LONG TERM INTERNSHIP

Track - Cyber Security with IBM QRadar

Team ID - LTVIP2024TMID11398

Team Size - 4

Team Leader - Bhargava Sai Jetti

Team Member - Avala Jyotheeshwar Rao

Team Member - Bharani Siva Charan Chitti

Team Member - Chitrada Pavan

College - Dr. L.B. Degree & P.G. College

Project Title - Understanding Cyber Threats : Exploring Nessus & Beyond scanning tools.

INTRODUCTION

Cybersecurity, within the realm of Artificial Intelligence (AI), embodies a critical frontier, aiming to fortify digital ecosystems by instilling intelligent defense mechanisms. AI in cybersecurity spans various technologies and methodologies, striving to emulate human cognitive abilities to detect, analyze and respond to evolving cyber threats.

Within this domain, AI leverages machine learning algorithms to discern patterns, anomalies and potential vulnerabilities within intricate datasets. This fusion of AI & cybersecurity fuels a diverse spectrum of applications.

Suggested Pre-requisities

→ Basic Knowledge of Operating Systems

An operating system is the most important software that runs on a computer. It manages the computer's memory and processes; as well as all of its software & hardware.

→ Foundational Networking Concepts

These include the following

- IP address
- Computer network
- Protocol
- Ethernet
- Nodes
- Port
- Router
- Topology

→ Understanding of Common Cyber Threats -

- Phishing
- Ransomware
- DDOS attack
- Malware
- Exploits
- Spyware

→ Knowledge of Security Tools & Technologies -

- Firewalls
- Encryption
- Metasploit
- Sniffers
- WireShark
- Burp Suite
- Nessus
- Kali Linux

→ Comprehension of Risk Management -

Risk management is the identification, evaluation and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, & control the probability or impact of unfortunate events.

→ Python for hacking -

Python is a versatile programming language that offers a wide range of tools and libraries, making it well-suited for tasks such as penetration testing & network manipulation. Its simplicity and readability are particularly advantageous for ethical hackers

EXECUTIVE SUMMARY

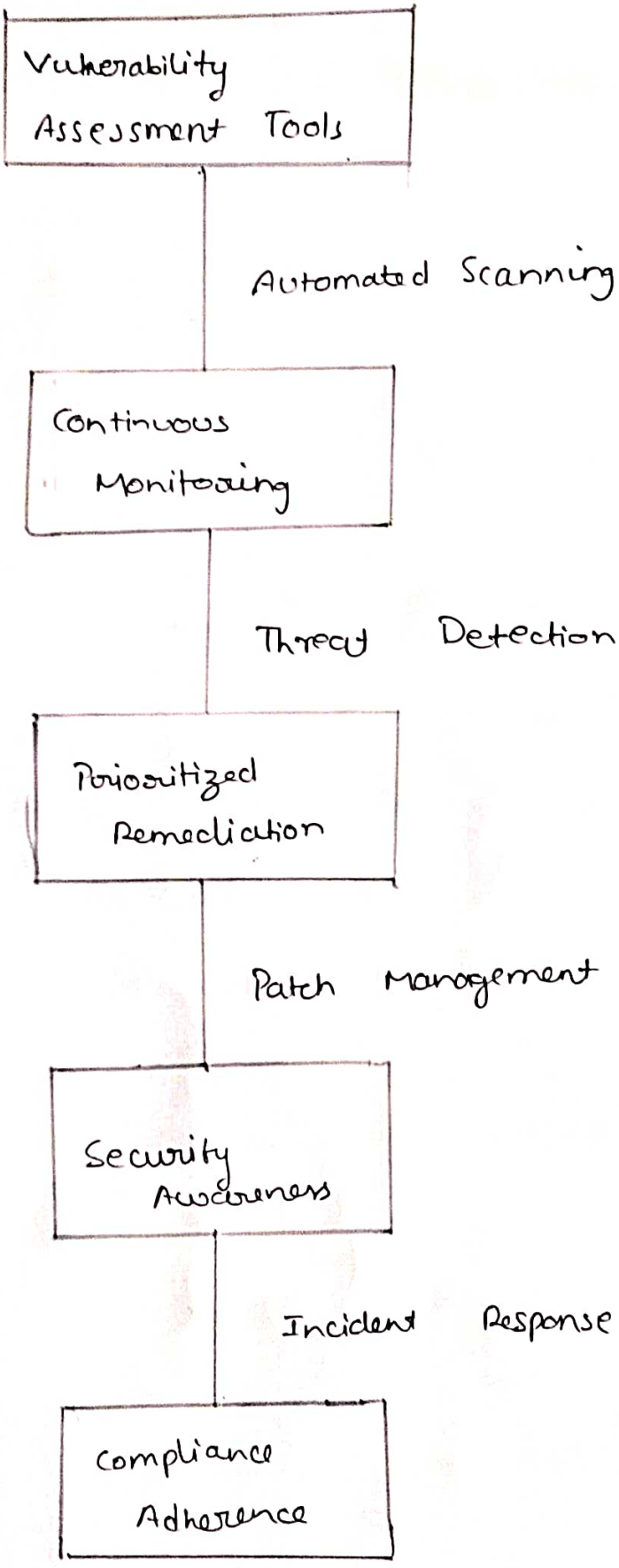
Our internship has successfully equiped participants with a comprehensive understanding of cybersecurity, covering a range of essential topics and practical skills. We decided to the latest trends and concepts in the field, including ethical hacking setting up Security Operations Center (SOC) & Security Information & Event management (SIEM). environments, & Cyber Threat intelligence (CTI). Through a meticulously designed curriculum, interns gained insights into ethical hacking methodologies; learning to identify vulnerabilities and propose effective strategies. They also acquired practical experiance in configuring & managing SOCs & SIEM environments.

INDUSTRY Profile

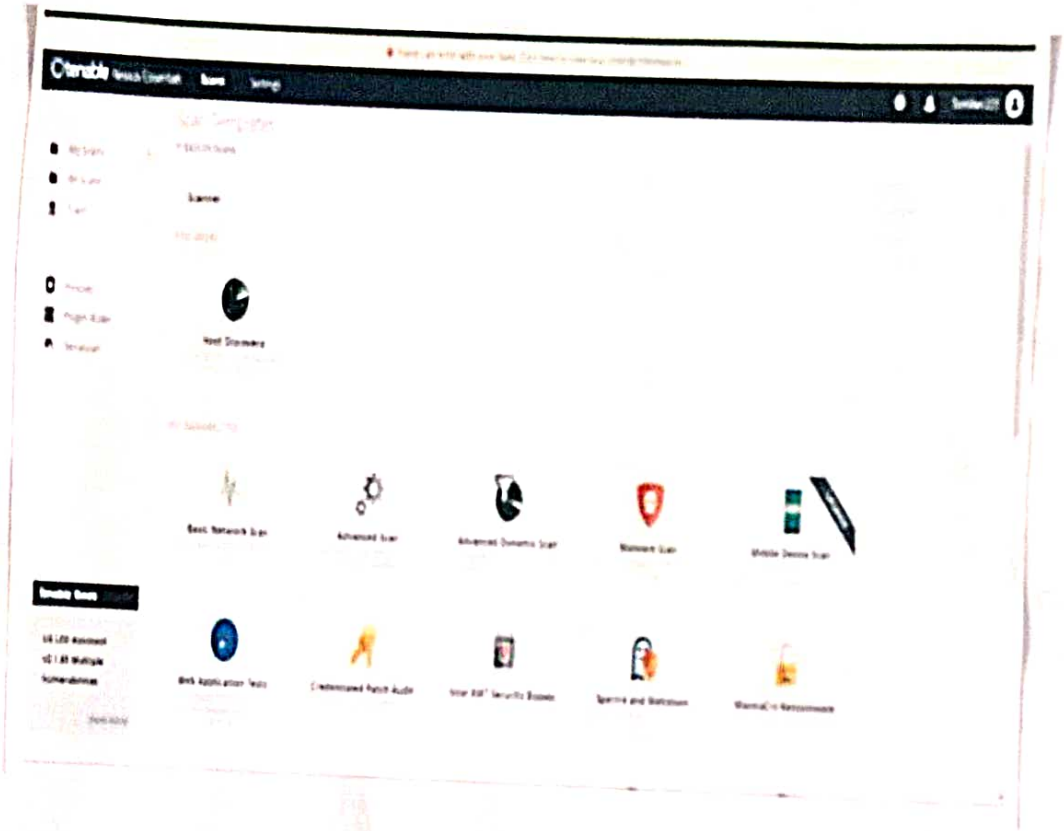
Smartbridge is an EdTech startup in Hyderabad, Telangana, India. It was founded in 2015 with the mission of bridging the gap between academics and industries. SmartBridge provides a platform for students, colleges, companies to connect and collaborate.

At SmartBridge our cutting-edge ed-tech platform, "SmartInterz", Project Based Learning & Remote Internship Platform serves as a catalyst for fostering collaboration between academia and industry. By providing project based, collaborative learning solutions intricately woven into the curriculum, it empowers students to cultivate the essential skills required to become job ready candidates.

Analyzing Scan –



About Nessus -

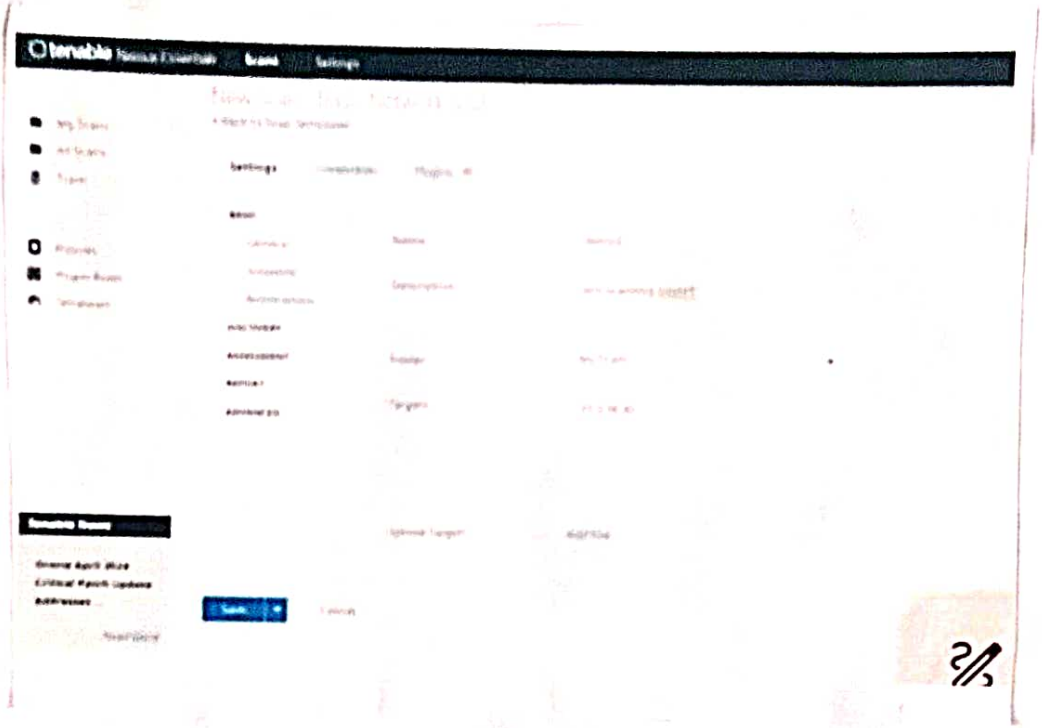


Nessus is one of the most widely used vulnerability assessment tools, known for its comprehensive scanning capabilities.

It performs network vulnerability scanning to identify security issues, misconfigurations, and potential threats within a network infrastructure.

The tool provides detailed reports on discovered vulnerabilities, prioritizing them based on severity levels and offering remediation recommendations.

Analysis of the Results -

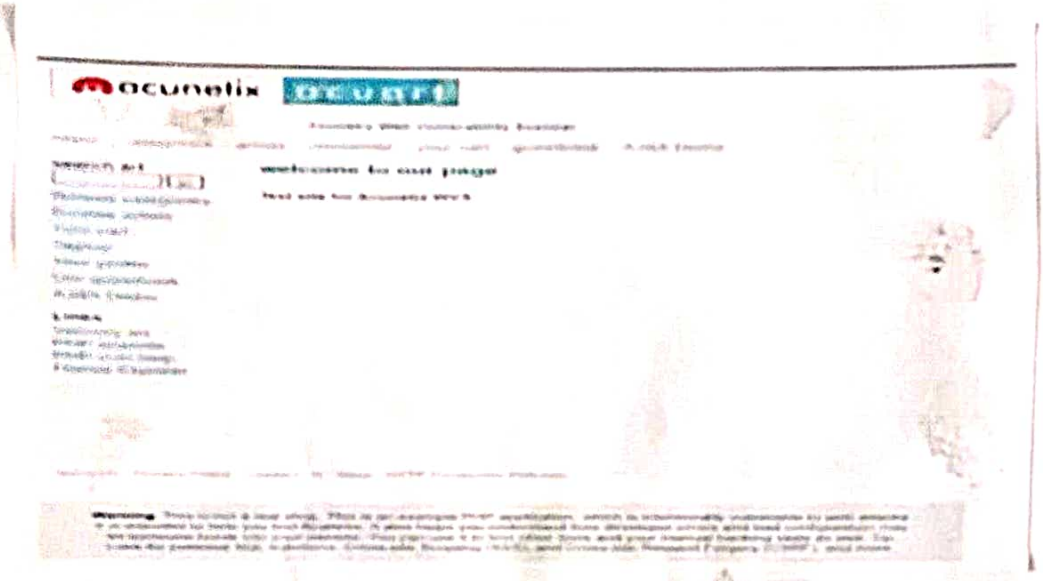


For this project we choose two sites one as the target & the other as practice site. The Scan which we performed on them is 'Basic Network Scan' & this is done in Nessus.

The practice site is Acunetix.

The target site is bLOAPP.

Report on Practice Site -



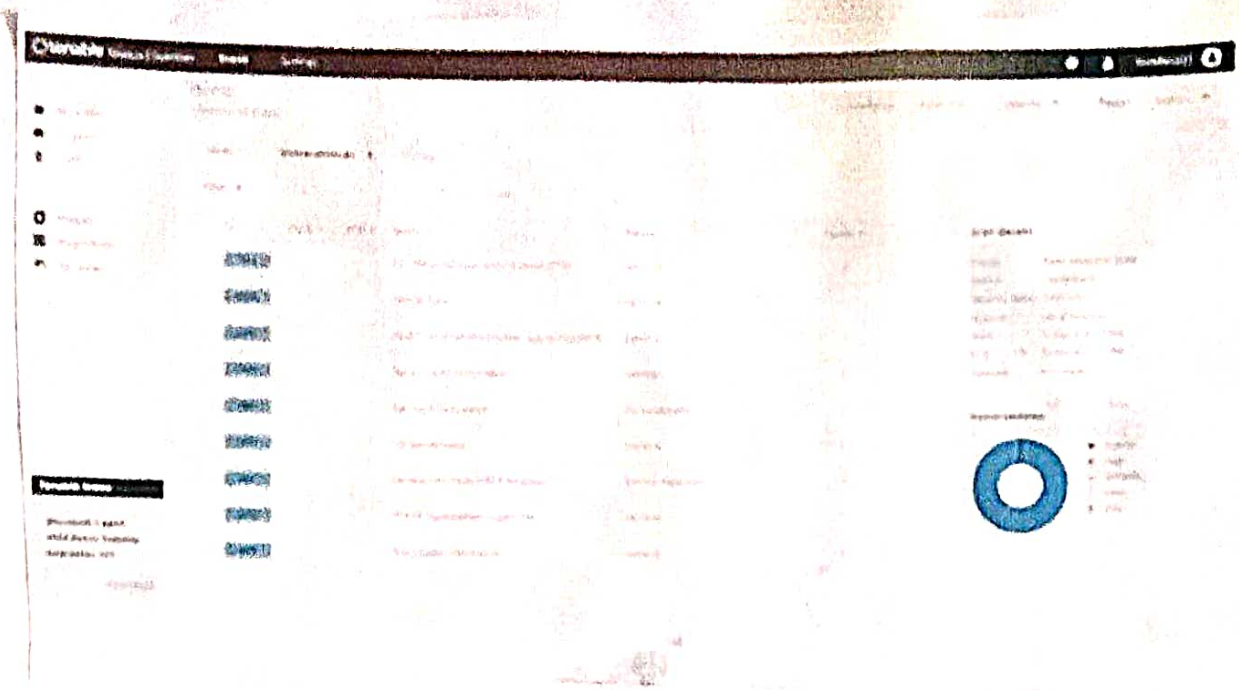
The practice site used is Acunetix.

First we use NSLOOKUP on this site to find the IP address.

Then we found that the IP address is 44.228.249.3.

Now use this IP address on Nessus and choose Basic Network Scan.

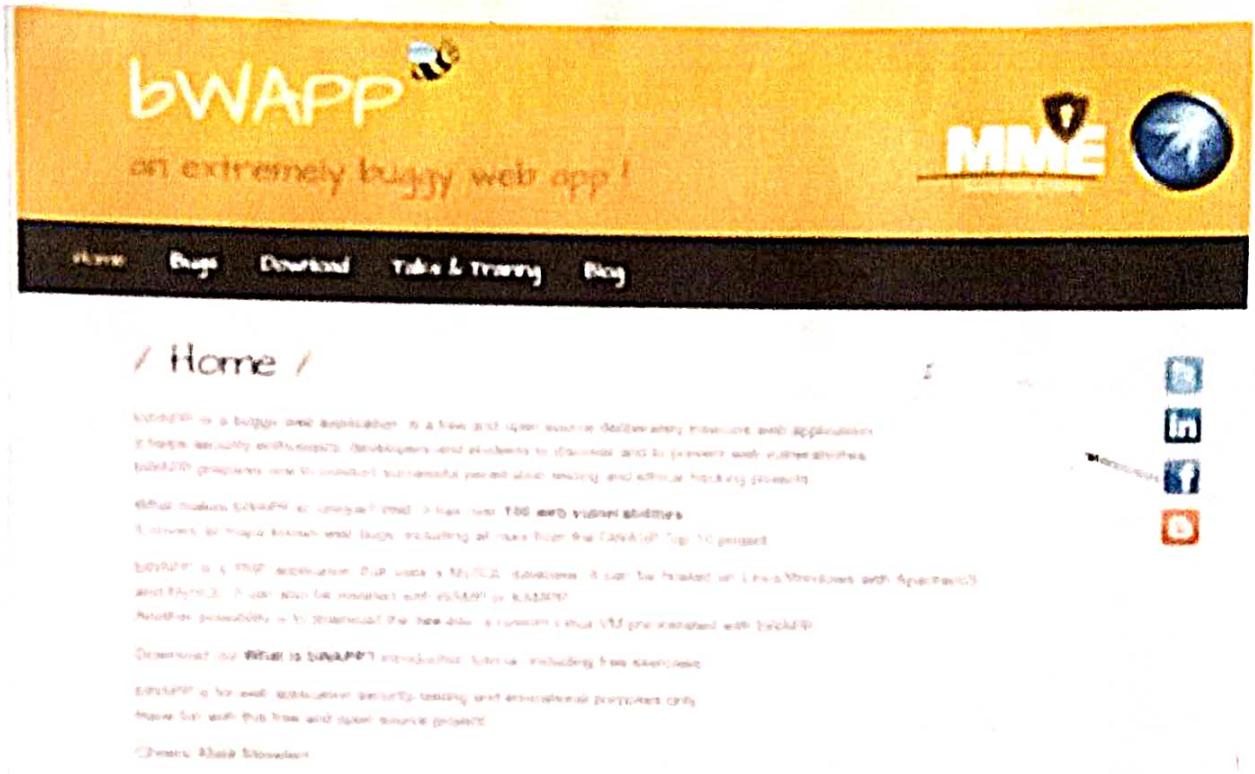
Click on save and hit launch button and wait for sometime till it gets completed.



After scan is completed the final report is as follows, total nine vulnerabilities are encountered.

1) Common Platform Enumeration
2) Device Type
3) Host Fully Qualified Domain Name Resolution
4) Nessus Scan information
5) Nessus SYN scanner
6) OS Identification
7) Service Detection
8) TCP / IP
9) Traceroute Information

Report on Target Site -

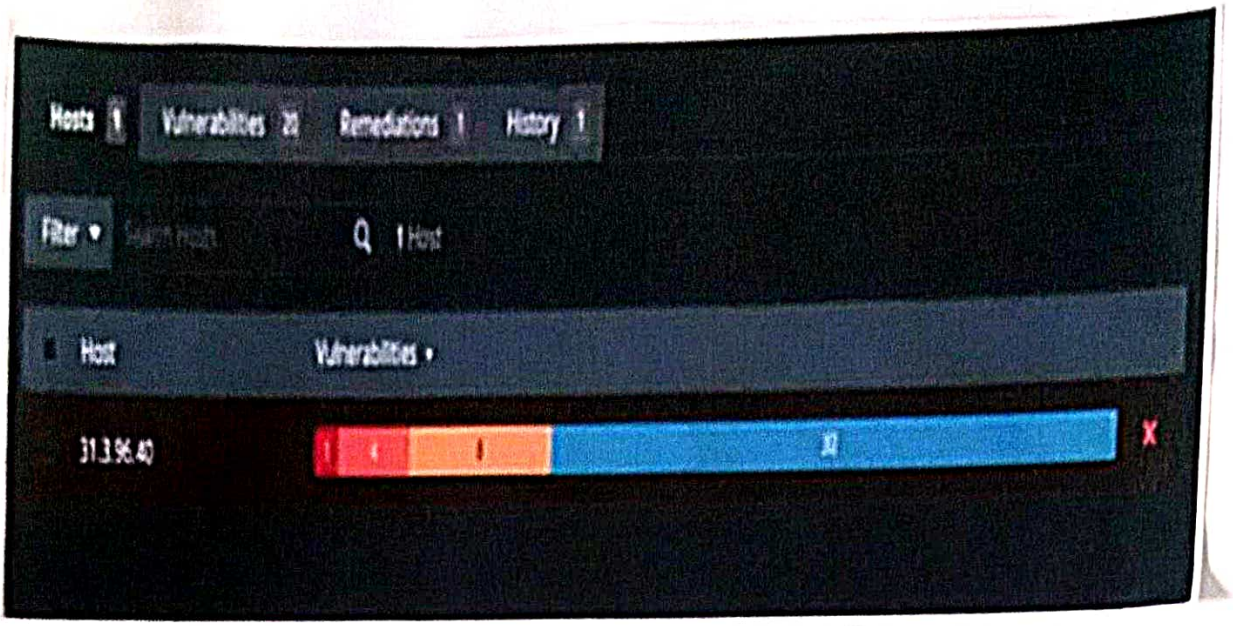


The target site for this project is bWAPP.

Use NSLOOKUP and get the IP address same like before.

The IP address which we got is 31.3.96.40.

Use Basic Network Scan on this IP address and save the scan. After that hit the launch button and wait for a while till it completed the process.



After the scan we encountered total 20 vulnerabilities,

1) Openbsd
2) Openssh
3) HTTP (Multiple issues)
4) SSH (Multiple issues)
5) Web Server (Multiple issues)
6) Service Detection
7) Nessus SYN Scanner
8) Apache HTTP Server Version
9) Common Platform Enumeration
10) Device Type
11) Drupal Software Detection
12) Host Fully Qualified Domain Name Resolution
13) Nessus Scan information
14) Open Port Re-check
15) OS identification
16) OS Security Patch Assessment Not Available
17) Patch Report
18) Solar Winds Server & Application Monitor Detection.
19) Target Credential Status
20) Traceroute Information

CONCLUSION:

In conclusion the project Understanding threats and beyond scanning tools has provided valuable insights into the realm of cybersecurity of the Vulnerability Project aimed to enhance our understanding of cyber security threat and Neuro are Beyond and the methodologies used to mitigate them

Throughout the Project several key and Outcomes have emerged

- Importance of Vulnerability Assessment Play a crucial role in identifying Vulnerability a crucial role

2. Comprehensive Scanning Capability Now one common Scanning capability enabling and stay latest in digital Vulnerability

3 Security awarness and incident response.