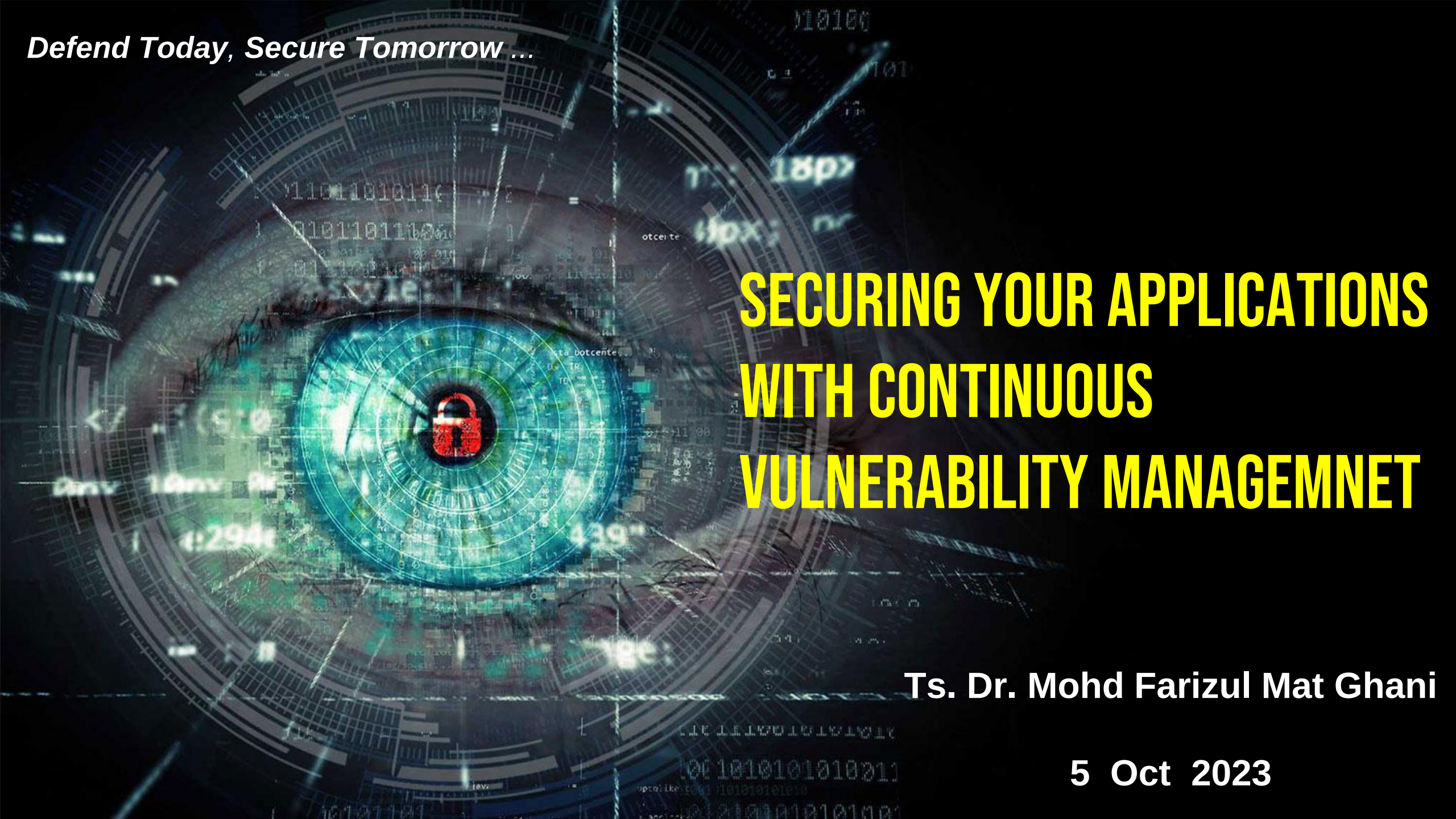


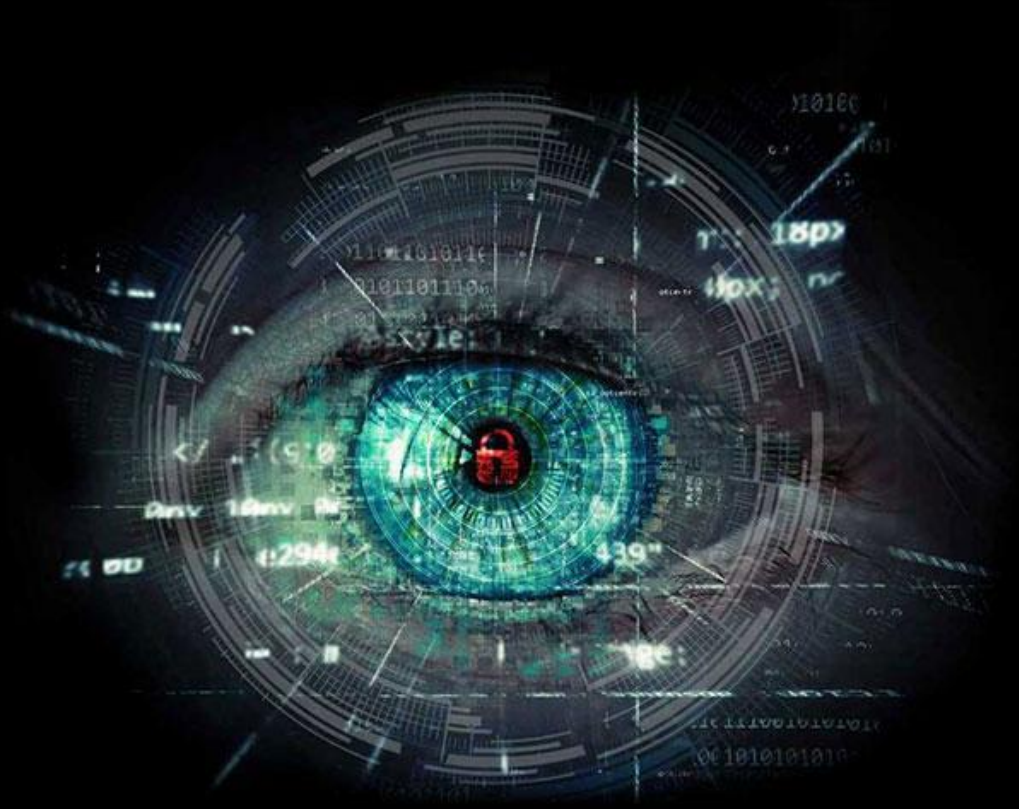
Defend Today, Secure Tomorrow ...

SECURING YOUR APPLICATIONS WITH CONTINUOUS VULNERABILITY MANAGEMNET

Ts. Dr. Mohd Farizul Mat Ghani

5 Oct 2023

CONTENTS



01 INTRODUCTION

- Introducing to Vulnerability Management
- Vulnerability Management Required

02 VULNERABILITY MANAGEMENT PROCESS

- How Are Vulnerabilities Detected

03 CONTINUOUS VULNERABILITY MANAGEMENT

- Vulnerability Scanning
- Security Use Cases - Playbook


INTRODUCTION

```
07:12:34.391018 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.394558 IP 192.168.0.4.55579 > 58.27.86.11.https: Flags [P.], seq 165:224, ack 149, win 16661, length 59
07:12:34.395709 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.395714 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.395716 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.395717 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.395844 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.395846 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.395848 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.395926 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.396001 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.397602 IP 192.168.0.4.55579 > 58.27.86.11.https: Flags [F.], seq 224, ack 149, win 16661, length 0
07:12:34.398043 IP 192.168.0.4.55581 > 58.27.86.11.https: Flags [S], seq 3413311610, win 8192, options [mss 1460,
nop,wscale 2,nop,nop,sackOK], length 0
07:12:34.399459 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.399463 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.401194 IP 192.168.0.4.55577 > 58.27.86.16.https: Flags [R.], seq 225, ack 186, win 0, length 0
07:12:34.401197 IP 192.168.0.4.55577 > 58.27.86.16.https: Flags [R], seq 117801277, win 0, length 0
07:12:34.401962 IP 192.168.0.4.38897 > 87.68.32.1.29006: UDP, length 20
07:12:34.404262 IP 192.168.0.4.38897 > 87.68.32.1.29006: UDP, length 20
07:12:34.406578 IP 192.168.0.4.38897 > 87.68.32.1.29006: UDP, length 20
07:12:34.409084 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.409132 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.411377 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.411656 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.411664 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.411798 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.411804 IP 192.168.0.4.38897 > 84.31.50.104.44537: UDP, length 1438
07:12:34.427886 IP 192.168.0.4.55581 > 58.27.86.11.https: Flags [.], ack 3064333554, win 16698, length 0
07:12:34.429549 IP 192.168.0.4.55581 > 58.27.86.11.https: Flags [P.], seq 0:165, ack 1, win 16698, length 165
07:12:34.442760 IP 192.168.0.4.55579 > 58.27.86.11.https: Flags [R.], seq 225, ack 186, win 0, length 0
07:12:34.442771 IP 192.168.0.4.55579 > 58.27.86.11.https: Flags [R], seq 4196853075, win 0, length 0
```

WHAT IS A VULNERABILITY?

A vulnerability is a weakness which can be exploited by a cyber attack to gain unauthorized access to or perform unauthorized actions on a computer system. Vulnerabilities can allow attackers to run code, access a system's memory, install malware, and steal, destroy or modify sensitive data.

VULNERABILITY MANAGEMENT??

- DATABASE
- PEOPLE
- PROPERTY
- INFORMATION

Vulnerability management is the process of identifying, evaluating, prioritizing, remediating and reporting on security vulnerabilities in Applications.

WHY IS VULNERABILITY MANAGEMENT BECOMING SO VITAL TODAY?

Vulnerability management is becoming ever so vital due to the increased complexity of technology stack and more alerts coming from various vulnerability assessment tools.

Managing vulnerabilities is a crucial part of information security management, as it helps you reduce the likelihood and impact of cyberattacks.

TAKE ONE!!!

- https://www.youtube.com/shorts/H4BbPf9oVNg

Industries Most Affected

By Data Breaches

Between 2021 and 2022

5,212 global businesses experienced confirmed data loss

statista.com/statistics/329608/security-incidents-confirmed-data-loss-industry-size

scmagazine.com/news/breach/anthem-reports-18500-members-involved-in-new-data-breach

bleepingcomputer.com/news/security/former-employee-arrested-for-trying-to-sell-companys-database-for-4-000

bleepingcomputer.com/news/security/data-breach-impacts-80-000-south-australian-govt-employees

tech.co/news/data-breaches-2022-so-far

next | NOWSOURCING

Industries included:

Finance Industry

690 incidents

UKRAINE

2018

100 GB of data was exfiltrated from a loan services company

Healthcare Industry

571 incidents

UNITED STATES

2017

An employee at Anthem Health Insurance forwarded 18,500 members records' to a third-party vendor

Public Administration Industry

537 incidents

UNITED KINGDOM

2020

British Airways suffered data exfiltration affecting 400,000 customers

Manufacturing Industry

338 incidents

AUSTRALIA

2021

The South Australian government saw the exfiltration of government employee data

Transportation Industry

137 incidents

JAPAN

2022

Toyota lost 300,000 customer emails to hackers

WHY IS VULNERABILITY MANAGEMENT REQUIRED?

This process allows organizations to obtain a continuous overview of vulnerabilities in IT environment and the risks associated with them.

VULNERABILITY MANAGEMENT PROCESS

Vulnerability Management Process

Detect vulnerability

Check the quantity and nature of vulnerabilites.

Assess the risk

Examine the extent of risk.

Prioritize remediation

Set the priority of fixing vulnerabilities.

Confirm remediation

Re-scan, confirm, and report.

HOW ARE VULNERABILITIES DETECTED?

- ✓ Authenticated scans
- ✓ Unauthenticated scans


CONTINUOUS
VULNERABILITY
MANAGEMENT

CONTINUOUS VULNERABILITY??

Continuous vulnerability management is integral to cybersecurity and network security and is on the Center for Internet Security's (CIS) list of basic security controls, citing that organizations need to “continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.”

TAKE ONE!!!

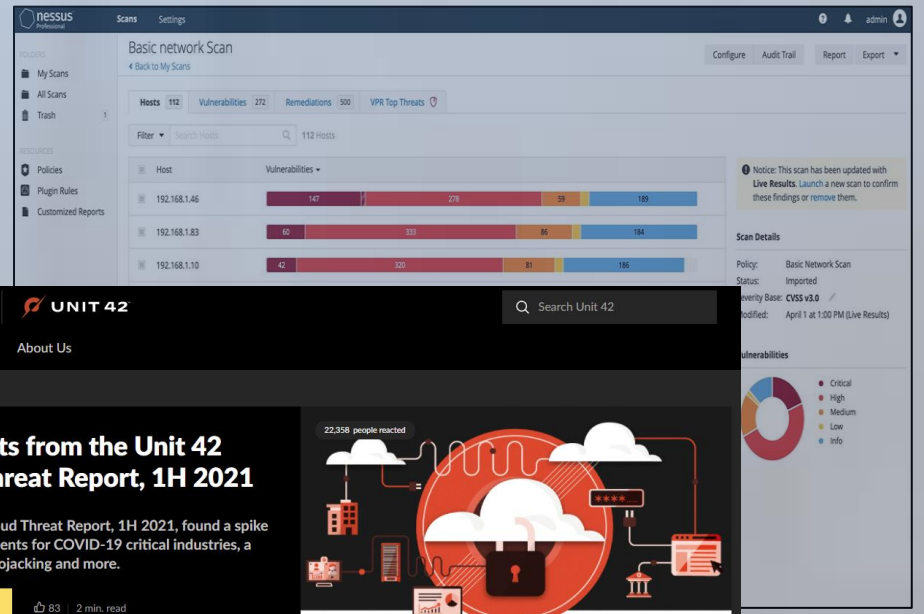
Find Vulnerabilities of Websites

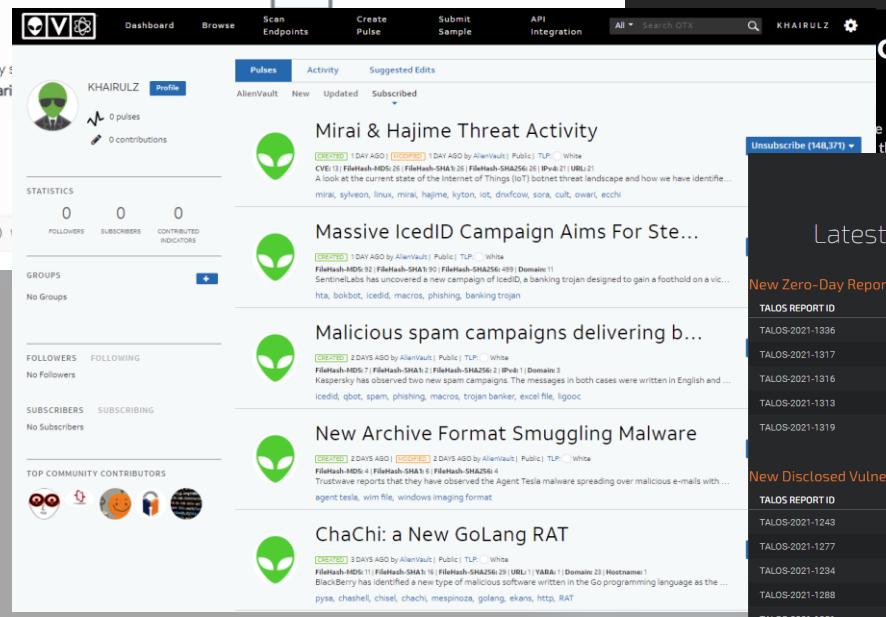
- https://www.youtube.com/watch?v=q6js1MI7XFY

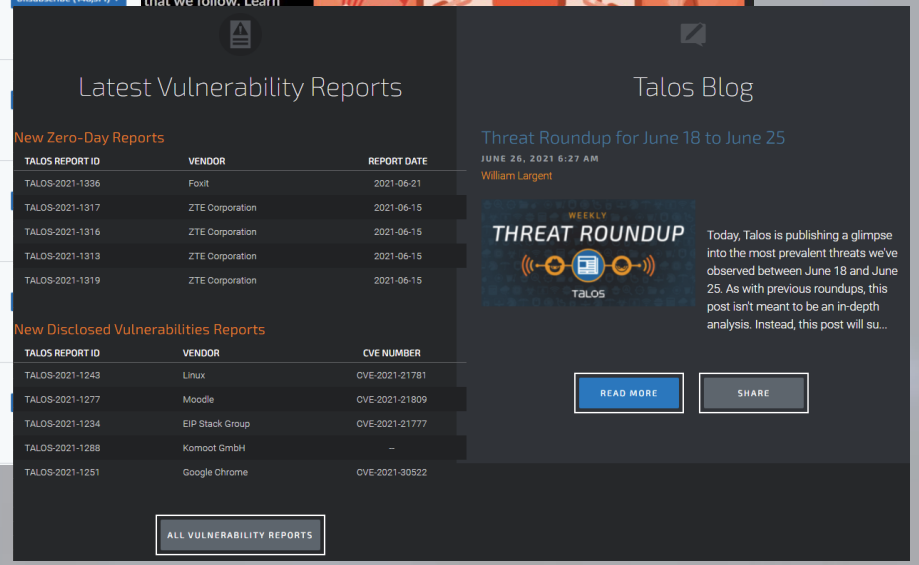
EXAMPLES VULNERABILITY SCANNING TOOLS

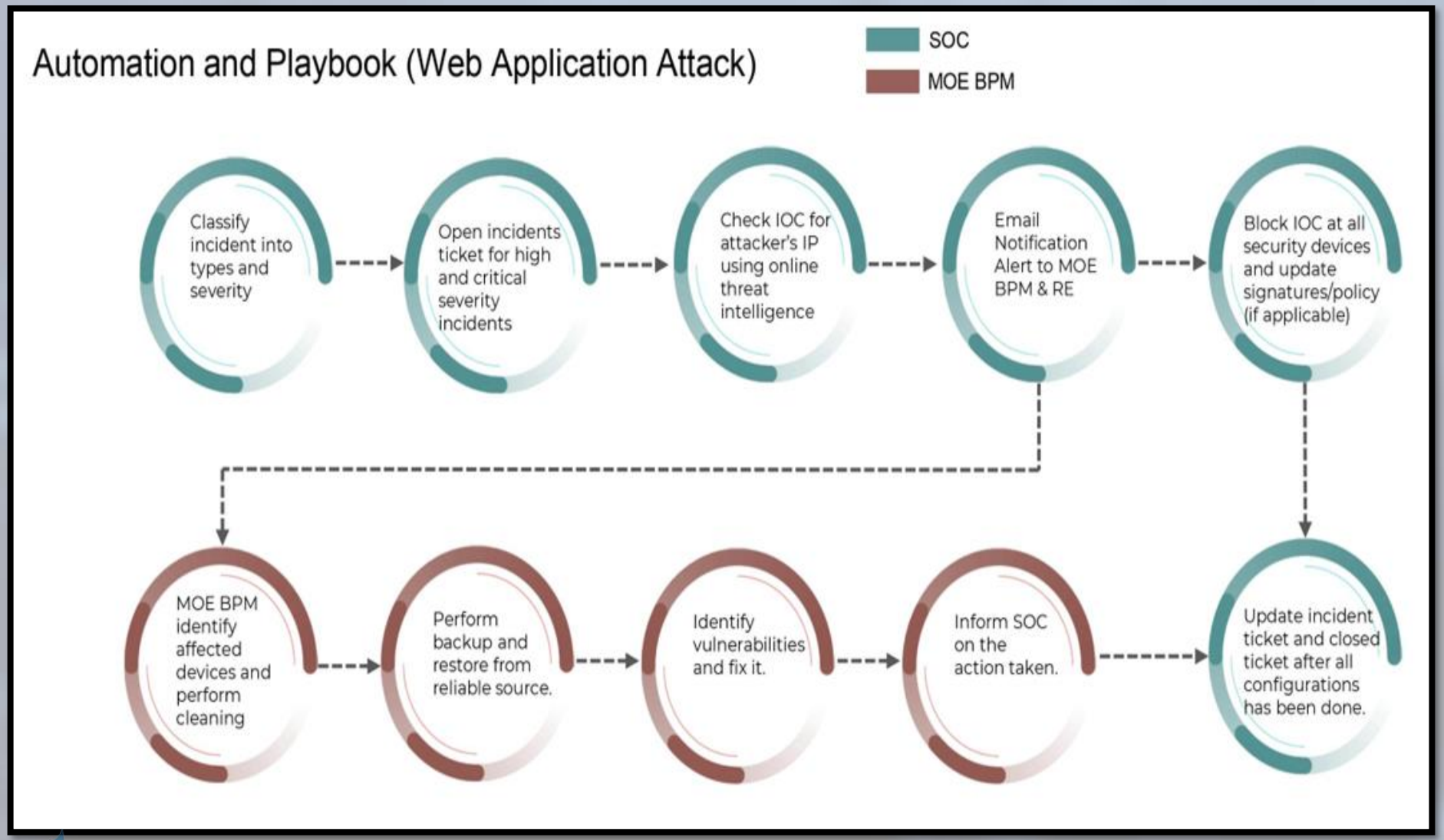
TECHNICAL SKILL REQUIRED

SIEM, Threat Intel








Automation and Playbook (Web Application Attack)
SOC
MOE BPM
Classify incident into types and severity
Open incidents ticket for high and critical severity incidents
Check IOC for attacker's IP using online threat intelligence
Email Notification Alert to MOE BPM & RE
Block IOC at all security devices and update signatures/policy (if applicable)
MOE BPM identify affected devices and perform cleaning
Perform backup and restore from reliable source.
Identify vulnerabilities and fix it.
Inform SOC on the action taken.
Update incident ticket and closed ticket after all configurations has been done.

Reply Reply All Forward

Thu 14/9/2023 3:36 PM

SOC (MSS-MOE)

MSS : MOE : ID : 30529 : Web Application Attack Threat Alert

To >@moe.gov.my

Cc noraidah.supangat@moe.gov.my; farizul.ghani@moe.gov.my; aida.salleh@moe.gov.my; mahathir.johari@moe.gov.my; Mohd Hafizuddin Bin Mohd Hamidi; Mohamad Noor Bin Hamdan; Noor Faizam Moslim; Mohd Sharuzman Bin Othman; Ahmad Zulfahmi Bin Ahmad Ezzat; Amirul Aiman Bin Ramli; Nur Ayuni Fatihah Binti Mahdir; Mohd Azri Bin Yazid; Aqil Azaim Bin Ramlee; **SOC GITN**

report_web_application_attack_1694664023776116917.pdf
125 KB

Assalamualaikum & Salam Sejahtera,

Pihak SOC mengesan serangan tinggi dalam tempoh 24 jam dari IP **Hong Kong (103.214.173.118)** membuat serangan **Illegal Resource Access & SQL Injection** ke atas website ..... .gov.my. Bagaimanapun, ancaman tersebut telah disekat diperingkat WAF Imperva. Mohon rujuk laporan PDF yang telah dikeluarkan dari Cortex XSOAR untuk maklumat lanjut.

Nama Ancaman : ***Web Application attack detected containing Cross Site Scripting

Attacker Info	
Source IP :	[“185.216.118.69”]
Country :	Japan
ISP :	HongKong Cloud Plus Technology Limited
Categories :	[“SQL Injection”,“Web Exploit”,“Cross Site Scripting”]
Event Count :	91

Senarai Event Name :

["Illegal Resource Access ",“Cross Site Scripting”]

Query String yang diinput oleh Attacker :

[“id\=1\u0026lang\=en\u0026Yzuu\=3049%20AND%201%3d1%20UNION%20ALL%20SELECT%201%2cNULL%2c%27%3cscript%3ealert%28%22XSS%22%29%3c%2fscript%3e%27%2ctable_name%20FROM%20information_schema.tables%20WHERE%202%3e1–%2f%2a%2a%2f%3b%20EXEC%20xp_cmdshell%28%27cat%20…%2f…%2f…%2fetc%2fpasswd%27%29%23”]

Request URL Path :

[“www.moe.gov.my/index.php”]

Request Method :

[“GET”]

Client Apps Tool :

[“Ruby HTTP library”]

Cadangan Pemulihan :

1. Escape user input. Escaping means to convert the key characters in the data that a web page receives to prevent the data from being interpreted in any malicious way. It doesn't allow the special characters to be rendered. Please revise and verified this query string :-
   Query string :
   ["id\=1\u0026lang\=en\u0026Yzuu\=3049%20AND%201%3d1%20UNION%20ALL%20SELECT%201%2cNULL%2c%27%3cscript%3ealert%28%22XSS%22%29%3c%2fscript%3e%27%2ctable_name%20FROM%20information_schema.tables%20WHERE%202%3e1--%2f%2a%2a%2f%3b%20EXEC%20xp_cmdshell%28%27cat%20..%2f..%2f..%2fetc%2fpasswd%27%29%23"]

2. Validate user input. Treat anything that originates data from outside the system as untrusted. Validate all the input data. Use an allowlist of known, acceptable, good input.

3. Sanitize data. Examine and remove unwanted data, such as HTML tags that are deemed to be unsafe. Keep the safe data and remove any unsafe characters from the data.

4. Closed any path/page that display any sensitive classified information data. Revise this Request URL path whether any sensitive classified information is displayed :-
   Request URL : ["www.moe.gov.my/index.php"]

Sekian Terima Kasih

Google Malaysia HackeD

By

TiGER-M@TE

#Bangladeshi HackeR

Greetz : w4l3xzy3 ; Ne0-h4ck3r ; W7sH.SyRiA ; c0de-X-1337 ; kinG oF coNTroL ; F0RTYS3V3N ; aBu.HaliL501 ; HolaKo ; surg4bij4k ; l0c@lh0st ; h311 c0d3 ;

#EOF

Thanks