Vulnerability Management

V Scanning + V Assessment + V Patching = V Management

Chintan Gurjar

ABOUT ME

- 8+ years of experience in the industry
- Penetration tester → DevSecOps → Management → Threat hunting and Intelligence → Security Management
- Creator of multiple mind maps and checklists on LinkedIn
- CVE-2016-7786 – Sophos UTM
- CEH, OSCP, CTIA, CCFH, CCFA
- Co-trainer of HackCon – HackCon - The Norwegian Cyber Security Conference
- Post graduated from UK in specialized in Cybersecurity
- Conducted nearly:
  - 400 Web Application Penetration Tests
  - 70 Infrastructure Penetration Tests (including external and internal)
  - 30 Static Code Security Reviews
  - 20 API Penetration Tests
  - 8 Incident Response Assessments
  - 7 Cyber Maturity Assessment Projects as a Key Member
  - 5 Threat Hunting Projects for a Period of 2 Years
  - 4 Red Teaming Assessments
  - 2 Physical SCADA Security Assessments

CONTENTS

#1

Introduction of Vulnerability Management

Introduction, key differences between VM, VS, VA, Who does VM, Where it fits in enterprise security management, What process/steps are involved

#2

Step 1 – Vulnerability Source Identification

Human and technology requirement, scoping, evaluating tools and scanning solution, integrating third-party monitoring, penetration test and incident response into your vulnerability management program

#3

Step 2 - Assessment of Identified Vulnerabilities

Detailed triage process, evaluation of vulnerabilities, analysis method, avoiding false positives, assign urgencies and setting priorities, communicating to various asset owners

#4

Step 3 – Remediation/Patching and future developments/improvements

Evaluate patching options, Defense-in-depth approach, patching test before implementation, remediation verification

KEY DIFFERENCES

Vulnerability Scanning

- Single activity
- Accomplished by tools (Acunetix, Nessus, Netsparker, etc.)
- Automated process
- Minutes/Hours
- **Goal:** To identify vulnerabilities in assets

Vulnerability Assessment

- Group of multiple activities
- Scanning + Assessment
- Accomplished by tools and a small number of employees
- Automated + Manual process
- Days
- **Goal:** to identify legitimate vulnerabilities, false positives, assign urgencies based on severity and likelihood of an attack

Vulnerability Management

- Program of multiple processes with multiple activities
- Accomplished by multiple tools, various cyber divisions, and multiple people.
- Automated + Manual Process
- Months/Years (Continuous Program)
- **Goal:** to maintain an on-going program which helps organization on identifying and mitigating vulnerabilities in their internal and external assets by integrating multiple processes into one such as security incidents, penetration testing, Shadow IT, Open source monitoring, etc.

VULNERABILITY SCANNING VS PENETRATION TESTING

V Scanning

Vulnerability scanning is an activity fulfilled by automated scanners to identify vulnerabilities in assets.

V Assessment

Vulnerability assessment is an activity to identify and classify vulnerabilities and assign urgencies for remediation.

Exploitation tools

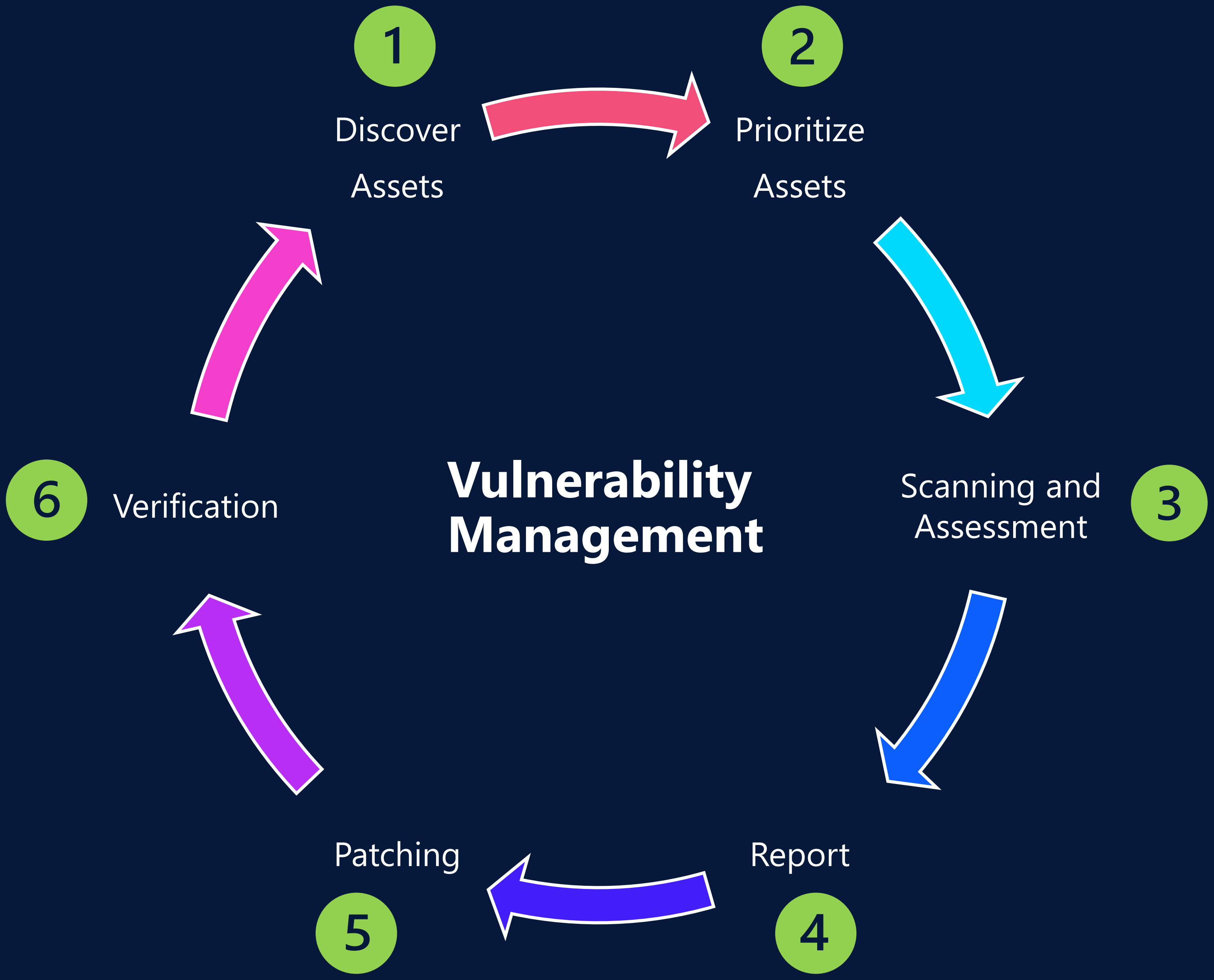
Specialised tools are used to identify whether the vulnerabilities are false positive or legitimate issues.

Penetration Testing

A penetration test simulates the actions of an attacker that aims to breach the organisation security. It covers vulnerability scanning, assessment and using **exploitation tools** to identify legitimate vulnerabilities and false positives.

DIFFERENCE

PROCESS



Vulnerability Management

1 Discover Assets

2 Prioritize Assets

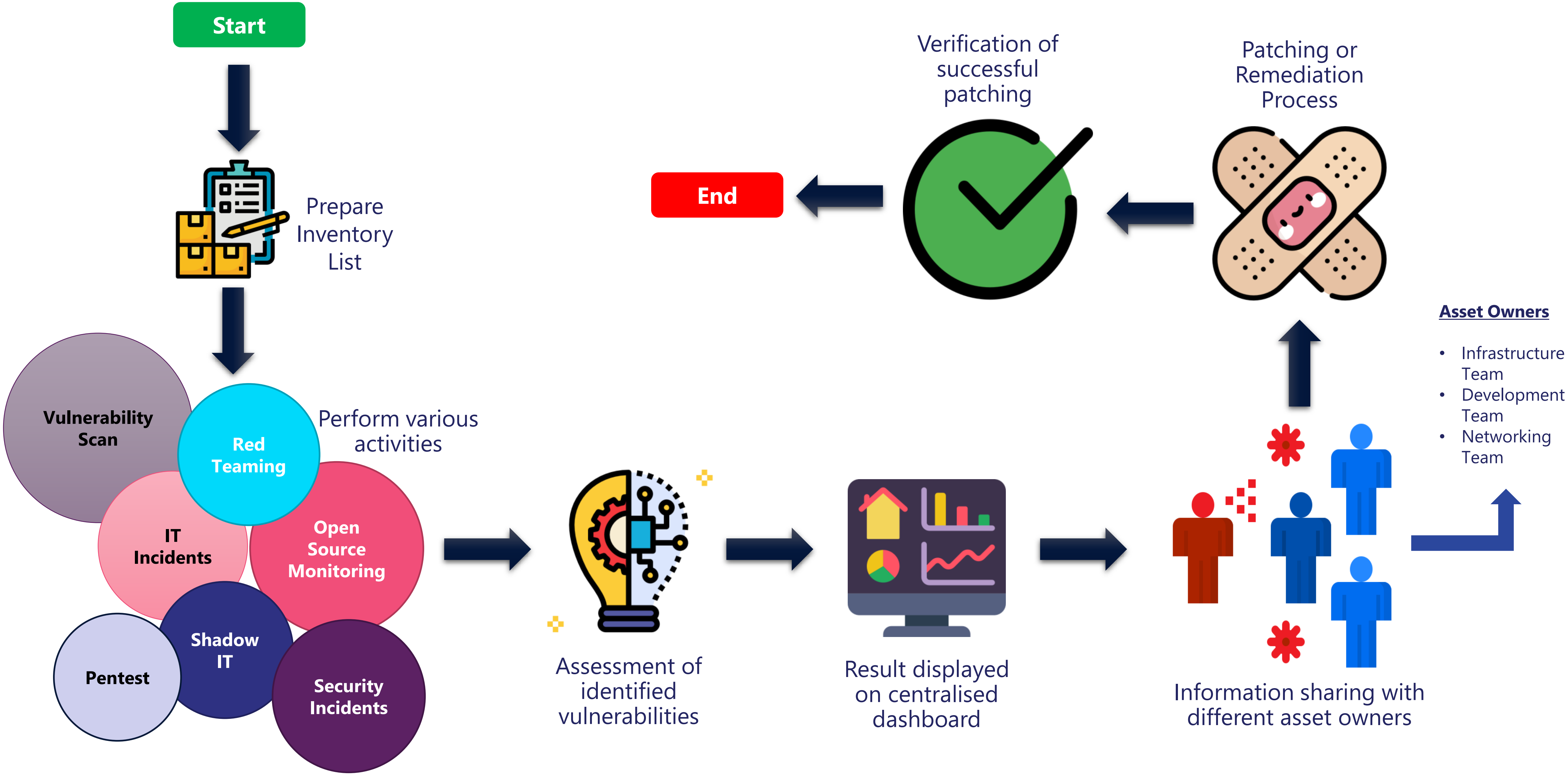
3 Scanning and Assessment

4 Report

5 Patching

6 Verification

VULNERABILITY MANAGEMENT PROCESS STEPS



Start

Prepare Inventory List

Vulnerability Scan

Red Teaming

IT Incidents

Open Source Monitoring

Shadow IT

Pentest

Security Incidents

Perform various activities

Assessment of identified vulnerabilities

Result displayed on centralised dashboard

Information sharing with different asset owners

Asset Owners

- Infrastructure Team
- Development Team
- Networking Team

Patching or Remediation Process

Verification of successful patching

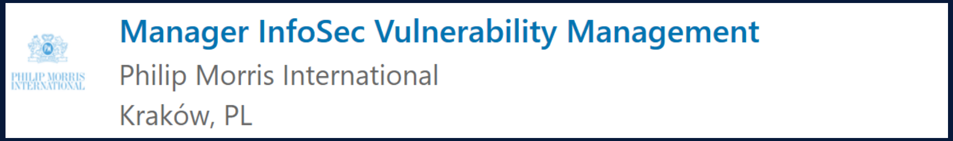
End

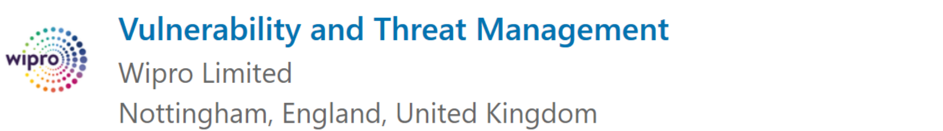
JOBS AROUND THE WORLD

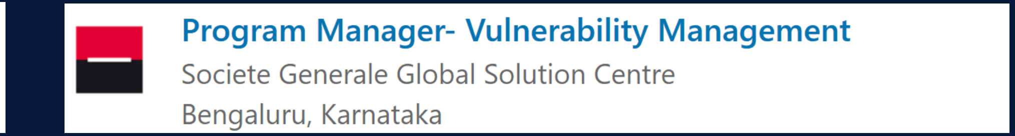
Vulnerability Manager
LT Harper - Cybersecurity Recruitment
London, England Metropolitan Area

Vulnerability Management Governance Associate
JPMorgan Chase & Co.
New York City, NY, US

Sr. Associate - Vulnerability Management Engineer
Amgen
Bucharest, RO

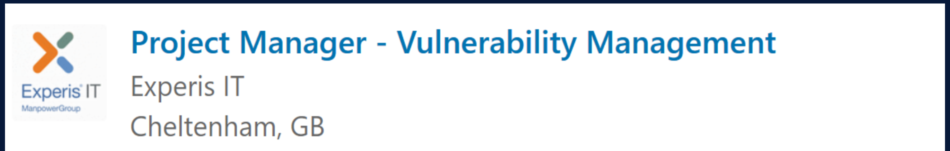

Manager InfoSec Vulnerability Management
Philip Morris International
Kraków, PL


Vulnerability and Threat Management
Wipro Limited
Nottingham, England, United Kingdom


Program Manager- Vulnerability Management
Societe Generale Global Solution Centre
Bengaluru, Karnataka

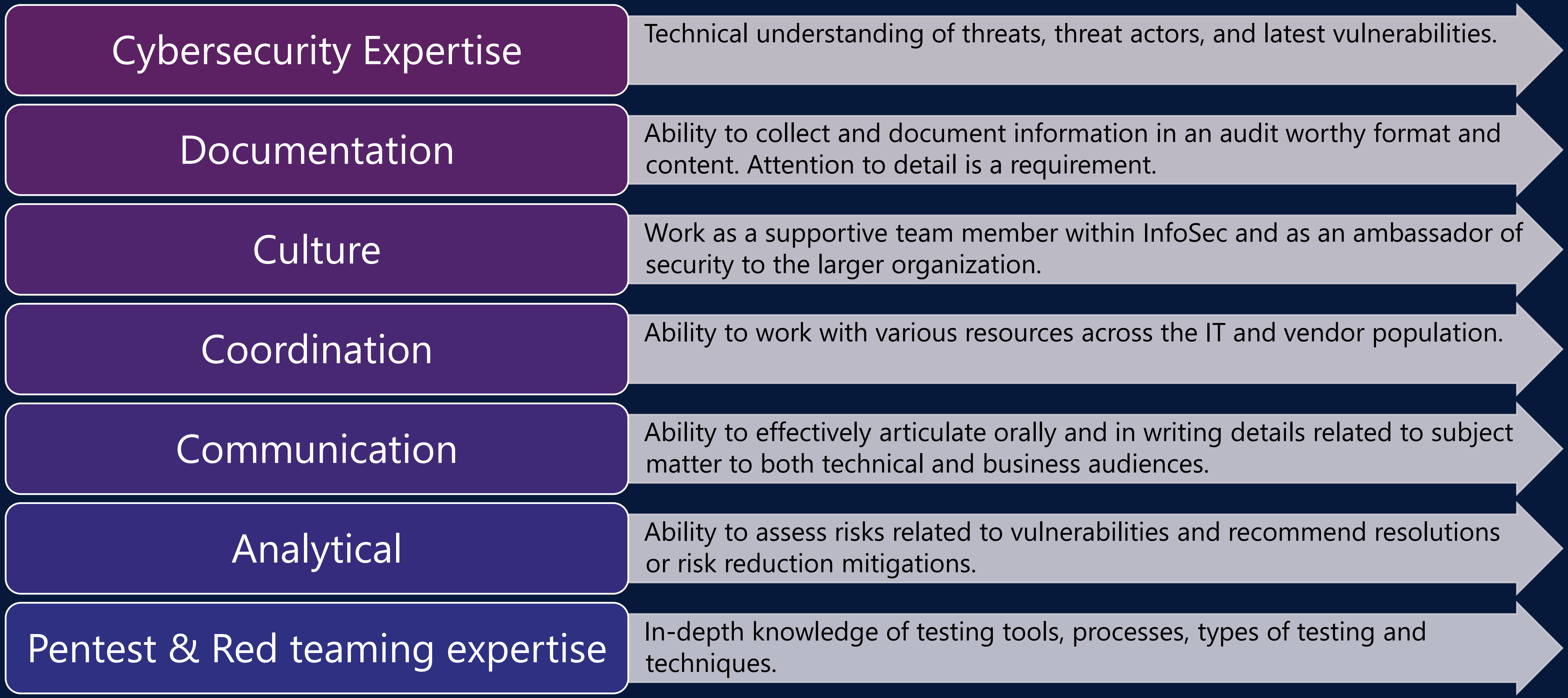
Security Engineer - SOC and Vulnerability Management (VM)
Infosys
Amsterdam, NL

Security Testing and Vulnerability Management Analyst
Allianz Insurance
South East, GB


Project Manager - Vulnerability Management
Experis IT
Cheltenham, GB

Vulnerability Manager
LT Harper - Cybersecurity Recruitment
London, England Metropolitan Area

SKILLS REQUIRED IN THIS DOMAIN



Cybersecurity Expertise

Technical understanding of threats, threat actors, and latest vulnerabilities.

Documentation

Ability to collect and document information in an audit worthy format and content. Attention to detail is a requirement.

Culture

Work as a supportive team member within InfoSec and as an ambassador of security to the larger organization.

Coordination

Ability to work with various resources across the IT and vendor population.

Communication

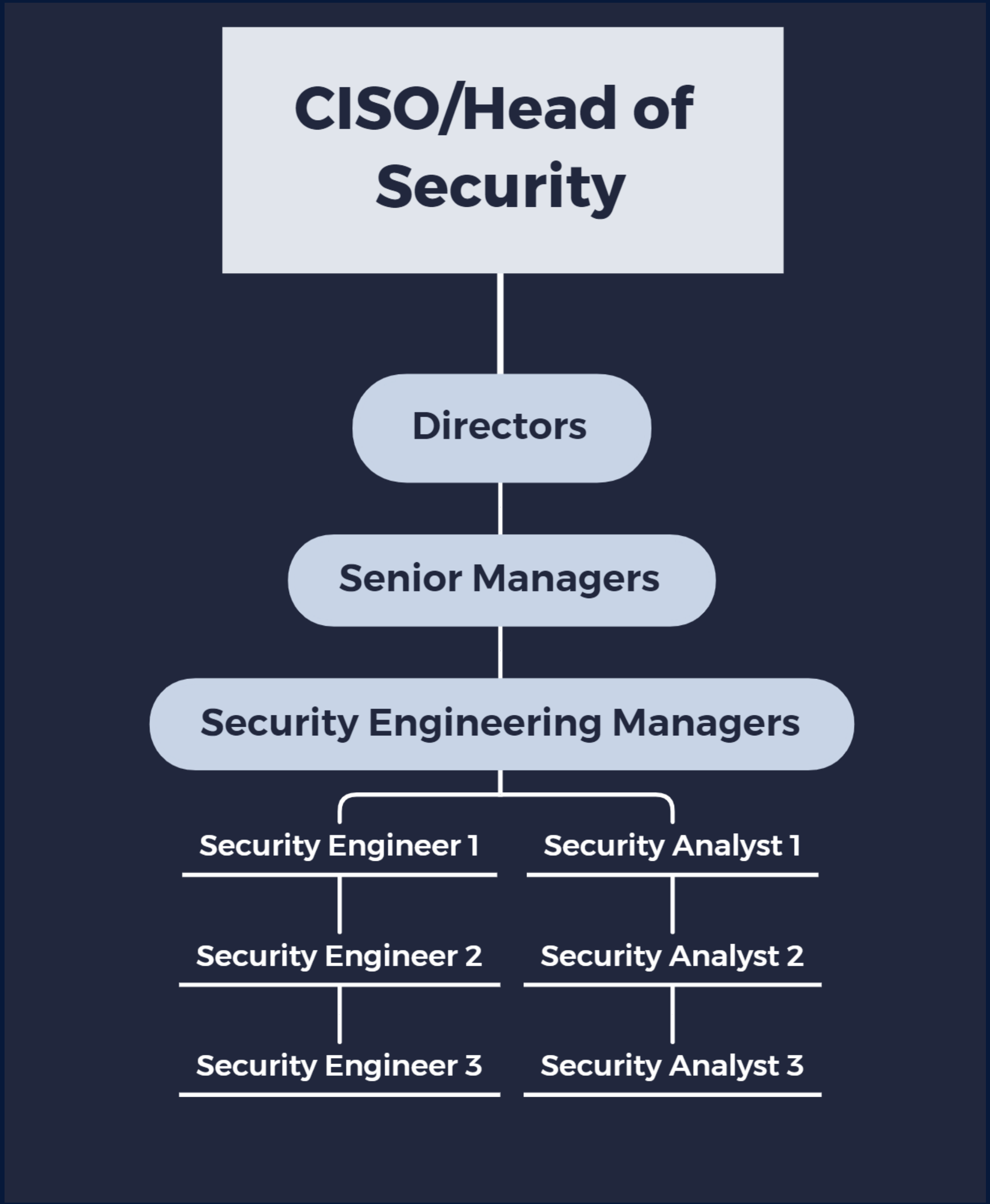
Ability to effectively articulate orally and in writing details related to subject matter to both technical and business audiences.

Analytical

Ability to assess risks related to vulnerabilities and recommend resolutions or risk reduction mitigations.

Pentest & Red teaming expertise

In-depth knowledge of testing tools, processes, types of testing and techniques.



CISO/Head of Security

Directors

Senior Managers

Security Engineering Managers

Security Engineer 1

Security Engineer 2

Security Engineer 3

Security Analyst 1

Security Analyst 2

Security Analyst 3

TEAM STRUCTURE

SECURITY ENGINEER VS. SECURITY ANALYST

ENGINEER

- Build things
- Implementing security
- Evaluate problems and research solutions
- Leverages security solutions, configure and deploy them
- Knows IT and security architecture in-depth

Skills required: Operational vulnerability analysis, incident response, real time network analysis, A big of Red team/pentest experience

ANALYST

- Break things/Examine things
- Testing/Breaking security
- Evaluate technical security weaknesses and propose remediation option to the management
- Leverages security scanning and pentest tools to identify weaknesses in assets
- Less clear idea about IT and security architecture

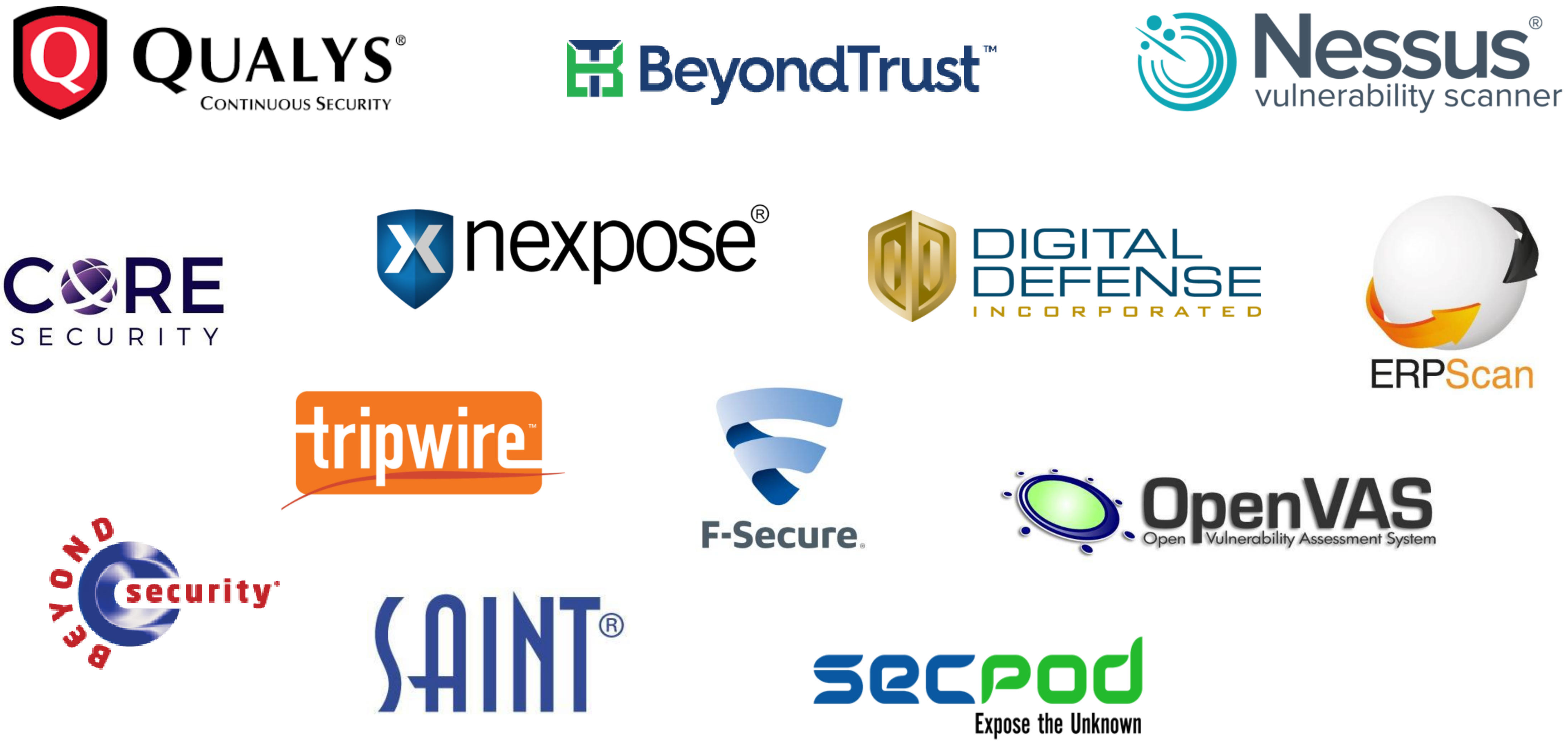
Skills required: security testing methodologies and standards, pentest and security testing tools and solutions knowledge, Extensive pentest and red teaming knowledge, Knowledge of testing variety of IT assets

Defence

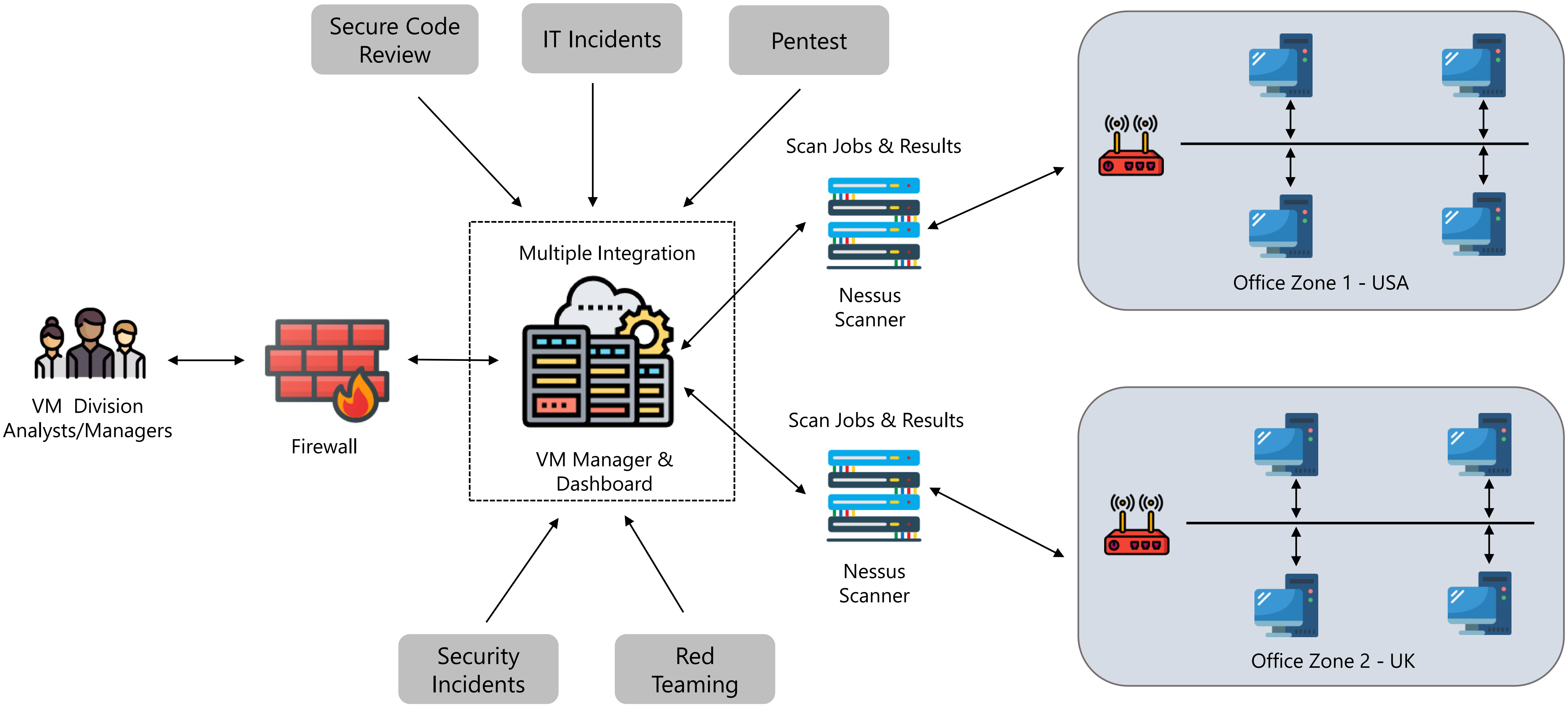
Offense

DIFFERENCE

A VARIETY OF VULNERABILITY SCANNERS AND MANAGEMENT SOLUTIONS



VULNERABILITY MANAGEMENT ENTERPRISE ARCHITECTURE



4 PHASES OF ENTIRE PROGRAM

01

DESIGN

02

DEVELOP

03

DEPLOY

04

OPERATE & MAINTAIN

01
DESIGN

Requirement Gathering for business and finance.

Defining program goals.

- ✓ Review needs of business for this program
- ✓ Review compliance requirements for this program
- ✓ Gather the master asset inventory
- ✓ Prioritize assets based on its criticality and risks
- ✓ Decide which assets are to be included in the scope
- ✓ Define roles and responsibilities of all stakeholders; prepare the RACI matrix
- ✓ Communicate with stakeholders and on requirements, project details, timeframe and possible risks of project execution
- ✓ Measure success criteria and milestones
- ✓ Create an entire VM strategy with timeframes, resources to be needed, compliance and regulation requirements, goals
- ✓ Calculate budget and get it approved by the management

02 DEVELOP

Technical requirement gathering, vendor selection and Evaluation, evaluate integration options

- ✓ Gather technical requirements (scanning tools/solutions, reporting methodologies and solutions, various reporting options for different stakeholders, etc.)
- ✓ Identify where automation can be done
- ✓ Identify where process integration can be done
- ✓ Identify resource requirement and evaluate skills-gap
- ✓ Identify possible risks, hurdles, exceptions during the process
- ✓ Define training programs for key individuals who are going to be a part of VM program
- ✓ Research on various vendors providing VM solutions
- ✓ Vendor evaluation criteria and factors to be considered
- ✓ Management approval to go ahead with a vendor solution

03

DEPLOY

Technical implementation

- ✓ Deploy solutions
- ✓ Provide training to different stakeholders which includes scanning, assessment and remediation
- ✓ Perform scheduling
- ✓ Assist various stakeholders in remediation
- ✓ Collaborate and communicate transparently with IT and security teams on identified vulnerabilities, remediation deadlines, etc.

04

OPERATE & MAINTAIN

Maintain ongoing operations, measure effectiveness of VM program, future improvements

- ✓ Scale the assessment process
- ✓ Measure effectiveness
- ✓ Constantly review and map the program output with stakeholder’s goals
- ✓ Suggest improvement points and best practices being followed in the industry

BEST PRACTICIES

IDENTIFY VULNERABILITIES FROM VARIOUS SOURCES

- Penetration Testing
- Red teaming activity
- Threat Hunting
- Threat Intelligence
- Support Tickets
- Crowdsourcing engagements
- Open source monitoring
- IT Incidents
- Security Incidents
- Vulnerability Scans

WHAT TO INCLUDE IN VM SCOPE

Code	IoT	DevOps	Web Applications	Mobile Devices
ICS & SCADA	Local storage	Mobile Applications	Thick & Thin Client Applications	IaaS & PaaS
Operating Systems	Dockers & Containers	Hypervisors	Databases	API

VULNERABILITY MANAGEMENT SOLUTION SELECTION DIFFERENTIATORS

- Platform Support
- Patch Integration
- Deployment Options
- Scanning Method
- Integration
- Vulnerability Updates
- Ticketing/ Workflow Integration
- Detailed Remediation Guidelines
- Pricing
- Threat Intelligence Feeds
- Risk Prioritization
- Scalability
- Scheduling Options
- Technical Support
- Delivery Model
- Reporting Options
- Ease of Use
- False Positive Ratio

HOW OFTEN TO PERFORM VULNERABILITY SCAN

Continuous Scanning

Compliance Scanning

On-Demand Scanning

Asset Priority Scans

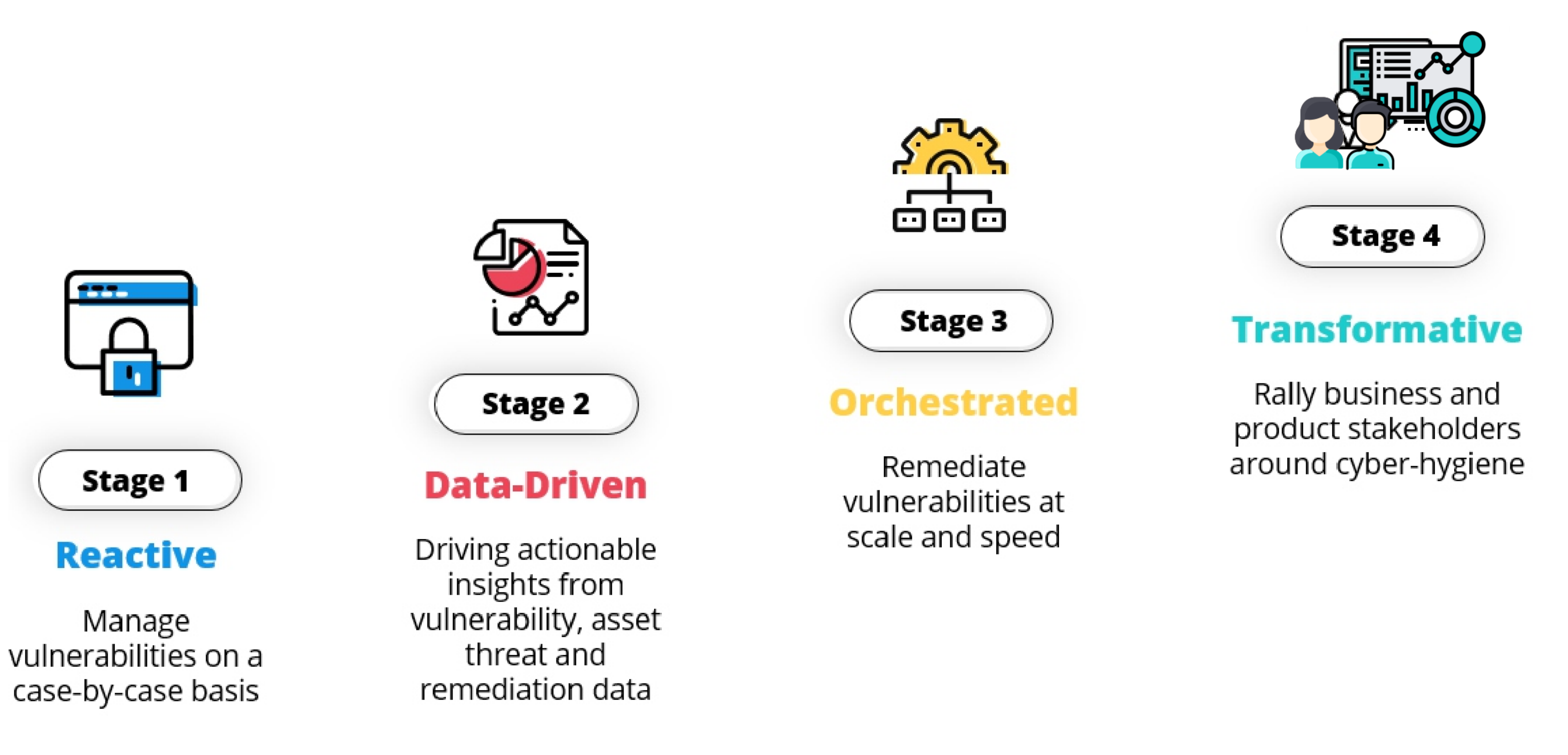
INTEGRATION IS THE KEY

Asset Database – Effective automation should be in place to periodically check the centralised asset list and it should pass the information to the vulnerability management solution about what has been scanned/assessed and what assets are remaining.

Penetration Testing – Effective automation should be in place to exchange data between penetration testing activity and issues identified by vulnerability scanning solutions. A pentest team can leverage information identified via vulnerability scanners. The team should be able to add vulnerabilities on the VM solution that are encountered during their pentest activity and not found by the vulnerability scanner tools. solution.

Threat Intelligence – Effective automation should be in place to ensure new threats identified by threat intelligence team/solutions are effectively being monitored/checked/scanned/tested by the vulnerability scanner/management solution.

VULNERABILITY MANAGEMENT MATURITY MODEL



Stage 1

Reactive

Manage vulnerabilities on a case-by-case basis

Stage 2

Data-Driven

Driving actionable insights from vulnerability, asset threat and remediation data

Stage 3

Orchestrated

Remediate vulnerabilities at scale and speed

Stage 4

Transformative

Rally business and product stakeholders around cyber-hygiene

THANK YOU

www.linkedin.com/in/chintangurjar/

chintangurjar@outlook.com

REFERENCES

- https://www.hitachi-systems-security.com/blog/vulnerability-scan-vs-vulnerability-assessment/
- https://www.freepik.com/free-photo/business-corporate-protection-safety-security-concept_3533269.htm#page=1&query=cyber%20security&position=0
- https://www.freepik.com/free-photo/futuristic-technology-screen-interface_7136702.htm#page=1&query=cyber&position=0
- VULCAN – The Vulnerability Remediation