A COMPREHENSIVE GUIDE TO PENETRATION TESTING

A CYBER SECURITY BUYER'S GUIDE

2024 / 2025 EBOOK EDITION

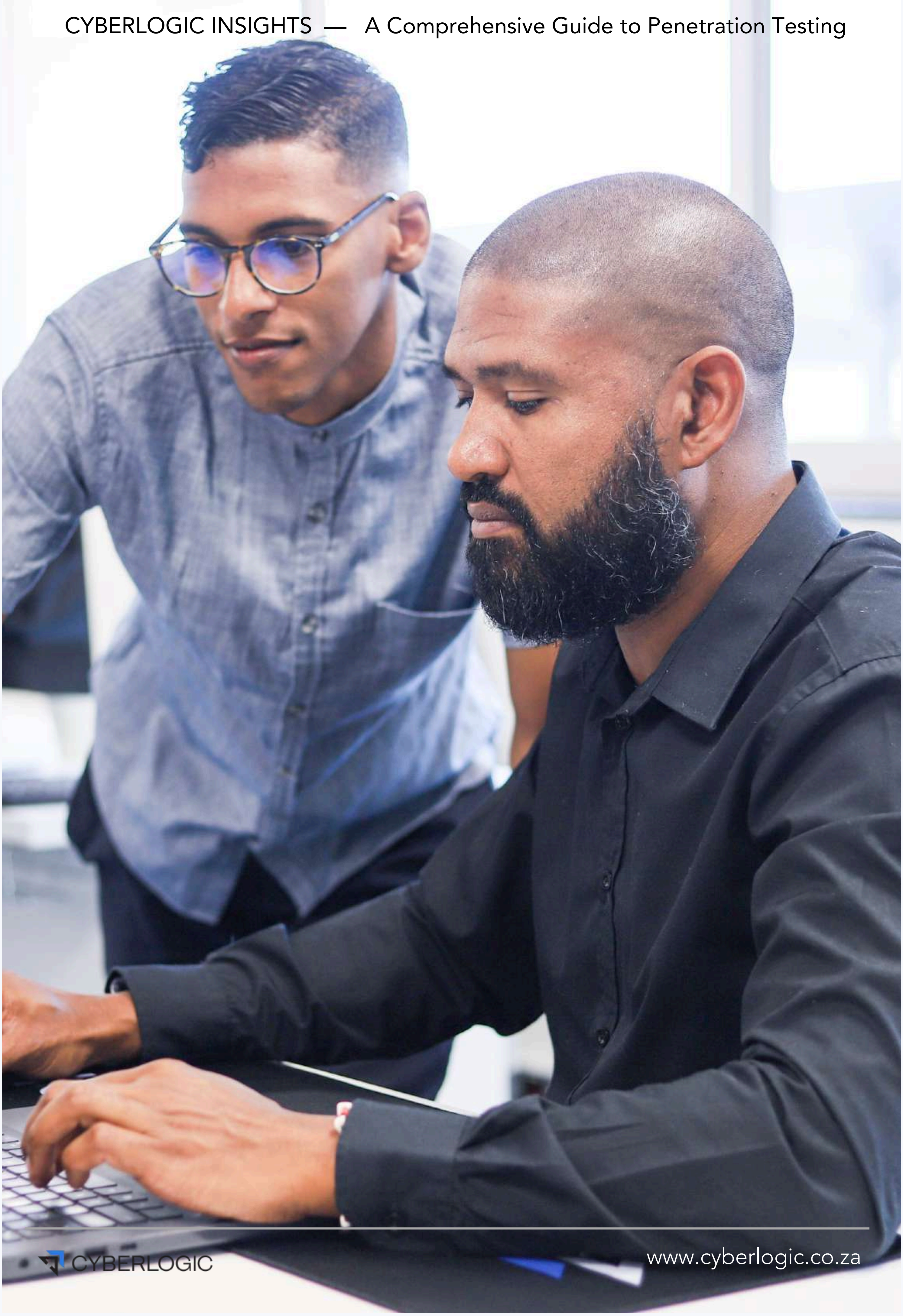


TABLE OF CONTENTS

UNDERSTANDING PENETRATION TESTING

2024 / 2025 EBOOK EDITION

This eBook is designed to help you better understand **penetration testing** and provide you with reliable information to make informed decisions when planning your future assessments. This document will give you the necessary information to ensure your penetration testing strategy is suited to your environment, in line with your cyber security risk management strategy, follows industry best practices and standards, and suits your budget.

WHAT IS PENETRATION TESTING?

Penetration testing, often referred to as "pen testing", is a proactive approach to assessing the security of an organisation's digital infrastructure, applications, and networks. It involves simulating real-world cyber-attacks to identify vulnerabilities that could be exploited by malicious attackers. Unlike other forms of testing, penetration testing goes beyond automated scans and vulnerability assessments by using human expertise to uncover complex security weaknesses.

WHY IS PENETRATION TESTING IMPORTANT?

The digital landscape is rife with cyber threats, ranging from data breaches to ransomware attacks. Penetration testing plays a crucial role in identifying and eliminating vulnerabilities before they can be exploited by attackers. Penetration testing is becoming an increasingly important part of risk management in organisations, whether to improve overall cyber security or as part of compliance initiatives. These tests should be conducted regularly or after any major change to the underlying technologies that support your daily operations to stay protected from attackers. By proactively testing their defences, organisations can improve their security posture, reduce the risk of data breaches and protect sensitive information.

THE RELATIONSHIP BETWEEN PENETRATION TESTING AND COMPLIANCE

Penetration testing not only enhances security, but is often a prerequisite for compliance with industry regulations and standards, such as POPIA, PCI DSS, HIPAA, GDPR, and ISO 27001. These regulations require regular security assessments, including penetration testing, to ensure the protection of customer data and adherence to security best practises.

Recent market insights from Statista project a significant rise in the global cost of cyber crime, expected to rise from $9.22 trillion in 2024 to $13.82 trillion by 2028.

THE BENEFITS OF EFFECTIVE PENETRATION TESTING

Although penetration testing is often a compliance requirement, the benefits extend far beyond that. From improving incident response and increasing customer confidence to optimising security investments, regular penetration testing benefits the organisation, its employees, and its customers.

Comprehensive vulnerability and security risk reporting.

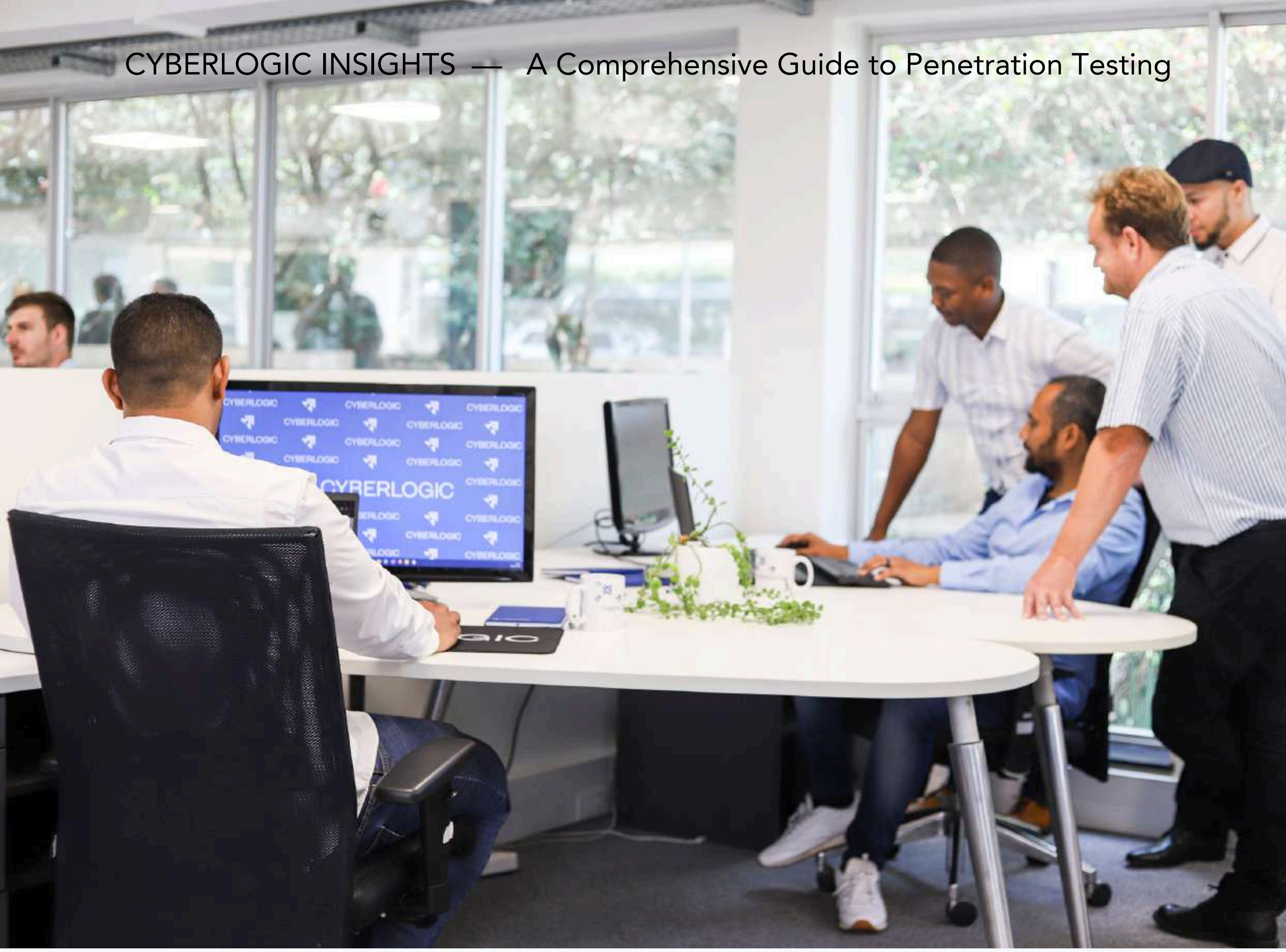
Mitigating the risk of data breaches, financial losses, and reputational damage.

Meeting regulatory and compliance requirements.

Assessing the effectiveness of security controls and measures.

Improving incident response preparedness.

Providing assurance to third-party stakeholders.



THE STAGES OF THE PENETRATION TESTING PROCESS

Penetration testing is a critical multi-stage process designed to strengthen an organisation's cyber defences. There are various industry methods for conducting pen tests, however, this eBook will specifically focus on a detailed exploration of the **six-phase approach** folllowed by our **Red Team**: Planning, Reconnaissance, Scanning, Vulnerability Assessment, Exploitation, and Reporting.

STAGE 1 - PLANNING: SETTING THE FOUNDATION

This is where the scope objectives, and parameters of the test are defined to ensure alignment with the organisation's goals and objectives. Key tasks include:

- Establishing rules of engagement, including the type of test (black box, white box, or grey box) and any limitations or constraints.
- Assembling the penetration testing team and assigning roles and responsibilities.
- Developing a test plan outlining the approach, methodology, and timeline for the test.

STAGE 2 - RECONNAISSANCE: LAYING THE GROUNDWORK

This is where penetration testers collect data about the target to help them understand its infrastructure, systems, and potential vulnerabilities. Key tasks include:

- Gathering information about the target organisation's network architecture, systems, and applications.
- Analysing the information collected to develop a comprehensive testing strategy.
- Ensuring compliance with legal and ethical considerations during information gathering activities.

STAGE 3 - SCANNING: IDENTIFYING THE GAPS

In this stage, various tools and techniques are used to scan the organisation’s environment for vulnerabilities and weaknesses. Key tasks include:

- Identifying open ports, misconfigured services, and other potential security vulnerabilities.
- Prioritising vulnerabilities based on severity and potential impact on the organisation's systems and data.
- Generating reports detailing the findings of the vulnerability scans and recommending steps for remediation.

STAGE 4 - VULNERABILITY ASSESSMENT

This where penetration testers analyse and assess the severity and potential impact exploitation of the identified vulnerabilities would have on the organisation's systems. Key tasks include:

- Categorising vulnerabilities based on their severity, likelihood of exploitation, and potential impact.
- Prioritising vulnerabilities for further investigation and remediation based on their risk profile.
- Generating reports detailing the findings of the vulnerability assessment and recommendations for remediation.

STAGE 5 - EXPLOITATION: SIMULATING REAL ATTACKS

In this stage, planned attacks are carried out, simulating a real-world breach. Techniques applied here can include social engineering attacks, such as phishing, smishing, or vishing. Key tasks include:

- Mimicking the tactics, techniques, and procedures (TTPs) of real-world attackers to simulate realistic attack scenarios.
- Demonstrating the impact of successful exploitation on the organisation's systems, data, and operations.
- Documenting the steps taken during the exploitation phase and the outcomes of the simulated attacks.

STAGE 6 - REPORTING: DISSECTING THE FINDINGS

This is where penetration testers analyse the results from stage 3 of the process, and provide actionable insights to improve security measures. Key tasks include:

- Documenting the findings of the test, including identified vulnerabilities, their severity, and potential impact on the organisation's systems and data.
- Providing recommendations for remediation, including prioritised action items and best practices for improving the organisation's security posture.
- Communicating the findings and recommendations to the organisation's stakeholders, including IT teams, management, and executive leadership.

Once the pen test is complete, the team hands its findings over to the **Remediation Team**, which then prioritises and addresses the identified vulnerabilities to strengthen the organisation's defences.

REMEDIATION

In our **Security Remediation guide**, we explain that this step is more than patching specific issues; it's a strategic move toward an enhanced cyber security posture. This stage also involves a feedback loop, where lessons learnt from the test are applied to continuously improve security measures. As part of the remediation process, the security team will prioritise the uncovered vulnerabilities, identifying those most likely to happen as well as those that will have the most severe impact on business. Remediation of these vulnerabilities can then either be done by a remediation provider or by an in-house team. There are pros and cons to both approaches, as outlined in our guide.

DOWNLOAD THE REMEDIATION GUIDE

Things to consider when deciding on a remediation approach:

Hybrid Approach:
Some organisations adopt a hybrid model, combining the strengths of external specialist providers and in-house teams for a balanced and effective remediation strategy.

Training and Skill Development:
Investing in training programmes for in-house teams can enhance their skills, making them more adept at handling complex cyber security challenges, but these skills development interventions can be costly– both in terms of the time taken to acquire the certifications and the cost thereof.

Clear Communication:
Whether relying on external specialists or an in-house team, a clear and open channel of communication between the IT department, management, and other relevant stakeholders is crucial for an efficient remediation process.

AUTOMATED VS. MANUAL APPROACHES FOR CYBER SECURITY

According to INTERPOL's 2024 African CyberThreat Assessment Report, in 2023, there was a 23% year-on-year increase in the average number of weekly cyberattacks per organisation in Africa.

In the world of cyber security, the analogy of household security is often used to provide a tangible example of this complex domain. Think of basic security measures as the digital equivalent of a reliable alarm system. This fundamental layer includes important things such as antivirus software and firewalls that protect your digital ‘home’ from common threats. The different levels of cyber security build on this and provide more sophisticated defences. **Network security** acts like a sturdy lock on doors and windows that prevents unauthorised access, application security is a vigilant guard that ensures individual software components remain resilient, and endpoint security reflects a comprehensive surveillance system that protects every device.

To test the effectiveness of your alarm system, you would simulate an intrusion to ensure that all the various components are doing what they are supposed to do. Now, imagine two scenarios: In the first scenario, the simulated ‘thief’ uses common tools and predefined tactics, while in the second scenario, he uses experience, intuition, and creativity to get into your home, testing every conceivable vulnerability, some of which you might not have even noticed. This analogy helps to illustrate the difference between **automated** and **manual** pen testing.

AUTOMATED PEN TESTING: THE QUICK SCAN APPROACH

Automated penetration tests use **pre-programmed tools** to check the security of an organisation's digital infrastructure. This approach offers speed and cost efficiency, for known vulnerabilities and basic exploits. However, it lacks the finesse of human intervention and can miss complicated vulnerabilities that only experienced professionals can detect.

MANUAL PEN TESTING: THE ART OF INTRUSION

Manual penetration testing uses **human expertise, experience and creativity** to uncover vulnerabilities that automated tools may miss. This approach simulates real-life attack scenarios and explores potential vulnerability chains. While manual testing is more time and resource sensitive, it provides a deeper understanding of an organisation's security landscape.

CONSIDERING COST, TIME, AND RESULTS

When deciding between automated and manual pen testing, several factors come into play, namely cost, time, and desired outcome.

Cost Implications:

Automated pen testing is an 'off-the-shelf' solution, offering standardised scans at a lower cost. Manual pen testing, on the other hand, involves skilled professionals who can explore vulnerabilities from multiple angles, potentially discovering critical exploits that automated tools might miss. These cyber security professionals are vastly experienced, have multiple certifications, and come at a premium price point in comparison with an automated scan.

Time/Resource Implications:

Automated tests are quicker, generating results faster than manual tests. However, manual tests offer the advantage of a human touch, enabling experts to identify complex vulnerabilities that could be exploited in ways that could be detrimental to your business. While they take longer, they are more thorough and provide a more in-depth view of vulnerabilities.

Expected Outcome:

The choice between automated and manual pen testing depends on your organisation's goals. Automated tests provide an overview of vulnerabilities, while manual tests dive deeper into intricate weaknesses. Regardless of the approach you opt for in your business, once you have a view of your vulnerabilities, remediating them is critical. Post-testing, it's essential to address and retest vulnerabilities to avoid inadvertently creating new security gaps in your effort to close others – something like accidentally bumping a window open while closing a door.

BLACK BOX, WHITE BOX, AND GREY BOX PENETRATION TESTING

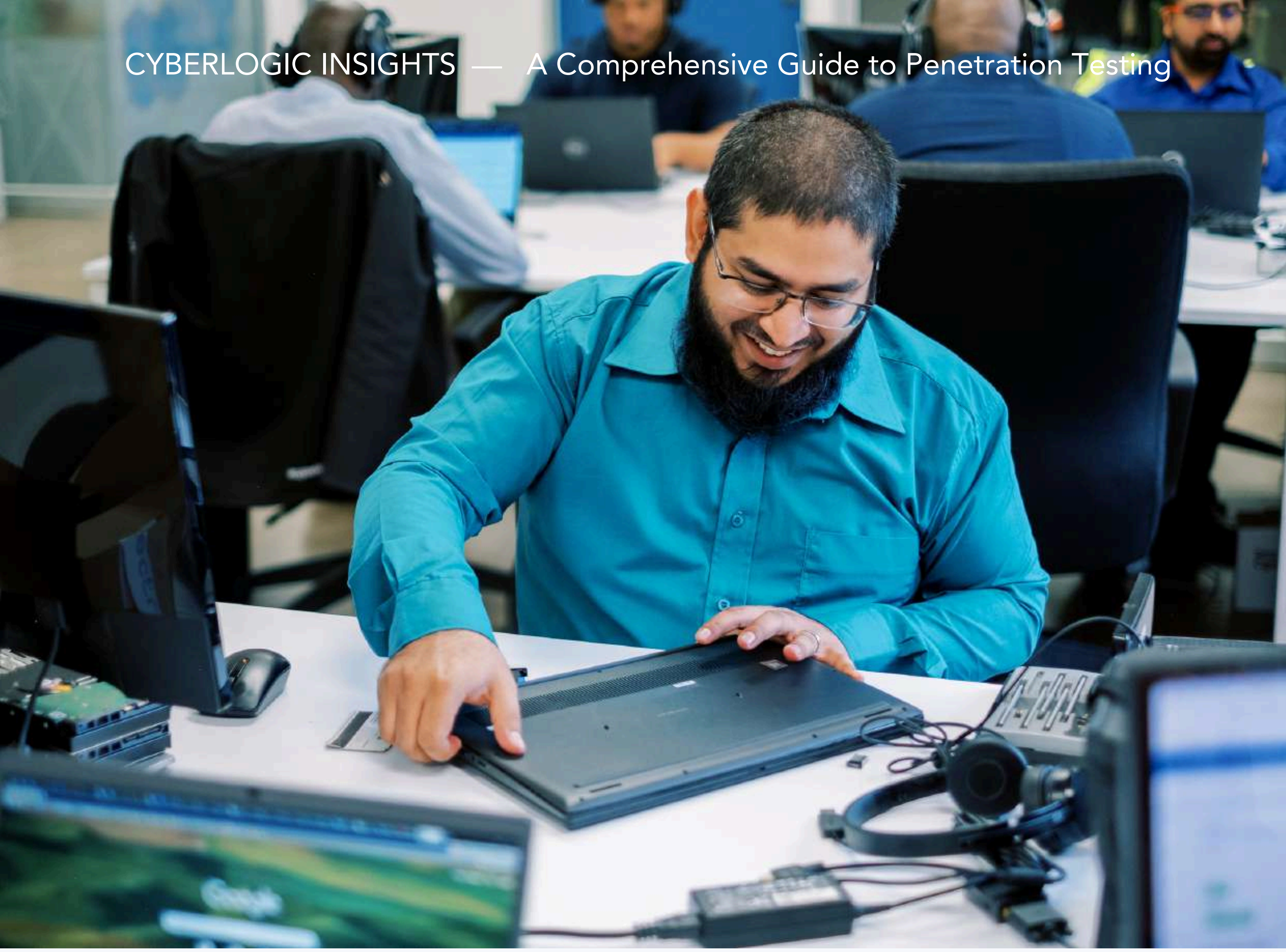
2024 / 2025 EBOOK EDITION

Black box, **white** box, and **grey** box testing each offer unique perspectives and evaluations, allowing organisations to take a holistic approach to security. The value of human intervention in this process cannot be overstated. Unlike automated scans or vulnerability assessments, the strategic implementation of penetration testing, with the help of experienced professionals simulating real-world cyber-attack scenarios, provides a more **comprehensive view** of vulnerabilities, and helps organisations strengthen their defences more effectively.

CHOOSING THE RIGHT APPROACH FOR YOUR ORGANISATION

When deciding which approach is best for a client, our team takes into consideration the scope of the penetration test, the client's specific needs and their current cyber security maturity level. This enables them to determine the right approach for each client. In some cases, the team will conduct a **hybrid** penetration test, starting with a black box approach and then moving to a grey box approach. In this way, we are able to tailor the approach to the client's needs, goals, and budget. Once you have a clear view of how you want to test your security posture, it's important understand the **pros** and **cons** of the different approaches as outlined in the table below. This ensures you use the methodology best aligned to your needs, resulting in the maximum value from your penetration testing investment:

	PROS	CONS
Black Box Testing	• Mimics real-world attack scenarios. • Uncovers blind spots that might evade detection. • Assesses security from an external viewpoint. • Emulates the perspective of an uninformed attacker.	• May overlook internal vulnerabilities. • Limited by lack of internal information and view into internal workings. • May require advanced reconnaissance for effective testing. • Testing may be limited to surface-level vulnerabilities.
White Box Testing	• Provides comprehensive internal insights. • Identifies intricate internal vulnerabilities. • Allows for targeted remediation strategies. • Enables precise vulnerability assessment.	• Relies heavily on system familiarity. • May miss external facing vulnerabilities. • May not reflect real-world attack scenarios. • May be time-consuming and resource-intensive. • Scope may be restricted to known systems and assets.
Grey Box Testing	• Strikes a balance between external and internal perspectives. • Offers a nuanced evaluation of security posture. • Considers internal security measures. • Provides insights into both external and internal aspects.	• Achieving a balanced assessment is a complex task. • May not provide as comprehensive insights as other methods. • Potential for overlooking certain types of vulnerabilities, such as weaknesses in specific network segments or protocols. • Requires skilled testers to navigate complexities.



THE DIFFERENT TYPES OF PENETRATION TESTING IN CYBER SECURITY

With cyber threats becoming more sophisticated, organisations must take a proactive approach to identifying weaknesses across their digital landscape. There are several types of penetration testing that focus on different areas of an organisation's security. Understanding these types can help in choosing the appropriate tests to strengthen defences and protect sensitive data. Below is a summary of the six most common types of penetration testing:

1. NETWORK PENETRATION TESTING

Network service penetration testing, or infrastructure testing, is one of the most commonly performed types of pen tests. The main objective is to identify exploitable vulnerabilities in networks, systems, hosts and network devices (e.g., routers and switches) before hackers discover and exploit them. Network penetration testing uncovers opportunities for hackers to compromise systems and networks to gain unauthorised access to sensitive data or even take over systems for malicious or non-business purposes.

2. WEB APPLICATION PENETRATION TESTING

A web application (web app) is an application or programme stored on a remote server and delivered over the Internet through a browser interface. Web services are, by definition, web applications and many, though not all, websites contain web applications. Users can access a web application via a web browser, such as Microsoft Edge, Google Chrome, Mozilla Firefox, or Safari. **Web application** penetration testing detects vulnerabilities in these web-based applications. Various penetration techniques and attacks are used to uncover potential vulnerabilities.

3. WIRELESS PENETRATION TESTING

In a wireless penetration test, the connections between all devices connected to the organisation's Wi-Fi are identified and analysed for vulnerabilities and weaknesses. These devices include laptops, tablets, smartphones and all other Internet of Things (IoT) devices. For many pen testers, 'wireless' used to be synonymous with 'Wi-Fi'," the standard network technology, and many organisations have deployed complex security systems to protect these networks. Today, the term 'wireless' has a much broader meaning, encompassing not only the security of Wi-Fi systems but also that of a range of different proprietary wireless systems such as Bluetooth, Radio Frequency, Zigbee or Z-Wave.

4. PHYSICAL PENETRATION TESTING

Physical penetration testing, or **physical intrusion** testing, is designed to uncover opportunities for malicious actors to compromise physical barriers (e.g., locks, sensors, cameras, keypads, mantraps, etc.) in a way that allows unauthorised physical access to sensitive areas. This can result in data breaches and system/network compromises, as once a malicious actor is inside the building, gaining network access is often easier.

5. INSIDER THREAT PENETRATION TESTING

An **insider threat** penetration test specifically targets the risks posed by malicious insiders, such as disgruntled employees or compromised contractors. Unlike broader internal testing, this type of assessment is more focused and simulates scenarios where an insider, like an employee with legitimate access, attempts to exploit their position. For example, we might be given access to a company laptop used by a staff member and simulate actions such as trying to access restricted areas like Finance or HR, deleting sensitive documents, or even collaborating with external attackers. This test aims to identify vulnerabilities in your organisation's internal systems, access controls, and monitoring processes, helping to enhance your ability to detect, prevent, and respond to potential insider threats.

6. SOCIAL ENGINEERING PENETRATION TESTING

Social engineers are hackers who exploit a weakness found in almost every organisation: human behaviour and psychology. These attackers use various tactics, including phone calls, social media, and especially e-mail, to trick people into granting access to sensitive data or other company resources. In **social engineering** tests, a malicious actor tries to persuade or trick users into giving them confidential information, such as usernames and passwords.

CHOOSING THE RIGHT SECURITY PROVIDER FOR YOUR ORGANISATION

Penetration testing is one of the best ways to assess the robustness of your cyber security defences. However, to reap maximum benefits, penetration tests must be correctly managed. It's essential to select a team with extensive industry experience, a plan for securing your data during testing, methodologies based on industry best practices, and sample reports for your review.

Having the right penetration testing partner could be the difference between the success and failure of your endeavour. If you plan to conduct the penetration tests collaboratively, include at least two external cyber security experts on the penetration testing team. An independent, external opinion is essential to avoid blind spots. When selecting external vendors, keep the following tips in mind:

- **Assess** the credentials, experience, and expertise of the external provider and each penetration testing team member. Each team member should have experience across various industries and organisations of all sizes and hold the requisite certifications.
- **Understand** how the penetration testers will protect your data during and after the test. Define and agree on how confidential data will be transferred, stored, and destroyed.
- **Review** the methodology your provider will use. It must be based on industry best practices and include automated and manual testing methods.
- **Ask** your provider for sample reports. Assess whether the reports are clear, easy to understand, and contain risk-prioritised recommendations.
- **Ensure** your provider offers retesting to verify your remediation efforts. Retesting is critical in the continuous penetration testing process.

PENETRATION TESTING BEST PRACTICES

2024 / 2025 EBOOK EDITION

To achieve maximum effectiveness and benefits of penetration testing, organisations must follow a set of **best practises**. These best practises cover various aspects of the penetration testing process, from scoping and planning to execution, analysis, and remediation. Below is an overview of the key best practises that organisations should consider when conducting penetration tests to strengthen their cyber security and effectively mitigate risk. By following these best practises, organisations can ensure comprehensive coverage of their digital infrastructure.

- **Comprehensive Test Coverage:** Assessing networks, applications, endpoints, and cloud environments to identify potential vulnerabilities across the entire attack surface to provide a holistic view of security posture.

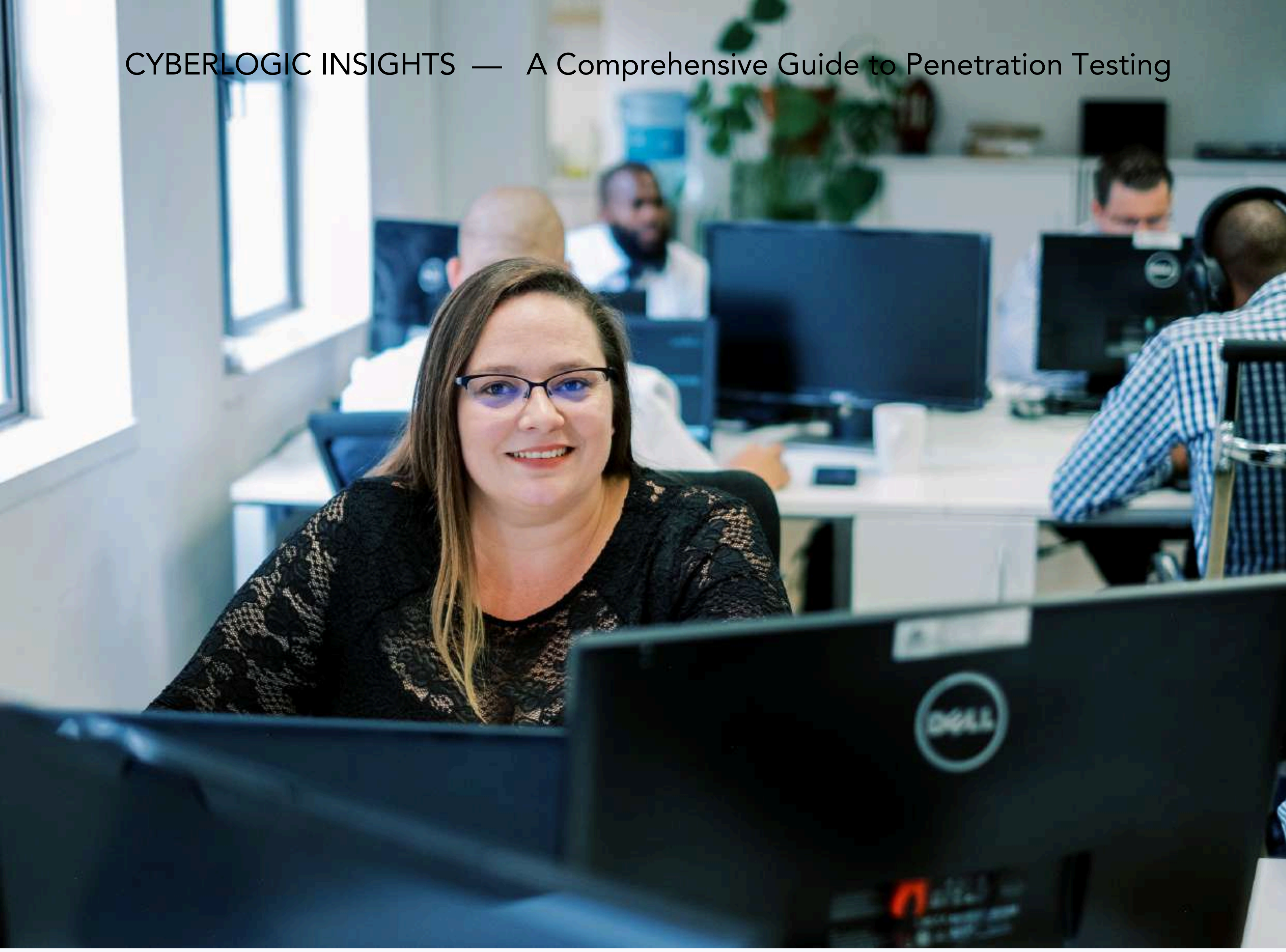
- **Regular Testing Cadence:** Establishing a regular cadence for conducting penetration tests to help identify and remediate vulnerabilities in a timely manner, reducing the risk of successful cyber-attacks and maintaining a proactive approach to cyber security.

- **Collaboration with IT and Security Teams:** Fostering collaboration between IT, security, and business teams throughout the penetration testing process is critical. Aligning test objectives with business goals, effectively implementing security controls, and prioritising remediation based on business impact will ensure a unified approach to improving the security posture.

- **Continuous Improvement and Remediation:** Penetration testing is a continuous journey of improvement and enhancement, not a one-time event. Implementing remediation recommendations based on risk prioritisation and establishing a feedback loop for continuous improvement ensures organisations stay one step ahead of cyber threats.

- **Incorporation of Threat Intelligence:** Using threat intelligence sources to inform penetration testing and prioritise testing efforts based on known threats and vulnerabilities is essential to enhancing the realism and effectiveness of pen testing scenarios.

- **Engagement with External Security Experts:** Engaging external security experts or third-party penetration testing providers can supplement internal capabilities and bring additional expertise to the testing process. External experts provide independent validation of security controls and offer insights into new threats and best practises.



QUESTIONS TO ASK YOUR PROSPECTIVE SECURITY PROVIDER

To ensure that you partner with a provider that is able to deliver comprehensive and effective testing services, it is important to ask the right questions. The following list of questions is designed to help you evaluate potential penetration testing providers thoroughly. From inquiring about the company's core offerings and certifications to understanding the team composition, testing methodologies, and approach to delivering results, these questions will allow you to make an informed decision and select a provider that meets your specific needs and requirements. Asking these questions will give you valuable insight into the provider's capabilities, expertise, and commitment to effectively protecting your organisation's digital assets.

ABOUT THE SECURITY PROVIDER

□ Is penetration testing part of your core offering?
□ Do you hold a professional liability insurance?
□ How do you stay up to date with the latest cyber security threats?
□ Do you hold any organisational certifications, such as ISO 9001 or SOC 2?
□ How many penetration testing projects do you conduct annually?
□ What measures are used to protect your client’s information?
□ Do you have a Penetration Testing as a Service (PtaaS) offering?
□ How is our data stored and secured?

ABOUT THEIR TEAM

□ Which team members would be assigned to our project?
□ Are your projects subcontracted? If so, how do you ensure the security of our information?
□ Which certifications do your specialists hold?
□ Do you have experience in my industry?

ABOUT THEIR PROCESS

□ Which penetration testing methodologies do you use?
□ What percentage of the test is automated vs. manual?
□ How will you protect my testing results during and after the tests?
□ How will you ensure the availability of my systems or services during the test?
□ Do you make a distinction between network and application testing?

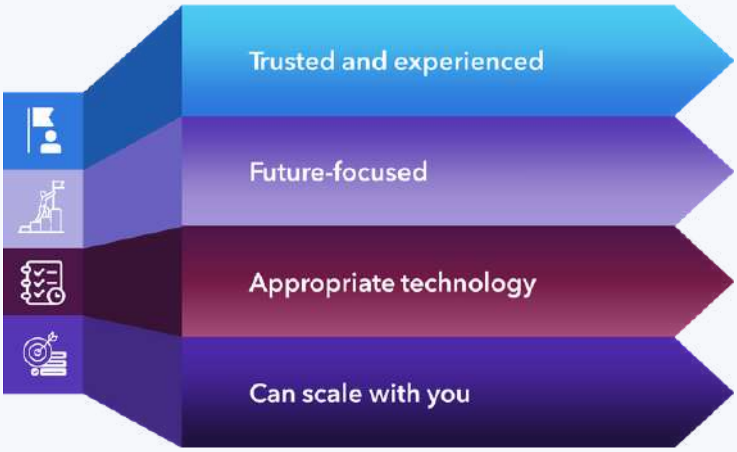
ABOUT THE RESULTS

□ What is covered by your report?
□ Do you have any sample reports available?
□ How do you ensure the consistency of your deliverables?
□ Will you help me fix my identified vulnerabilities?
□ Are retests of identified vulnerabilities included in the project scope and cost?

CYBERLOGIC CYBER SECURITY SOLUTIONS

AT CYBERLOGIC, OUR JUST CAUSE IS ENABLING DIGITAL TRANSFORMATION THROUGH DELIVERING UNQUESTIONABLE VALUE

We invest heavily in training, coaching and in our Go4Growth culture to ensure we build a high- performance team that focuses on DELIVERY.



Trusted and experienced

Our core capabilities are in **IT leadership, cyber security, and cloud.** We have almost **three decades of experience** in infrastructure and support services and a **breadth of knowledge across various technologies and industries**.

Future-focused

We work with **Gartner** to ensure our services are **industry leading** and can **evolve as the technology landscape changes**.

Appropriate technology

We are **technology agnostic** and believe in using only the best and most appropriate solution for the problem. We both a **Microsoft Tier 1 Direct Cloud Solutions Partner and a Dell Gold Partne**r.

Can scale with you

We have a proven **ability to work with large businesses** of more than 2000 people and have experience in onboarding clients who have outgrown their existing Managed Service Providers

Our Secured Service is for organisations who place a high priority on protecting their data and IT assets. The service intends to reduce the attack surface for cyber-criminal activity by taking an inside-out and outside-in perspective on security.

The service includes traditional managed services which focuses on core infrastructure management as well as active penetration testing. Vulnerabilities are scanned and reported on with recommendations on remediation.

Infrastructure
Advanced monthly patching with third party applications. Managed workload Antivirus with threat protection. Cloud storage of backups for Servers and Office 365.

Vulnerability Management
Active scanning for vulnerabilities will be reported and logged across the landscape. Agents deployed on all endpoints and a central network scanner will be deployed.

Threat Protection
Best practice approach for the back-up of information and systems.

End Point Protection
Raising IT risks and working together to mitigate risks and impact to the business.

Reporting & Remediation
Reporting and priority management of the landscape with the IT portfolio owner.

At Cyberlogic, we offer a comprehensive suite of cyber security solutions, which includes penetration testing, vulnerability management, and remediation solutions. To find out more, visit the Security Solutions page on our website or reach out to us at hello@cyberlogic.co.za.

READY TO TALK ABOUT YOUR SECURITY NEEDS?

CONTACT US