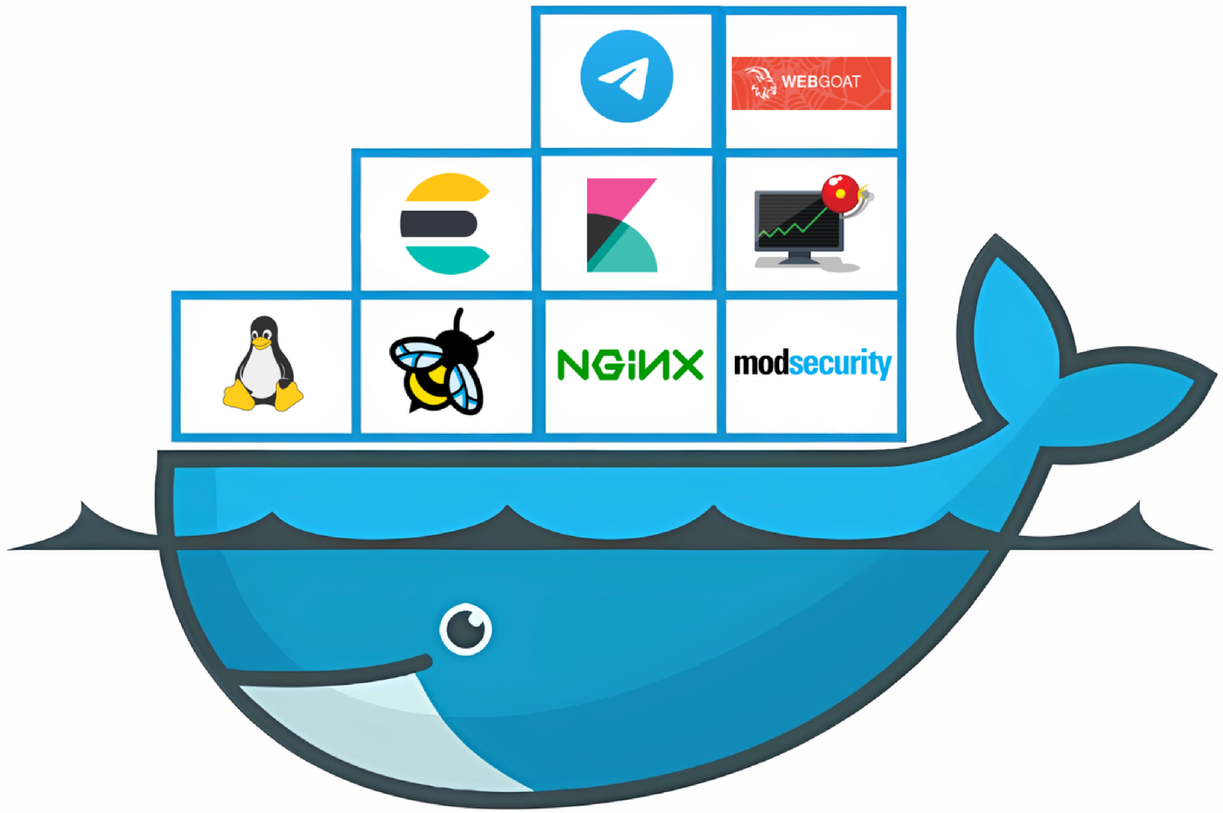
SECURE WITH

Web Application Firewall



GROUP 6

Lê Mậu Anh Phong - 21520087

Nguyễn Duy Huy - 21520042

LIST OF

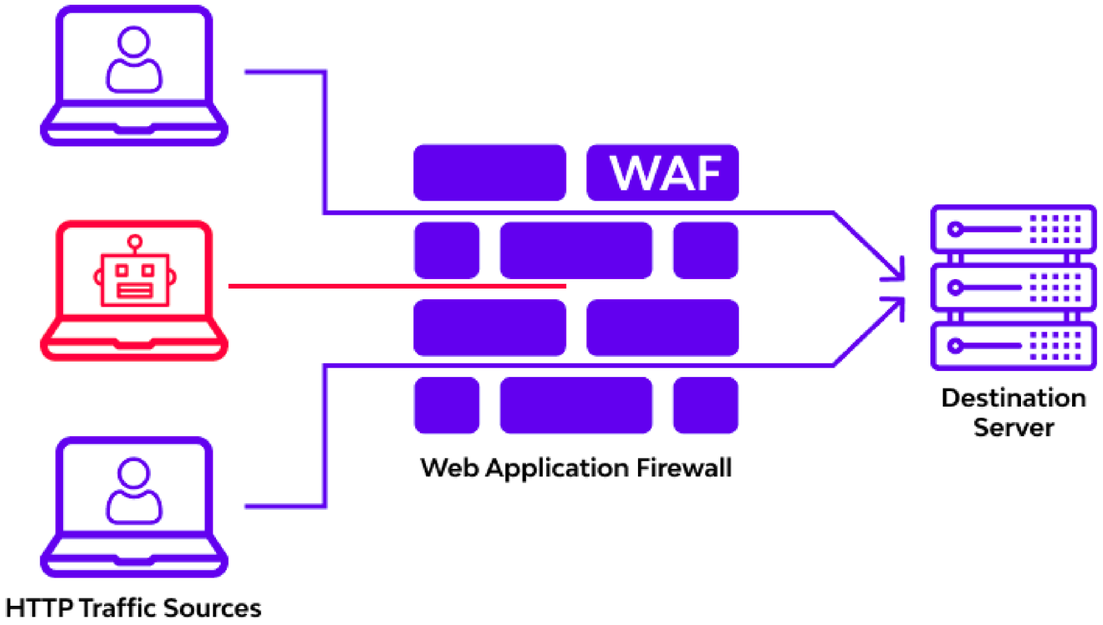
CONTENTS

0 1

INTRODUCTION

Payload attack, malware located deeply in the application layer

Need a stronger firewall to check those fields



02

PROPOSAL

NGINX + ModSecurity to protect vulnerable web app (WebGoat) ✅

ENHANCEMENT

ELK for searching and logs analysis ✅

eBPF for more inspection ✅

Alert for quick action ✅

AI, Machine Learning integration ✅

03

GOAL

- Learn about ModSecurity's features
- Deploy WAF on Linux to protect web app
- Understand how it works
- Pros and cons
- Workaround suggestions

04

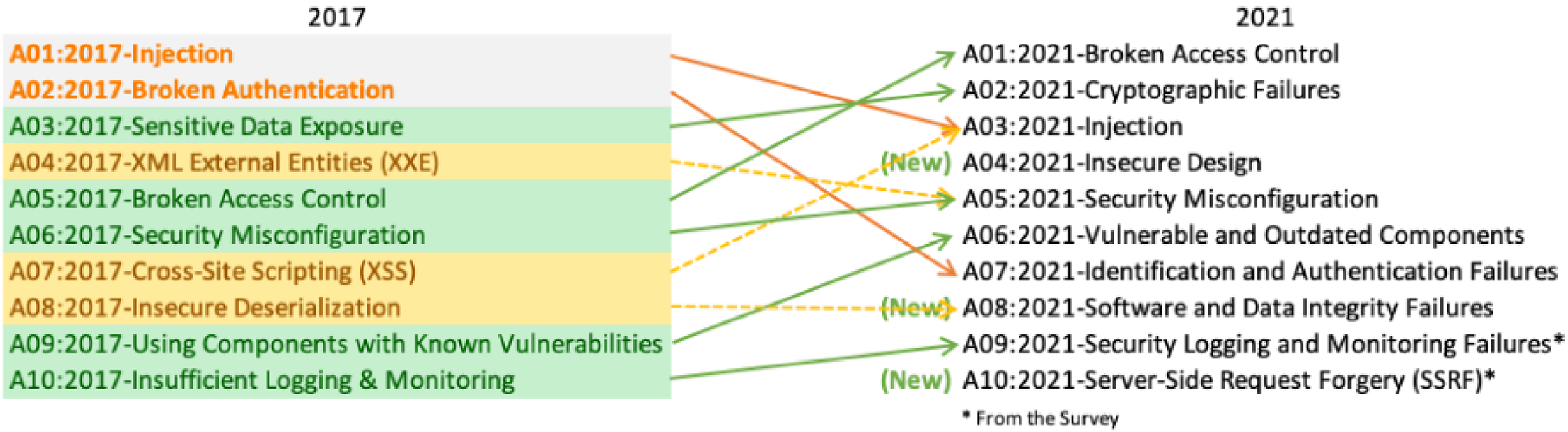
APPROACH

- Learn about NGINX + ModSecurity ✅
- Dive into WebGoat and attacks methods ✅
- Research and integrate Elasticsearch ✅
- Deploy a fully working system ✅
- Test protection, logging and alert functions ✅

04

APPROACH

- **Top 10 OWASP: https://owasp.org/www-project-top-ten/**



05

modsecurity

Introduction:

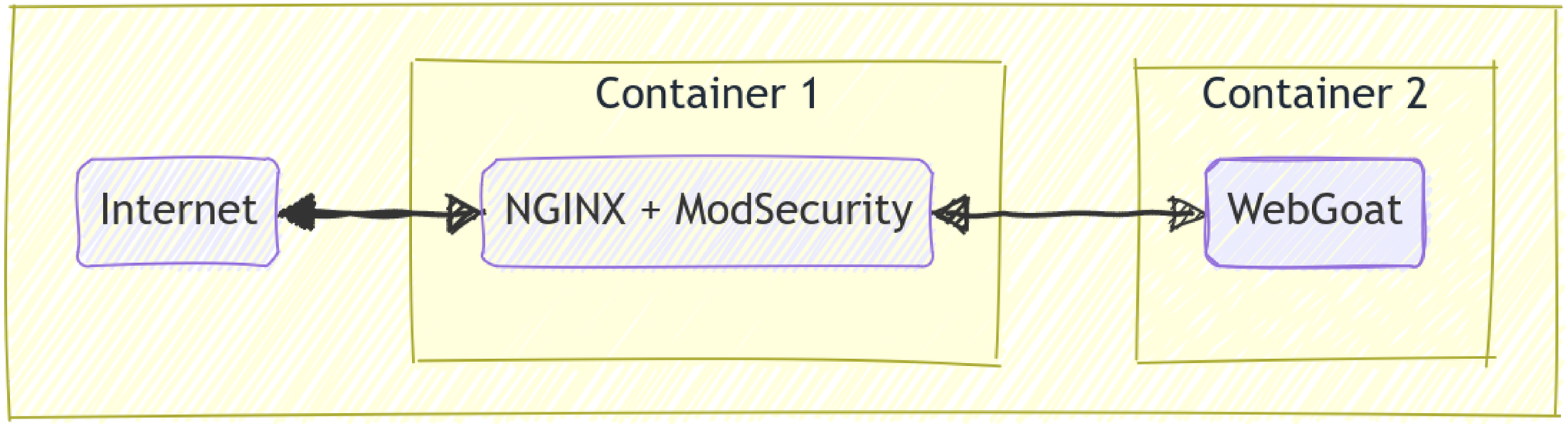
- Web application firewall
- Open source
- Multiplatform
- Lots of features
- Support Apache, IIS, Nginx,..

Features:

- HTTP Traffic Logging
- Real-Time Monitoring and Attack Detection
- Attack Prevention and Virtual Patching
- Flexible Rule Engine
- Portability

05

WAF ARCHITECTURE



WAF system's architecture to protect WebGoat

06

ENHANCEMENT - ELK

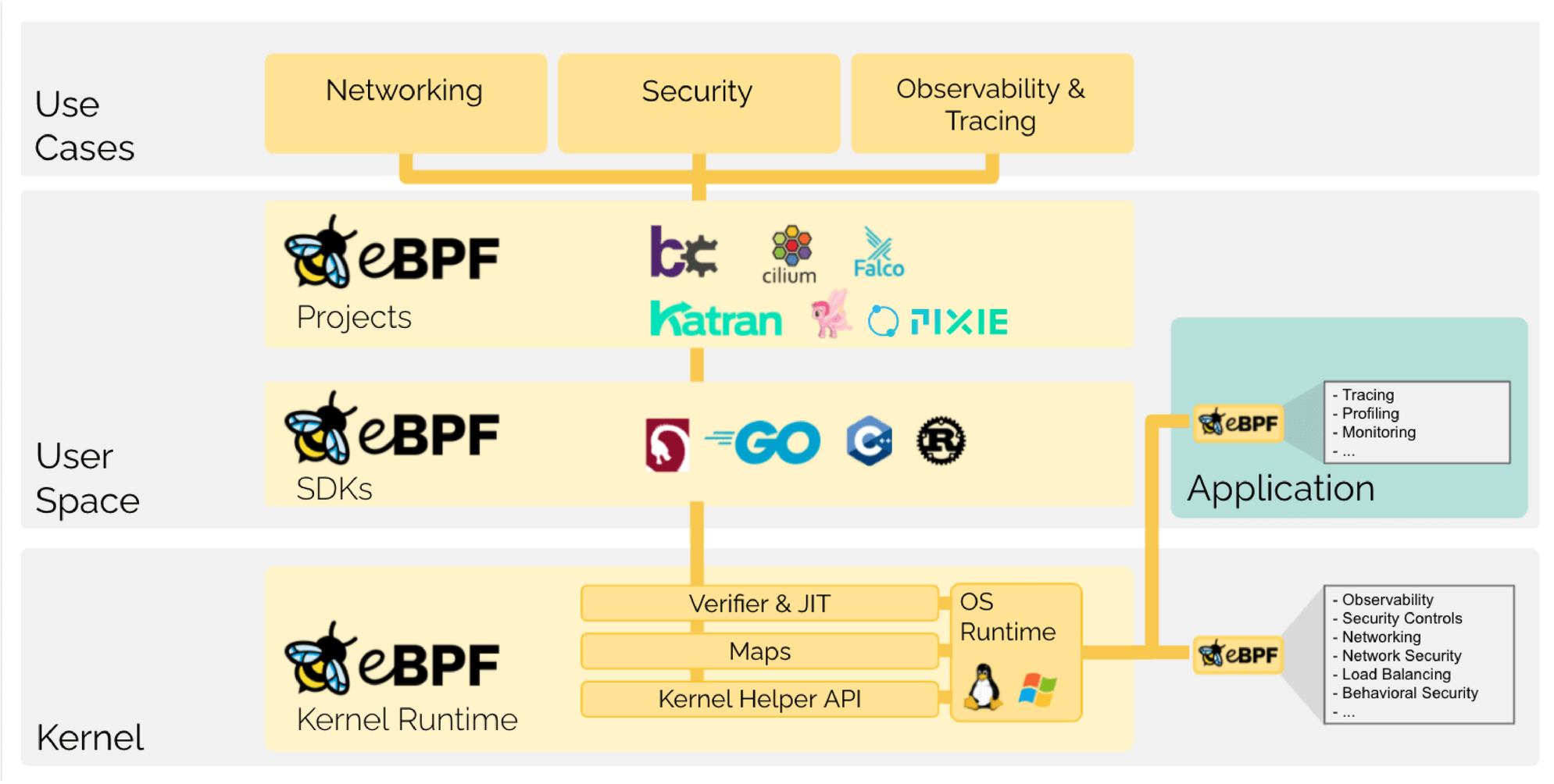
- Logging
- Analyzing
- Visualizing

Features:

- Powerful Query DSL
- Real-time Data Analysis
- Distributed and Scalable
- Document-oriented
- RESTful API
- Aggregation and Analytics
- ...

06

ENHANCEMENT - ELK'S EBPF

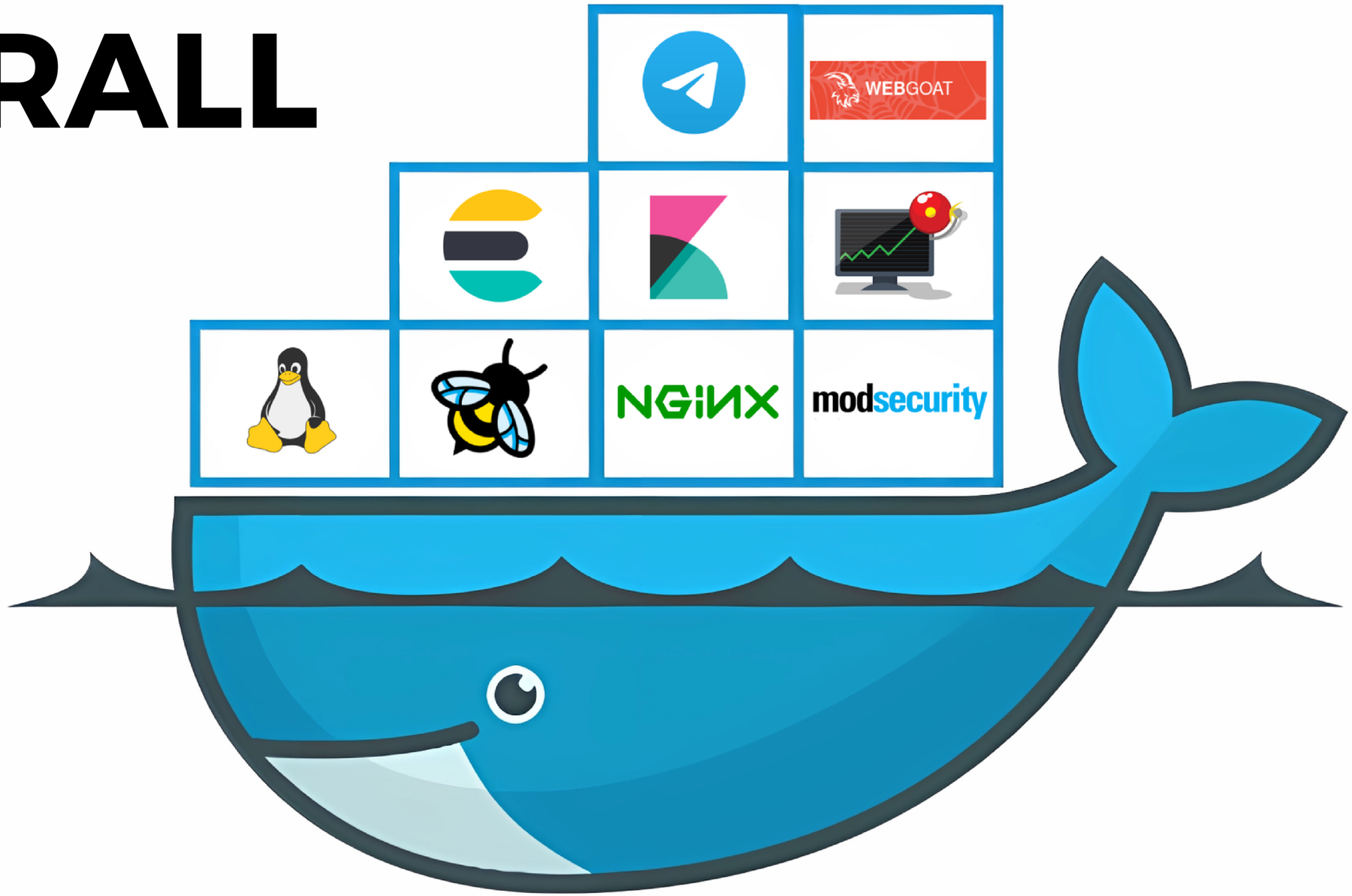


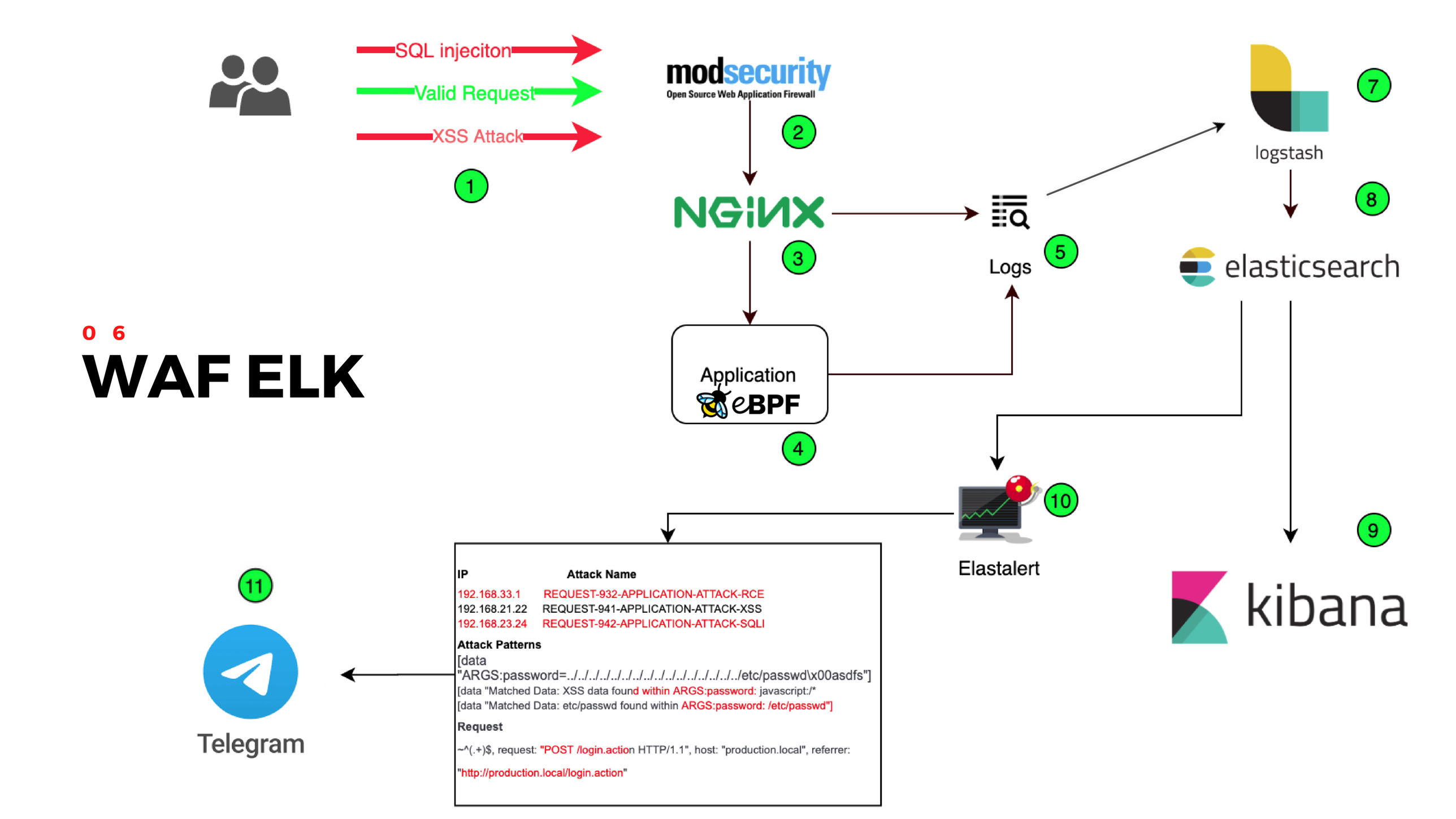
06

ENHANCEMENT - ELASTALERT

- Alerting on anomalies, patterns of interest from data in Elasticsearch
- Alert when a match is found
- Work with Email, Telegram, Slack, ...

OVERALL



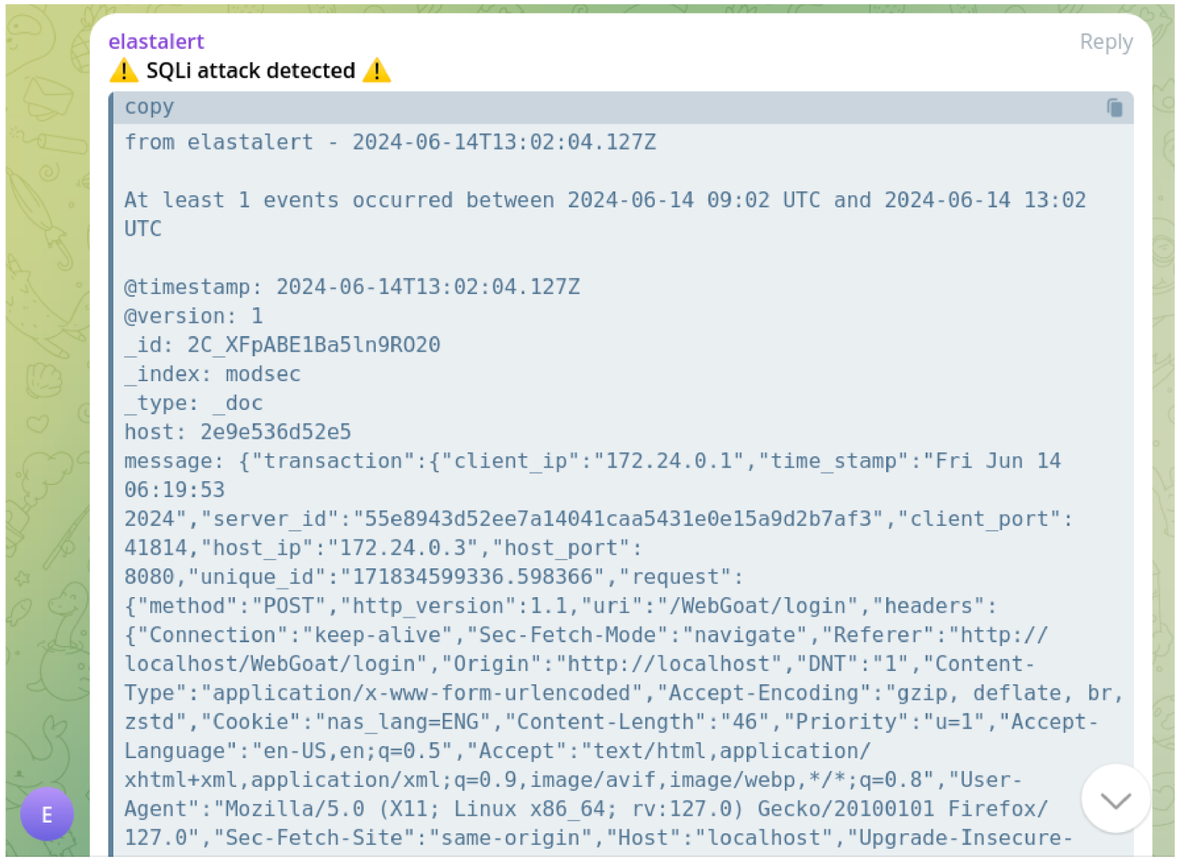

SQL injeciton
Valid Request
XSS Attack
1
modsecurity
Open Source Web Application Firewall
2
NGINX
3
Application
eBPF
4
Logs
5
logstash
7
8
elasticsearch
9
kibana
10
Elastalert
11
Telegram
IP
Attack Name
192.168.33.1 REQUEST-932-APPLICATION-ATTACK-RCE
192.168.21.22 REQUEST-941-APPLICATION-ATTACK-XSS
192.168.23.24 REQUEST-942-APPLICATION-ATTACK-SQLI
Attack Patterns
[data "ARGS:password=../../../../../../../../../../../../../../../etc/passwd\x00asdfs"]
[data "Matched Data: XSS data found within ARGS:password: javascript:/*
[data "Matched Data: etc/passwd found within ARGS:password: /etc/passwd"]
Request
~^(.+)$, request: "POST /login.action HTTP/1.1", host: "production.local", referrer:
"http://production.local/login.action"

06

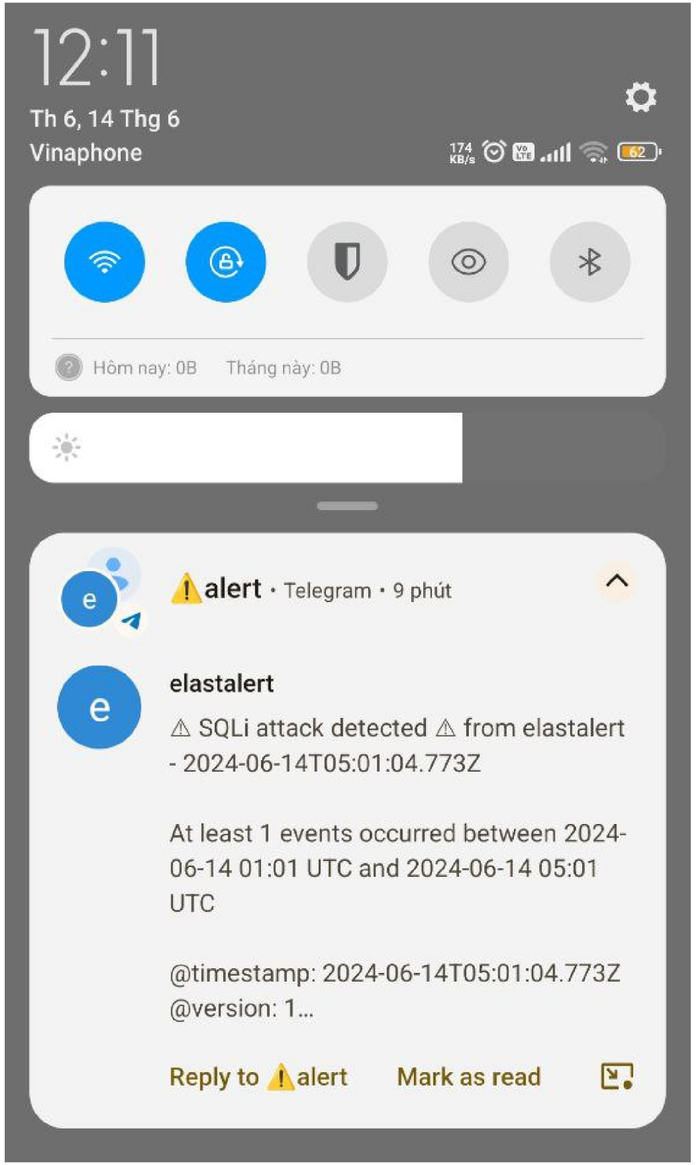
WAF ELK

Cross platform

Telegram



Desktop

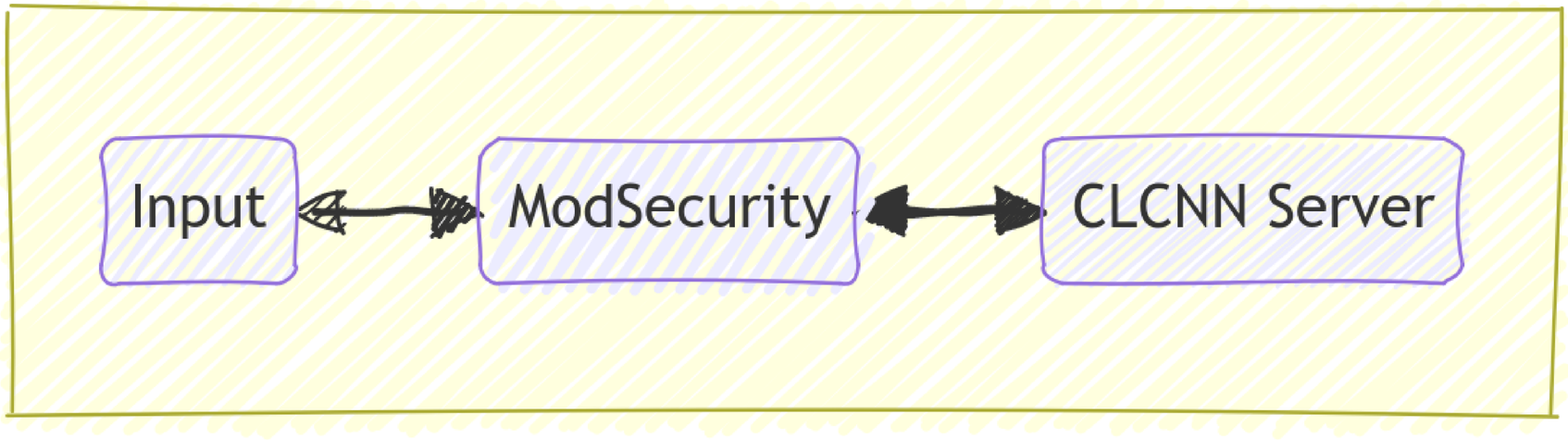


Android

06

ENHANCEMENT - AI, ML

- Rule-based WAFs have the drawback of false positives
- Requiring ongoing rule adjustment and updates to defend against new attack vectors



07

ENVIRONMENT

Deployment's environment

01 Docker (WebGoat, ModSecurity, ...)

02 Host: Linux x86_64

03 RAM: 8GB

04 CPU: Ryzen 5 5600H

05 SSD: 512GB

0 8

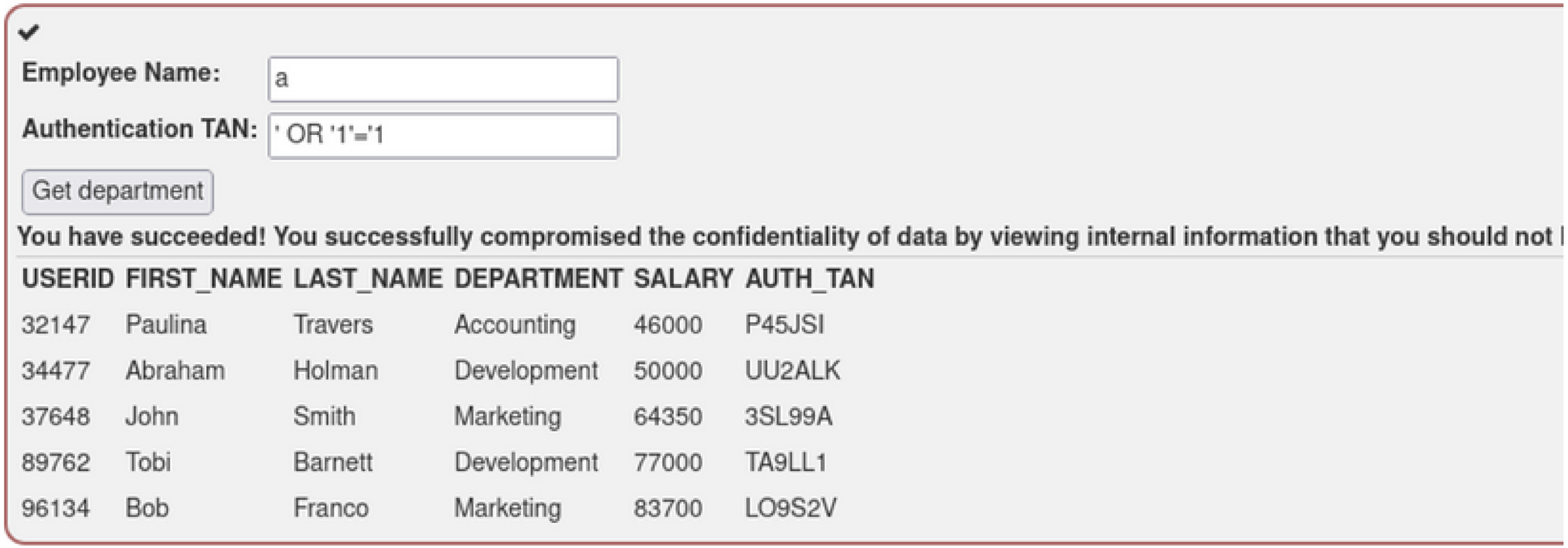
TEST SCHEMES & DEMO

- SQLi, XSS when WAF is working ✅
- Virtual Patching ✅
- Alert when the server is under attack ✅
- Alert when malicious binaries is run ✅
- Logs checking, visualizing to analysis and investigate ✅

0 8

SQL INJECTION

No WAF -> Successfully exploited



✔

Employee Name: a

Authentication TAN: ' OR '1'='1

Get department

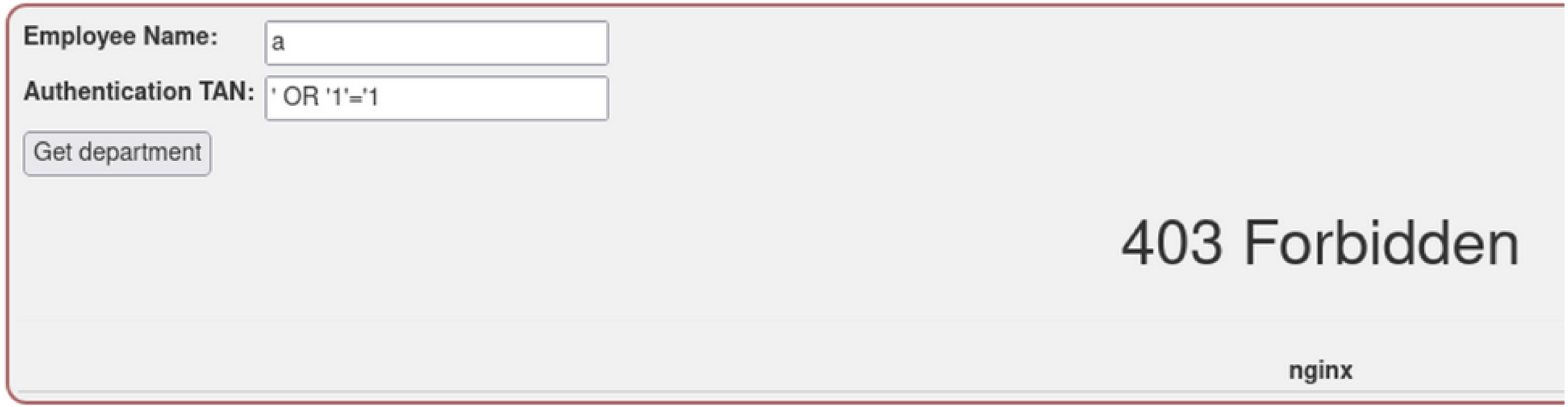
You have succeeded! You successfully compromised the confidentiality of data by viewing internal information that you should not

USERID	FIRST_NAME	LAST_NAME	DEPARTMENT	SALARY	AUTH_TAN
32147	Paulina	Travers	Accounting	46000	P45JSI
34477	Abraham	Holman	Development	50000	UU2ALK
37648	John	Smith	Marketing	64350	3SL99A
89762	Tobi	Barnett	Development	77000	TA9LL1
96134	Bob	Franco	Marketing	83700	LO9S2V

0 8

SQL INJECTION

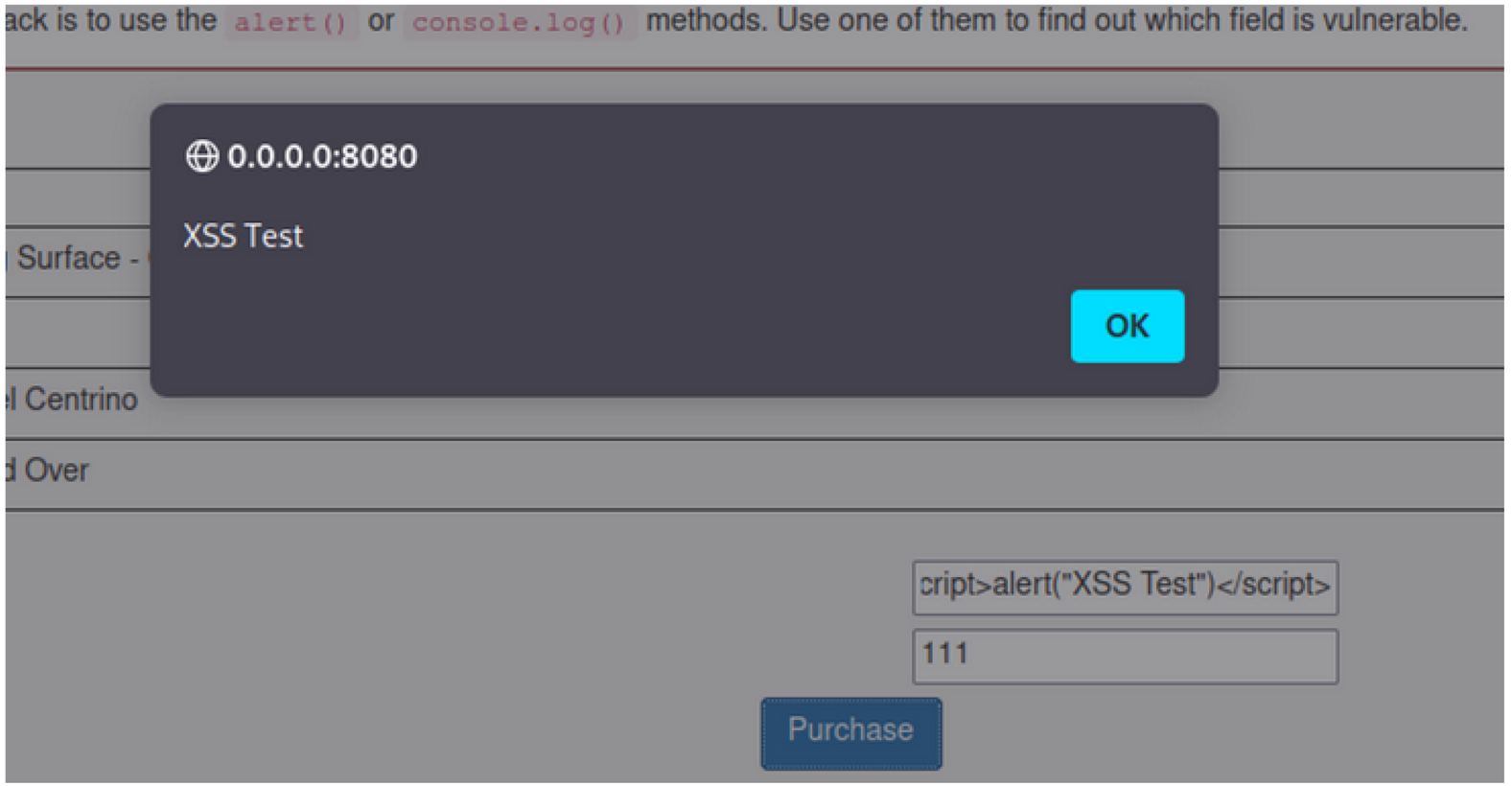
WAF -> Exploit has been blocked



0 8

XSS

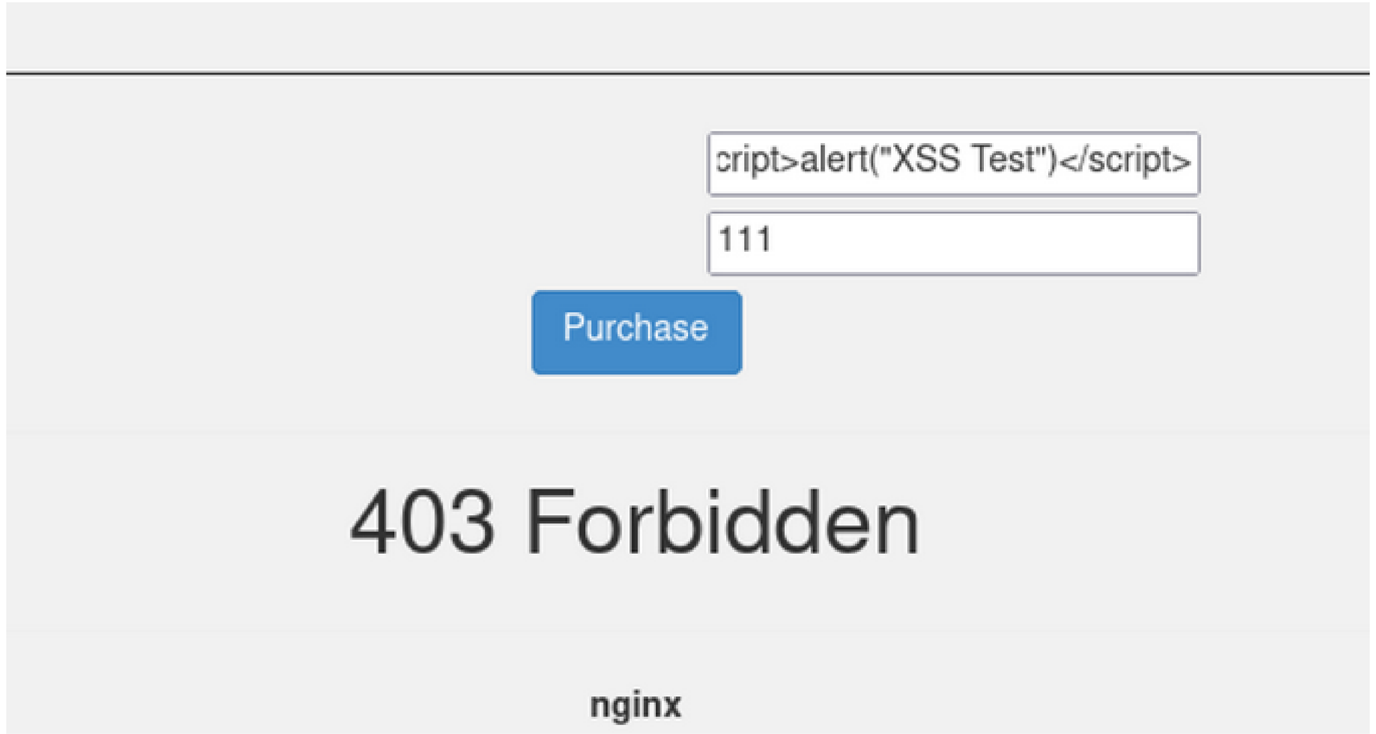
No WAF -> Successfully exploited



0 8

XSS

WAF -> Exploit has been blocked



0 8

DIRSEARCH

No WAF -> Endpoints are found, some returns 404

```
[22:19:10] Starting: WebGoat/
[22:19:28] 200 -    2KB - /WebGoat/login
[22:19:29] 404 -    0B  - /WebGoat/META-INF/
[22:19:29] 404 -    0B  - /WebGoat/META-INF
[22:19:29] 404 -    0B  - /WebGoat/META-INF/app-config.xml
[22:19:29] 404 -    0B  - /WebGoat/META-INF/application.xml
[22:19:29] 404 -    0B  - /WebGoat/META-INF/beans.xml
```

```
[22:19:29] 404 -    0B  - /WebGoat/META-INF/ra.xml
[22:19:29] 404 -    0B  - /WebGoat/META-INF/jboss-ejb3.xml
[22:19:29] 404 -    0B  - /WebGoat/META-INF/weblogic-ejb-jar.xml
[22:19:34] 200 -    4KB - /WebGoat/registration
[22:19:40] 404 -    0B  - /WebGoat/WEB-INF
[22:19:40] 404 -    0B  - /WebGoat/WEB-INF/application-client.xml
[22:19:40] 404 -    0B  - /WebGoat/WEB-INF/application_config.xml
```

0 8

DIRSEARCH

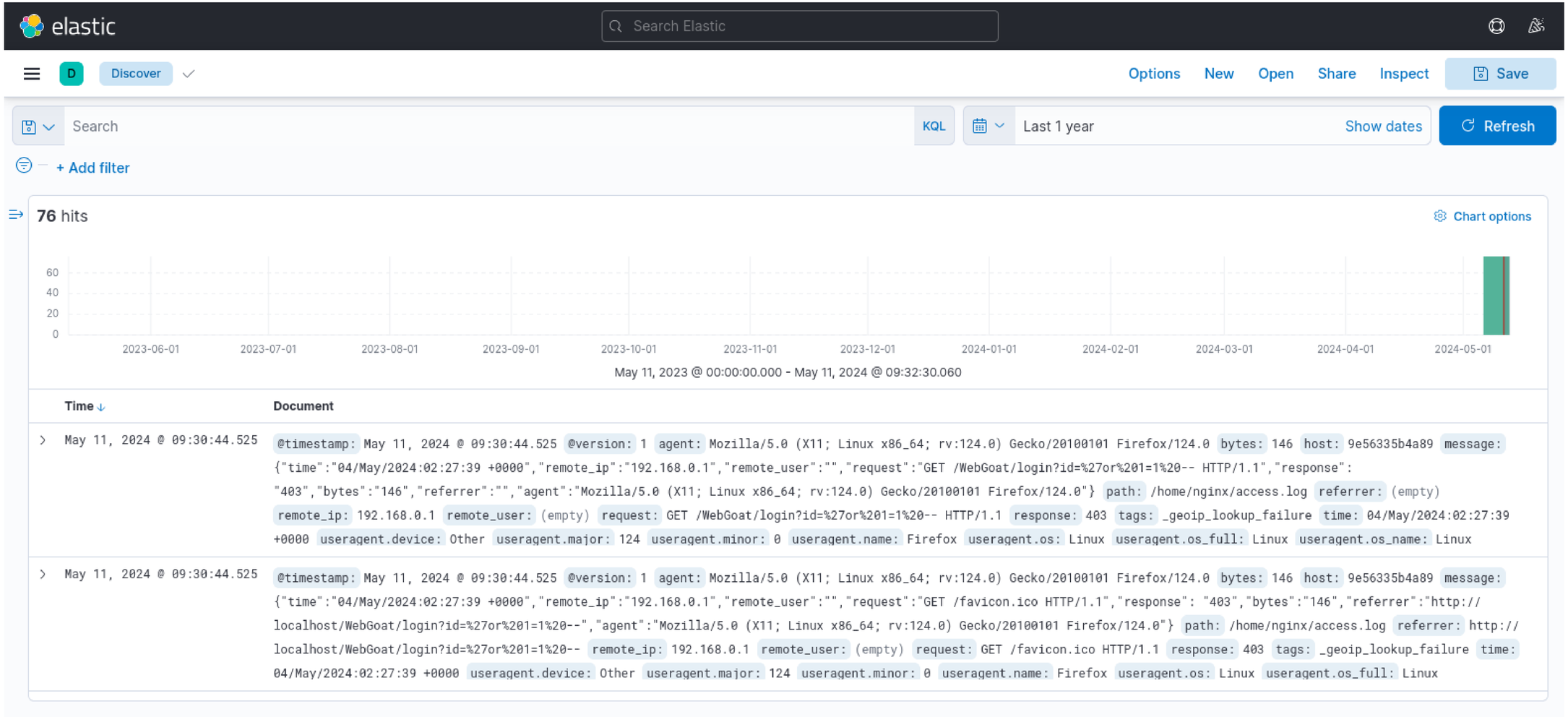
WAF -> Endpoints are found but sensitive ones are blocked

```
[22:25:03] Starting: WebGoat/
[22:25:03] 403 -  548B  - /WebGoat/aspx.old
[22:25:03] 403 -  548B  - /WebGoat/html.old
[22:25:03] 403 -  548B  - /WebGoat/jsp.bak
[22:25:03] 403 -  548B  - /WebGoat/php.old
[22:25:03] 403 -  548B  - /WebGoat/aspx.bak
[22:25:03] 403 -  548B  - /WebGoat/js.old
[22:25:03] 403 -  548B  - /WebGoat/%2e%2e//google.com
[22:25:03] 403 -  548B  - /WebGoat/%C0%AE%C0%AE%C0%AF
```

```
[22:25:26] 403 -  548B  - /WebGoat/log/server.log
[22:25:26] 403 -  548B  - /WebGoat/log/www-error.log
[22:25:26] 403 -  548B  - /WebGoat/log/librepag.log
[22:25:26] 403 -  548B  - /WebGoat/log/production.log
[22:25:27] 200 -    2KB - /WebGoat/login
[22:25:27] 403 -  548B  - /WebGoat/logs.mdb
[22:25:27] 403 -  548B  - /WebGoat/logs/error.log
[22:25:27] 403 -  548B  - /WebGoat/logs/access.log
```

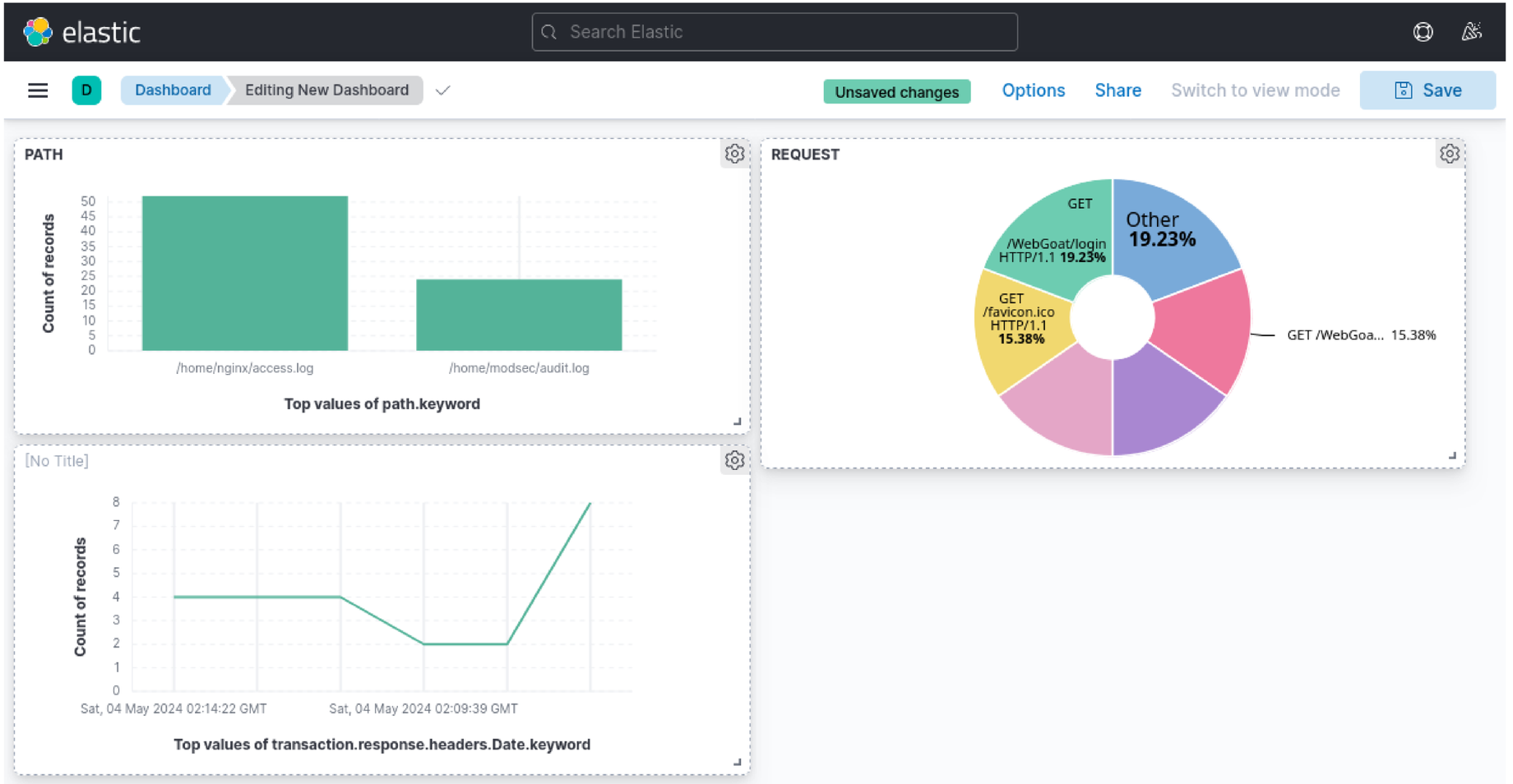
0 8

ELK


elastic
Search Elastic
D
Discover
Options
New
Open
Share
Inspect
Save
Search
KQL
Last 1 year
Show dates
Refresh
+ Add filter
76 hits
Chart options
60
40
20
0
2023-06-01
2023-07-01
2023-08-01
2023-09-01
2023-10-01
2023-11-01
2023-12-01
2024-01-01
2024-02-01
2024-03-01
2024-04-01
2024-05-01
May 11, 2023 @ 00:00:00.000 - May 11, 2024 @ 09:32:30.060
Time
Document
May 11, 2024 @ 09:30:44.525
@timestamp: May 11, 2024 @ 09:30:44.525 @version: 1 agent: Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0 bytes: 146 host: 9e56335b4a89 message: {"time":"04/May/2024:02:27:39 +0000","remote_ip":"192.168.0.1","remote_user":"","request":"GET /WebGoat/login?id=%27or%201=1%20-- HTTP/1.1","response": "403","bytes":"146","referrer":"","agent":"Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"} path: /home/nginx/access.log referrer: (empty) remote_ip: 192.168.0.1 remote_user: (empty) request: GET /WebGoat/login?id=%27or%201=1%20-- HTTP/1.1 response: 403 tags: _geoip_lookup_failure time: 04/May/2024:02:27:39 +0000 useragent.device: Other useragent.major: 124 useragent.minor: 0 useragent.name: Firefox useragent.os: Linux useragent.os_full: Linux useragent.os_name: Linux
May 11, 2024 @ 09:30:44.525
@timestamp: May 11, 2024 @ 09:30:44.525 @version: 1 agent: Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0 bytes: 146 host: 9e56335b4a89 message: {"time":"04/May/2024:02:27:39 +0000","remote_ip":"192.168.0.1","remote_user":"","request":"GET /favicon.ico HTTP/1.1","response": "403","bytes":"146","referrer":"http://localhost/WebGoat/login?id=%27or%201=1%20--","agent":"Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"} path: /home/nginx/access.log referrer: http://localhost/WebGoat/login?id=%27or%201=1%20-- remote_ip: 192.168.0.1 remote_user: (empty) request: GET /favicon.ico HTTP/1.1 response: 403 tags: _geoip_lookup_failure time: 04/May/2024:02:27:39 +0000 useragent.device: Other useragent.major: 124 useragent.minor: 0 useragent.name: Firefox useragent.os: Linux useragent.os_full: Linux

0 8

ELK


elastic
Search Elastic
D
Dashboard
Editing New Dashboard
Unsaved changes
Options
Share
Switch to view mode
Save
PATH
Count of records
50
45
40
35
30
25
20
15
10
5
0
/home/nginx/access.log
/home/modsec/audit.log
Top values of path.keyword
REQUEST
GET
/WebGoat/login
HTTP/1.1 19.23%
Other
19.23%
GET
/favicon.ico
HTTP/1.1
15.38%
GET /WebGoa... 15.38%
[No Title]
Count of records
8
7
6
5
4
3
2
1
0
Sat, 04 May 2024 02:14:22 GMT
Sat, 04 May 2024 02:09:39 GMT
Top values of transaction.response.headers.Date.keyword

0 8

DEMO VIDEO

09

REFERENCES

- https://github.com/WebGoat/WebGoat/releases
- https://github.com/owasp-modsecurity/ModSecurity
- https://www.docker.com/blog/how-to-use-the-official-nginx-docker-image/
- https://docs.nginx.com/nginx-waf/admin-guide/nginx-plus-modsecurity-waf-installation-logging/
- https://notsosecure.com/continuous-security-monitoring

T H A N K S

FOR WATCHING