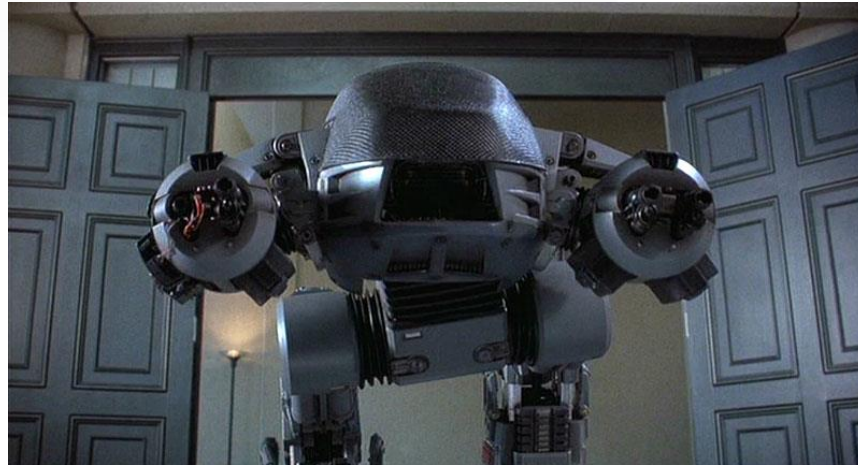


Building a shield of security - Vulnerability Management by the numbers and dumb robots!



me

Rahim Jina

- Director BCC Risk Advisory
- OWASP Contributor & OWASP Ireland ex-board member
- Co-Architect of edgescan.com
- Ex-Head of Security of Fonality (US VOIP Provider)
- Ex-Big 4 Consultant



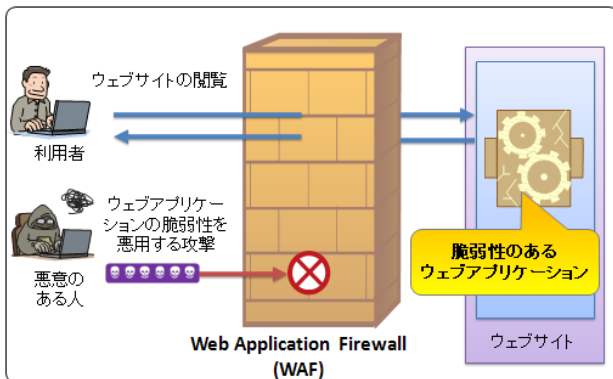
RISK



Automation



+



Context



Context



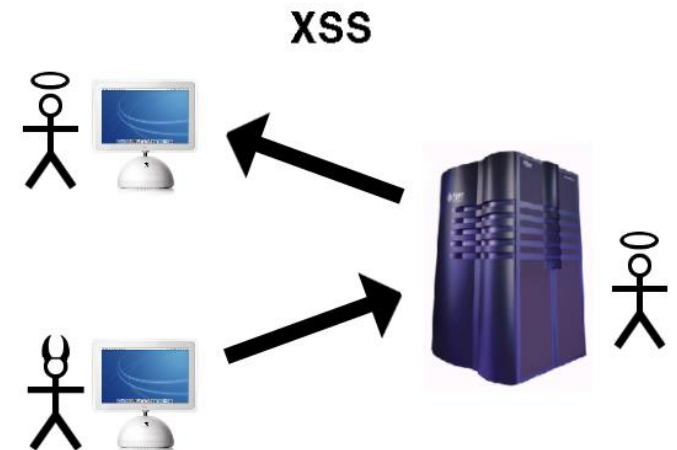
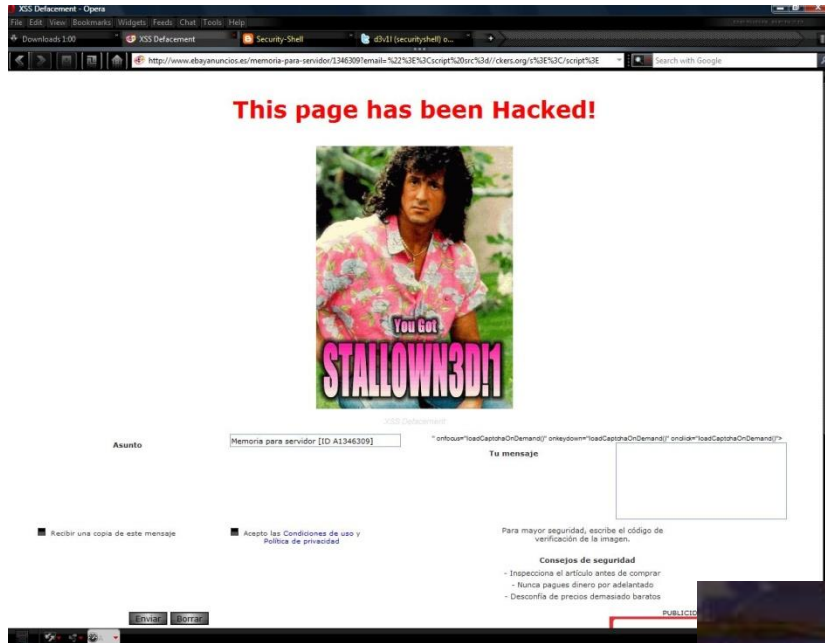
Automation



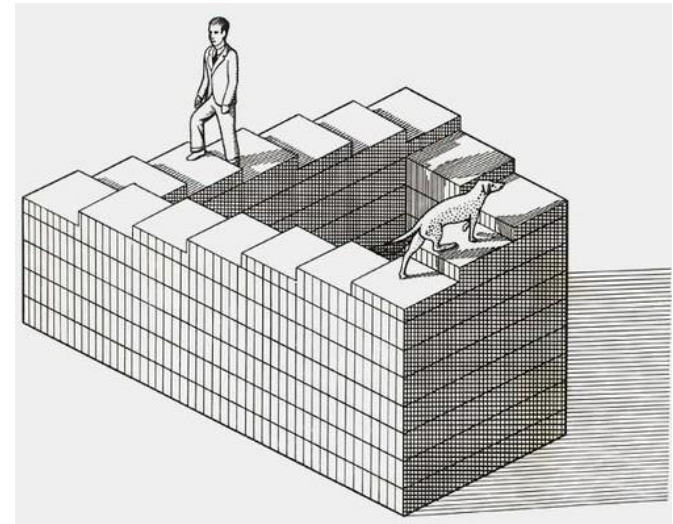
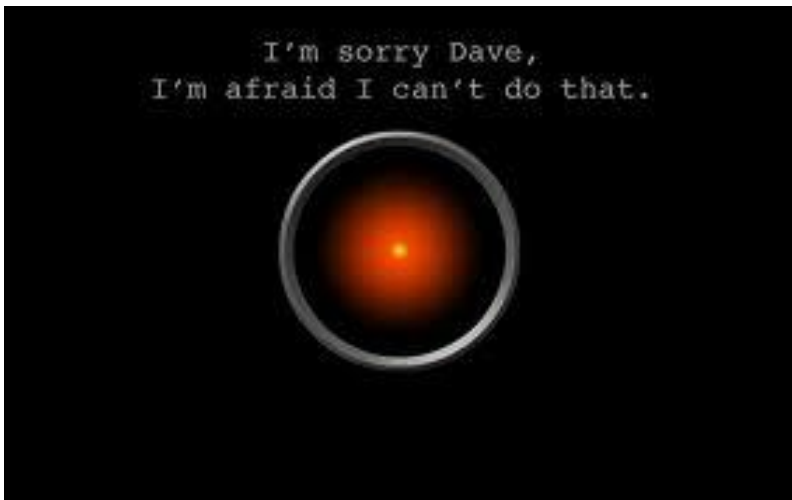
We Know Memes



Fraud - Technical Vulns



Fraud - Logic Vulns



"40% of applications tested by BCC Risk Advisory in the last 12 months had a critical business logic vulnerability"

“(Cyber crime is the) second cause of economic crime experienced by the financial services sector” – PwC

“One
hundred
BILLION
dollars”
- Dr Evil

*Globally,
every
second, 18
adults
become
victims of
cybercrime
- Symantec*

2012 Cyber Crime

- US \$20.7 billion in direct losses
- Global \$110 billion in direct losses
- Global \$338 billion + downtime

“The loss of industrial information and intellectual property through cyber espionage constitutes the greatest transfer of wealth in history” - Keith Alexander

Almost 1 trillion USD was spent in
2012 protecting against cybercrime

“Jimmy, I didn’t click it”
– My Grandma

“556 million adults across the world have first-hand experience of cybercrime -- more than the entire population of the European Union.”

Example 1 - Loan Calculator & Approval



Example 1 - Loan Calculator & Approval



Example 2 - Coupon Abuse

Stacking

DISC10



Trust the Machine



Example 2 - Coupon Abuse



Example 3 - Flight Booking

Following seats are available for this flight. You can select specific seats once you have purchased the ticket.

	A	B	C	G	H	J	
7	Occupied	Available	Available	Available	Occupied	Occupied	7
8	Occupied	Occupied	Occupied	Available	Occupied	Available	8
9	Occupied	Available	Occupied	Available	Occupied	Occupied	9
10	Occupied	Available	Available	Available	Available	Occupied	10
11	Occupied	Occupied	Available	Available	Occupied	Available	11
12	Available	Available	Available	Available	Available	Available	12
13	Available	Available	Available	Available	Available	Available	13
14	Occupied	Available	Available	Available	Available	Available	14
15	Available	Available	Available	Available	Available	Occupied	15
16	Occupied	Occupied	Occupied	Available	Available	Occupied	16
17	Available	Available	Available	Available	Available	Available	17
18	Available	Available	Available	Occupied	Occupied	Available	18
19	Available	Available	Available	Available	Available	Available	19
20	Available	Available	Available	Available	Available	Available	20
21	Available	Available	Available	Available	Available	Available	21
22	Available	Available	Available	Available	Available	Available	22
23	Available	Available		Available	Available	Available	23

Wing

Available

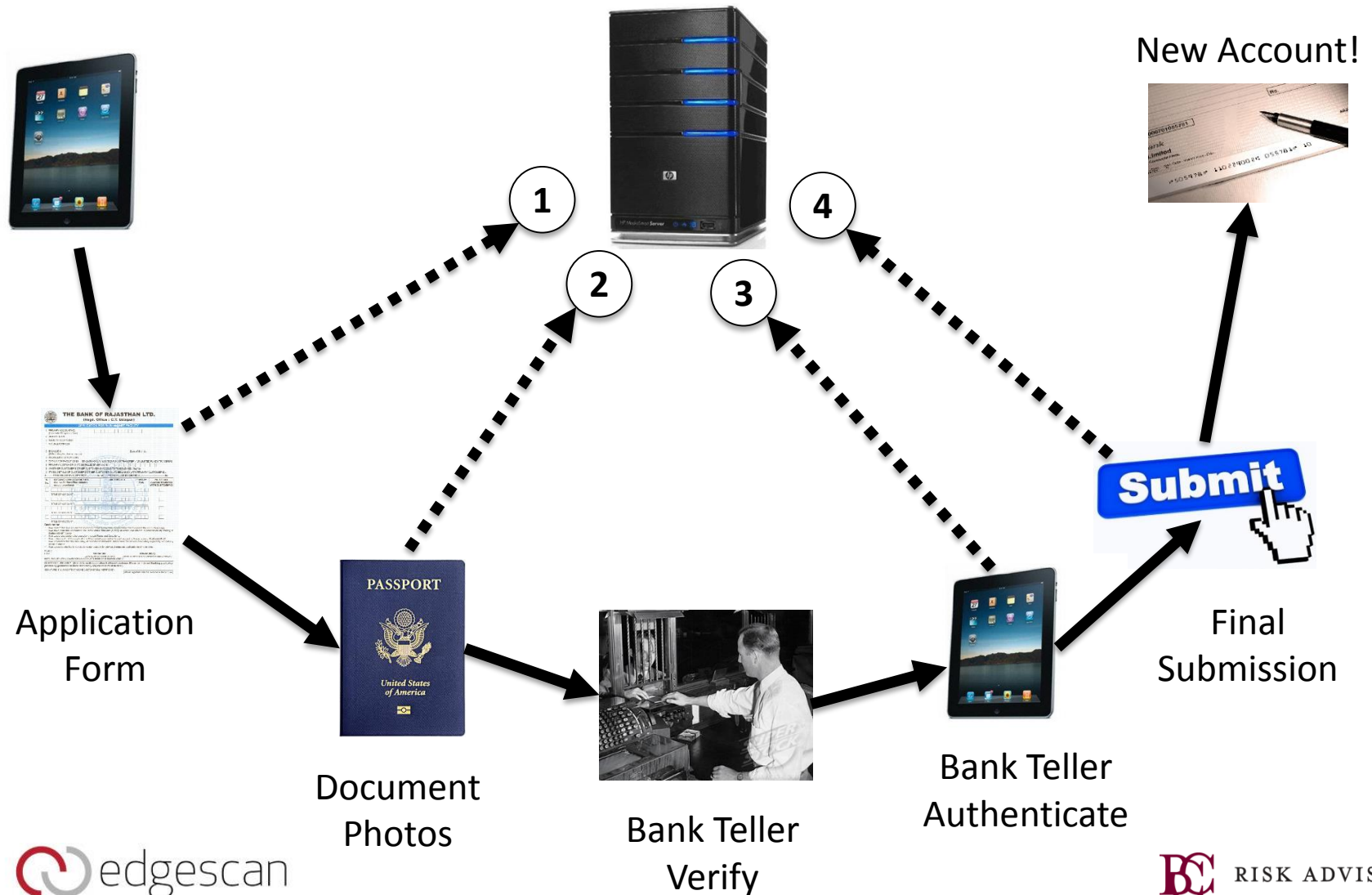
Preferential

Occupied

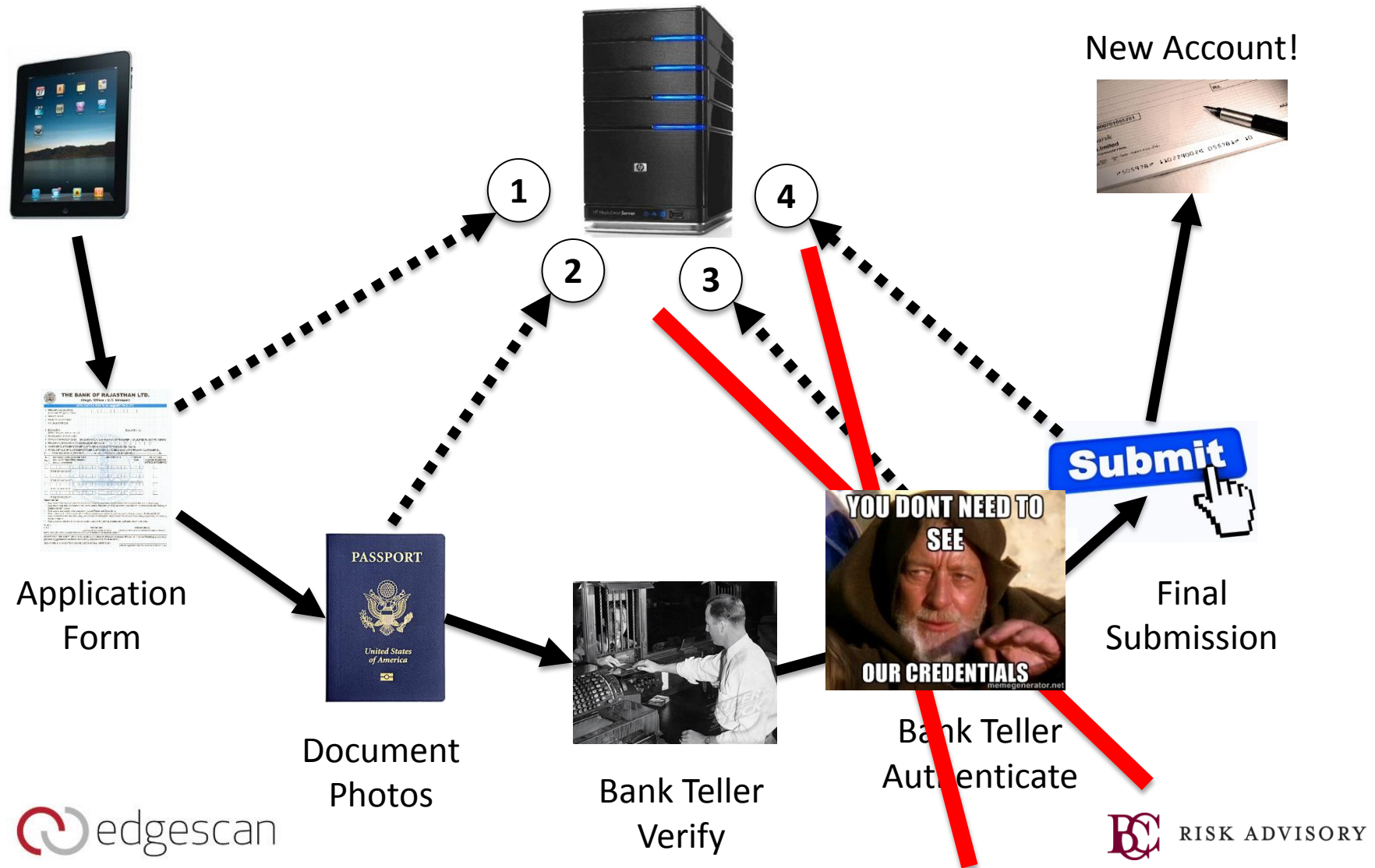
Example 3 - Flight Booking



Example 4 - 'Smart' Bank



Example 4 - 'Smart' Bank



Example 4 - 'Smart' Bank



My Money went to
NIGERIA
*and all I got was
this lousy T-Shirt*

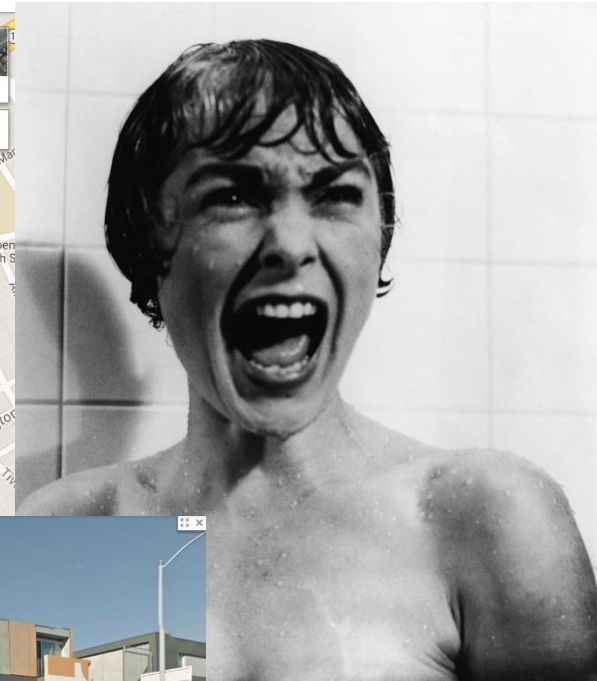
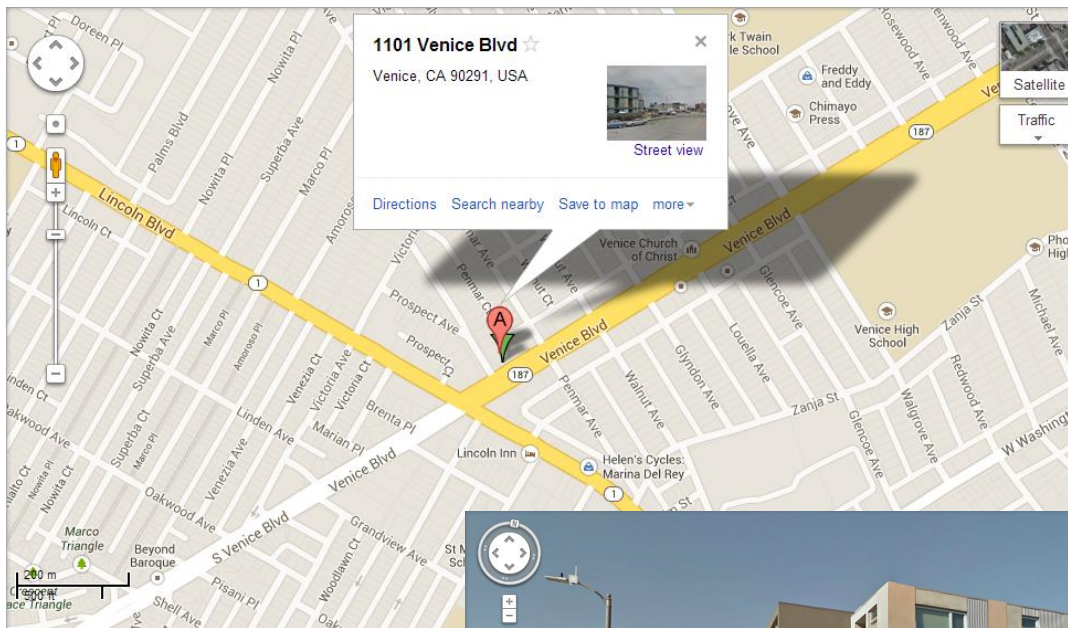
Example 5 - e-Dating

```
Raw Hex
{"d":{"__metadata":{"uri":"https://xxx.xxx.xxx/odata/odata.svc/categories(0)","type":"DataServiceProvider.User"},"ID":"5417941693314901239916885277994380789982676302480655096623826024650600486455105797236042943841668699","mt00":"amltIGlvcnJpc29uIHJvY2tz","U1RBVEVMWswgUExVTVAgQ1VDSyBNVUxMSUdBTiBDQU1FIEZST00gVEhFIFNUQUU":{"__deferred":"U1RBVEVMWswgUExVTVAgQ1VDSyBNVUxMSUdBTiBDQU1FIEZST00gVEhFIFNUQU1SSEVBRCwgYmVhcm1uZyBhIGJvd2wgb2YgbGF0aGVyIG9uIHdoaWNoIGegbWlycm9yIGFuZCBhIHJhem9yIGxheSBJcm9zc2VklBBIH1lbGxvdyBkcmVzc2luZyBnb3duLCBibmdpcmRsZWQsIHdhcyBzdXNOYW1uZWQgZ2VudGx5LWJlLaGluZCBoaW0gYnkkgdGhlIGl1pbGQgbW9ybmluZyBhaXIuIEhlIGhlbGQgdGhlIGJvd2wYwvZnQgYW5kIGludG9uZWQ6Ci0tIEludHJvaWJvIGFkIGFsdGFyZSBZwkuCgoKSGFsdGVkLCBoZSBwZWVvZWQgZG93biBOaGUgZGFyayB3aW5kaW5nIHNOYWlycyBhbmQgY2FsbGVkIHVwIGNvYXJzZW50OgoKLS0gQ29tZSB1cCwgS2luY2guIENvbWUgdXAs"},"https://xxx.xxx.xxx/odata/odata.svc/"},"101":"33.994721","102":"-118.451978","mid":"d652075702c20796f75206665617266756c206a65737569742e0a0a536f6c656d6e6c792068652063616d6520666f727761726420616e64206d6f756e7465642074686520726f756e642067756e726573742e2048652066616365642061626f757420616e6420626c65737365642067726176656c79207468726963652074686520746f7765722c2074686520737572726f756e64696e6720636f756e74727920616e6420746865206177616b696e67206d6f756e7461696e732e205468656e2c206361746368696e67207369676874206f66205374657068656e20446564616c675732c2068652062656e7420746f77617264732068696d20616e64206d6164652072617069642063726f7373657320696e20746865206169722c20677572676c696e6720696e20686973207468726f","cid":"6420757020636f617273656c793a0a0a2d2d20436f6d652075702c204b696e63682e20436f6d652075702c20796f75206665617266756c206a65737569742e0a0a536f6c656d6e6c792068652063616d6520666f727761726420616e64206d6f756e7465642074686520726f756e642067756e726573742e2048652066616365642061626f757420616e6420626c65737365642067726176656c79207468726963652074686520746f7765","fid":"kbGUGyWdlcy4gQSBwbGVhc2FudCBzbWlsZSBicm9rZSBxdWl1dGx5IG92ZXIgaGlzIGxpcHMucGogLSBUaGUgbW9ja2VyeSBvZiBpdCwgaGUgc2FpZCBnYWlseS4gWW91ciBhYnNlcmQgbmFtZSwgYW4gYW5jaWVudCBHcmVlay4KCkh1IHBvaW50ZWQgaGlzIGZpbmdlc1Bpb1Bmcm1lbmRseSBqZXNOIGFuZCB3ZW50IG92ZXIgdG8gdGhlIHBhcmFwZXQsIGxhdWdoaW5nIHRvIGhpbXNlbGYuIFNOZXBoZW4gRGVkyYX1cyBzdGVwcGVkIHVwLCBmb2xsb3dlZCBoaW0gd2Vhcm1seSB0YXNmIHdheSBhbmQgc2F0IGRvd24gb24gdGhlIGVkb2Z0b2YgdGhlIGdlbnJlc3QsIHdhZGNoaW5nIGhpbSBzdGlsbCBhcyBoZSBwcm9wcGVkIGhpcyBtaXJyb3Igb24gdGhlIHBhcmFwZXQsIGRpcHB1ZCB0aGUgYnJlc2ggaW4gdGhlIGJvd2wYwvZnQgYW5kIGxhdGhlcmVkc1IHRoZWVrcyBhbmQgbmVjay4KCkh1IY2sgTXVsbGlnYW4ncyBnYXkgdm9pY2Ugd2VudCBvb14KCi0tIE15IG5hbWUgaXMGyWJzdXJkIHRvb3ogTWFsYWNoaSBNdWxsaWdhbiwgdHdvIGRhY3R5bHMueIEJldCBpdCB0YXMGySB1ZWxsZW5pYyByaW5nLCBoYXN1Z3QgaXQvIFRyaXBwaW5nIGFuZCBzdW5ueSBsaWt1IHRoZSBidWNRIGhpbXNlbGYuIFdlIGl1c3QgZ28gdG8gQXRoZW5zLiBkaWxsIHlvdSBjb211IGlm"},"bid":"zLiBUaGVuLCBjYXRjaGluZyBzaWdodCBvZiBtdGVwaGVuIERlZGFsdXMsIGhlIGJlbnQgdG93YXJkeSB0aW0gYw5kIGl1hZGUcmFwaWQgY3Jvc3NlcyBpb1B0aGUgYWlyLCBndXJnbGluZyBpb1B0aXMGdGhyb2F0IGFuZCBzaGFraW5nIGhpcyBoZWFkLiBtdGVwaGVuIERlZGFsdXMsIGRpc3BsZWZzZWQgYW5kIHNSZWVweSwgbGVhbmVkc1IhpcyBhcm1zIG9uIHRoZSB0b3Agb2YgdGhlIHNOYWlyY2FzZSBhbmQgbG9va2Vkc1NvbGRseSBhdCB0aGUgc"}}}
```


Example 5 - e-Dating

[illegible]

Example 5 - e-Dating ^{Stalking}~~e-Dating~~
















What's your point?

- Robots don't have curiosity
- SIMPLE
- COMMON
- LEGALITIES

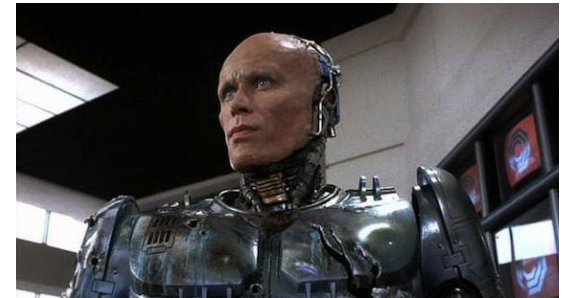


"We need an Onion"

- SDL*
-  *Design review*
 -  *Threat Modeling*
 -   *Code review/SAST/Continuous Integration/IAST*
 -   *Negative use/abuse cases/Fuzzing/DAST*
- Live/
Ongoing*
-   *Continuous/Frequent monitoring/Testing*
 -  *Manual Validation*
 -   *Vulnerability management & Priority*
 -   *Dependency Management*

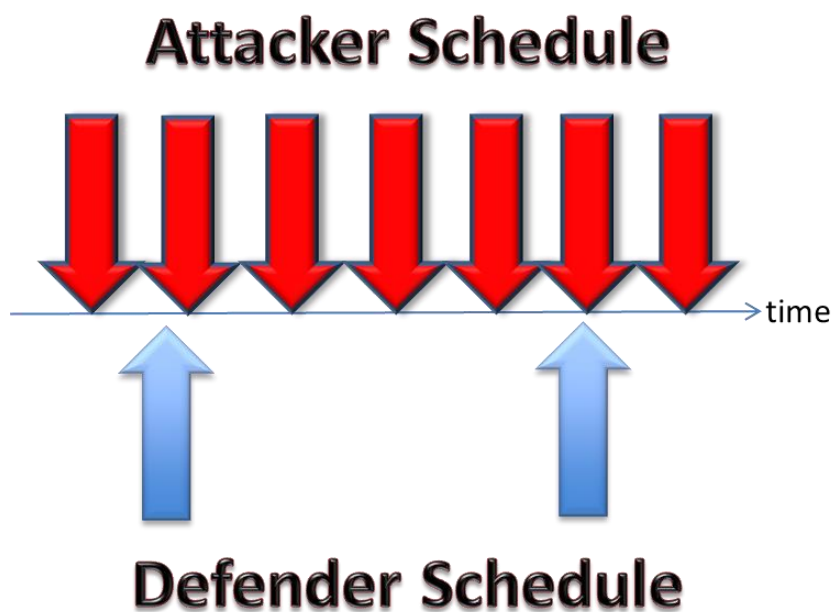
"Robots are good at detecting known unknowns"

"Humans are good at detecting unknown unknowns"

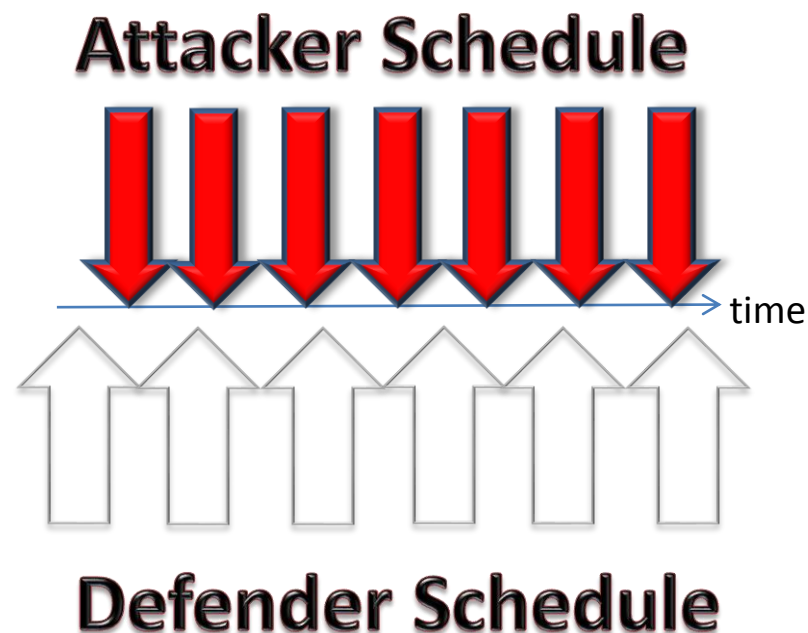


Continuous Security

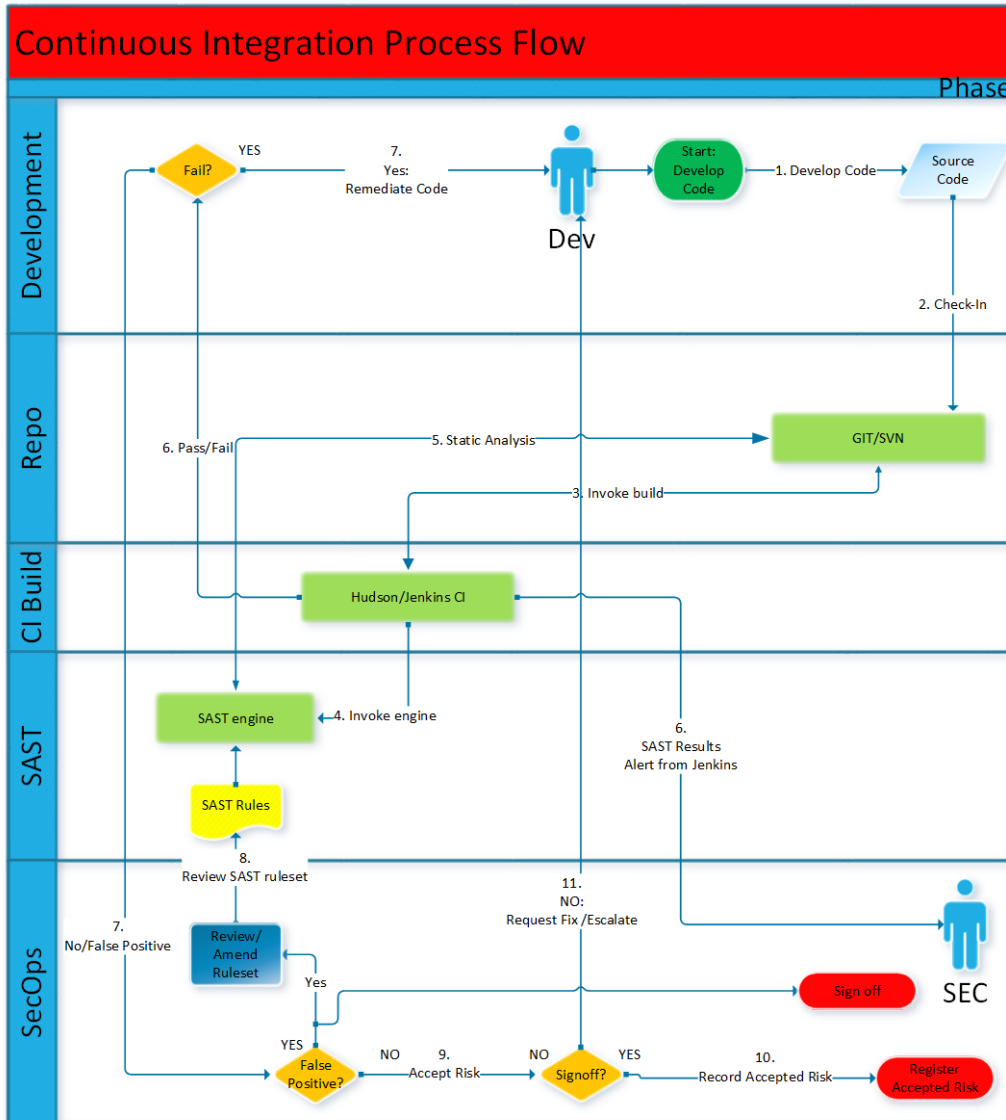
Traditional Security Assessment Approach:



Continuous Security Assessment Approach:




Continuous Integration with SAST

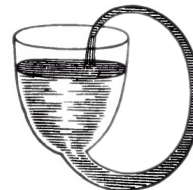


Code changes invoke SAST
Build Pass/Fails
SAST Rules control
Rule Tuning
False Positive Tuning
Framework awareness

Really, what's your point?



- There is no big button
- Automation helps but is only part of the solution
- Pure blackbox tests are dumb
- Manual effort
- Onion Approach 
- Think C-O-N-T-I-N-U-O-U-S



Thanks for Listening

Some websites were harmed during the making of this presentation



RISK ADVISORY

rahim@bccriskadvisory.com

rahim.jina@owasp.org



www.bccriskadvisory.com

© BCC Risk Advisory Ltd 2014.
All rights reserved.