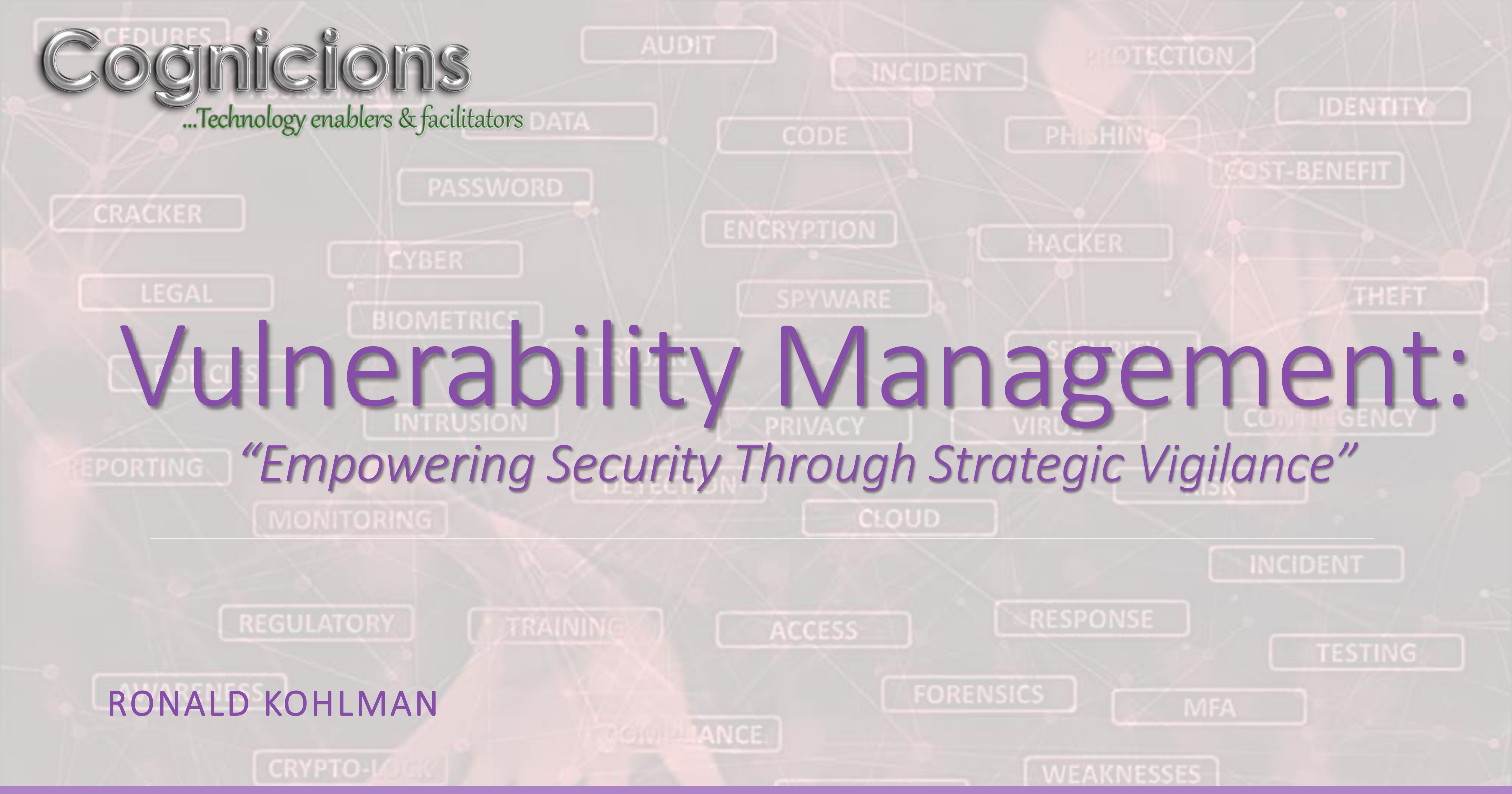
Cognicions

...Technology enablers & facilitators



# Vulnerability Management:

## *“Empowering Security Through Strategic Vigilance”*

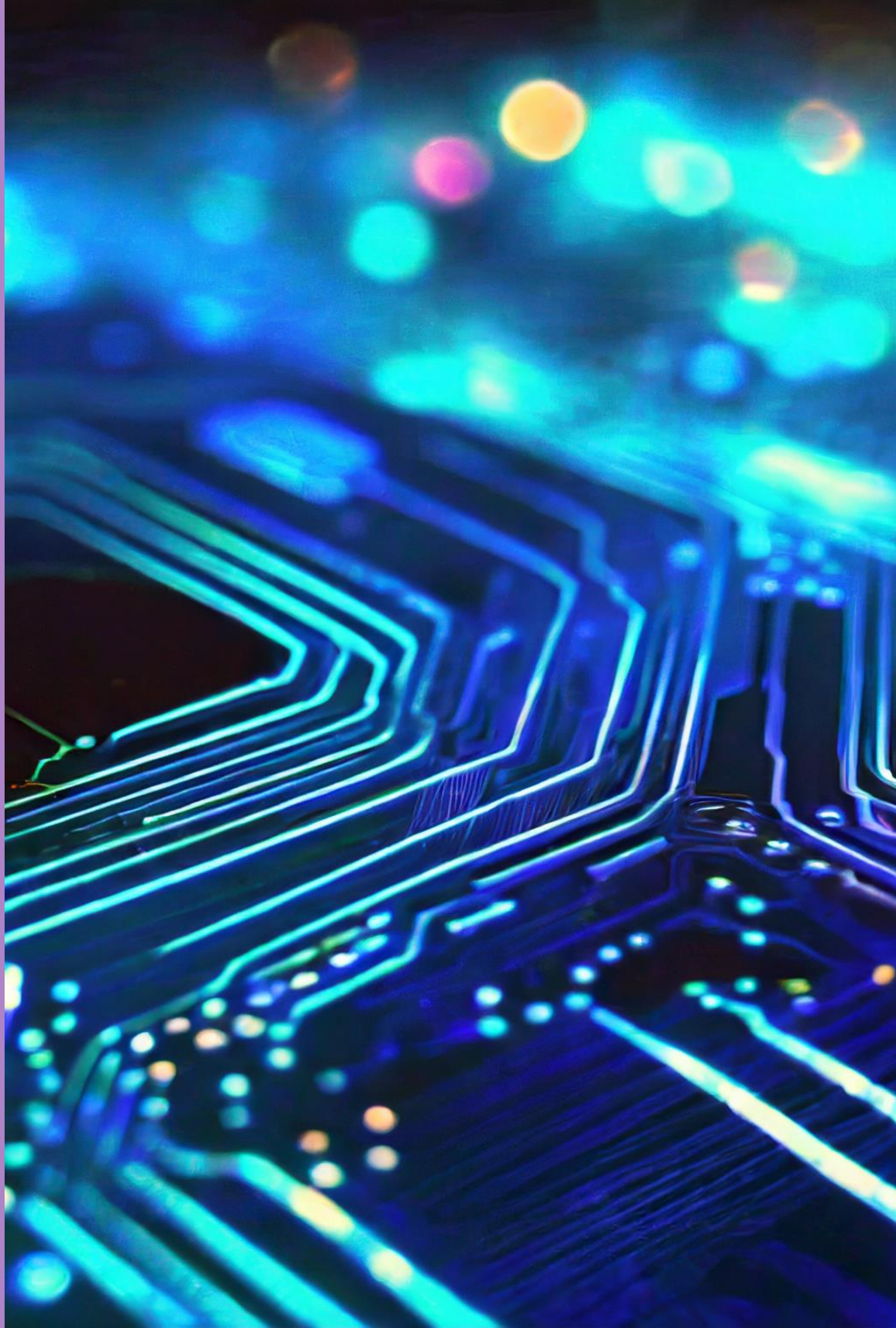
RONALD KOHLMAN

# What is Vulnerability Management (VM)

Vulnerability management encompasses a thorough process involving the identification, assessment, prioritisation, and mitigation of security vulnerabilities across an organisation's systems, networks, applications, and infrastructure.

The primary objective is to proactively handle and diminish the risk of exploitation by addressing potential weaknesses before they become susceptible to malicious exploitation.

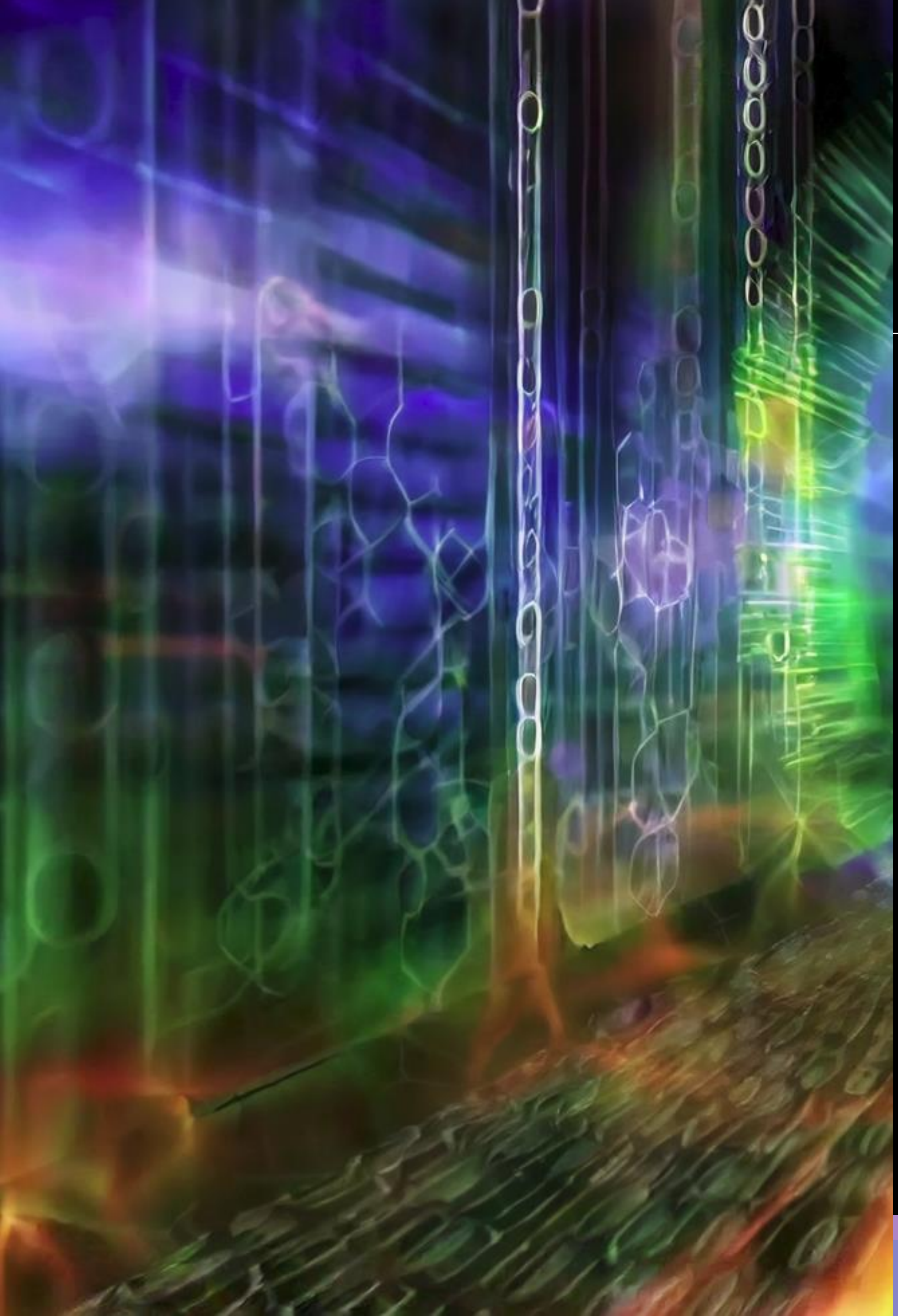
The significance of establishing a vulnerability management framework has seen a substantial rise, primarily due to the swift proliferation of newly identified vulnerabilities.



# Purpose of VM

The purpose of a vulnerability management methodology is to identify, assess, prioritise, and mitigate security vulnerabilities within an organisation’s IT infrastructure systematically and proactively.

The primary objective is to proactively handle and diminish the risk of exploitation by addressing potential weaknesses before they become susceptible to malicious exploitation.



# Principles

- The principles of vulnerability management revolve around establishing a systematic and proactive approach to identifying, assessing, prioritizing, and mitigating security vulnerabilities within an organisation's systems, networks, applications, and infrastructure. Here are key principles that guide effective vulnerability management:

- Continuous Identification
- Comprehensive Assessment
- Prioritisation
- Risk Analysis
- Timely Remediation
- Patch Management
- Communication and Collaboration
- Penetration Testing
- Automation and Technology Integration
- Documentation, Training, and Awareness
- Regulatory Compliance
- Continuous Improvement

- By adhering to these principles, organisations can establish a resilient vulnerability management program that effectively minimises security risks and enhances overall cyber security posture.

# Key Challenges

### Complexity

Managing vulnerabilities across diverse and complex IT environments can be challenging.

### Resource Constraints

Limited resources may hinder the ability to address all vulnerabilities promptly.

### Patch Management Issues

Applying patches without disrupting operations can be challenging.

### Emerging Threats

Continuous monitoring is essential to address newly identified vulnerabilities and emerging threats.

***Vulnerability management (VM) is a critical aspect of a robust cyber security strategy, ensuring organisations can identify, assess, and mitigate potential risks proactively.  It requires a systematic and ongoing effort to stay ahead of evolving threats and maintain a secure and resilient IT environment.  A well-implemented Vulnerability Management approach is fundamental to maintaining a robust cyber security posture, adapting to emerging threats, and safeguarding the integrity and confidentiality of organisational assets and information.***

# High Level Content of VM

- ❑ An operating framework for VM that covers:
  - ❑ Vulnerability Management
  - ❑ Patch Management
  - ❑ Penetration Testing

- ❑ Required to be in place for each of the above are:
  - ❑ Policies
  - ❑ Procedures
  - ❑ Tools

  - ❑ Coverage also for:
    - ❑ Threat Hunting
    - ❑ External Attack Surface management
    - ❑ Threat Exposure Management

# Benefits of good VM

**Risk Reduction:** Proactively identify and address vulnerabilities to reduce the risk of exploitation.

**Compliance:** Assist organisations in meeting regulatory and compliance requirements related to cyber security.

**Resource Optimisation:** Optimise the allocation of resources by focusing on high-priority vulnerabilities that pose the greatest risk.

**Business Continuity:** Enhance the resilience of systems and infrastructure, contributing to business continuity.

**Improved Security Posture:** Strengthen the overall security posture of the organisation by addressing weaknesses in a systematic manner.

**Cost Savings:** Reduce the potential financial impact of security incidents by preventing exploitation of vulnerabilities.

**Enhanced Incident Response:** Provide a foundation for effective incident response through proactive vulnerability management.

# Approach Coverage – VM

- Discovery
- Vulnerability Assessment
- Risk Assessment
- Prioritisation
- Remediation Planning
- Patch Management
- Compensating Controls
- Security Controls
- Continuous Monitoring
- Incident Response Integration
- User Awareness and Training
- Verification and Validation
- Documentation and Reporting
- Regulatory Compliance
- Metrics and Key Performance Indicators (KPIs)
- Automation and Technology Integration
- Training and Skill Development

# Approach Coverage – Patch Management

- Vulnerability Assessment
- Patch Identification
- Risk Assessment
- Testing
- Deployment Planning
- Deployment
- Verification
- Documentation
- Monitoring

Patch management is a systematic process of planning, testing, deploying, and maintaining software updates or patches to fix vulnerabilities, enhance security, and improve the functionality of computer systems, applications, and networks. The goal is to ensure that software remains up-to-date, secure, and protected against potential exploits.

Patch Management is a component of Vulnerability Management and is usually performed prior to delivery of a solution into a production environment. Thereafter on a periodic basis, e.g.  at least Monthly, or within a short timeframe of when patch updates becoming available.  New Patches should be tested within your environment to ensure that there are no unforeseen impacts of the patch on the rest of your environment.

Patch management is not just about patching.  It’s about how well we do it. There are 3 important things you have to take care of in patch management: **timeliness, efficiency, and quality**.

# Approach Coverage – Penetration Testing

- Planning
- Reconnaissance
- Scanning
- Enumeration
- Exploitation
- Post-Exploitation
- Analysis and Reporting

Ensure that penetration testing activities are thorough, methodical, and aligned with the organisation's security objectives and risk tolerance levels.

Enable organisations to identify and address security vulnerabilities effectively, thereby reducing the risk of security breaches and unauthorised access.

Define the extent and depth of the methodologies, techniques, and tools that are employed to assess the security posture of a system, network, or application.

Including the breadth and thoroughness with which penetration testing is conducted to identify vulnerabilities and potential points of exploitation.

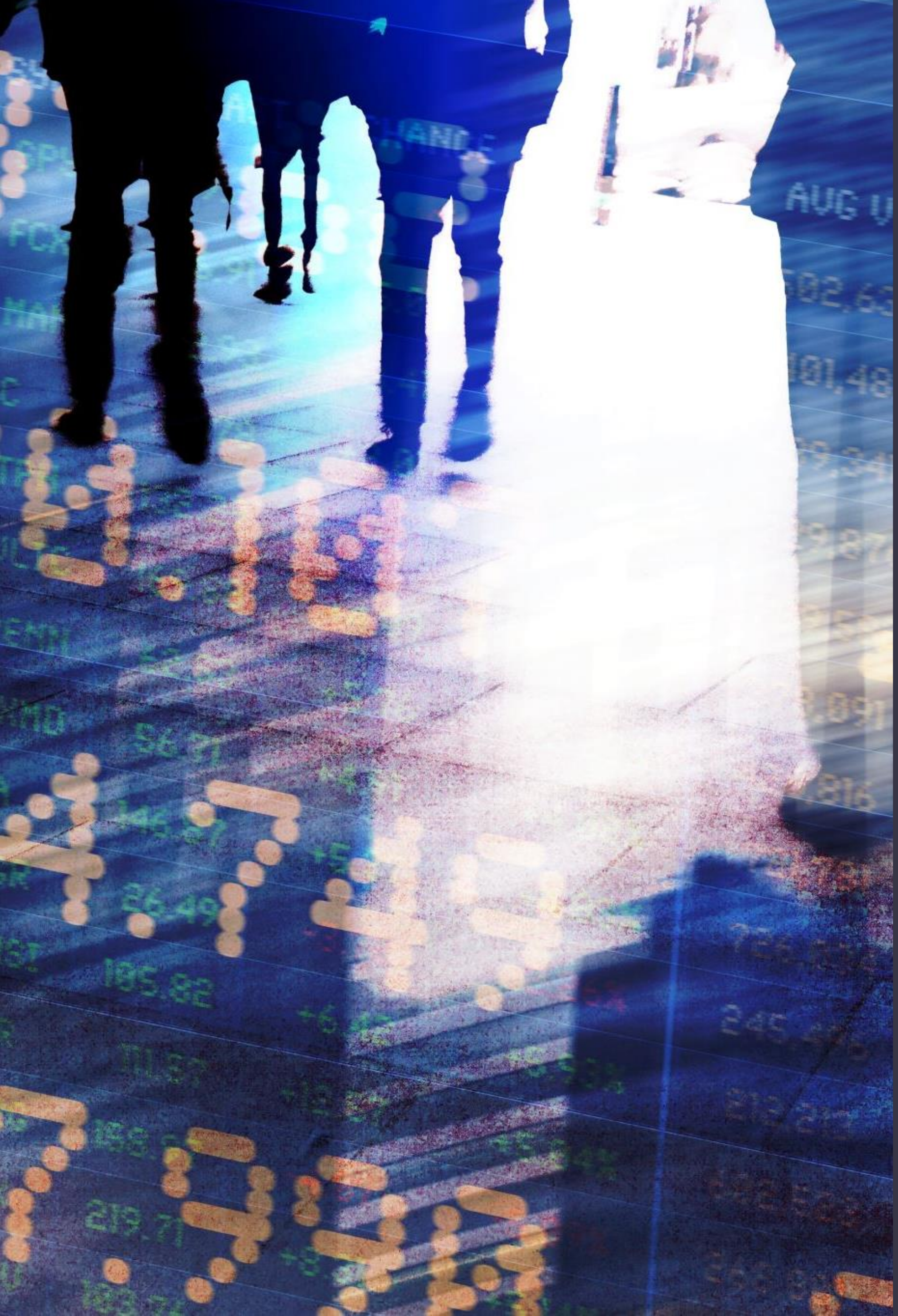
# Approach Coverage – Threat Hunting

- Continuous monitoring
- Proactive Search for Indicators of Compromises (IoCs)
- Behavioural Analysis
- Threat Intelligence Integration
- Vulnerability Assessment Integration
- Data Correlation
- User and Entity Behaviour Analytics (UEBA)
- Honeypots and Deception Technologies
- Incident Response Planning
- Continuous Skill Development
- Documentation and Reporting

Threat hunting in vulnerability management refers to the proactive and systematic search for potential cyber security threats and vulnerabilities within an organisation's IT environment.

It involves skilled cyber security professionals actively seeking out indicators of compromise, unusual patterns, or vulnerabilities that may not be easily detectable through automated tools alone.

The goal of threat hunting is to identify and mitigate security risks before they are exploited by malicious actors.



# Approach Coverage – External Attack Surface Management

- ❑ Discovery of Assets and Services
- ❑ Vulnerability Identification and Assessment
- ❑ Prioritisation Based on Risk Exposure
- ❑ Integration with Vulnerability Management Tools
- ❑ Automated Scanning and Monitoring
- ❑ Mapping Attack Paths and Exploitation Scenarios
- ❑ Visibility into Shadow IT and Unsanctioned Assets
- ❑ Regulatory Compliance and Reporting
- ❑ Incident Response Readiness
- ❑ Continuous Improvement

*External Attack Surface Management complements vulnerability management by offering a proactive and holistic approach to identifying, prioritising, and mitigating vulnerabilities in the external-facing assets of an organisation.  By integrating EASM into the overall cyber security strategy, organisations can enhance their resilience to external threats and reduce the likelihood of successful cyberattacks.*

# Approach Coverage – Threat Exposure Management

- ❑ Continuous Assessment Practices
- ❑ Attack Surface Complexity
- ❑ Programmatic Approach - CTEM: Continuous Threat Exposure Management (CTEM)
- ❑ Risk Fatigue Mitigation
- ❑ Real-time Visibility
- ❑ Adaptive Security Posture
- ❑ Integration with Threat
- ❑ Cross-functional Collaboration

In the dynamic landscape of modern enterprises, understanding and managing the evolving threat landscape is a critical aspect of cyber security.

Threat Exposure Management (TEM) emerges as a proactive approach to assess and mitigate the risks associated with an organisation's attack surface.

This is particularly essential in the face of increasing complexity and the continuous evolution of cyber threats.

# Tools for VM

Vulnerability Management (VM) tools are security applications designed to scan enterprise networks, identifying potential weaknesses that could be exploited by intruders. Upon detecting vulnerabilities, these tools recommend or trigger remediation actions, effectively minimising the risk of a network attack.

Vulnerability Management (VM) tools begin the assessment of the network using a variety of tools such as network and port scanners, IP scanners, and more.

Following this assessment, they prioritise remediation, ensuring that the most critical issues are promptly addressed, while lower-priority issues are scheduled for future evaluations. These tools can be configured to execute limited scans and address identified vulnerabilities immediately, avoiding the delays associated with comprehensive scans.

The prolonged duration of extensive scans can result in vulnerabilities identified during the scan remaining unaddressed until the scan concludes. Therefore, swift remediation aligned with the prioritisation schedule recommended by the vulnerability software is crucial.

This approach systematically eliminates network weaknesses, reducing reliance on peripheral intrusion detection technologies.

Additionally, in situations where network access is compromised, rapid remediation of vulnerabilities exploited by intruders can effectively minimise the impact of cyberattacks.

There are many and varied tools available on the marketplace to choose from. Organisations will need to perform their own due diligence to identify what VM tools are suitable for their environment and budget.

Selecting effective Vulnerability Management Tools is crucial for maintaining a robust cyber security posture.

# Key Takeaways

1. Understand the shared responsibility model of cloud security.
2. Implement strong access controls and data encryption.
3. Establish a regular vulnerability management process.
4. Provide regular security awareness training to employees.
5. Have a plan for responding to cyberattacks.
6. Regularly test, train, and update incident response plans.

# Summary

- ❑ Vulnerability management is a critical aspect of a robust cyber security strategy, ensuring organisations can identify, assess, and mitigate potential risks proactively.  It requires a systematic and ongoing effort to stay ahead of evolving threats and maintain a secure and resilient IT environment.

- ❑ The primary objective of VM for organisations is to proactively handle and diminish the risk of exploitation by addressing potential weaknesses before they become susceptible to malicious exploitation.

- ❑ A well-implemented Vulnerability Management Methodology is fundamental to maintaining a robust cyber security posture, adapting to emerging threats, and safeguarding the integrity and confidentiality of organisational assets and information.

- ❑ Foremost is for a solid VM approach that covers these key areas:
  - ❑ Vulnerability Management
  - ❑ Patch Management
  - ❑ Penetration Testing
  - ❑ Threat Hunting
  - ❑ External Attack Surface management
  - ❑ Threat Exposure Management

# About Ronald

Ronald is a highly experienced and knowledgeable IT professional in the field of program and test management.

He has had many roles working across transformational initiatives and complex enterprise technology solutions.

- Leadership in Transformational Programs
- Global Experience and Cross-Continental Team Leadership
- Governance Frameworks and Tools
- Delivery of Complex Technology Solutions
- Executive-Level Engagement and Consulting

He has been writing and publishing technology industry specific documents for several years. Imparting his practical working experience within these documents.

You can purchase his technology & project books on Amazon:

**Vulnerability Management – Empowering Security Through Strategic Vigilance**
You’ve had a Cyber Attack - Now what?
Securing Tomorrow, Today: Navigating Cyber Security Risks with Strategic Precision
How to Create a Cyber Security Roadmap: A necessity for your organisation
Program Management Plan: A usable Template for you
Business Case Template: An approach to documenting your next IT business case
Successfully Delivering User Acceptance Testing for your project
IT Deployment Management Framework
Steering Committee Terms of Reference and Charter
UAT Planning & Execution Guide
Defect Management Plan
And others…

Cognicions

*...Technology enablers & facilitators*

# Thank You

COGNICIONS.COM

COGNICIONS PTY LTD

ABN 83 611 219 642

MELBOURNE

PO BOX 125, OLINDA,
VICTORIA 3788

+61 (0) 402 448 050

INFO@COGNICIONS.COM