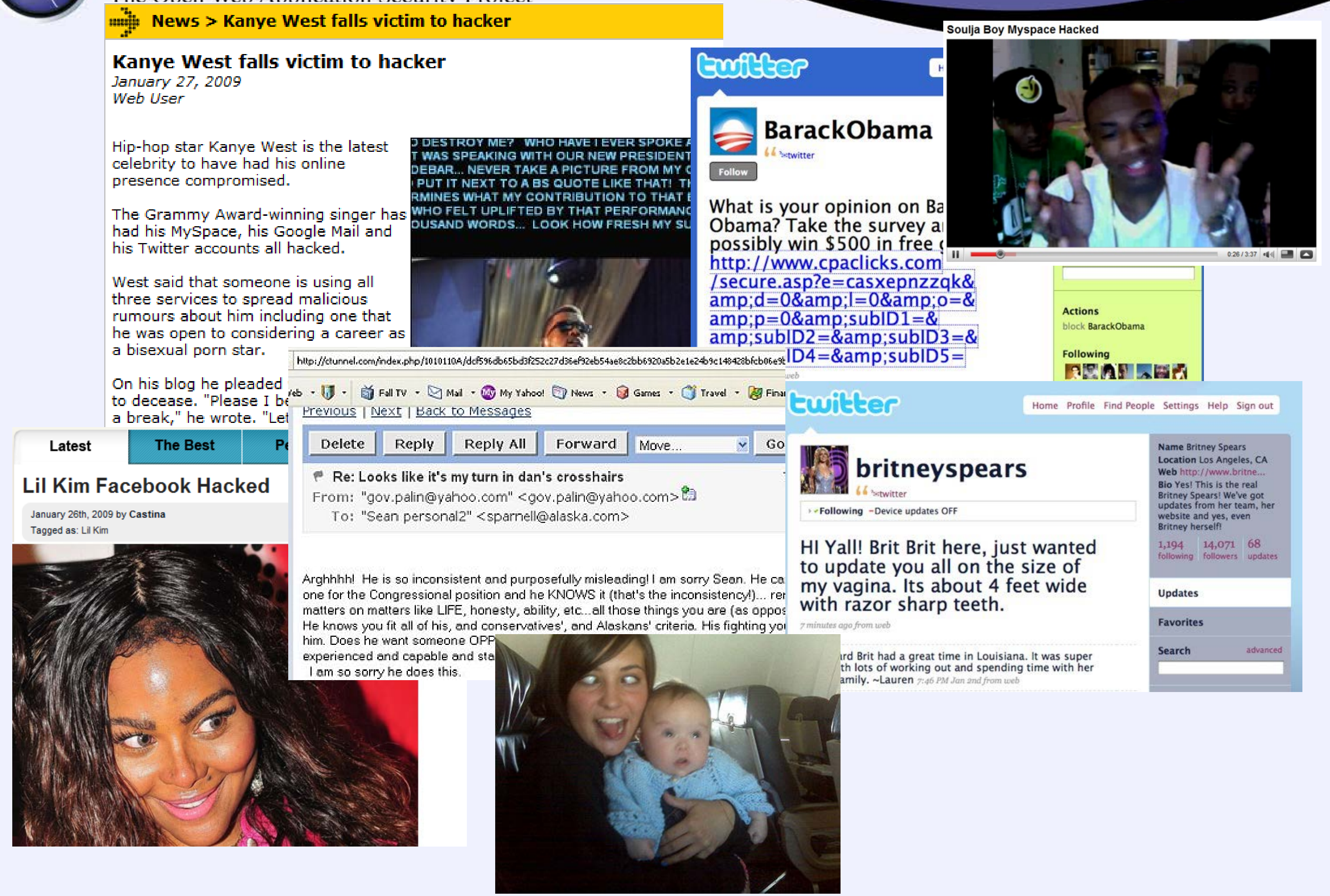
google.com/trends/hottrends?sa ...

1. rohm and haas
2. jesse jackson

>> 3. 卐

4. monarch butterfly biosphere reserve
5. sc education lottery

Those Damn Rappers (and Politicians)



News > Kanye West falls victim to hacker

Kanye West falls victim to hacker

January 27, 2009
Web User

Hip-hop star Kanye West is the latest celebrity to have had his online presence compromised.

The Grammy Award-winning singer has had his MySpace, his Google Mail and his Twitter accounts all hacked.

West said that someone is using all three services to spread malicious rumours about him including one that he was open to considering a career as a bisexual porn star.

On his blog he pleaded to decease. "Please I be a break," he wrote. "Let

D DESTROY ME? WHO HAVE I EVER SPOKE A
T WAS SPEAKING WITH OUR NEW PRESIDENT
DEBAR... NEVER TAKE A PICTURE FROM MY C
PUT IT NEXT TO A BS QUOTE LIKE THAT! TH
RMINES WHAT MY CONTRIBUTION TO THAT E
WHO FELT UPLIFTED BY THAT PERFORMANC
OUSAND WORDS... LOOK HOW FRESH MY SU

BarackObama

What is your opinion on Ba Obama? Take the survey a possibly win $500 in free http://www.cpaclicks.com/secure.asp?e=casxepnzzqk&amp;d=0&amp;l=0&amp;o=&amp;p=0&amp;subID1=&amp;subID2=&amp;subID3=&amp;subID4=&amp;subID5=

web

Actions
block BarackObama

Following

Soulja Boy Myspace Hacked

Latest | The Best | Pe

Lil Kim Facebook Hacked

January 26th, 2009 by Castina
Tagged as: Lil Kim

http://cltunnel.com/index.php/1010110A/dcf596db65bd3f252c27d36ef92eb54ae8c2bb6920a5b2e1e24b9c148428bfcb06e9

Web | Fall TV | Mail | My Yahoo! | News | Games | Travel | Finan
Previous | Next | Back to Messages
Delete | Reply | Reply All | Forward | Move... | Go

Re: Looks like it's my turn in dan's crosshairs
From: "gov.palin@yahoo.com" <gov.palin@yahoo.com>
To: "Sean personal2" <sparnell@alaska.com>

Arghhhh! He is so inconsistent and purposefully misleading! I am sorry Sean. He ca one for the Congressional position and he KNOWS it (that's the inconsistency!)... rer matters on matters like LIFE, honesty, ability, etc...all those things you are (as oppos He knows you fit all of his, and conservatives', and Alaskans' criteria. His fighting you him. Does he want someone OPP experienced and capable and sta
I am so sorry he does this.

britneyspears

twitter

Following - Device updates OFF

HI Yall! Brit Brit here, just wanted to update you all on the size of my vagina. Its about 4 feet wide with razor sharp teeth.

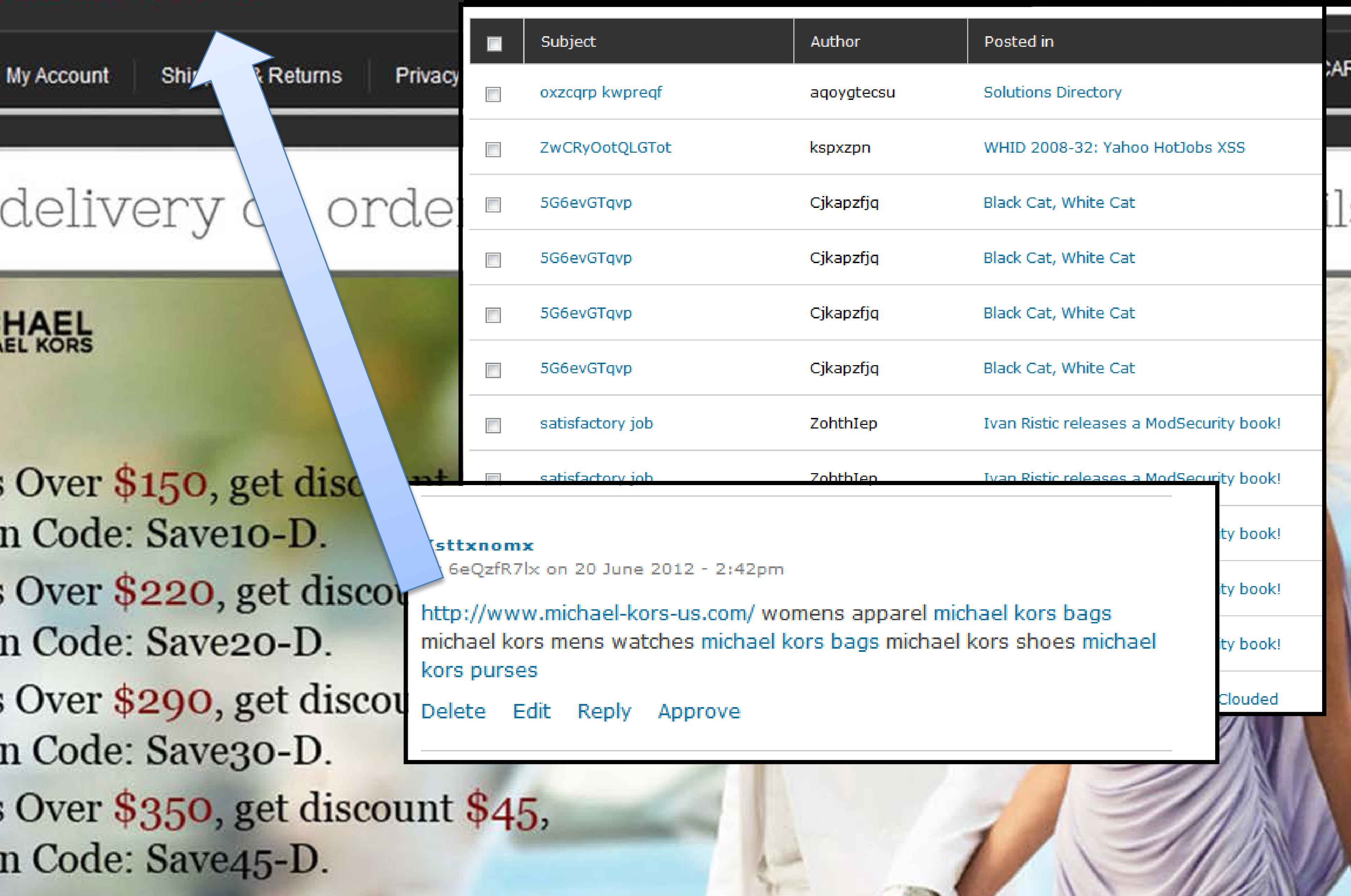
7 minutes ago from web

rd Brit had a great time in Louisiana. It was super th lots of working out and spending time with her amily. ~Lauren 7:46 PM Jan 2nd from web

Name Britney Spears
Location Los Angeles, CA
Web http://www.britne...
Bio Yes! This is the real Britney Spears! We've got updates from her team, her website and yes, even Britney herself!

1,194 following | 14,071 followers | 68 updates

SEO and Comments Spam



□	Subject	Author	Posted in
□	oxzcqrp kwpreqf	aqoygtecsu	Solutions Directory
□	ZwCRyOotQLGTot	kspxzpn	WHID 2008-32: Yahoo HotJobs XSS
□	5G6evGTqvp	Cjkapzfjq	Black Cat, White Cat
□	5G6evGTqvp	Cjkapzfjq	Black Cat, White Cat
□	5G6evGTqvp	Cjkapzfjq	Black Cat, White Cat
□	5G6evGTqvp	Cjkapzfjq	Black Cat, White Cat
□	satisfactory job	ZohthIep	Ivan Ristic releases a ModSecurity book!
□	satisfactory job	ZohthIep	Ivan Ristic releases a ModSecurity book!
			ty book!
			ty book!
			ty book!
			Clouded

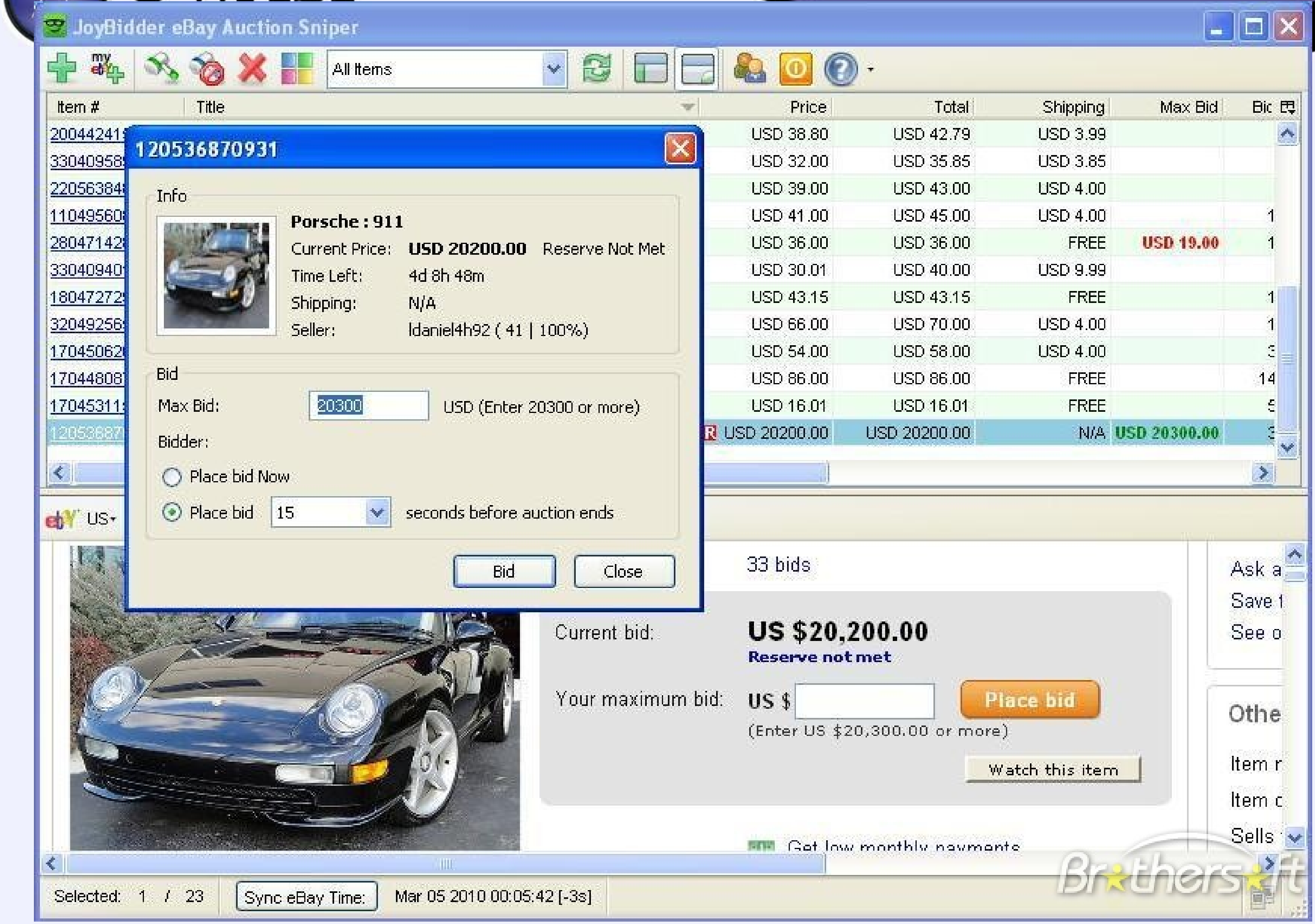
sttxnomx

6eQzfR7lx on 20 June 2012 - 2:42pm

http://www.michael-kors-us.com/ womens apparel michael kors bags michael kors mens watches michael kors bags michael kors shoes michael kors purses

Delete Edit Reply Approve

Auction Sniping



JoyBidder eBay Auction Sniper

Item #	Title	Price	Total	Shipping	Max Bid	Bic
20044241		USD 38.80	USD 42.79	USD 3.99		
33040958		USD 32.00	USD 35.85	USD 3.85		
22056384		USD 39.00	USD 43.00	USD 4.00		
11049560		USD 41.00	USD 45.00	USD 4.00		1
28047142		USD 36.00	USD 36.00	FREE	USD 19.00	1
33040940		USD 30.01	USD 40.00	USD 9.99		
18047272		USD 43.15	USD 43.15	FREE		1
32049256		USD 66.00	USD 70.00	USD 4.00		1
17045062		USD 54.00	USD 58.00	USD 4.00		3
17044808		USD 86.00	USD 86.00	FREE		14
17045311		USD 16.01	USD 16.01	FREE		5
12053687		R USD 20200.00	USD 20200.00	N/A	USD 20300.00	3

120536870931

Info

Porsche : 911

Current Price: **USD 20200.00** Reserve Not Met

Time Left: 4d 8h 48m

Shipping: N/A

Seller: ldaniel4h92 (41 | 100%)

Bid

Max Bid: 20300 USD (Enter 20300 or more)

Bidder:

○ Place bid Now

● Place bid 15 seconds before auction ends

Mar 05 2010 00:05:42 [-3s]

33 bids

Current bid: **US $20,200.00**

Reserve not met

Your maximum bid: US $

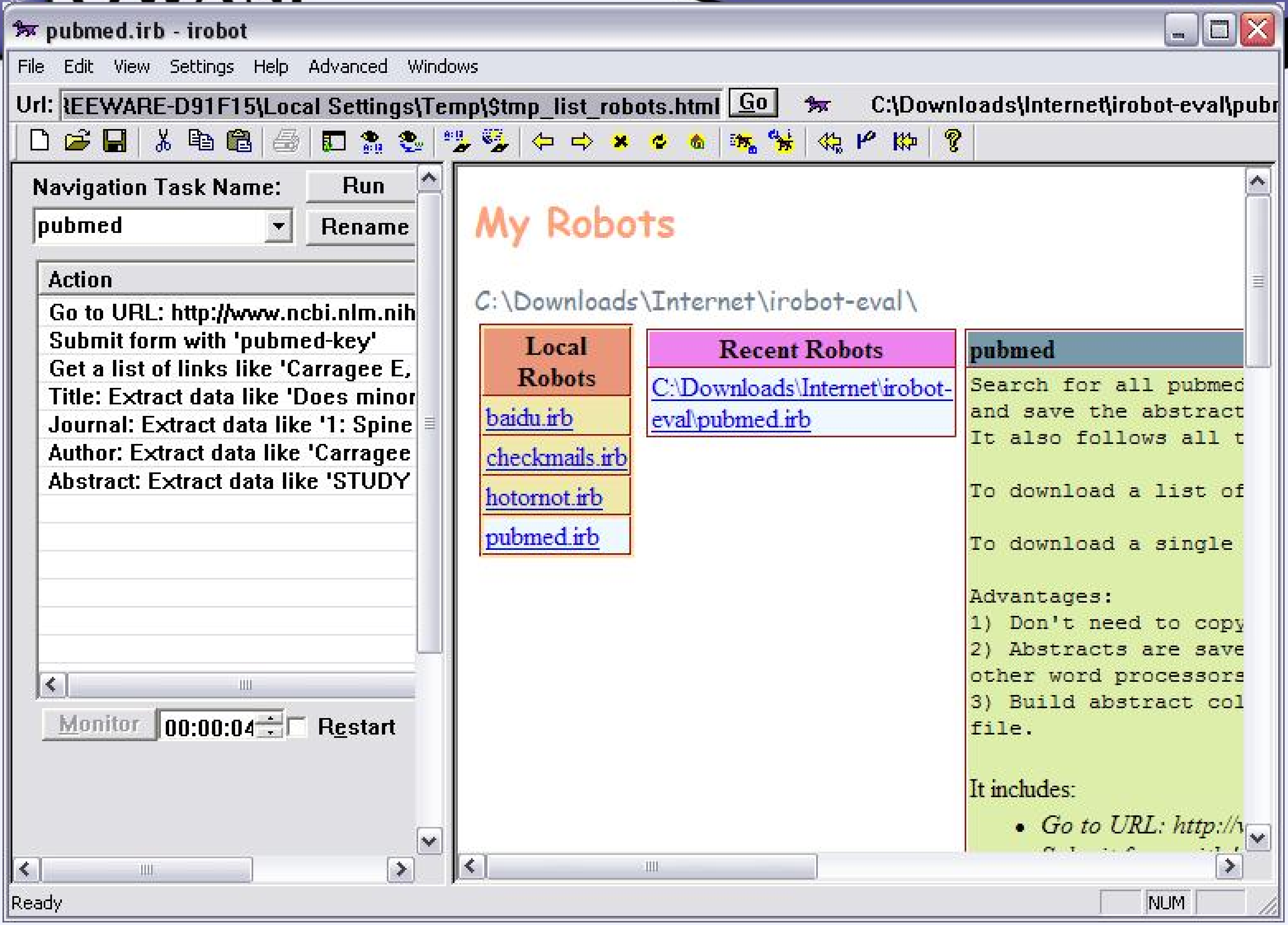
(Enter US $20,300.00 or more)

Exclusive: Google’s Click Fraud Rate is Less than 2%

Of $36 Billion!

It’s $720 Million for god sake!

Web Scraping



Url: :EEWARE-D91F15\Local Settings\Temp\$tmp_list_robots.html

C:\Downloads\Internet\irobot-eval\pubr

Navigation Task Name: pubmed

Action
Go to URL: http://www.ncbi.nlm.nih
Submit form with 'pubmed-key'
Get a list of links like 'Carragee E,
Title: Extract data like 'Does minor
Journal: Extract data like '1: Spine
Author: Extract data like 'Carragee
Abstract: Extract data like 'STUDY

00:00:04 □ Restart

My Robots

C:\Downloads\Internet\irobot-eval\

Local Robots
baidu.irb
checkmails.irb
hotornot.irb
pubmed.irb

Recent Robots
C:\Downloads\Internet\irobot-eval\pubmed.irb

pubmed

```
Search for all pubmed
and save the abstract
It also follows all t

To download a list of

To download a single

Advantages:
1) Don't need to copy
2) Abstracts are save
other word processors
3) Build abstract col
file.
```

It includes:

- *Go to URL: http://v*

And I did not have time for

Ticket Scalping

Automated Stock Trading

Game Bots

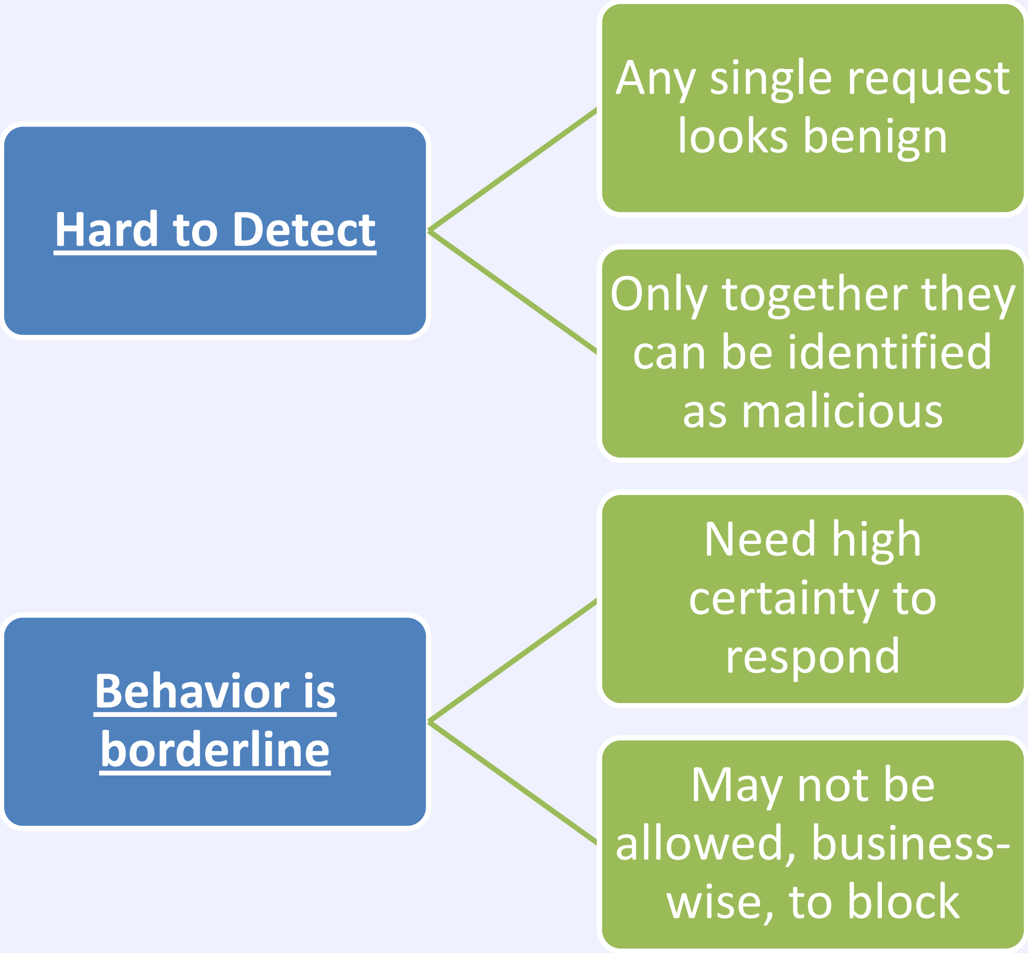
And the Usual Lengthy Attacks

Slow rate Reconnaissance

Brute Force

Distributed Denial of Service

What's Common to Those Attacks?



Hard to Detect

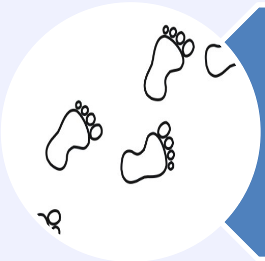
- Any single request looks benign
- Only together they can be identified as malicious

Behavior is borderline

- Need high certainty to respond
- May not be allowed, business-wise, to block

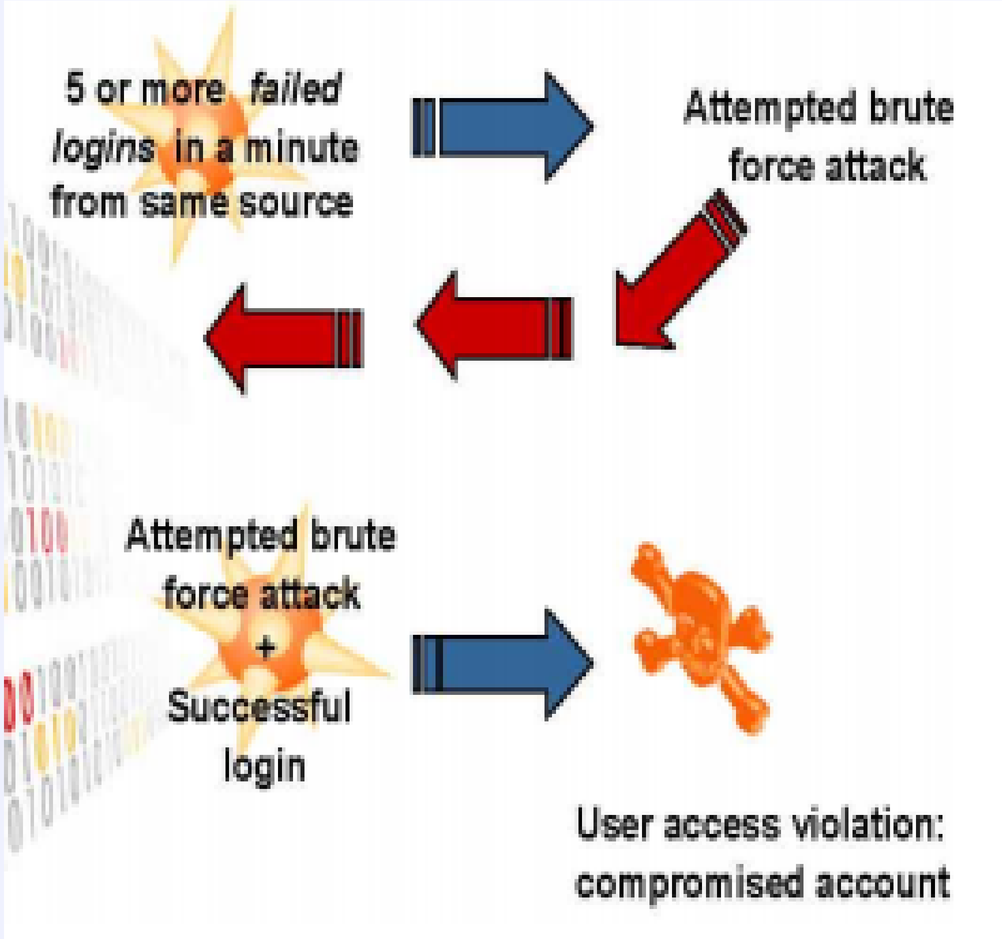
CORRELATIONS TO THE RESCUE

Follow Sequences



Multi-Stage Attacks

HTTP Session Tacking



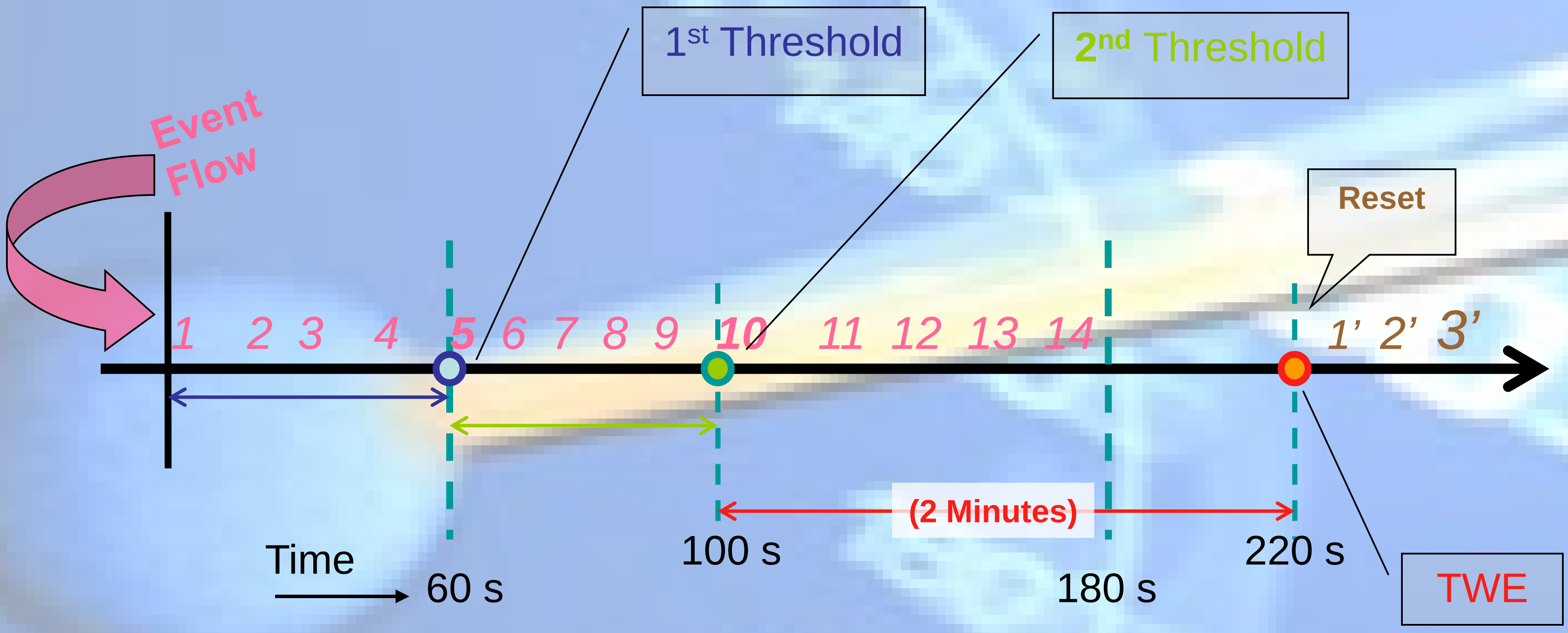
5 or more *failed logins* in a minute from same source

Attempted brute force attack

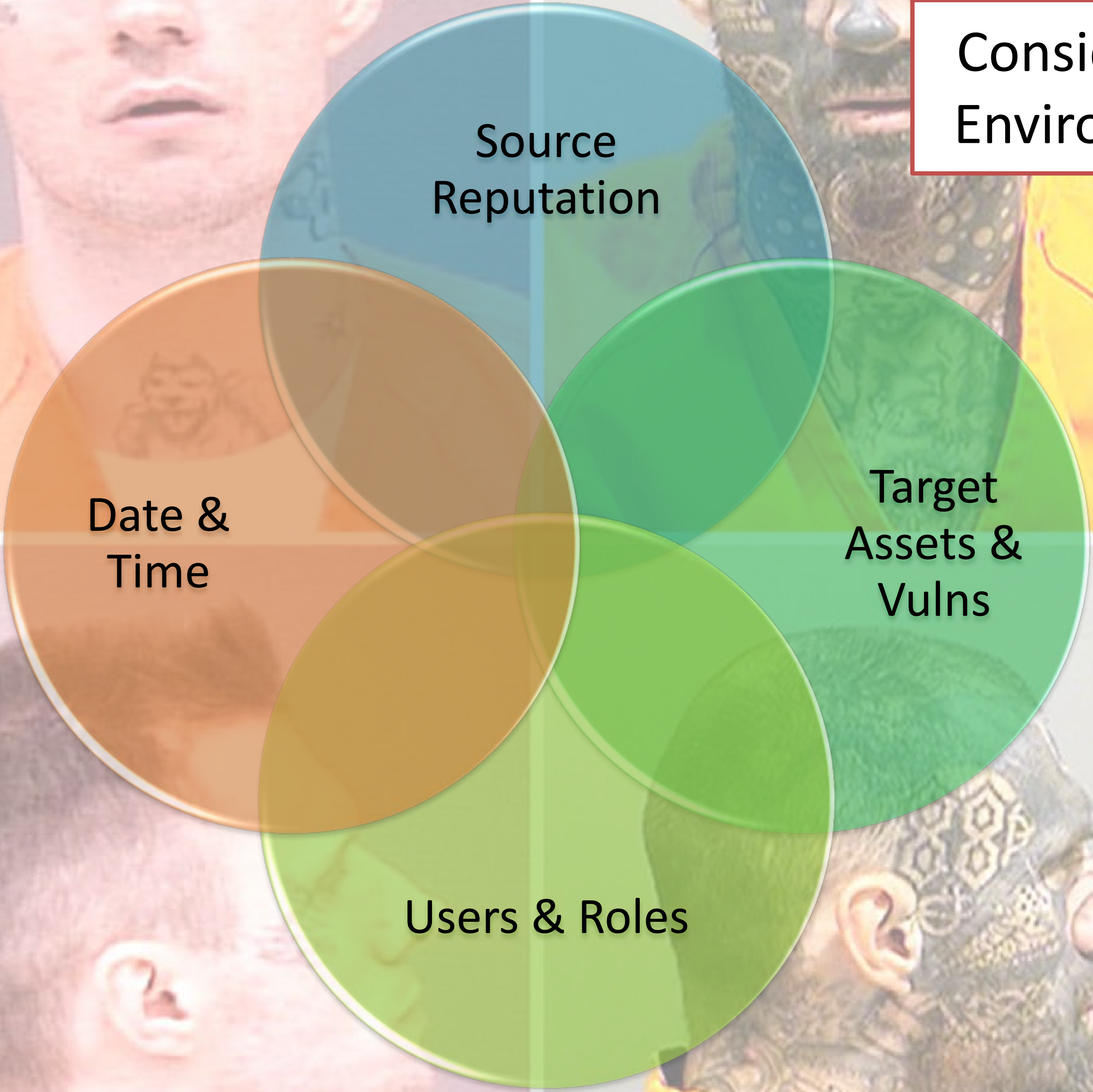
Attempted brute force attack + Successful login

User access violation: compromised account

Determine Rate



Consider the Environment



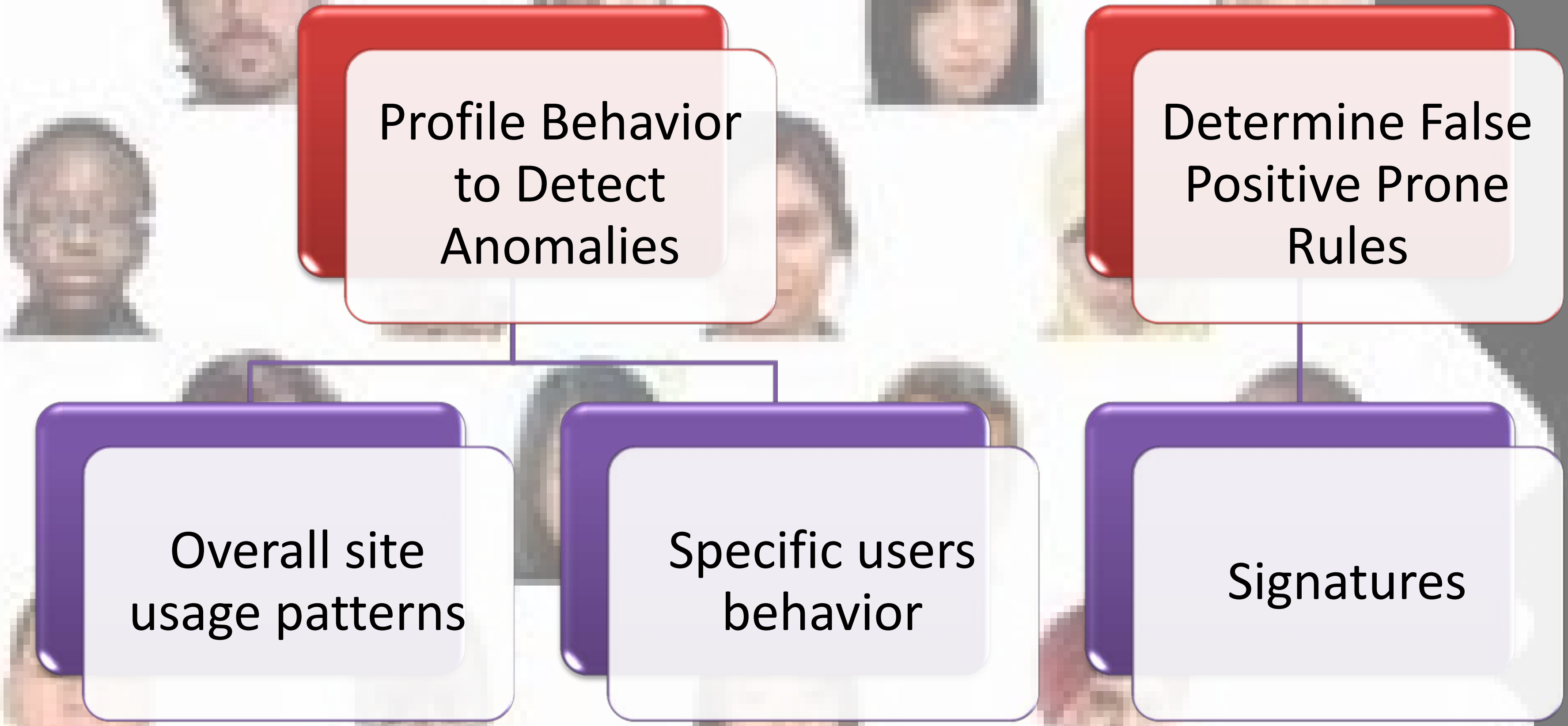
Source Reputation

Date & Time

Target Assets & Vulns

Users & Roles

Statistics & Behavior Analysis



Profile Behavior to Detect Anomalies

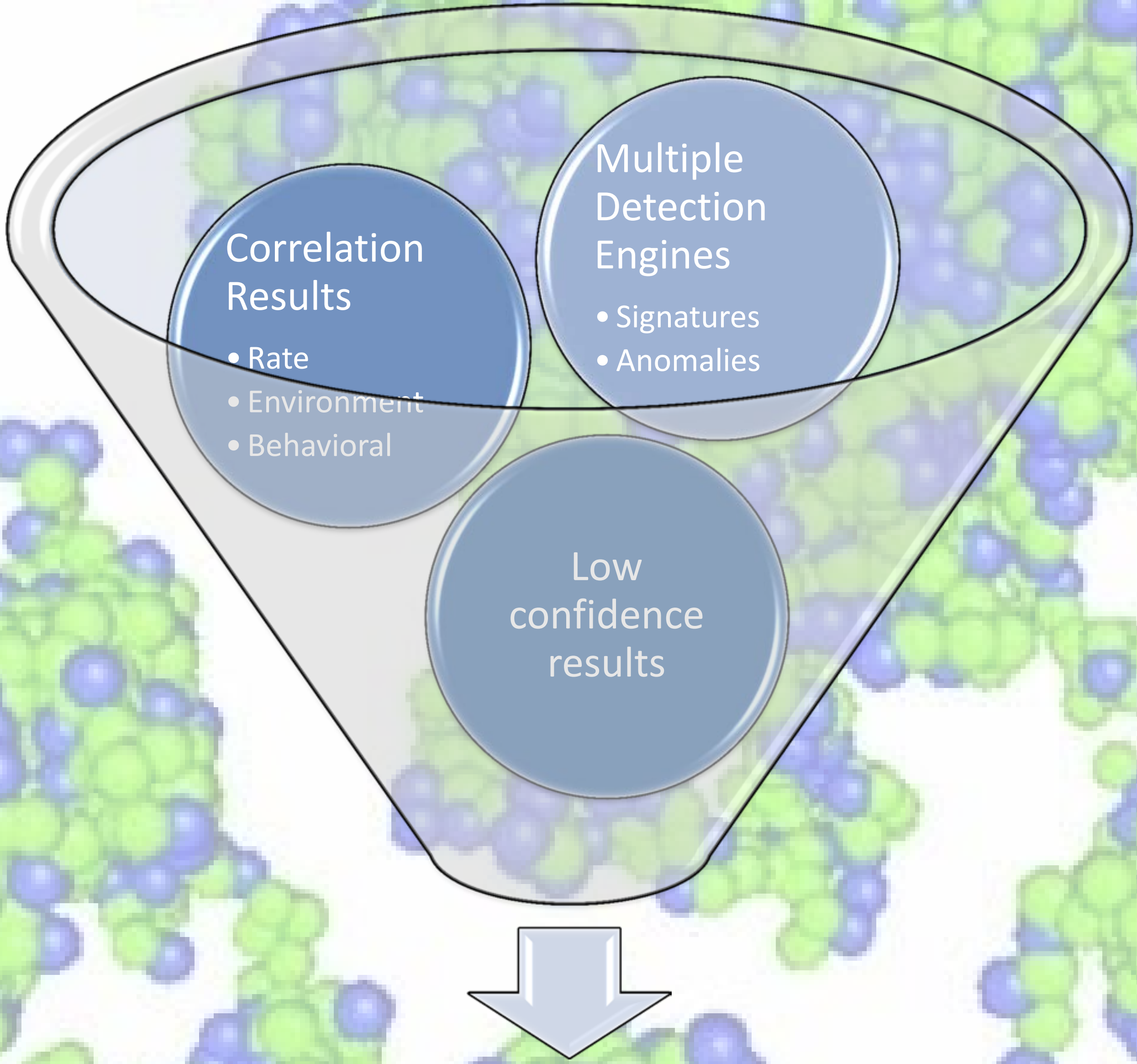
Overall site usage patterns

Specific users behavior

Determine False Positive Prone Rules

Signatures

Aggregate Indicators



Correlation Results

- Rate
- Environment
- Behavioral

Multiple Detection Engines

- Signatures
- Anomalies

Low confidence results

Conclusive Answer

CURRENT WAF IMPLEMENTATIONS

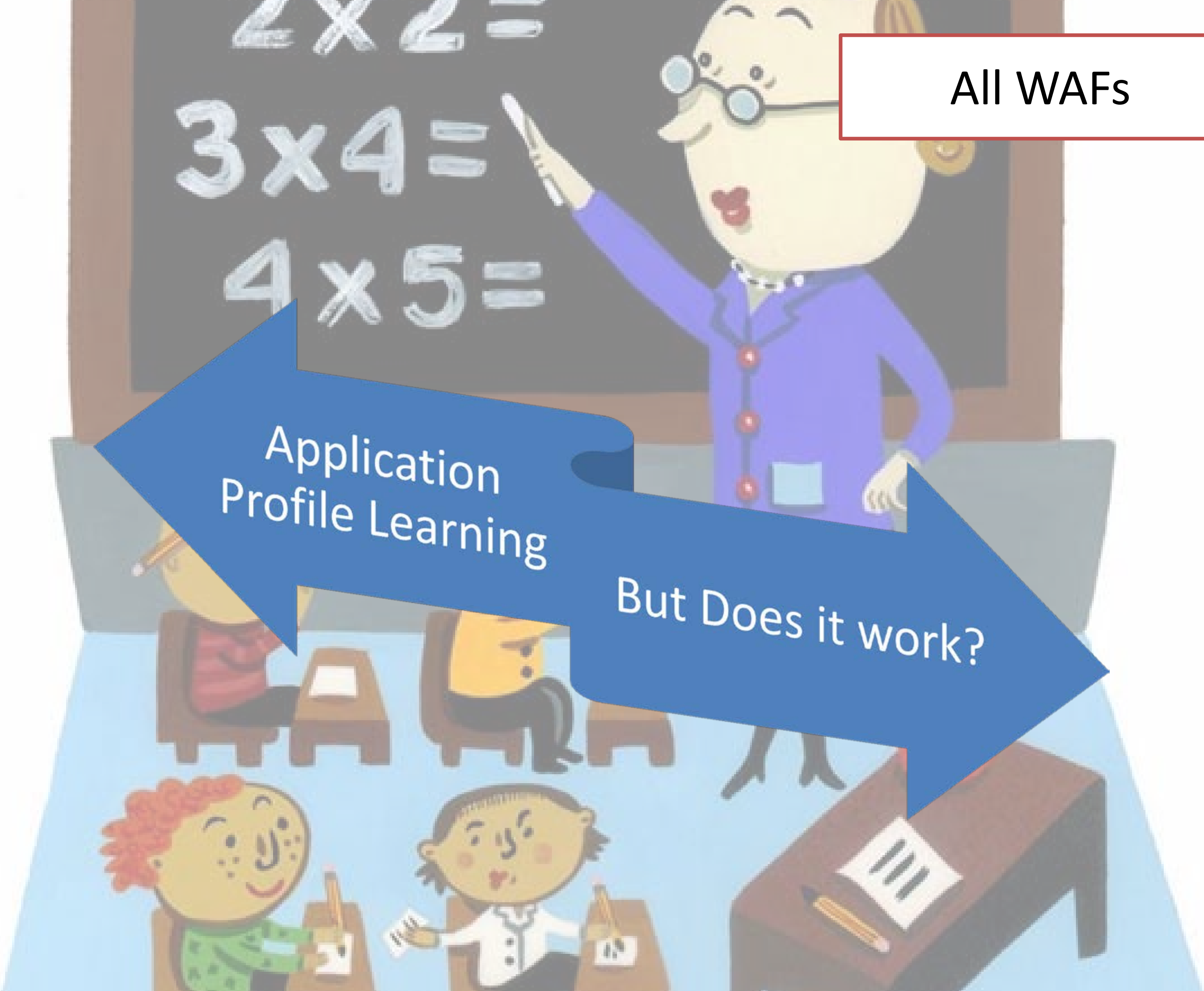
Rules of Engagement

I say only good things

I am limited to what’s publicly available or disclosed by companies specifically for this project

If I get customers input (from you…) I will add it

All WAFs

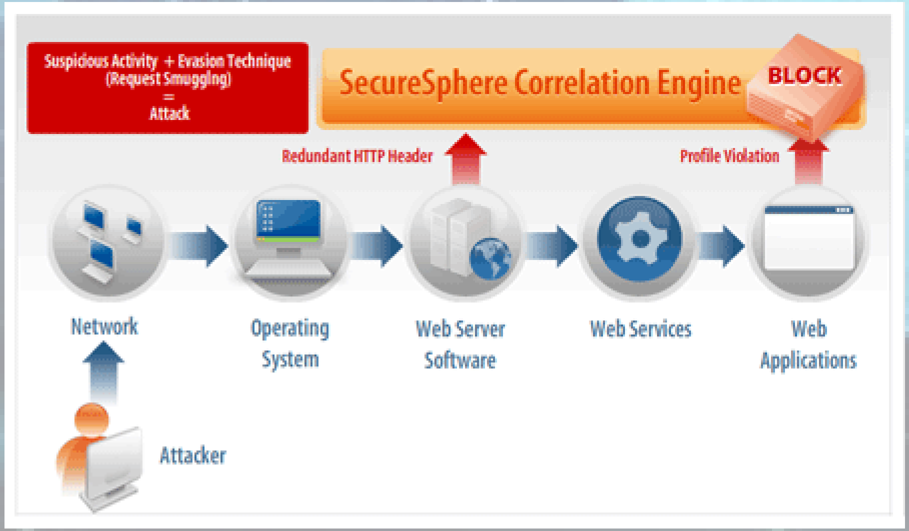


Application Profile Learning

But Does it work?

Imperva

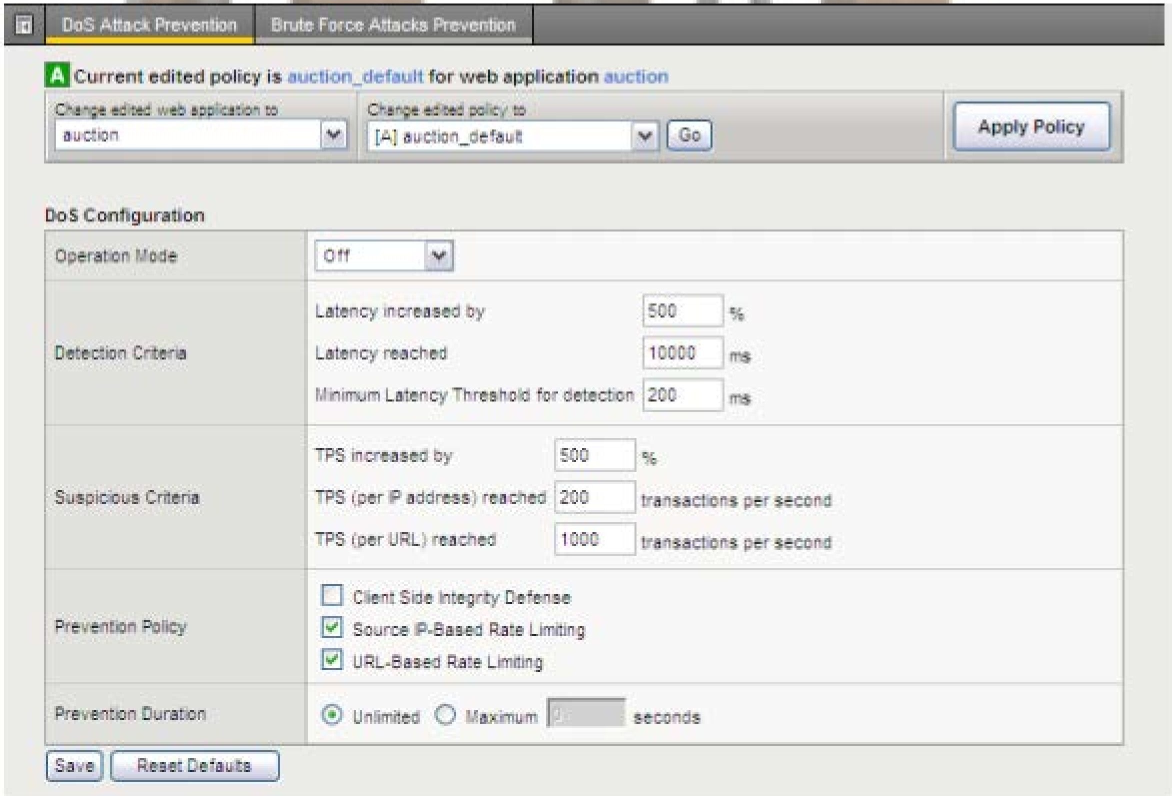
- Multi-Layered Analysis for Accurate Decision Making
- Threat Intelligence



http://www.imperva.com/products/ssp_technology-correlated-attack-validation.html

F5

- Anti-Automation:
  - Rate or latency Based Detection
  - Latency based detection
  - Challenge Response
- IP Intelligence
- Signature based line learning



A Current edited policy is auction_default for web application auction

Change edited web application to: auction

Change edited policy to: [A] auction_default

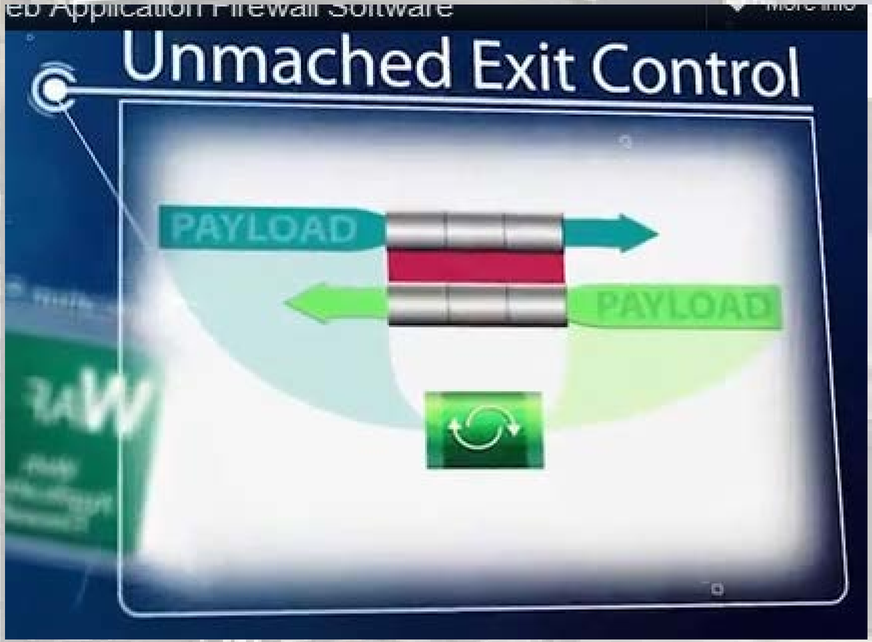
DoS Configuration

Operation Mode	Off
Detection Criteria	Latency increased by 500 % Latency reached 10000 ms Minimum Latency Threshold for detection 200 ms
Suspicious Criteria	TPS increased by 500 % TPS (per IP address) reached 200 transactions per second TPS (per URL) reached 1000 transactions per second
Prevention Policy	□ Client Side Integrity Defense ☑ Source IP-Based Rate Limiting ☑ URL-Based Rate Limiting
Prevention Duration	● Unlimited ○ Maximum seconds

http://www.f5.com/pdf/white-papers/intelligent-layer7-protection-wp.pdf
https://www.youtube.com/watch?v=H2PQBlhxL9I

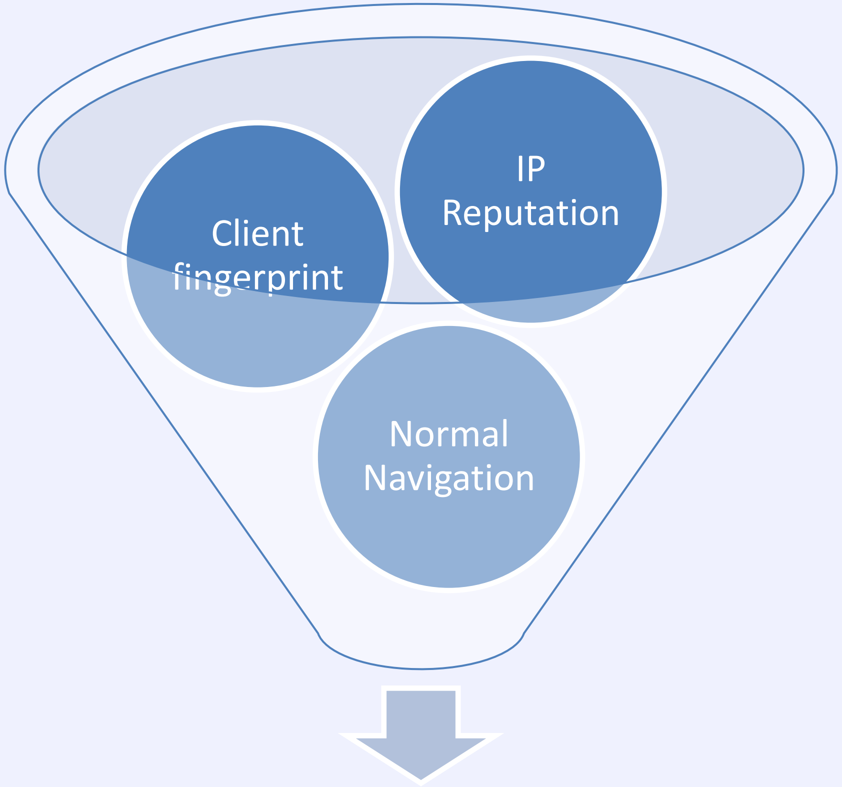
Trustwave

- Bi-directional traffic inspection correlation
- Excessive Access Rate Detection



https://www.trustwave.com/web-application-firewall/#learn
https://www.trustwave.com/downloads/Trustwave_WP_Scraping_Denial_of_Service_and_Brute_Force_Attacks.pdf
(registration required)

Bee-Ware



Indicators Aggregation

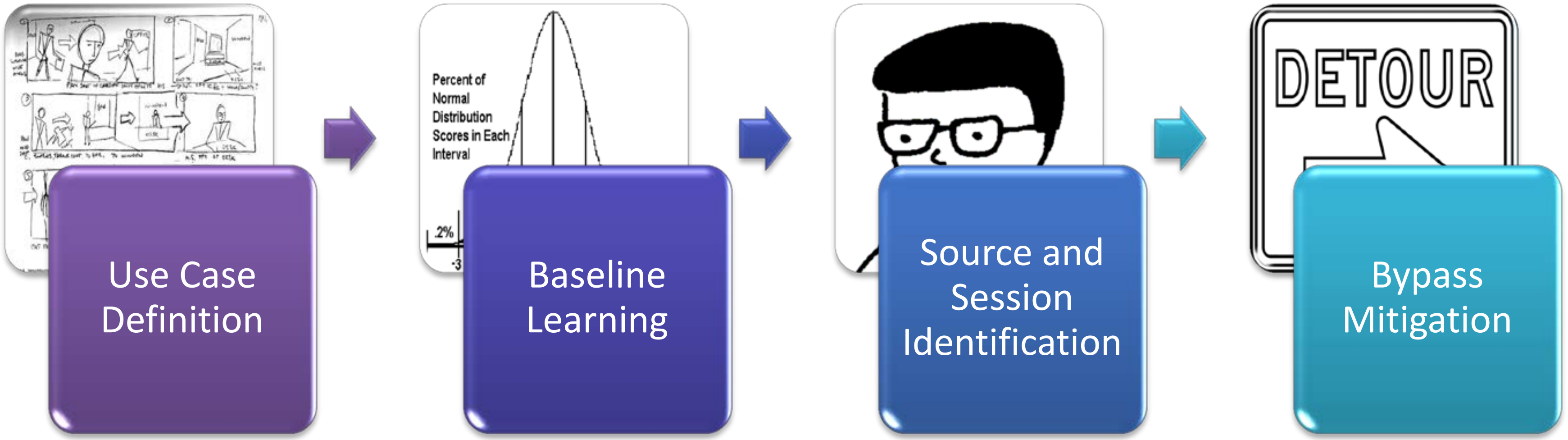
Thanks to Matthieu Estrade for the information

ModSecurity/CRS

- Anomaly scoring
- Messages aggregation
- Inbound & outbound correlation
- Bad robots

```
SecRule REQUEST_FILENAME|ARGS_NAMES|ARGS|XML:/*
"\bselect\b.{0,40}\buser\b“
…
setvar:tx.sql_injection_score=+%{tx.critical_anomaly_score},
setvar:tx.%{rule.id}-WEB_ATTACK/SQL_INJECTION-
%{matched_var_name}=%{tx.0}"
```

Challenges



Use Case Definition

Baseline Learning

Source and Session Identification

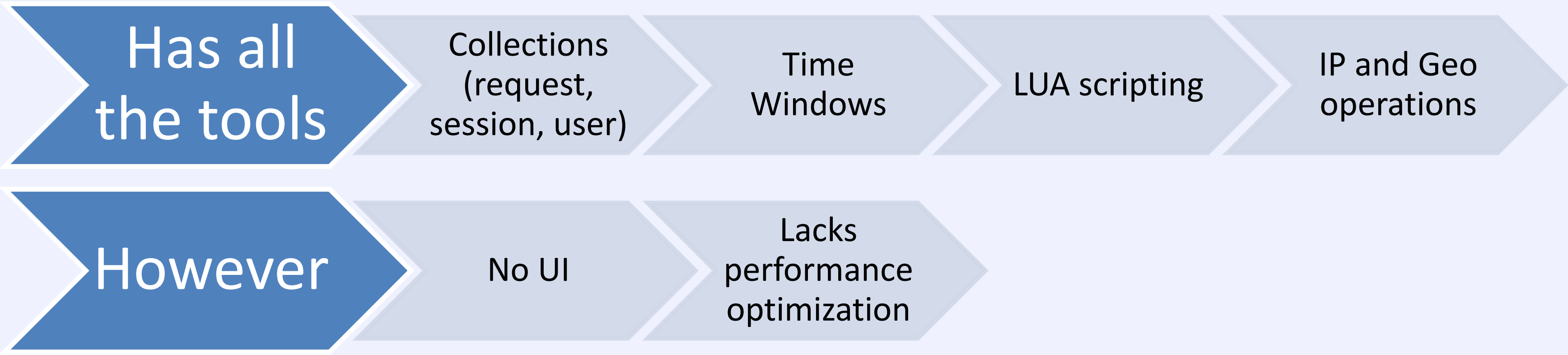
Bypass Mitigation

Flexibility

OWASP
The Open Web Application Security Project

SIEM CORRELATIONS TO THE RESCUE

ModSecurity



Has all the tools

Collections (request, session, user)

Time Windows

LUA scripting

IP and Geo operations

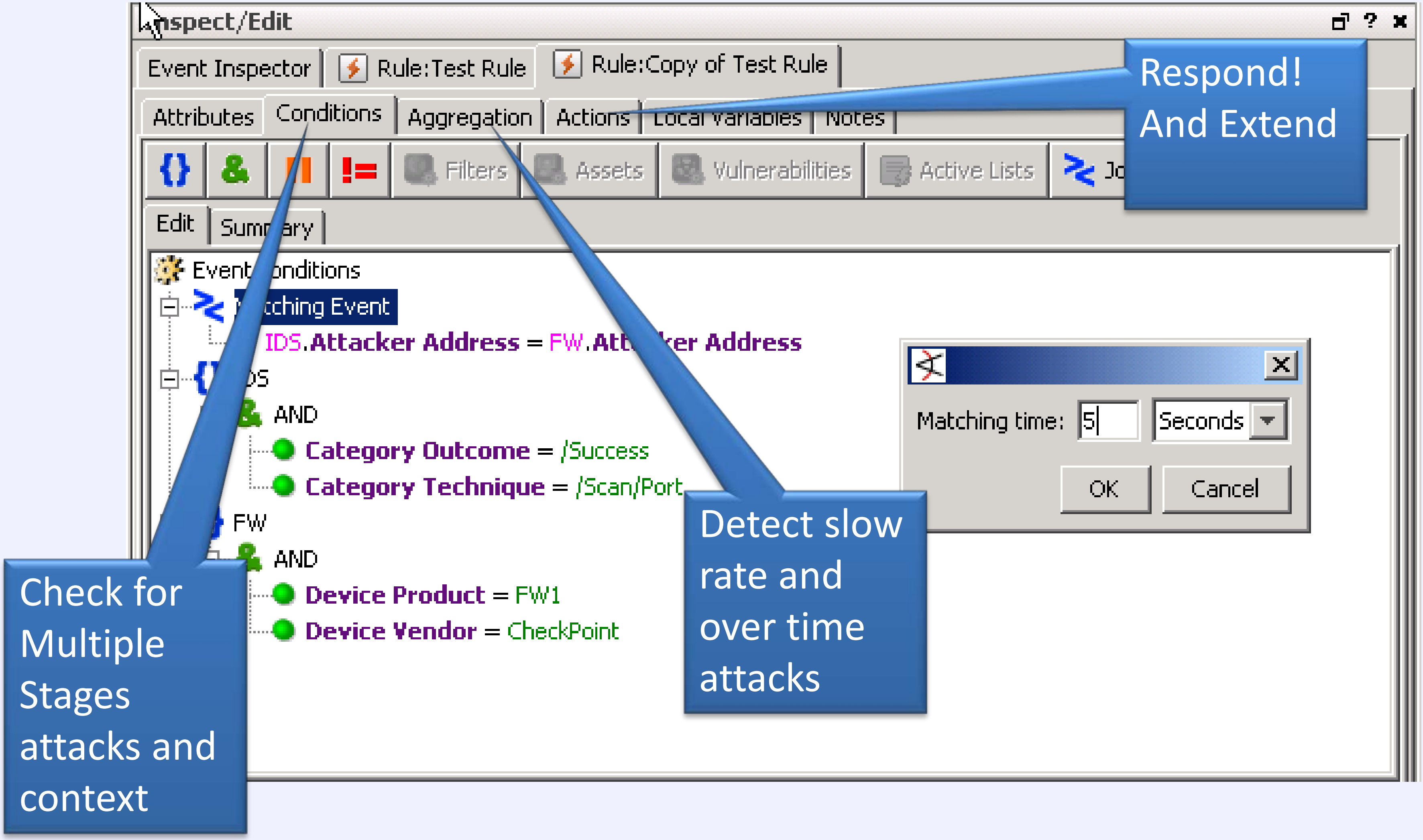
However

No UI

Lacks performance optimization

SIEM Correlations

OWASP
The Open Web Application Security Project



Event Conditions
- Matching Event
  - IDS.Attacker Address = FW.Attacker Address
- IDS
  - AND
    - Category Outcome = /Success
    - Category Technique = /Scan/Port
- FW
  - AND
    - Device Product = FW1
    - Device Vendor = CheckPoint

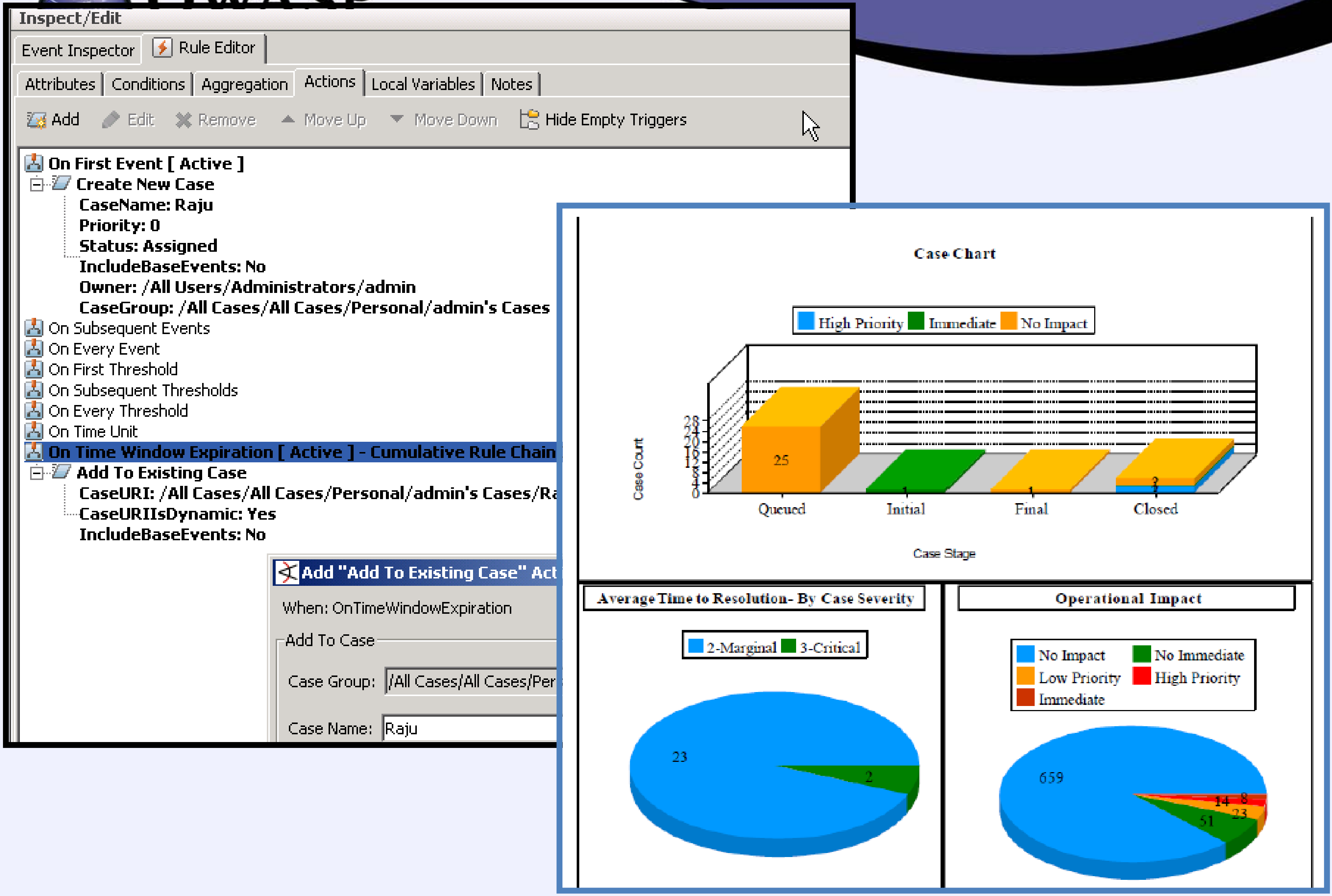
Matching time: 5 Seconds

Respond! And Extend

Detect slow rate and over time attacks

Check for Multiple Stages attacks and context

SIEM Human Interaction



Inspect/Edit

Event Inspector | Rule Editor

Attributes | Conditions | Aggregation | Actions | Local Variables | Notes

Add Edit Remove Move Up Move Down Hide Empty Triggers

- On First Event [Active]
  - Create New Case
    - CaseName: Raju
    - Priority: 0
    - Status: Assigned
    - IncludeBaseEvents: No
    - Owner: /All Users/Administrators/admin
    - CaseGroup: /All Cases/All Cases/Personal/admin's Cases
- On Subsequent Events
- On Every Event
- On First Threshold
- On Subsequent Thresholds
- On Every Threshold
- On Time Unit
- On Time Window Expiration [Active] - Cumulative Rule Chain
  - Add To Existing Case
    - CaseURI: /All Cases/All Cases/Personal/admin's Cases/Ra
    - CaseURIIsDynamic: Yes
    - IncludeBaseEvents: No

Add "Add To Existing Case" Act

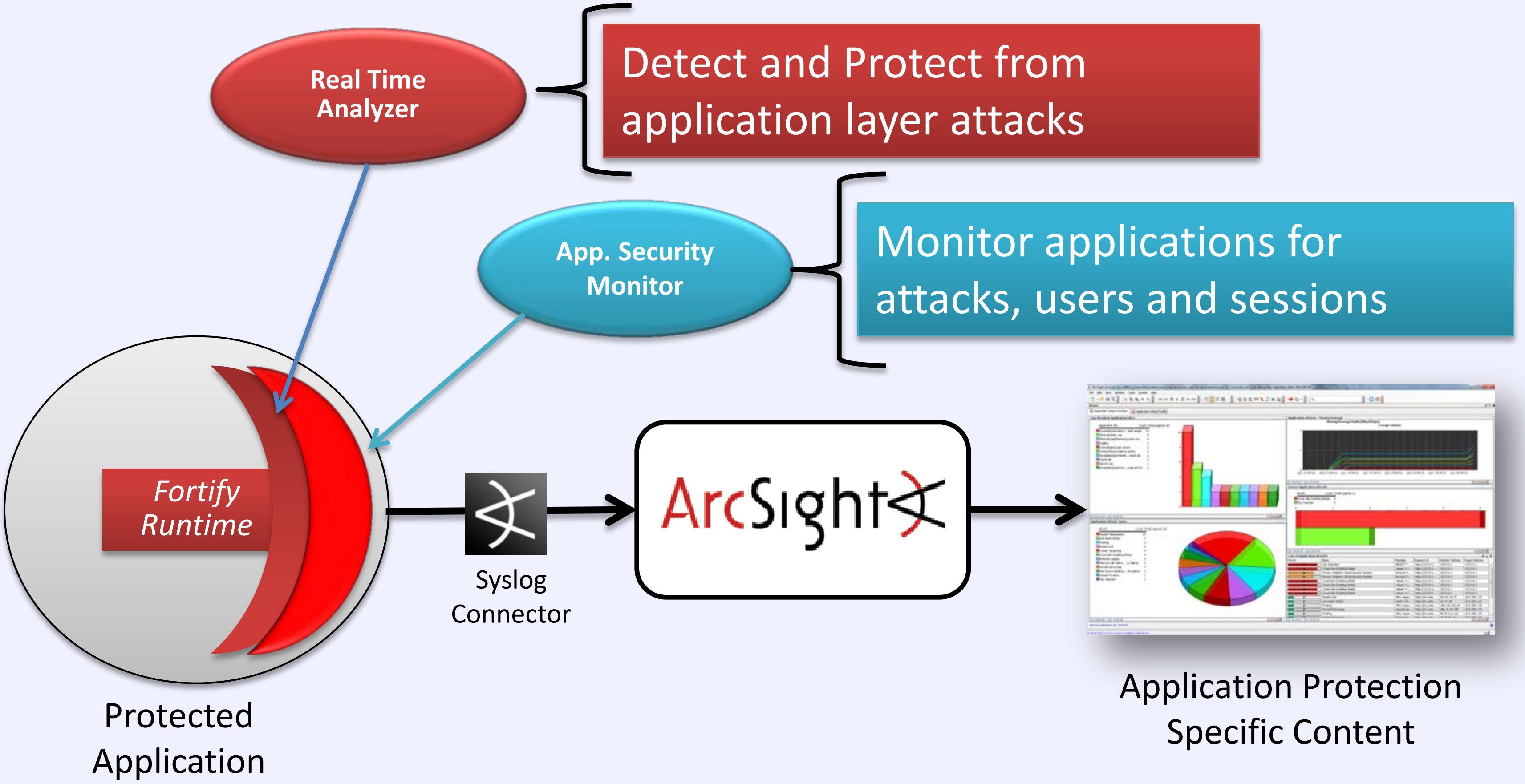
When: OnTimeWindowExpiration

Add To Case

Case Group: /All Cases/All Cases/Per

Case Name: Raju

Connecting to the Application



Real Time Analyzer

Detect and Protect from application layer attacks

App. Security Monitor

Monitor applications for attacks, users and sessions

Fortify Runtime

Protected Application

Syslog Connector

ArcSight

Application Protection Specific Content

For Further Questions contact:

Ofer Shezaf
ofr@hp.com

Feedback Form