The WAF book

Web App Firewall

introduction

Practical Defensive Security for Security Engineers

By: Lior Rotkovitch

- *Email: lior.rotkovitch@gmail.com*
- *Twitter: @Rotkovitch*
- *LinkedIn: Lior Rotkovitch*
- *Instagram: l.rotkovitch*

https://SIRT.club DSMM *Ref: 052921DSMM-TWB-HB-V1.P, SOT:S,B.*

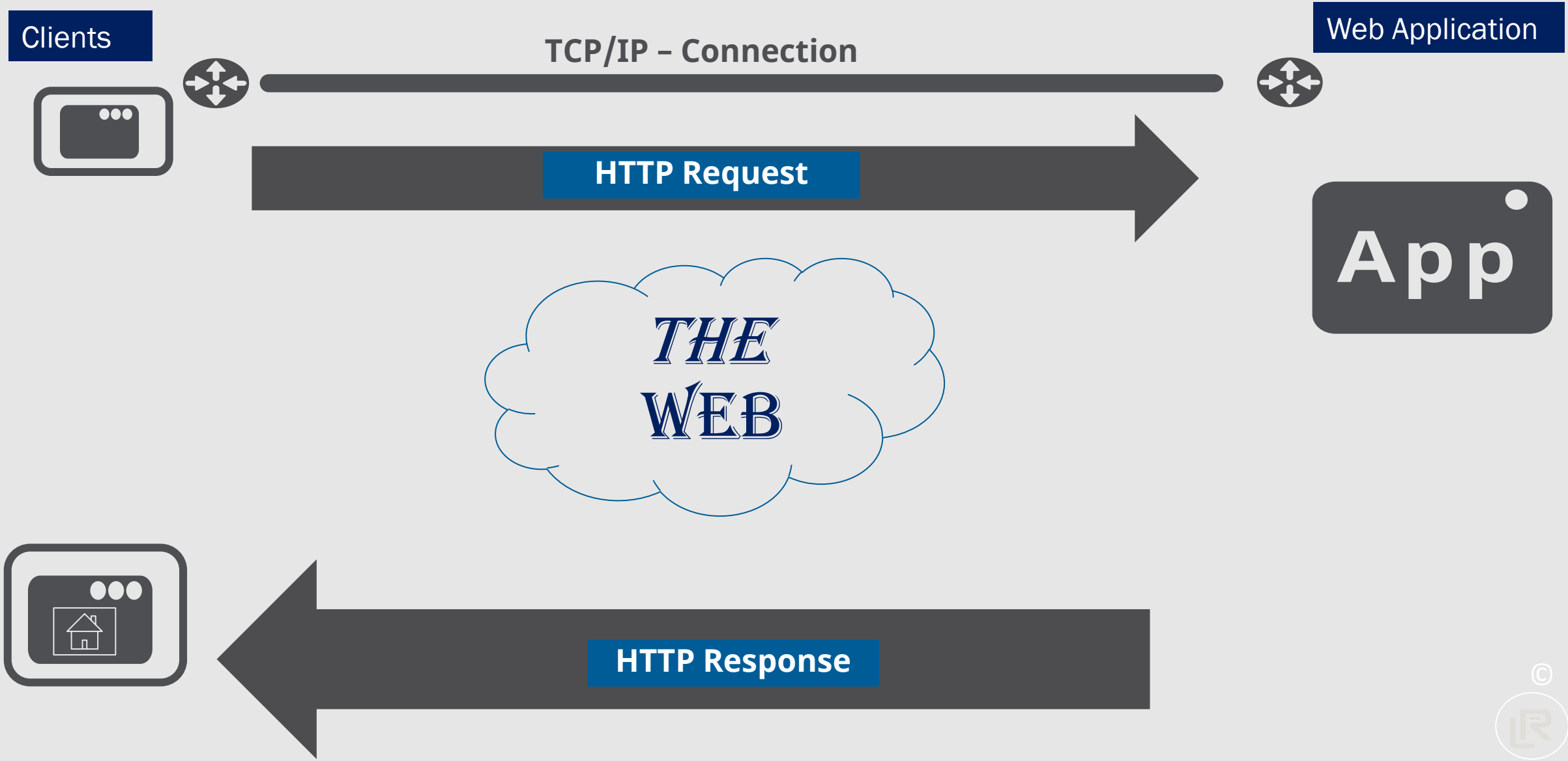
The WAF book

introduction

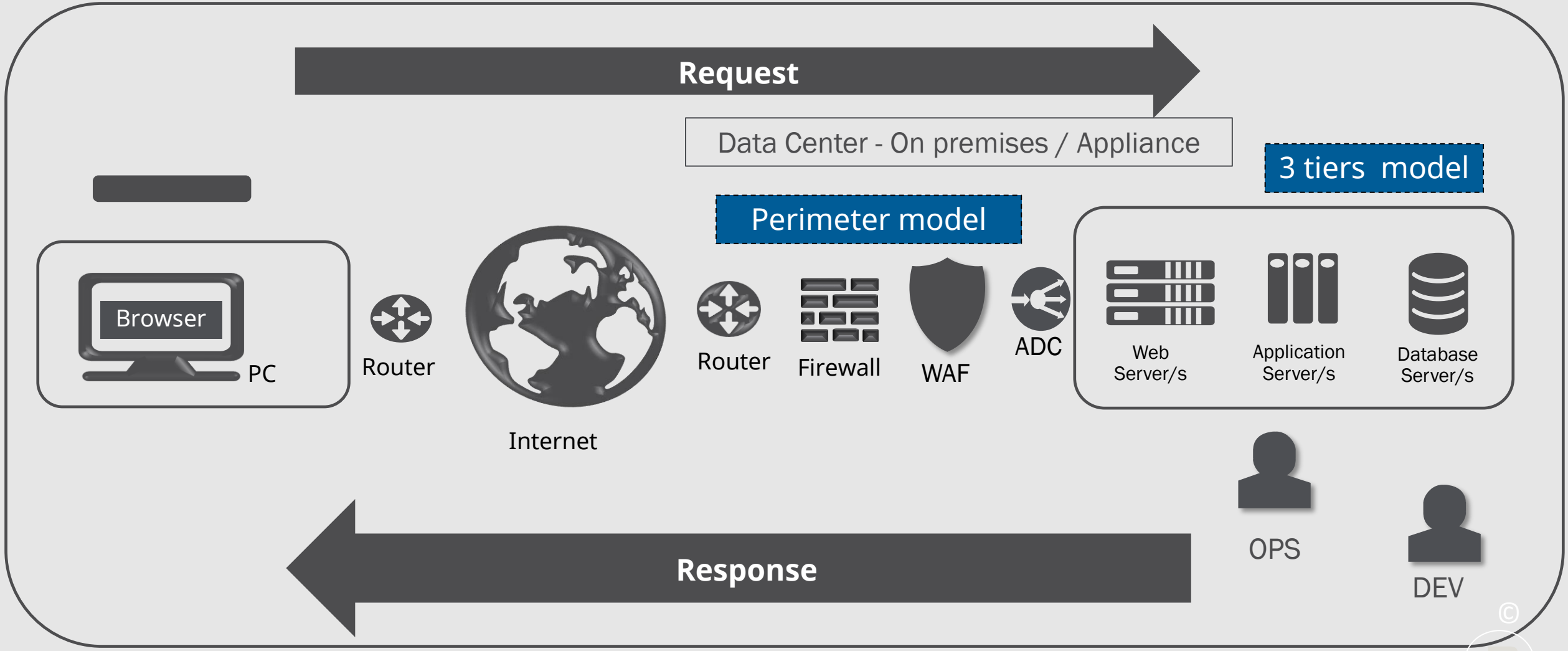
- *The target - Web Application*
- *The Attack / attacking*
- *The Protect / protecting*
- *WAF Policy*
- *WAF SIR*
- *Summary*

The target – web App

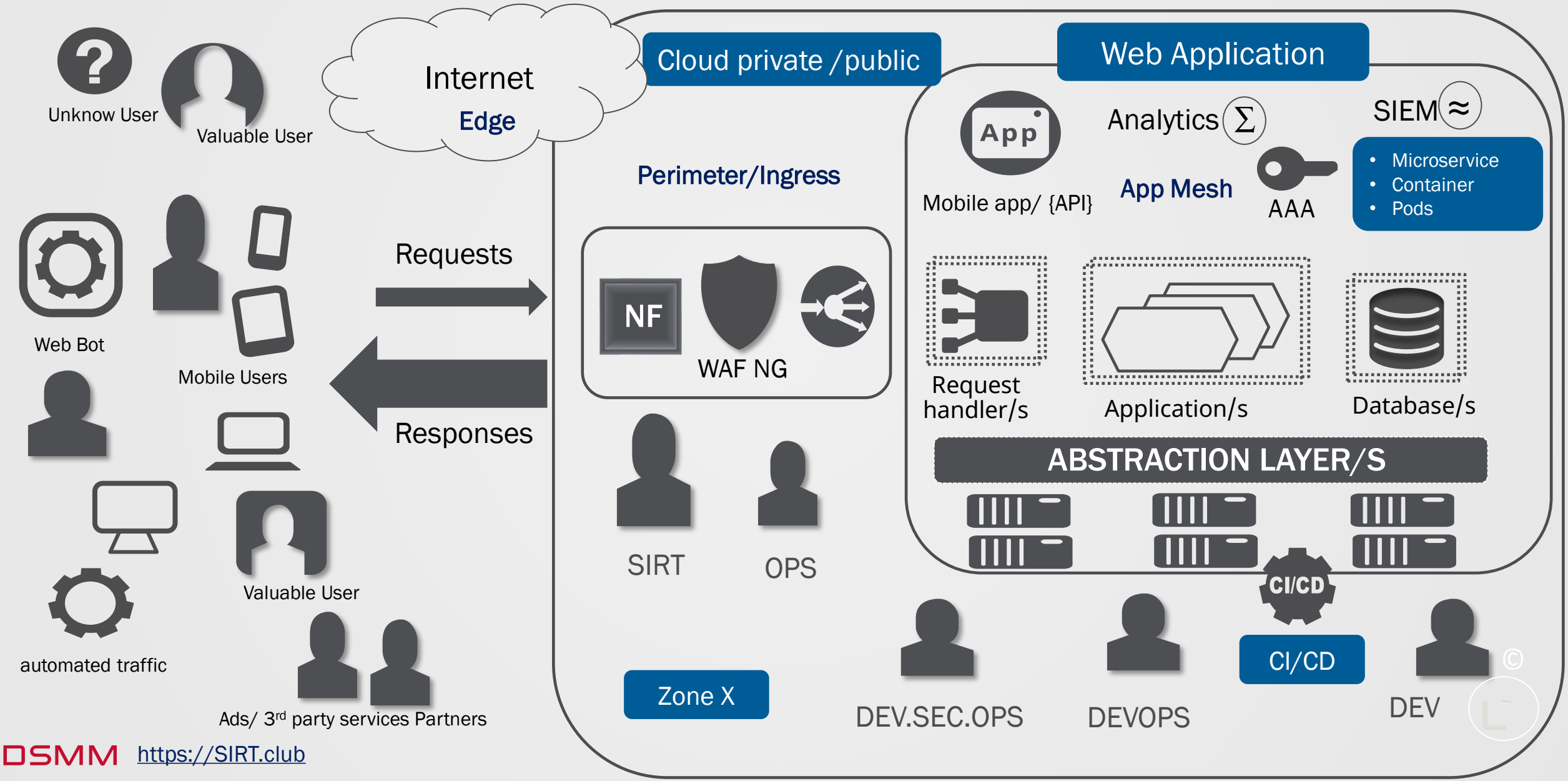
Web App Paradigm



Web App ecosystem – classic



Web App ecosystem - Modern

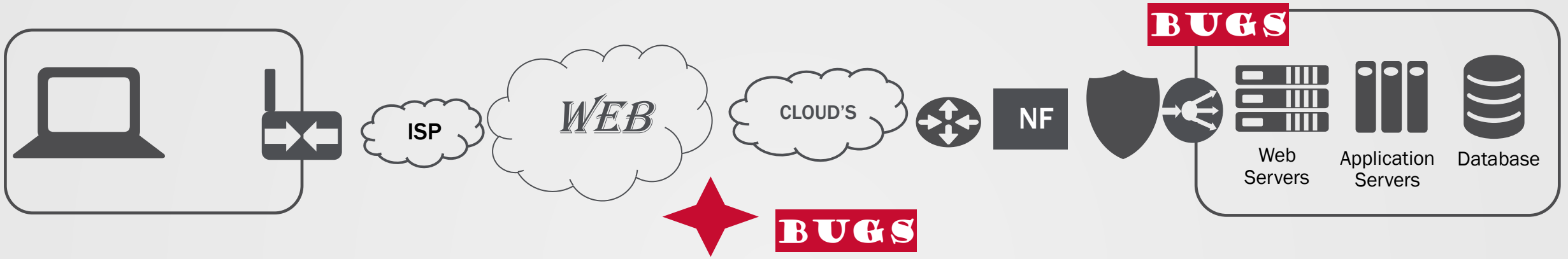


DSMM https://SIRT.club

Software Bug

by Thomas Edison

Software Security



Attacks :

- SQL injection
- Directory traversal
- Cross site attack
- .....

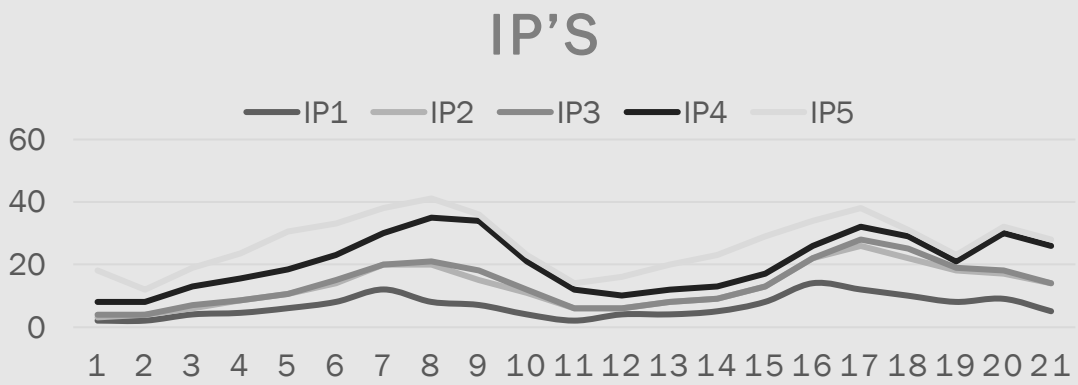
- Bugs = glitch– "unexpected condition in software"*LR*
- Security bug - bug can be utilized to take advantages

Application Security

Attacks :

- Floods
- Brute force
- Scraping
- ...

Load	%	Statistics
CPU	70%	0/1/2
Memory	72%	80GB
Throughput	35%	11.7Mbps
RPS	25%	10k

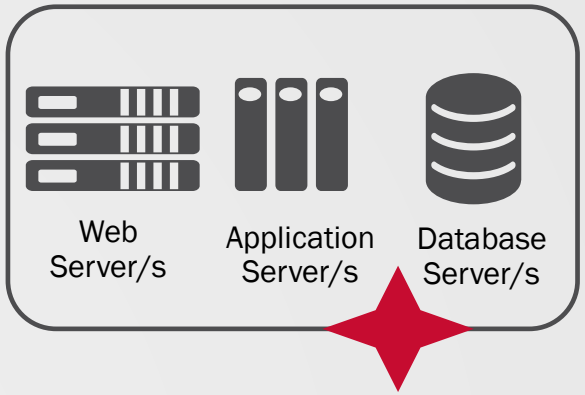


Aggregated	21.21k	23.57	36.72k
172.29.46.6	2.75k	3.05	4.08k
10.0.0.138	2.26k	2.51	5.27k
192.168.1.1	2.25k	2.50	3.10k
172.29.44.44	2.23k	2.48	4.64k
192.168.1.254	2.01k	2.23	2.82k

Attack

Attacking the Web App

Attack:
Offending traffic that violates the expected usage

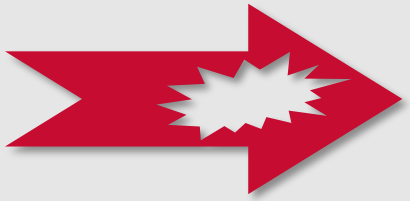


Attack goals:

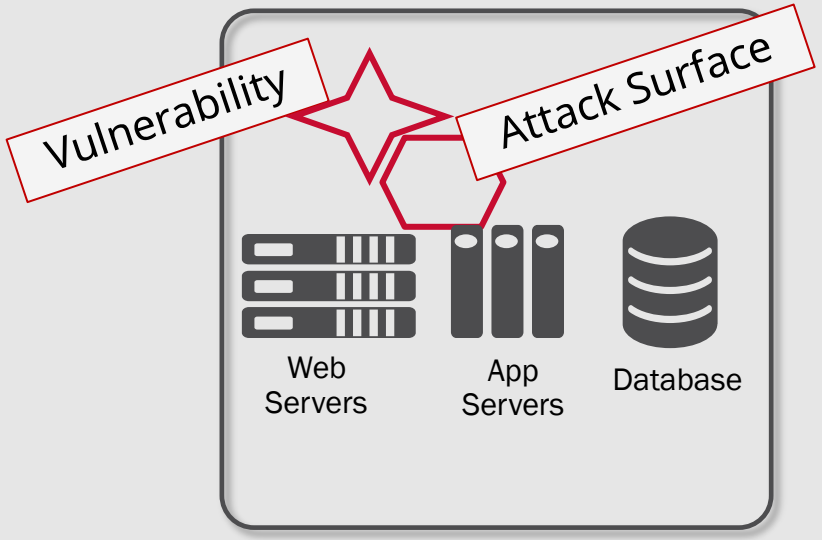
- Damage - Affect services
- Data - leakage / manipulation
- Computing power – usage

Load	%	Statistics
CPU	100%	0/1/2
Memory	100%	80GB
Throughput	100%	11.7Mbps
RPS	100%	10k

Attack Elements

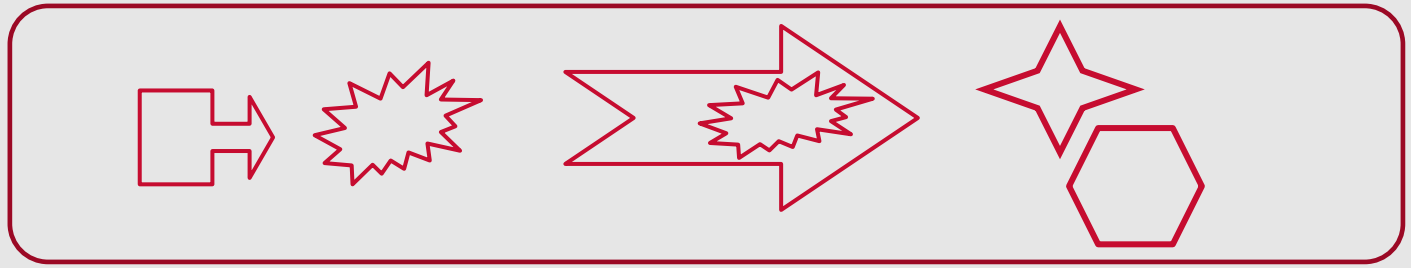


Web Application



"Attack occurs when: attack agent is sending exploit to execute the vulnerability that resides in the attack surface

Attack Elements



Vulnerability

Vulnerability – is a software condition aka bug in the software with security implication that create a risk to the application assets - security bug

Attack Surface

Attack surface – the location where the vulnerability exists. Also refer to the entry point for the exploit or the meeting place between the exploit and the vulnerability.

Attack agent

Attack agent – the client software that is used to sends the exploit to the attack surface that contains vulnerability.

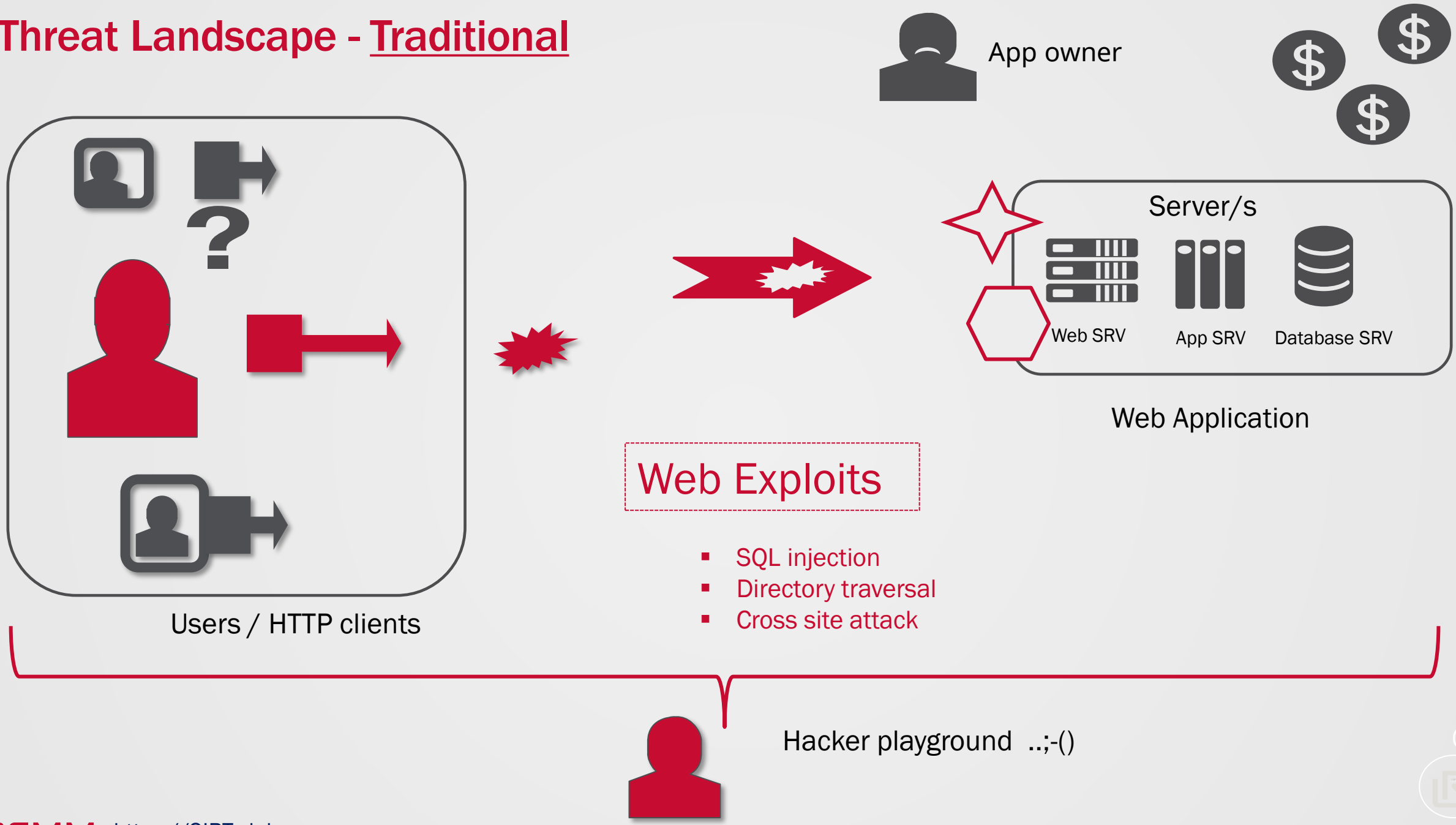
Exploit

Exploit – the code/payload that active the vulnerability and allow exploitation of the vulnerability.

Attack Vector

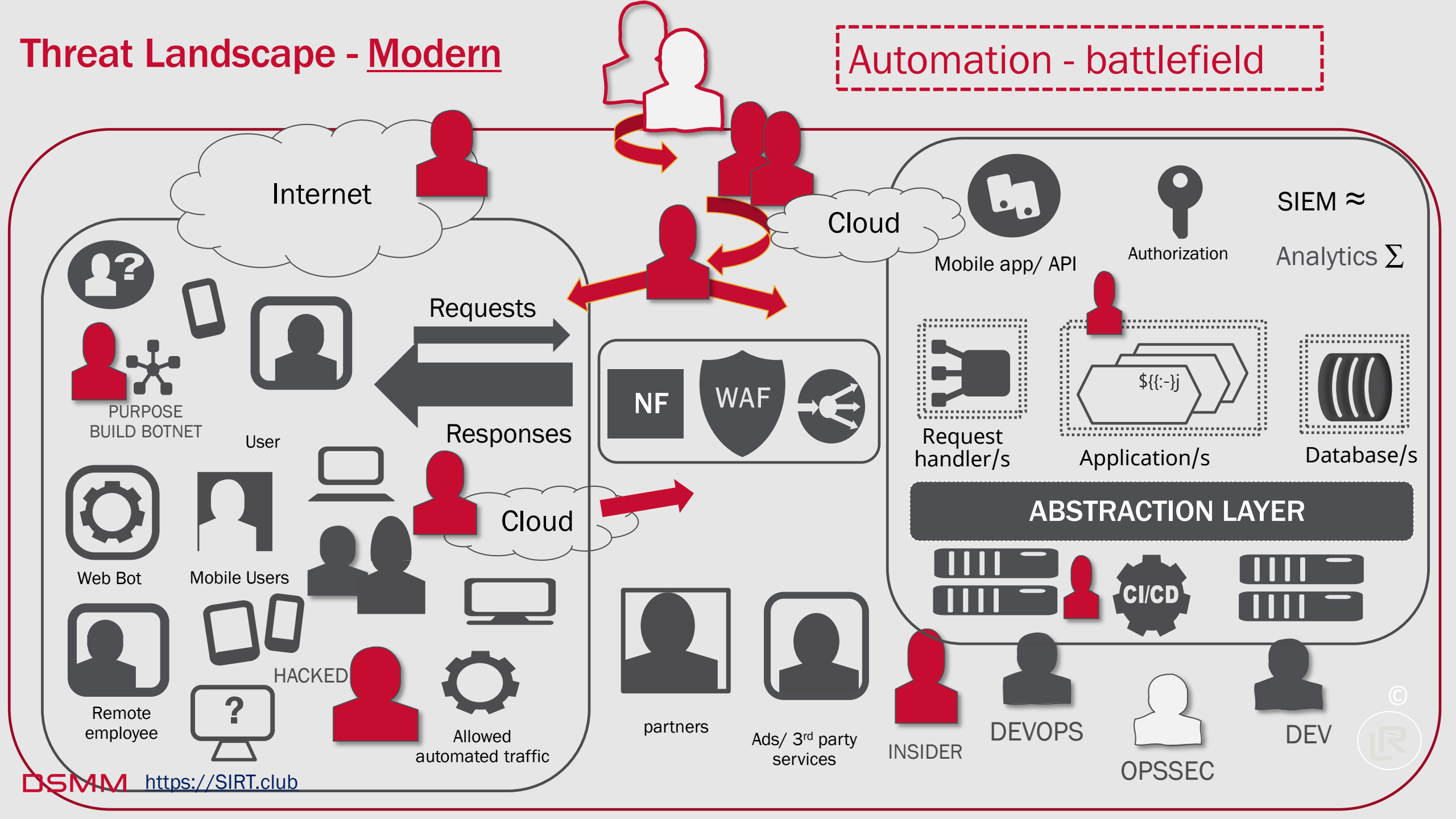
We use the same attack elements for all the attacks. The vector is the technique used to achieve the goal

Threat Landscape - Traditional



Threat Landscape - Modern

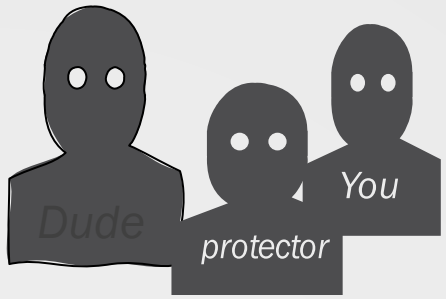
Automation - battlefield



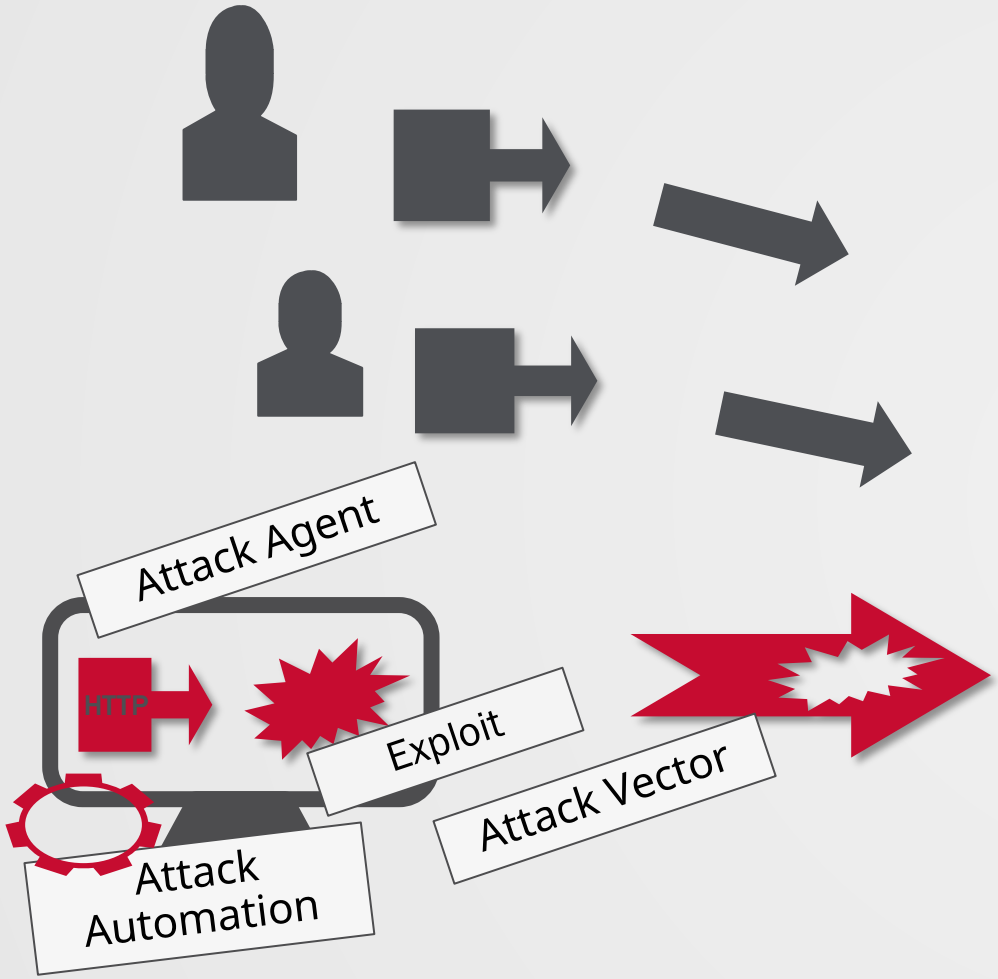
DSMM https://SIRT.club

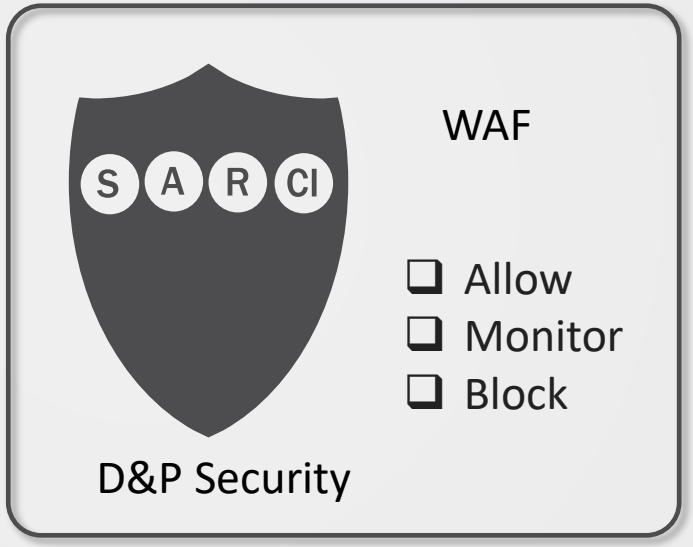
Protect

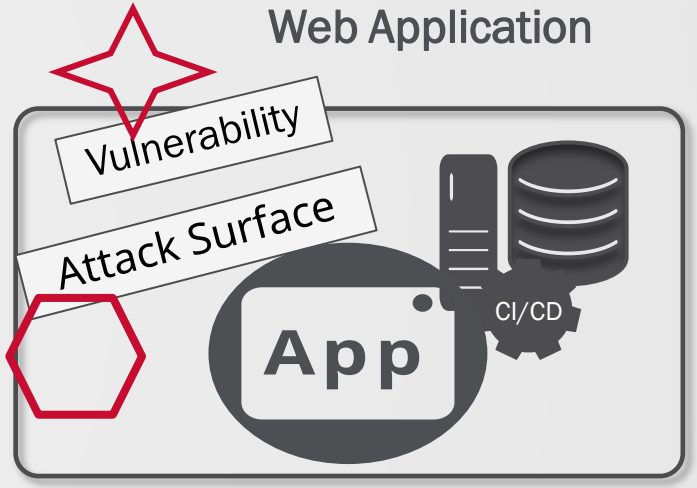
WAF– Web App Firewall



Protect







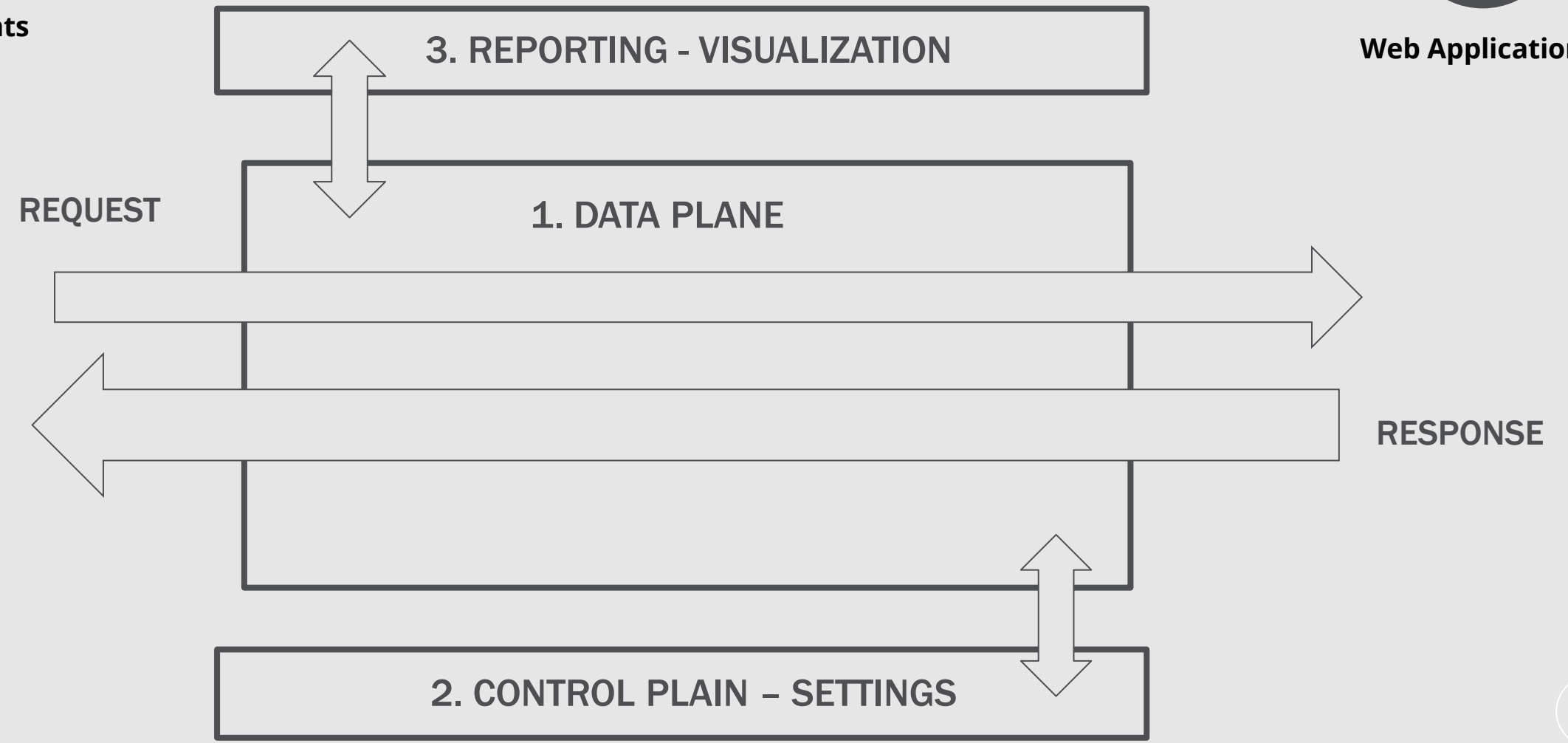
D&P= detect & prevent

WAF STRUCTURE

1. Data Plane - WAF Engines
2. Control Plain – Settings
3. Reporting - Visualization

Web Clients

Web Application

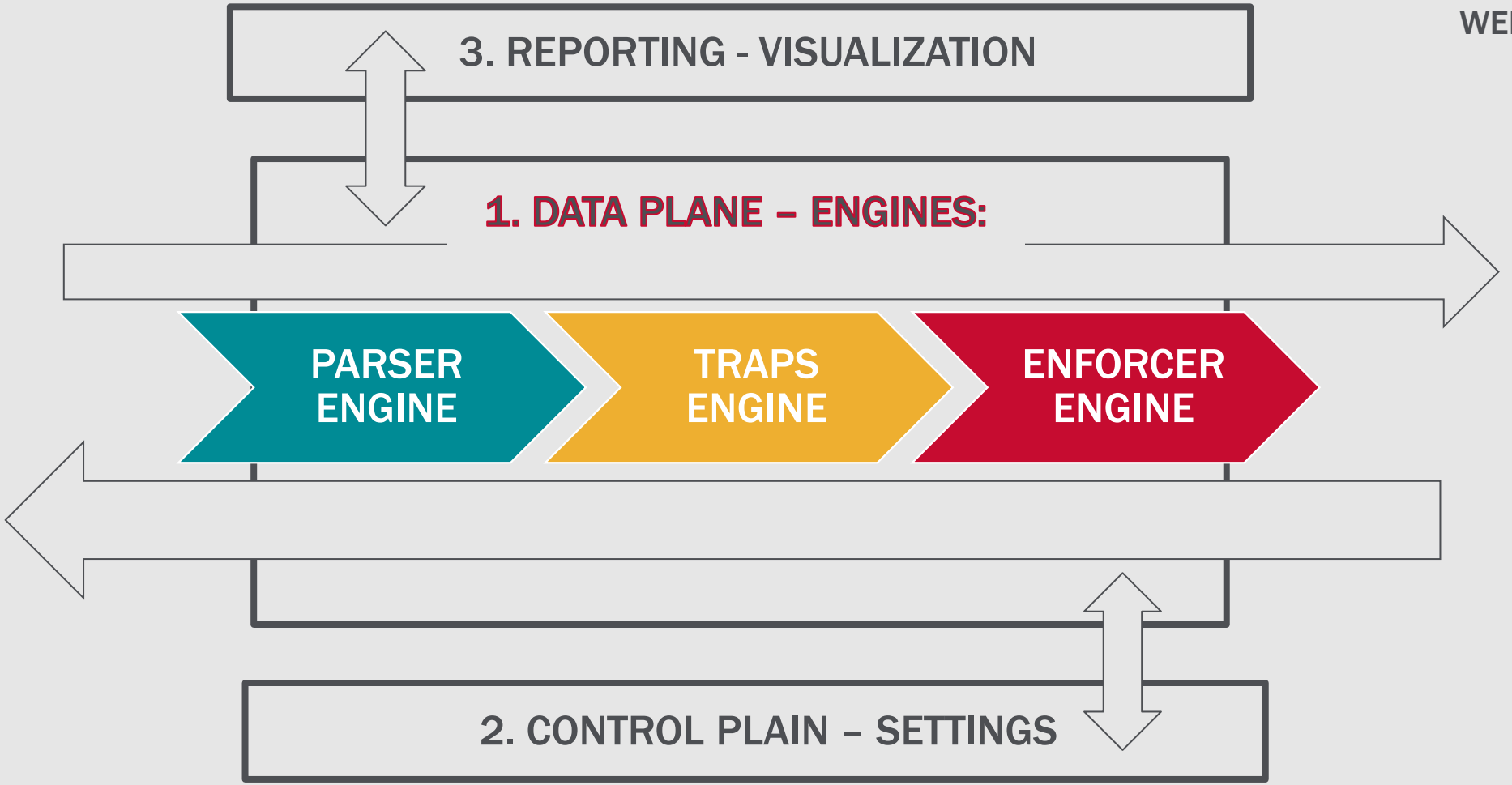


DATA PLANE – ENGINES

WAF SECURITY ENGINEER

WEB CLIENTS

WEB APPLICATION



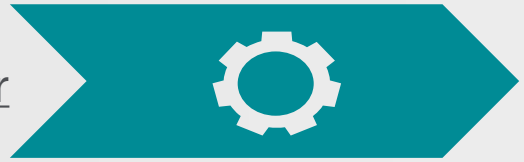
Request engines phases in WAF

```
GET / HTTP/1.1
Host: sirt.club
User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007240)
```

Web Application

Application Firewall Engines

Parser



Traps

Enforcer

Parser (entities)	Value
Verb (Method)	GET
Protocol	HTTP 1.1
URL	/index.php
User-Agent:	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007240)
Source IP	192.168.1.1
Time	01:32:44

Detections: Signatures - User Agent
Python-urllib/2.6
Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007240)
Mozilla/4.0 (Hydra)

Prevention action
Alarm
Block page
Reset conn

WEB CLIENTS

PROTECTION ELEMENTS (PE)

App

Parser
ENTITIES

Traps
DETECTIONS

Enforcer
PREVENTION ACTION

Protocol

Payload

User input

REQUEST

https://sirt.club/home/search.php?q=cve&cat=all

Protocol: https

Host: sirt.club

Path: /home/

Object: search.php

Query Sting:

Parameter name: q

Parameter value: cve

2nd Parameter name: cat

2nd Parameter value: all

Parser:

Entities: - URL	
Protocol:	https
Host:	sirt.club
Path	/home/
Object	search.php
Query Sting	?
Parameter name	q
Parameter value	cve
2nd Parameter name	cat
2nd Parameter value	all

REQUEST

http://sirt.club/home/search.php?q=lala

```
GET /search.php?q=lala HTTP/1.1
Host: sirt.club
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,he;q=0.8
Cookie: SESSION=a6f77f584b48467c32d18a20aa0a13ed
```

	Entities	
Protocol	VERB	GET
	URL	/search.php
	HTTP version	HTTP/1.1
User input	Parameter name	q
	Parameter value	lala
Payload (headers)	Host:	sirt.club
	Connection:	keep-alive
	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
	Accept-Encoding:	gzip, deflate
	Accept-Language:	en-US,en;q=0.9,he;q=0.8
	Cookie:	SESSION=a6f77f584b48467c32d18a20aa0aa13ed

WEB CLIENTS

Parser - HTTP Response

Entities	
Response Status Code	HTTP/1.1 200 OK
Date:	Sat, 08 Jan 2022 13:53:00 GMT
Server:	Apache X-Powered-By: PHP/7.4.26
Cache-Control:	no-cache, must-revalidate, max-age=0
Keep-Alive:	timeout=5
Connection:	Keep-Alive
Content-Type:	text/html; charset=UTF-8
Content-Length:	8326
Response body	<HTML> <HEAD> <TITLE></TITLE> </HEAD> <Body> SIRT protectors of the realm </Body> </HTML>

Protocol

```
HTTP/1.1 200 OK
```

Payload (headers)

```
Date: Sat, 08 Jan 2022 13:53:00 GMT
Server: Apache X-Powered-By: PHP/7.4.26
Cache-Control: no-cache, must-revalidate, max-age=0
Connection: Keep-Alive
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 8326
Keep-Alive: timeout=5
Content-Type: text/html; charset=UTF-8
```

Server output

```
<html lang="en">
<head>
                <meta http-equiv="X-UA-Compatible"
content="IE=Edge"/>
                 <meta charset="UTF-8" />
                <title>SIRT Club: Security Incident Response Teams
Club</title>
                <script type="text/javascript">
                </script>
</head>
<body>
        <div id="logo">
        <p> Text </p>
</body>
</html>
```

WEB CLIENTS

PROTECTION ELEMENTS (PE)

WEB APP

ENTITIES
Parser

DETECTIONS
Traps

PREVENTION ACTION
Enforcer

- Protocol
- Payload
- User input

1. SIGNATURES
2. ANOMALY
3. RESTRICTIONS
4. CLIENT INTERROGATION

Detection: Signature


```
GET /search.php?q= SELECT * FROM products where id =* HTTP/1.1
Host: sirt.club
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/95.0.4638.54
```

Parser	
Entities	**Value**
Verb (Method)	GET
Protocol	HTTP 1.1
Parameter name	q
Parameter value	SELECT * FROM products where id =*
User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54
Source IP	192.168.1.1

WAF Signature
SELECT * FROM
where id =*
.....

Detection: Signature

```
POST / query.php HTTP/1.1
Connection: Keep-Alive
Host: sirt.club
Content-Length: 59
User-Agent: Apache-HttpClient/4.5.7 (Java/1.8.0_221)
Content-Type: application/x-www-form-urlencoded

action=' or 1=1--
```

ENTITIES

DETECTIONS

Parser (entities)	Value
Verb (Method)	POST
Protocol	HTTP 1.1
URL	/query.php
User-Agent:	Apache-HttpClient/4.5.7 (Java/1.8.0_221)
Source IP	192.168.1.1
Post Data – param	01:32:44
Post Data – Value	' or 1=1--

WAF User Agent signature
Python-urllib/2.6
Apache-HttpClient/4.5.7 (Java/1.8.0_221)
Mozilla/4.0 (Hydra)

WAF exploit Signature
../../../../../../etc/passwd
<script>alert('XSS')</script>
' or 1=1--
" or ""="

WEB CLIENTS

PROTECTION ELEMENTS (PE)

WEB APP

ENTITIES
Parser

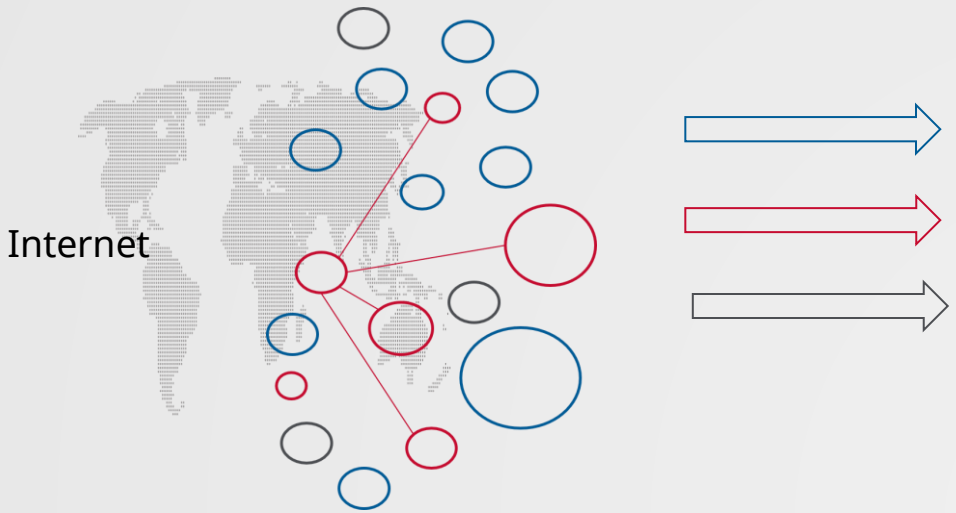
DETECTIONS
Traps

PREVENTION ACTION
Enforcer

- Protocol
- Payload
- User input

- 1.SIGNATURES
- 2.ANOMALY
- 3.RESTRICTIONS
- 4.CLIENT INTERROGATION

Detection: Anomaly



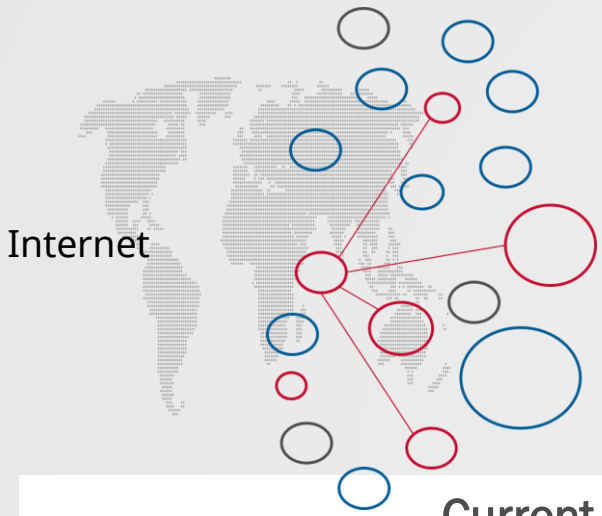
Anomaly – increase in **RPS** form IP's

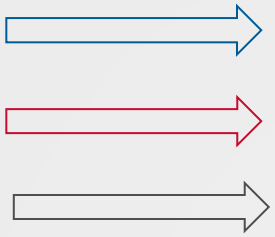
IP (Parser)	5 min	20 min	1 hour AVG
10.0.0.138	50	60	180
192.168.1.1	180	0	0
172.29.44.6	400	350	3000
172.29.46.9	250	100	1000
10.1.1.1	1800	1200	800
192.168.24.24	0	100	150

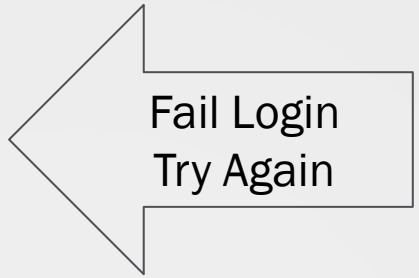
Aggregated data – Policy limit per IP

Source IP: ANY @ 5 Min	RPS limit
Min	220
Max	280

Detection: Anomaly







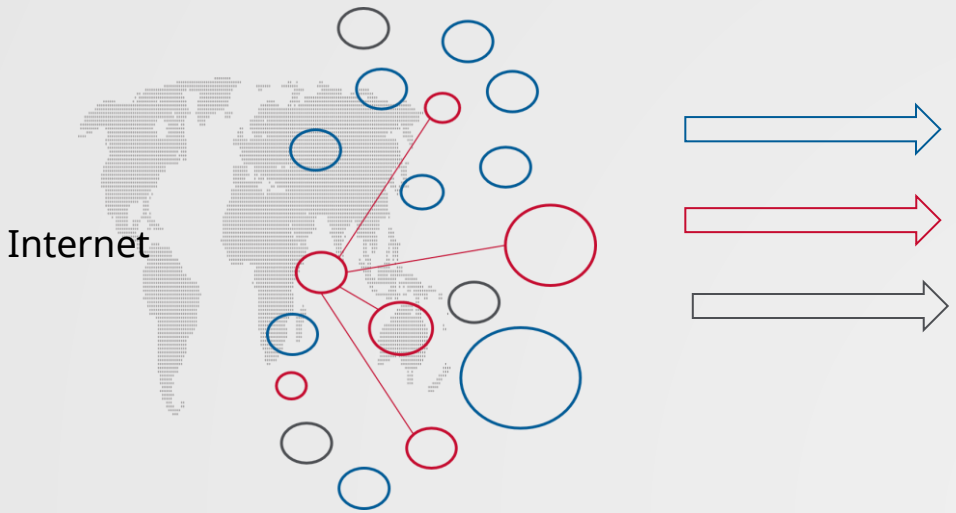
IP (Parser)	Current FLI /5min	60min FLI
10.0.0.138	60	180
192.168.1.1	0	0
172.29.44.6	35	40
172.29.46.9	100	1000
10.1.1.1	1800	3000
192.168.24.24	10	150

Anomaly – increase in **FLI** form IP's

Aggregated data – Policy limit: FLI per IP

Source IP: ANY @ 5 Min	FLI/IP over 5 min limit :
Min	300
Max	1000

Detection: Anomaly



Anomaly – increase **Sig** from IP

IP (Parser)	Sig count 5 min	Sig count 20min	Sig count 1H
10.0.0.138	500	600	1800
192.168.1.1	20	50	100
172.29.44.6	0	1	0
172.29.46.9	0	0	4
10.1.1.1	4	4	4
192.168.24.24	1	1	1

Aggregated data – Policy limit: Signatures per IP	
Source IP: ANY @ 1 Min	Max signature from IP / 1min
Min	20
Max	30
Post max	150 -> shun for 12 hours

WEB CLIENTS

PROTECTION ELEMENTS (PE)

WEB APP

ENTITIES
Parser

- Protocol
- Payload
- User input

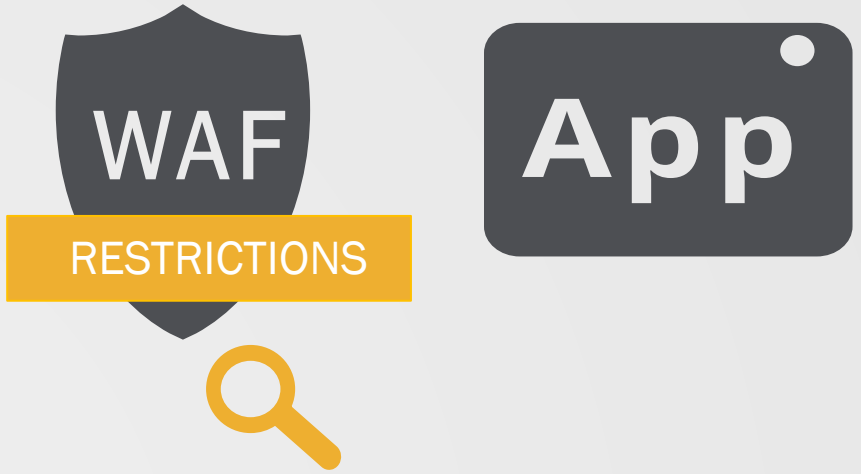
DETECTIONS
Traps

1. SIGNATURES
2. ANOMALY
3. RESTRICTIONS
4. CLIENT INTERROGATION

PREVENTION ACTION
Enforcer

Detections: Restrictions

http://sirt.club/search.php?q=longlonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglong
Host: sirt.club
User-Agent: Mozilla/5.0
Accept: text/html,application/,*/*;



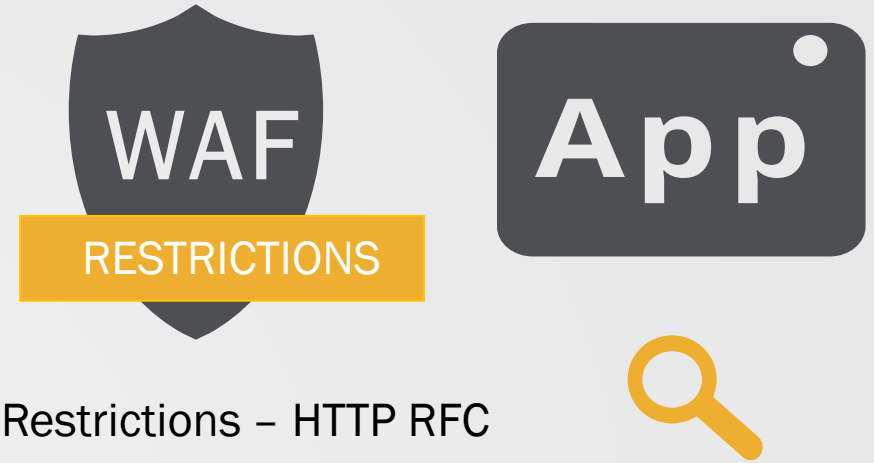
Parser (entities)	Value	Length - found
Verb (Method)	GET	
Protocol	HTTP 1.1	
Parameter name	q	
Parameter value	longlonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglonglong	136 chars
Source IP	192.168.1.1	
Time	01:32:44	

Length check policy

Length	Min Chars	Max chars
GET Param value	Min 3 chars	Max 130 chars

Detections : Restrictions

```
OPTIONS /search.php?q=mc'merHTTP/1.0
Host: sirt.club
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114
Safari/537.36
Accept: text/html,application/,*/* %00;
Host: sirt.club
Header123:
```



Restrictions – HTTP RFC

Parser (entities)	Value
Verb (Method)	OPTIONS
Protocol	HTTP 1.0
Parameter name	q
Parameter value	mc'mer
Host header	Sirt.club www.sirt.club
Time	11:11:11
Header123	
Accept	text/html,application/,*/* %00;

RFC @ any request	Policy: Allow/ Block
Header with no value	Block
Double host header	Block
HTTP verbs: POST Get HEAD	Block
Null in request	Block
Parameter value with '	Block
Protocol versions 1.1	Allow
Protocol versions 1.0	Block

WEB CLIENTS

PROTECTION ELEMENTS (PE)

WEB APP

ENTITIES
Parser

- Protocol
- Payload
- User input

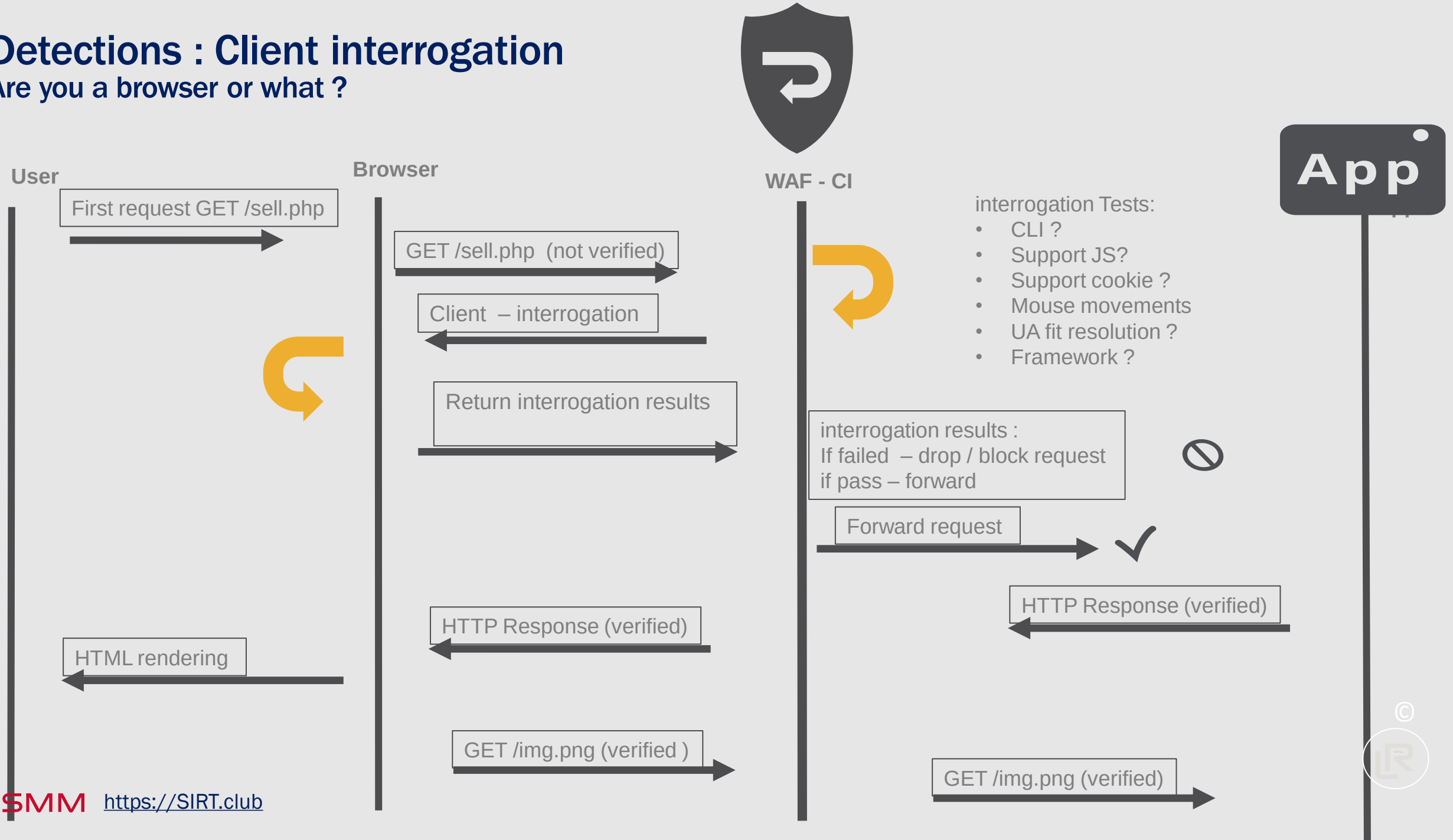
DETECTIONS
Traps

1. SIGNATURES
2. ANOMALY
3. RESTRICTIONS
4. CLIENT INTERROGATION

PREVENTION ACTION
Enforcer

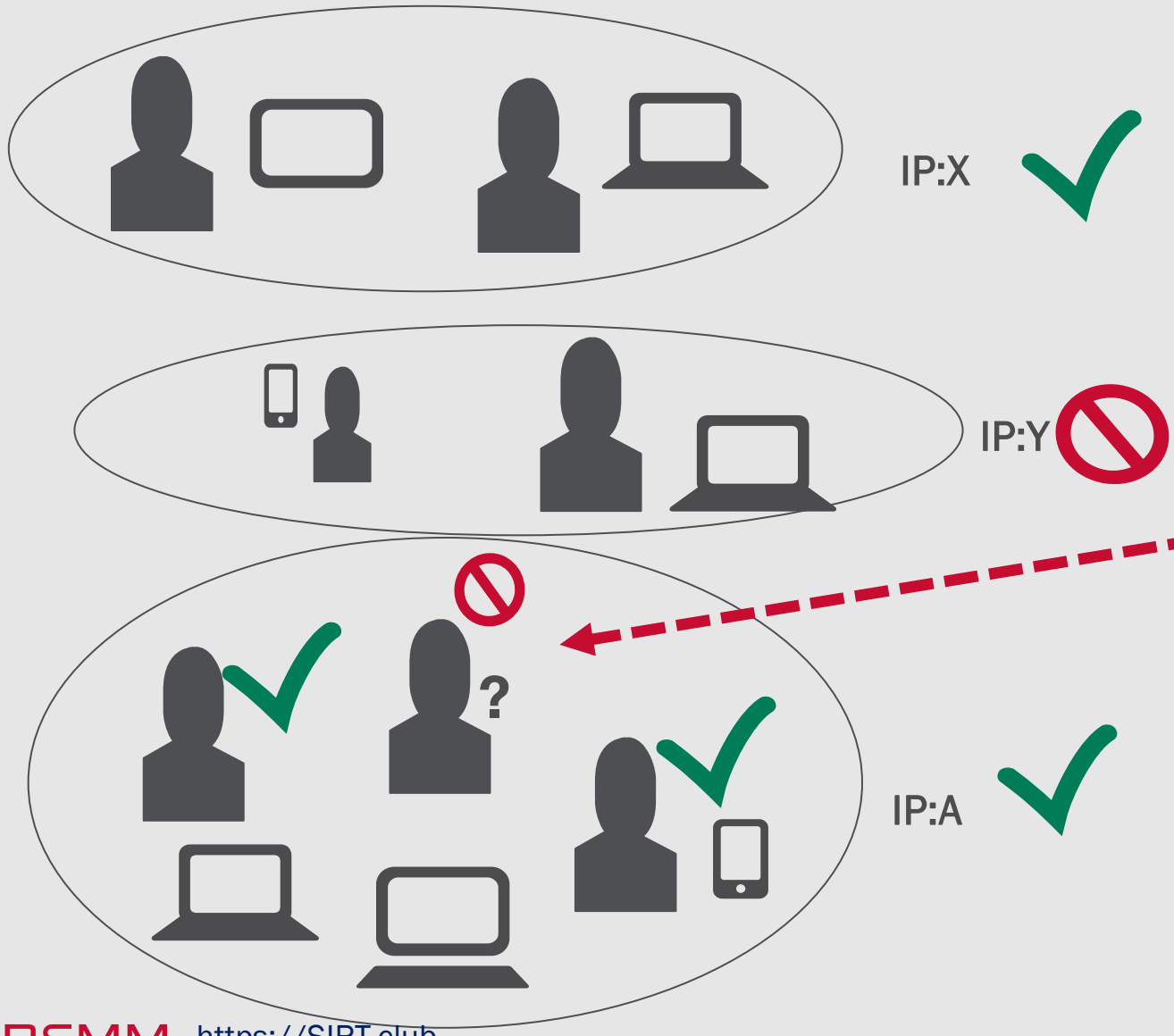
Detections : Client interrogation

Are you a browser or what ?



Detections: Client interrogation

NATed clients query



Who are you ?

CI results	Allowed
Browser	Yes
CLI	**No**
JS capable	Yes
Cookie set	Yes

DP ENGINE: TRAPS -> DETECTIONS:

- **S** Signatures - Pattern matching
- **A** Anomaly - Aggregation and thresholds
- **R** Restrictions - Allow / Block lists
- **CI** Client Interrogation - HTTP client inspection

WEB CLIENTS

PROTECTION ELEMENTS (PE)

ENTITIES
Parser

- Protocol
- Payload
- User input

DETECTIONS
Traps

- SIGNATURES
- ANOMALY
- RESTRICTIONS
- CLIENT INTERROGATION

PREVENTION ACTION
Enforcer

- ALERT
- BLOCK
- LIMIT
- FOLLOW UP

ALERT

- Alert – GUI
- Alert – Log
- SMS
- Messaging – slack
- Email

To: WAF admin

BLOCK

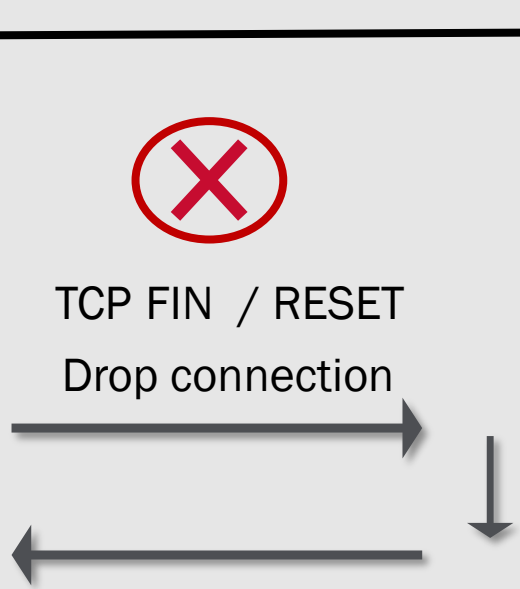
Browser

This request has been blocked

Your traffic is violating the site policy.
If this continues, please contact our support
111-111
Block ID: 10ABC

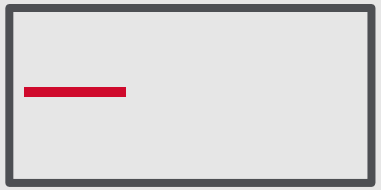
TCP FIN / RESET

Drop connection



To: End Users

Semi blocking:
Stripping / Cloaking



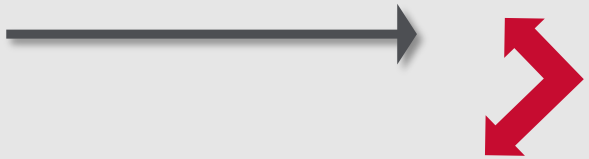
LIMIT

- Limiting rate of RPS on specific IP
- Limiting RPS on site
- Limiting RPS on specific URL
- Limiting time
- Limiting access – 4 hours ban

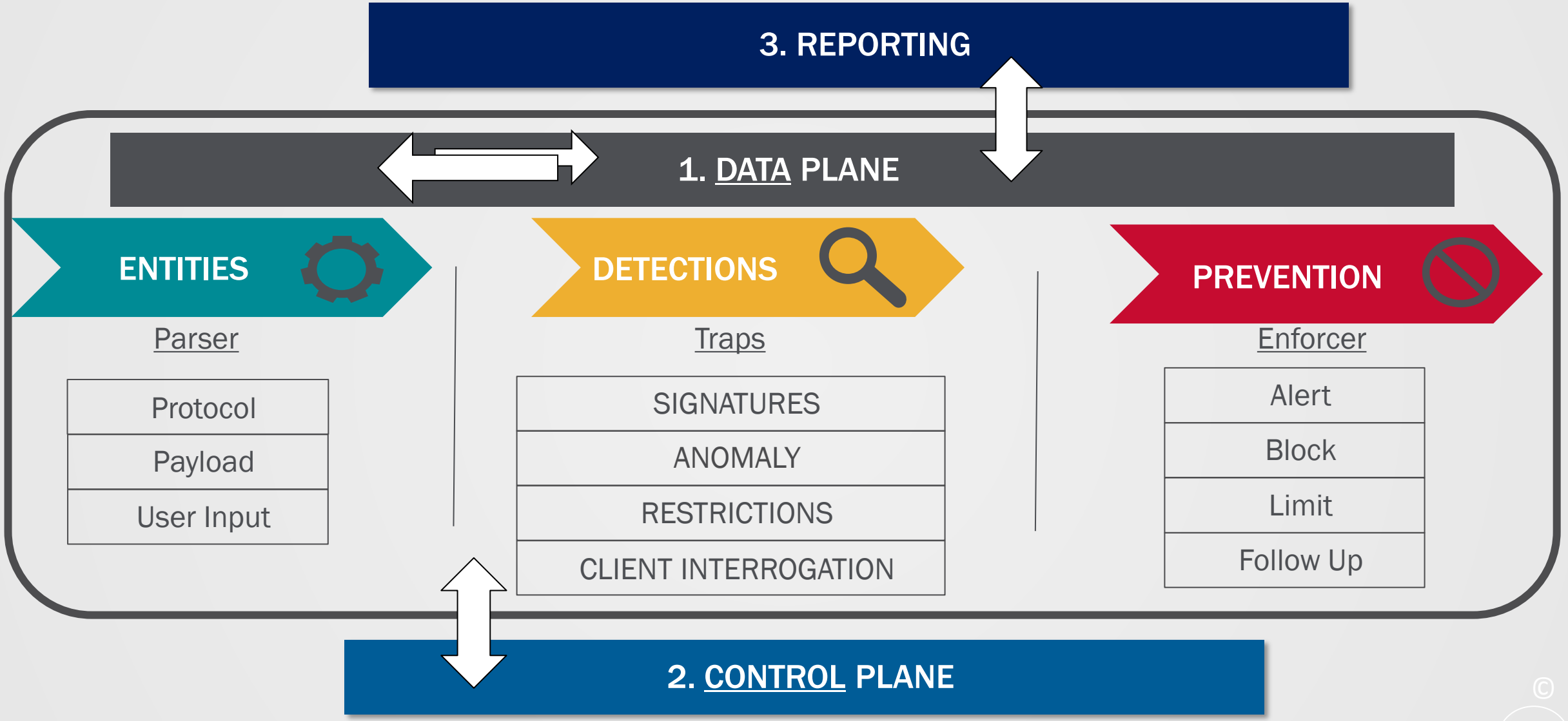
FOLLOW UP

Resent browser to main page

Send users to honeypot for inspections

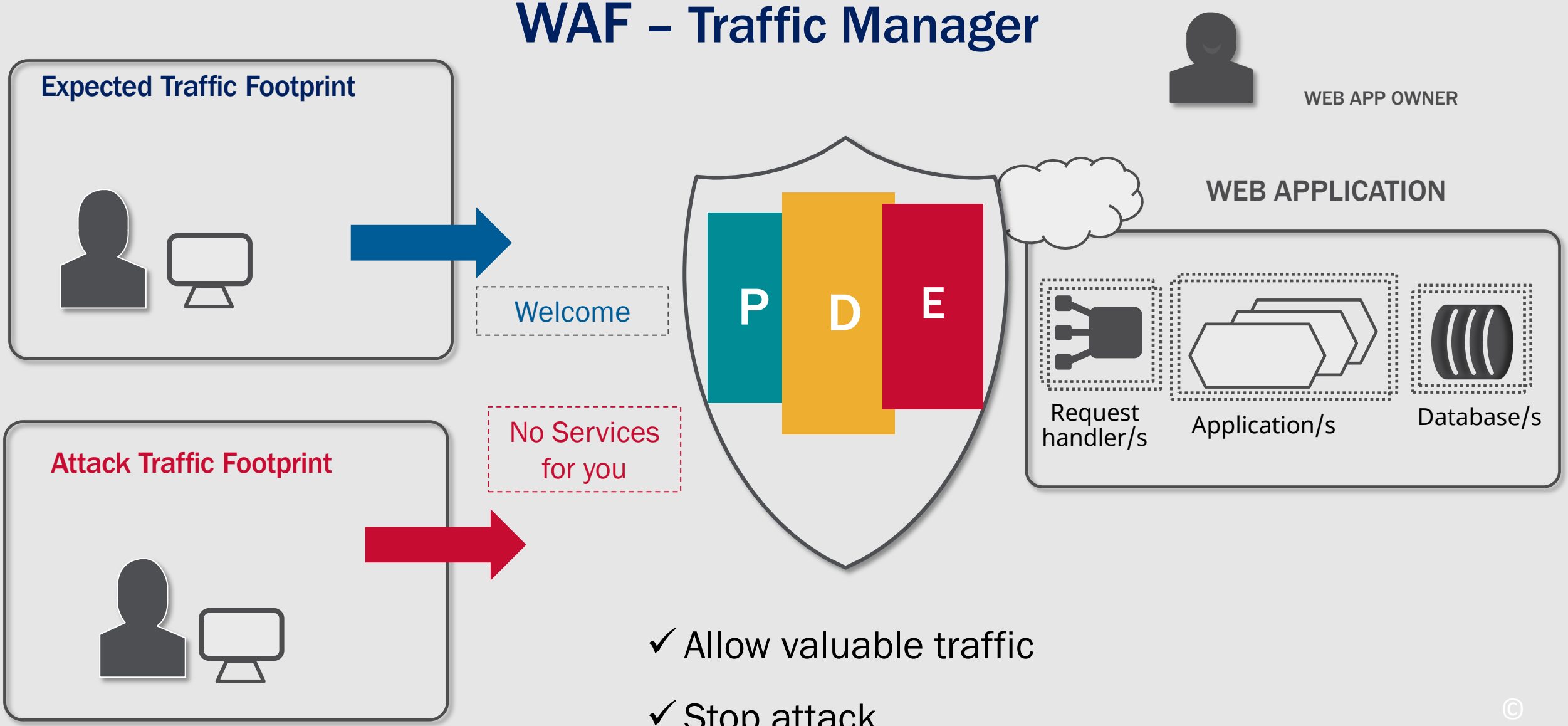


WAF PROTECTION ELEMENTS



WAF Policy

WAF – Traffic Manager



✓ Allow valuable traffic

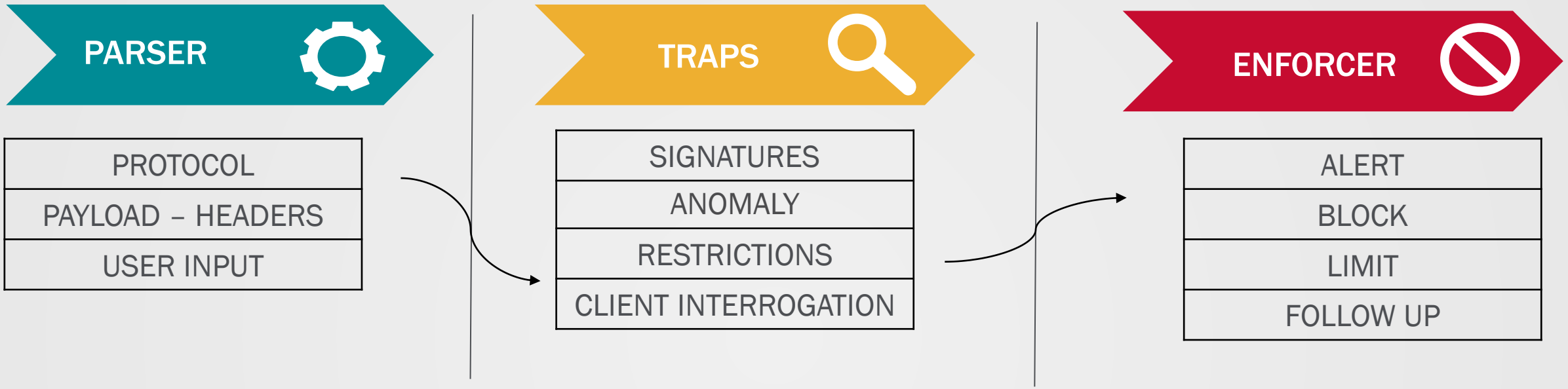
✓ Stop attack

WAF – PE and Rules

PROTECTION ELEMENTS (PE)		
Entity	**Detections**	**Prevention**
1. PROTOCOL 2. PAYLOAD 3. USER INPUT	1. SIGNATURES 2. ANOMALY 3. RESTRICTIONS 4. CLIENT INTERROGATION	1. ALERT 2. BLOCK 3. LIMITING 4. FOLLOW UP

Rule

Rules Concept



Rule: E D P

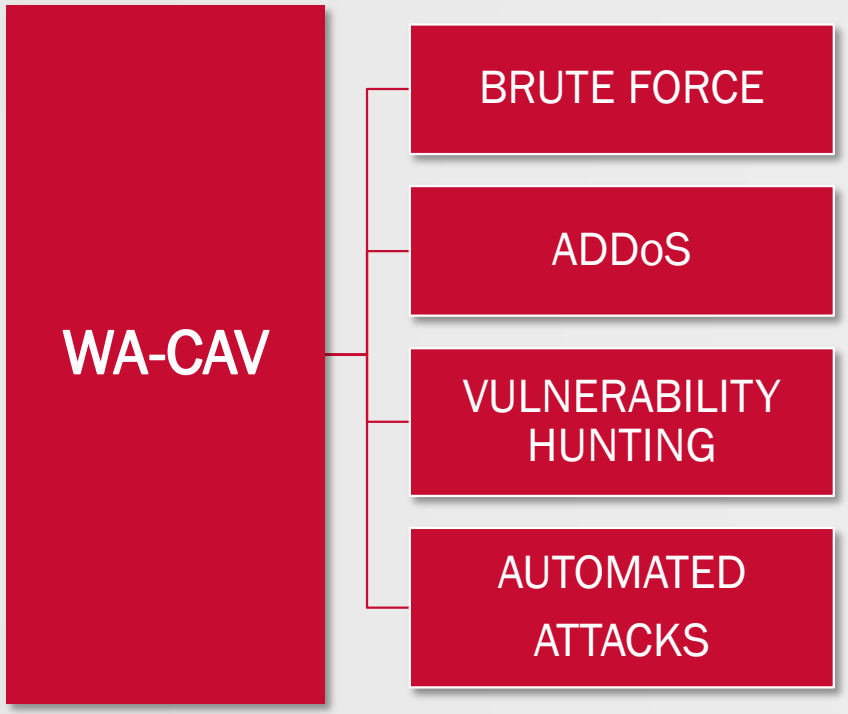
PR1 PE:S CAV: WE-SQLi

- Entity : user input parameter value
- Detection: Signature SQLi select * from
- PA: Blocking page

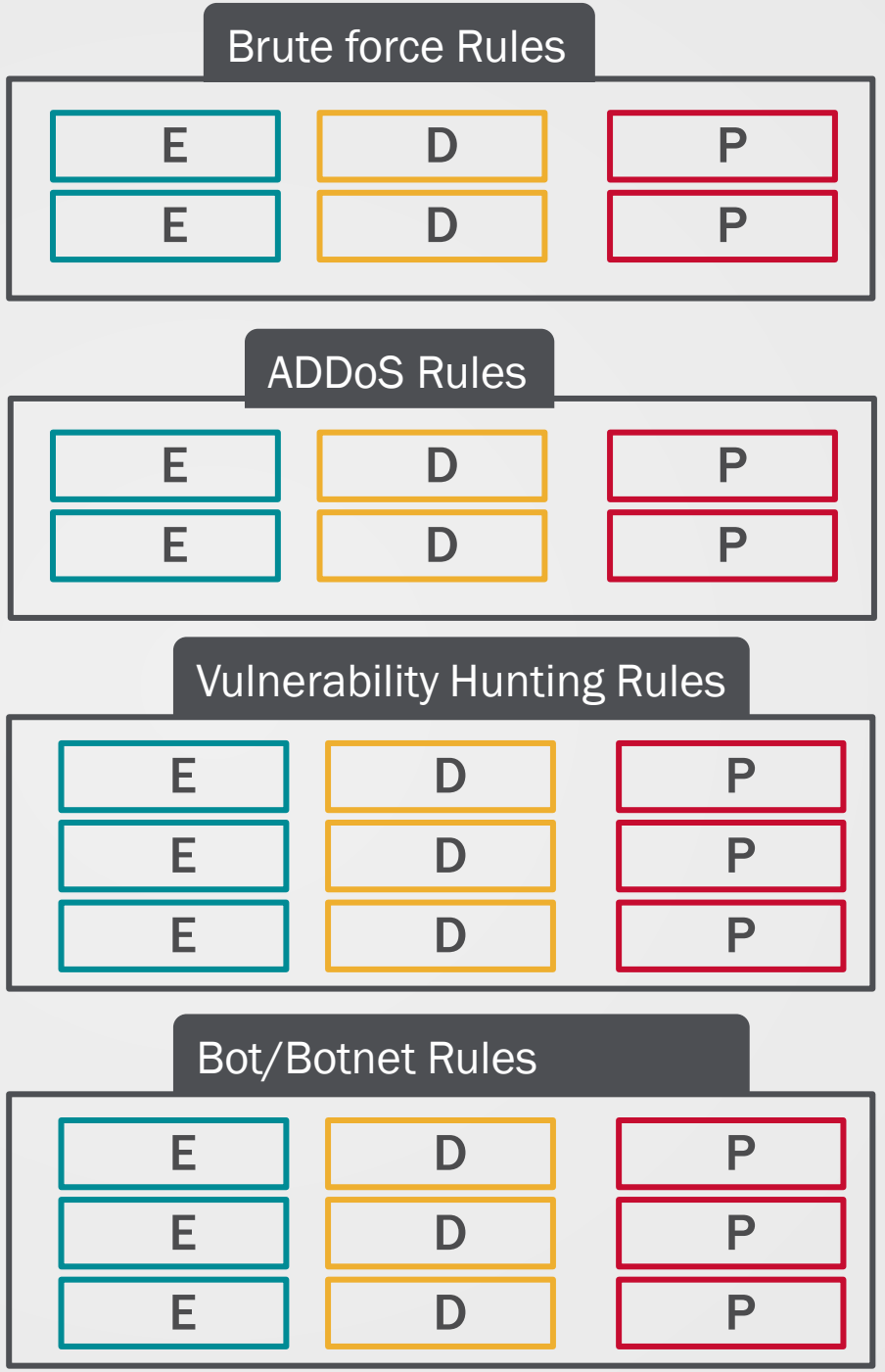
PR2 PE:S CAV: Auto

- Entity: user agent header
- Detection: Signature hydra
- PA: RST connection

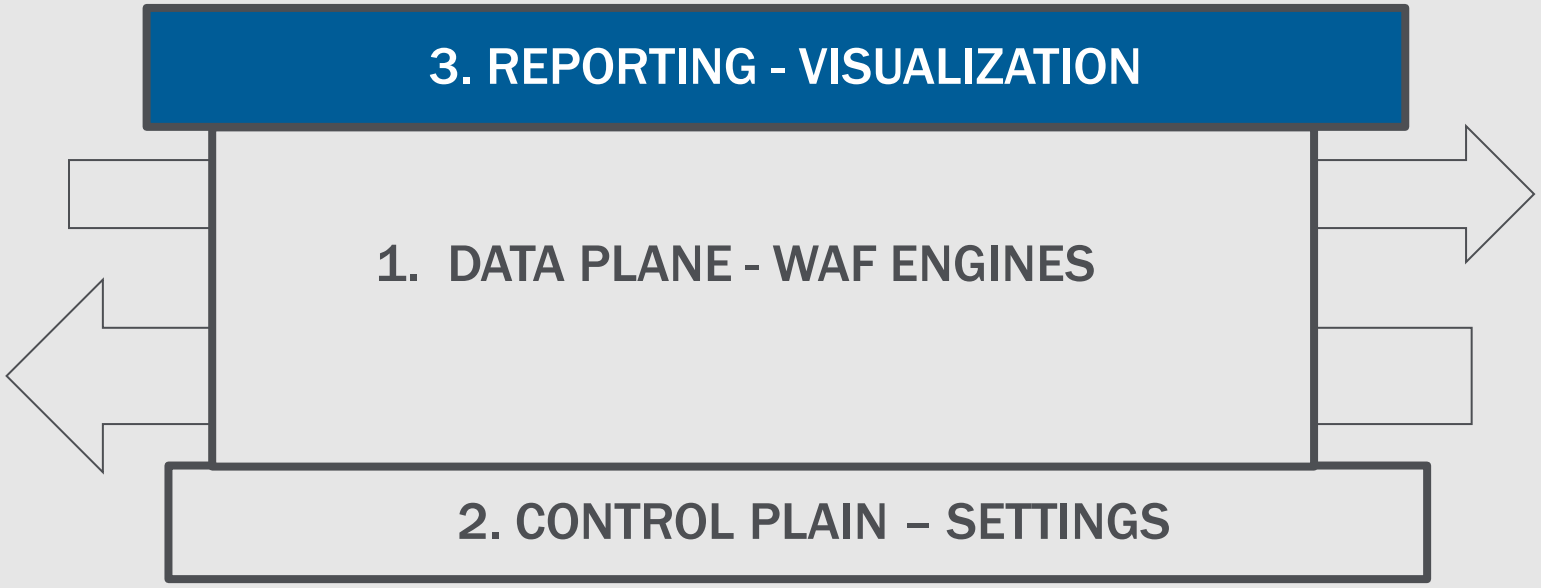
WAF Policy – CAV Base policy



**Common Attack Vector – CAV*



Reporting



SECURITY REPORTING

- DASHBOARD
- GRAPHS
- STATISTICS
- LOGS

SUPPORT REPORTING

- Audit – who did what – changes to policy
- Maintenance – update / upgrade fails
- System – memory, configuration

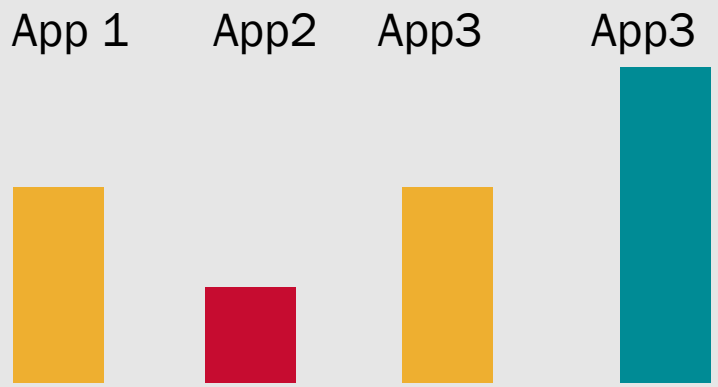
- WAF LOGS
- AUDIT
- MAINTENANCE
- SYSTEM

Dashboard

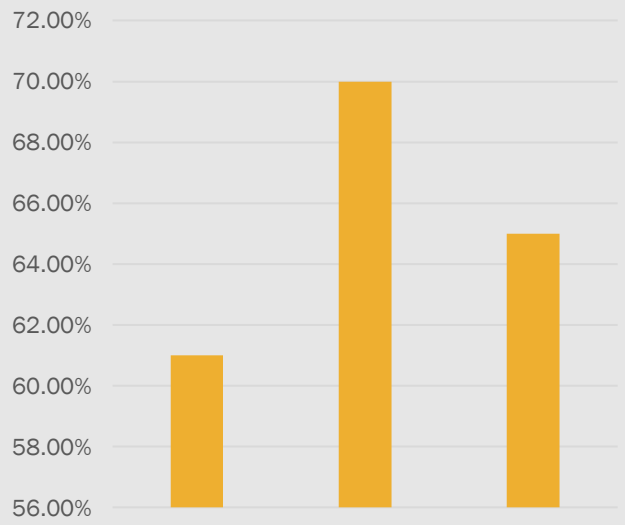
Incidents

Critical	E:H	D:S	BLOCK	1IP 100 Req
High	E:IP	D:R	RATE LIMIT	1IP 10Req
Medium	E:URL	D:A	ALARM	10IP 1000Req

App Health



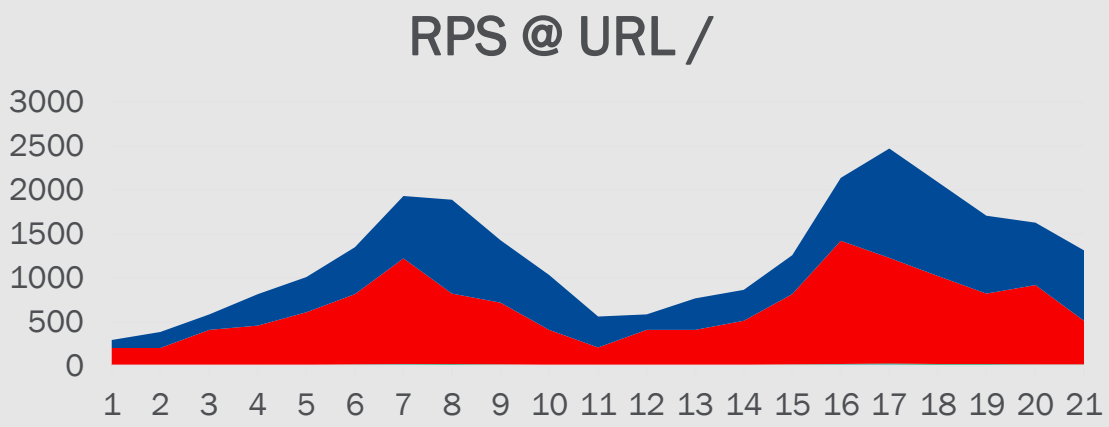
Traffic ETF

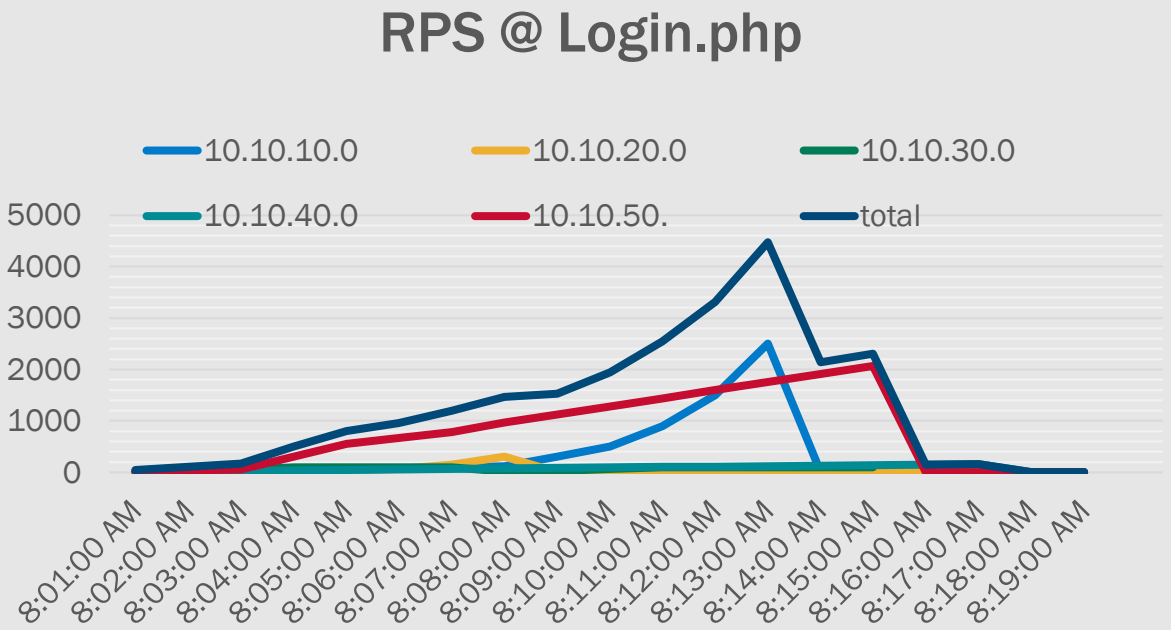


Action items:

- Update signature for CVE XXXXX
- False positive on parameter q
- Update swagger schema

Graphs



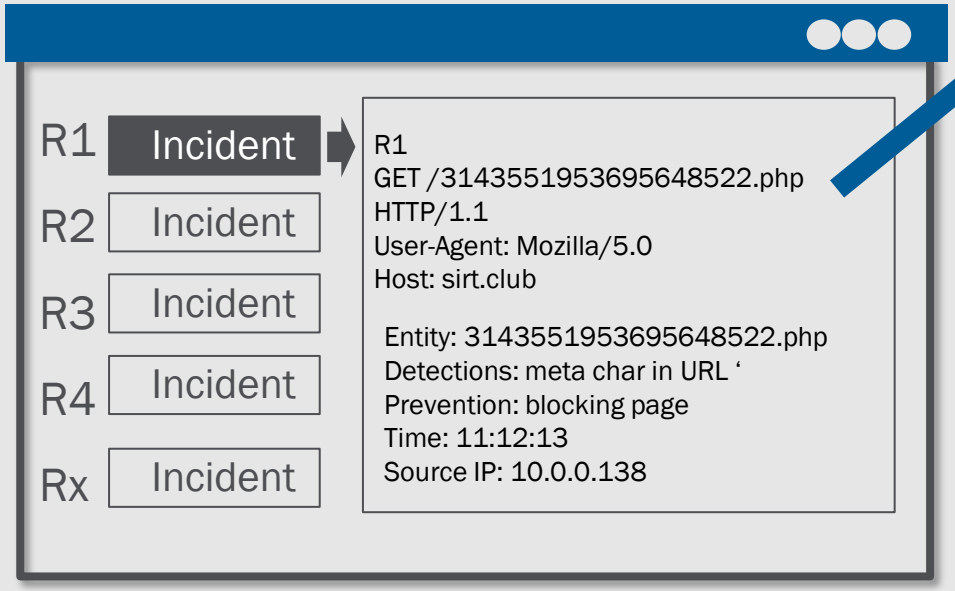


Statistics

Top URL's	RPS
/	21.21k
/search.php	2.75k
/login.php	2.26k
/sell.php	2.25k
/user_login.php	2.23k
/blog.php	2.01k

Aggregated	21.21k	23.57	36.72k
10.10.1.12	2.75k	3.05	4.08k
72.1.38.240	2.26k	2.51	5.27k
192.168.1.1	2.25k	2.50	3.10k
172.16.184.126	2.23k	2.48	4.64k
192.168.1.12	2.01k	2.23	2.82k

Security Request log



R1
GET /3143551953695648852'2.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: sirt.club

R2

TRACK / HTTP/1.1

Connection: Keep-Alive

Host: sirt.club

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36

(KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36

Trace-Test: Nikto

R3

OPTIONS /API/V1/login HTTP/1.1

User-Agent: Mozilla/5.0 Firefox/11.0

Accept: image/webp,*/*

Accept-Language: en-US,en;q=0.5

Host: sirt.club

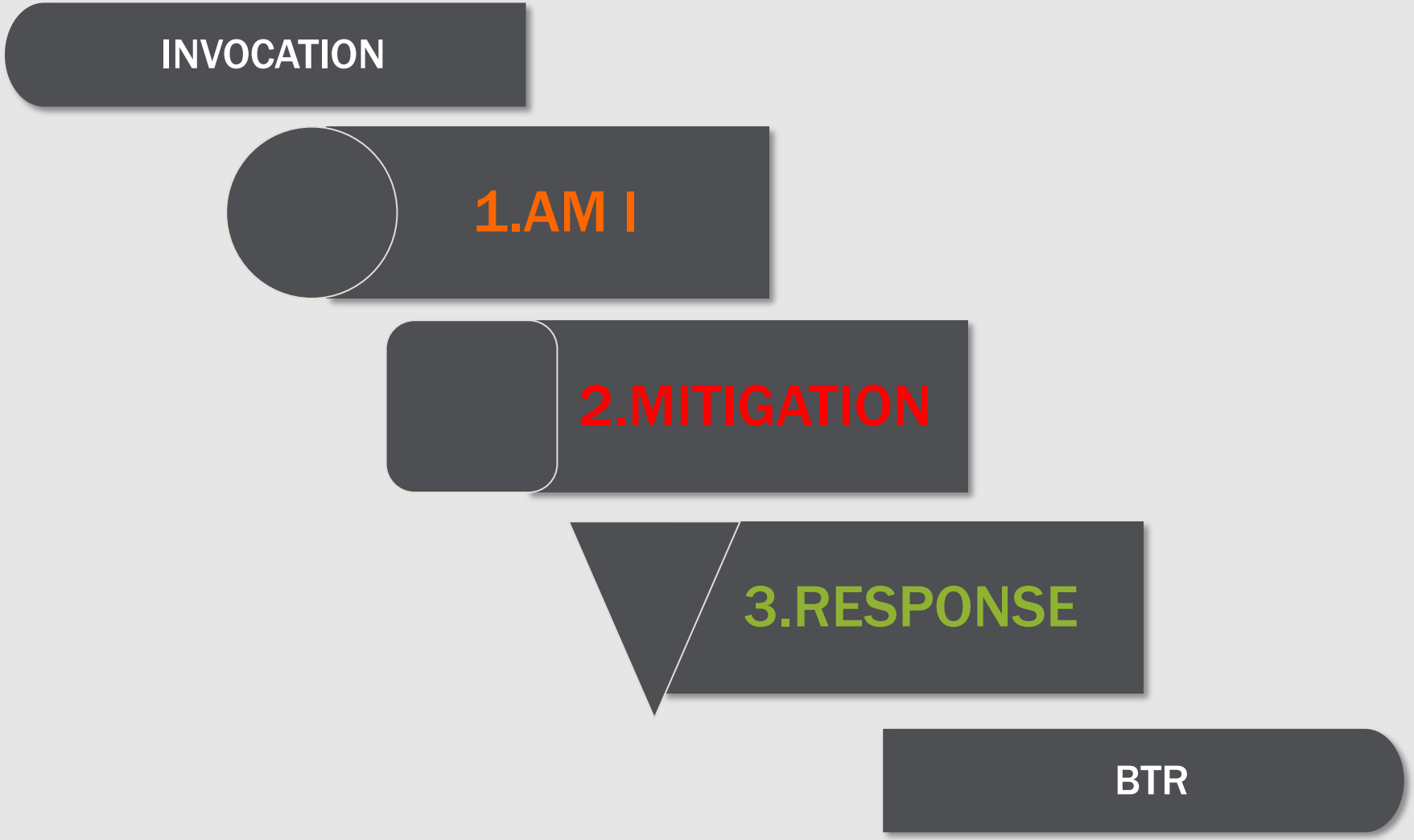
"Outlook view of incident and their request details

WAF aSIR

Security Incident Response

SIR

Security Incident Response



INVOCATION

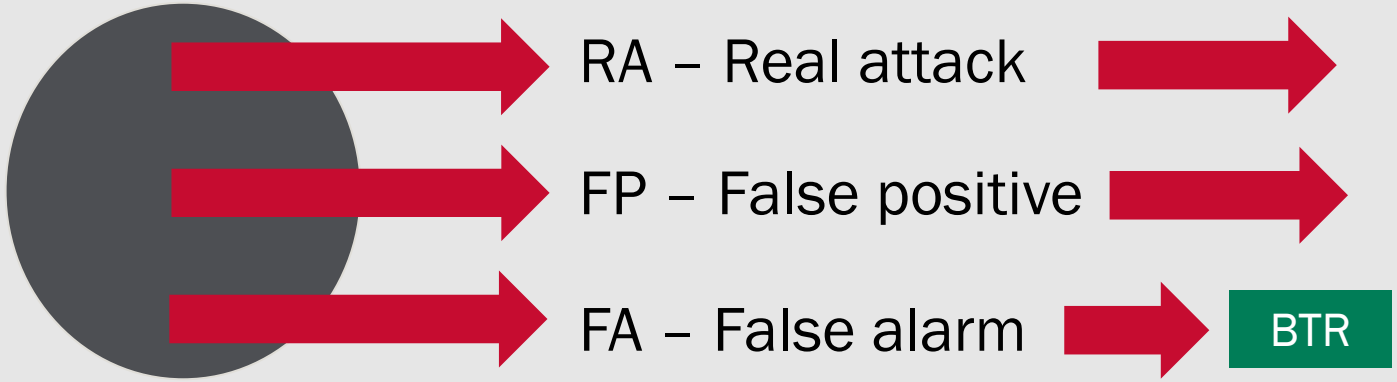
Invocation – a possible security related issue/s needs attention, Now

- Security Device
- App monitoring
- Humans

1. AM I

Am I under attack ?

Declare the incident type and Determine the impact



Impact:

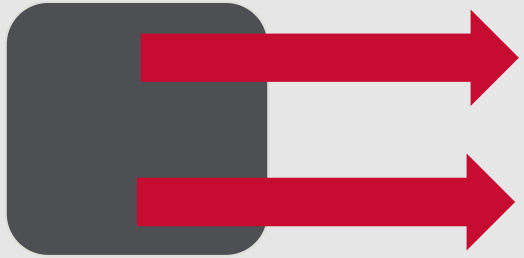
- S1 – Service down
- S2 – Major impact
- S3 – General impact

P2.MITIGATION

2. MITIGATION

How to mitigate (S&D)

Find Suspicious Indicators (SIN) & Compose Prevention Rule (PR)



- ❑ Suspicious indicators (3SIN)
- ❑ Compose prevention rule (PR)

P3.RESPONSE

3. RESPONSE

Response – Apply & Verify

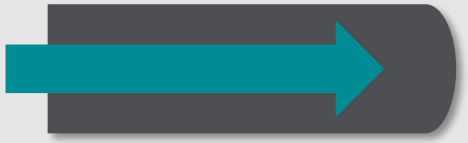
Apply prevention rule and verify attack mitigation

- ❑ Apply mitigation strategy
- ❑ Monitor mitigation

BTR

Back To Routine (BTR)

Declaring back to routine when attack is being blocked or attack stopped



- ✓ BTR – monitoring attack
- ✓ BTR – EoA – end of attack

Summary

WA-CAV

Vulnerability

Web Application

Attack Surface

SQLi | XSS | LFI/ RFI | RCE | CSRF | BF | CS | PS | Floods | Loads

Web Exploits | ATO | DDoS

BOT/S
BOTNET/S

ORCHESTRATION – NODE'S

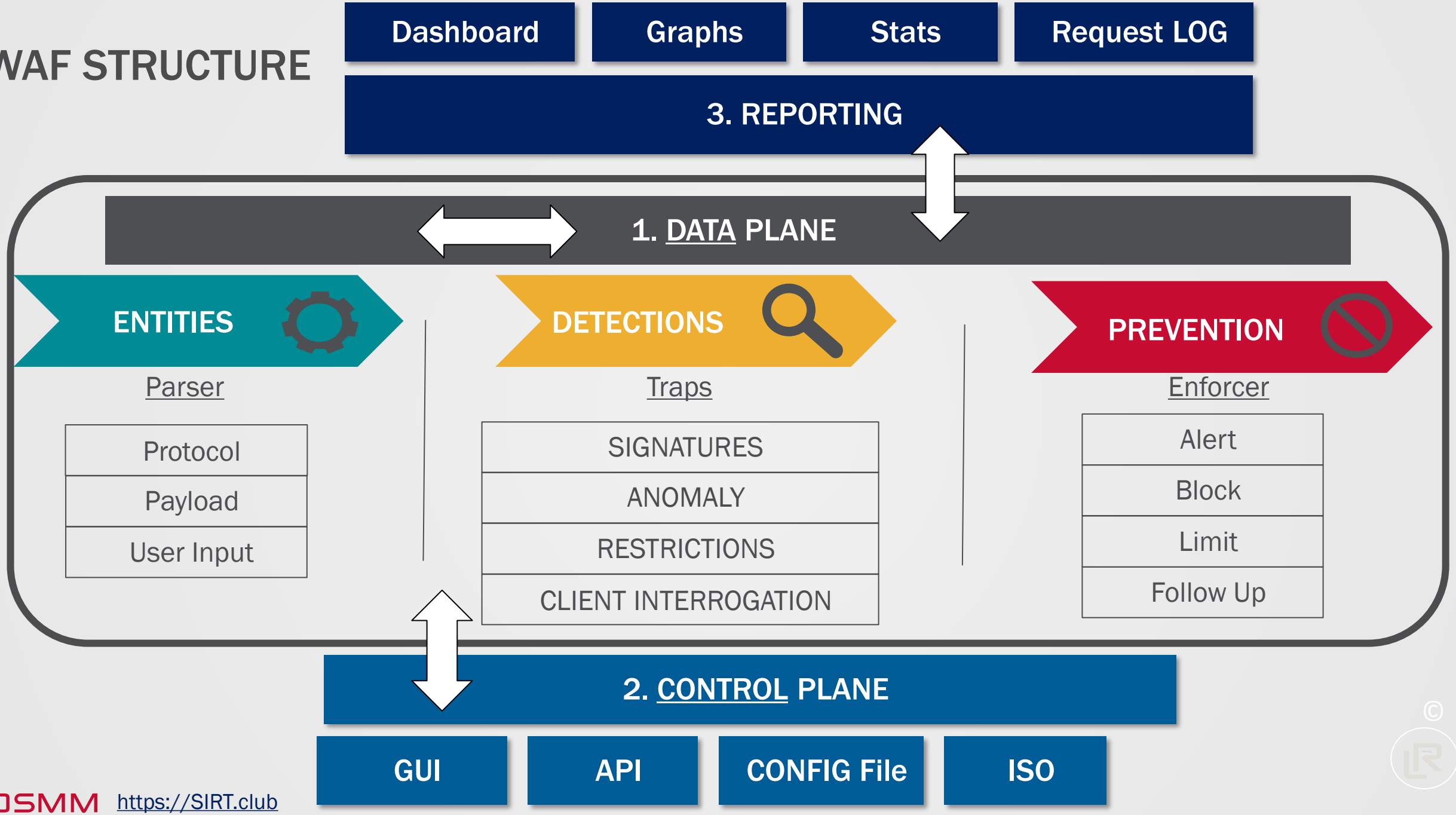
Exploit

Attack Agent

AUTO

ATTACK AUTOMATION

WAF STRUCTURE

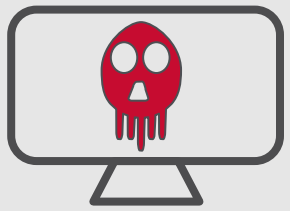


WA-CAV

Security Arsenal

WEB APP

Web Application Firewall



AA

e

AUTO

Web Exploits

- SQLi
- XSS
- LFI/ RFI
- CSRF
- RCE

SIGNATURES

RESTRICTIONS

ANOMALY

ATO

- BF
- CS
- PS

ANOMALY

CLIENT INTG

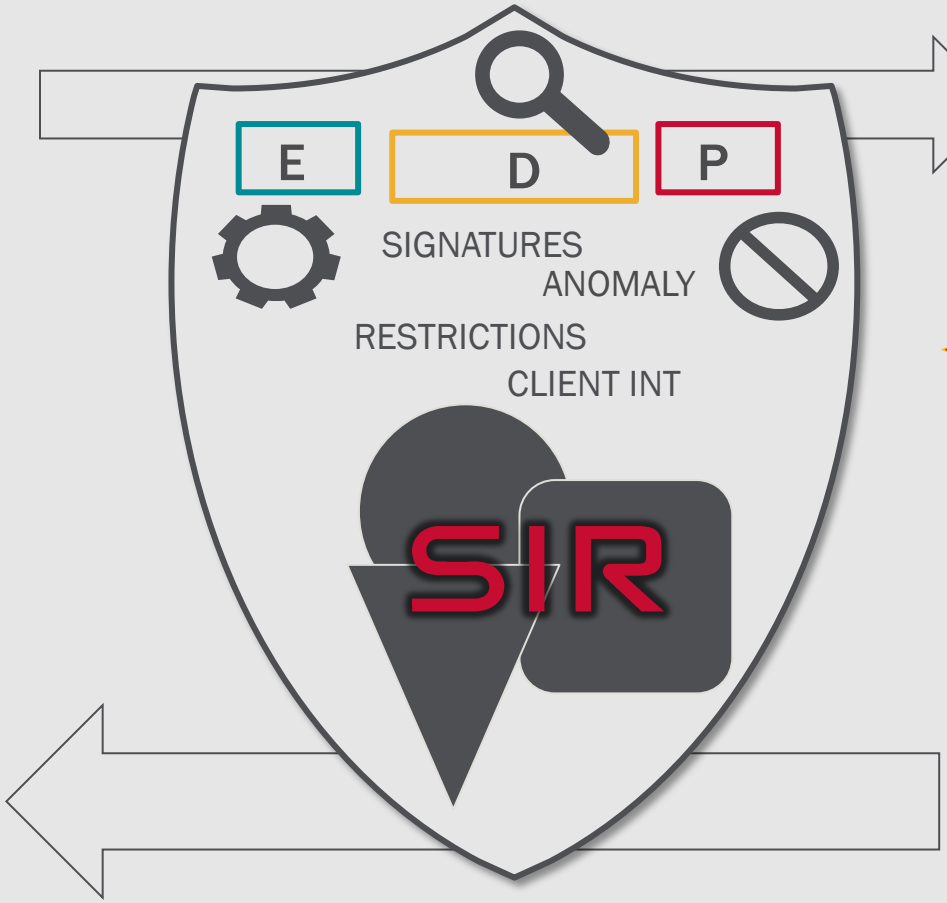
RESTRICTIONS

DDoS

- Floods
- Loads

ANOMALY

CLIENT INTG



V

AS

The WAF book ©

Practical Defensive Security for Security Engineers

Part of: Defensive Security Management Methodology

DSMM

By: Lior Rotkovitch

- *Email: lior.rotkovitch@gmail.com*
- *Twitter: @rotkovitch*
- *LinkedIn: Lior Rotkovitch*
- *Instagram: l.rotkovitch*

"Man's biggest obstacle is he himself" *LR*

https://SIRT.club