SERVICE CATALOGUE

COGNISYS
Smarter Cyber Security

CONTENTS

Company Overview	2
Internal Penetration Testing	4
External Penetration Testing	6
Web Application Security Testing	8
Mobile Application Security Testing	10
Cyber Security Review	12
Red Team Exercise	14
Phishing Simulation	16
Dark Web Monitoring	18
Lost or Stolen Device Assessment	20
Wireless Security Assessment	22
Cloud Security Assessment	24
Microsoft 365 Tenant Review	26
Attack Path Analysis	28
OSINT Analysis	30
Cyber Essentials	32
Governance & Compliance	34
Virtual CISO	36
Managed Security	38
SmartScan	40
SmartView	42

COMPANY OVERVIEW

Cognisys Group is an expert cyber security company, specialising in penetration testing. We protect businesses from attack by showing them the weaknesses in their defences.

Our team of experienced consultants deliver point in time assessments and, leveraging SmartView (our innovative client portal), are able to provide ongoing vulnerability management.

As part of our mission to improve the security of every company we work with, we also support organisations in achieving compliance, through standards such as ISO27001 and Cyber Essentials, as well as via our vCISO and Governance team.

OUR MISSION:

to improve cyber security in every organisation we touch.

Our people are our greatest strength, and we value their skill, intelligence and the difference they make to our clients.

We actively develop our team through funded accreditation, training and learning.

We encourage everyone to uphold our values, emphasising empathy, equality and respect.

OUR VALUES

INTEGRITY

We strive each day to do the right thing in any given situation. Our team work with integrity and honesty, ensuring clients receive an excellent level of service.

INTELLIGENCE

Customers value our knowledge, experience, and intellectual capabilities, which is why we allow time and budget for our whole team to up-skill throughout the year.

EMPATHY

We recognise and understand the challenges of others on a technical, commercial, and personal level. We appreciate other perspectives, which helps us to grow and learn ourselves.

Internal Penetration Testing

It takes the average company 280 days to realise an attacker is in their network.

Do you know how far an attacker could get within your environment in that time?

Internal Infrastructure Testing is an integral part of any organisation's security strategy, assessing how misconfigurations or vulnerabilities within your internal network, both on premise and in the cloud, could be exploited by an attacker who has insider access to your environment.

Working to an agreed scope, our consultants attempt to compromise hosts, including Active Directory, Windows & Linux servers, and database servers, using non-destructive attack methods. Where possible, this may lead to the exfiltration of data.

The outcome of an internal infrastructure test is a list of confirmed vulnerabilities within the specified hosts and a solid remediation plan for mitigating the risks.

The testing aims to highlight vulnerabilities and misconfigurations of systems, which can lead to privilege escalation, theft of data, and even the ability to gain a persistent foothold within the network.

Although methods used will vary for each engagement, dependent on the services in use and the client's appetite for risk, we follow a similar methodology in each project. Initially, our consultants run vulnerability scans to quickly highlight potential risks. They then manually investigate issues, which leads to the exploitation of vulnerabilities and the eventual compromise of the host or system where possible.

As part of the engagement, our consultants provide risk ratings for each vulnerability based on the ease of exploitation and the potential impact should the exploit be used. This helps you to prioritise your remediation efforts, and manage your risks accordingly.

Given that every environment is constructed slightly differently, all of our internal infrastructure penetration tests are tailored to your specific requirements.

Following the delivery of the report, we recommend a follow-up call to run through the findings and ensure that remediation advice is clear. This also allows your team to ask any further questions and clarify any areas of uncertainty.

ANALYSIS AND POTENTIAL EXPLOITATION

This testing is designed to assess security posture against best practices and attempts are made, where safe and permitted, to exploit any vulnerabilities discovered. This may involve escalating privileges if possible, accessing key systems and ultimately exfiltrating confidential data if practical.

OVERVIEW

The following can be included within the assessment:

- Host discovery & port scanning.
- Vulnerability assessment.
- Manual identification and fingerprinting of services.
- Privilege escalation attempts.
- Password evaluation.
- VLAN assessments.
- Analysis of VOIP services.
- Network mapping.
- Exfiltration of data.

The hosts are scanned, with exposed services being assessed using a combination of manual and automated techniques. This includes a vulnerability assessment of all exposed hosts and their services.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

External Penetration Testing

In an increasingly connected world, our internet-facing systems are critical to the running of our businesses, and they're often the first port of call for a malicious actor.

Regular testing of your external infrastructure, to highlight vulnerabilities that can be exploited, is an essential security measure.

Testing attempts to discover and expose system weaknesses within a specific brief, focused on web-facing technology such as firewalls, remote access gateways, and web servers.

Working with a strict scope, our consultants attempt to compromise specified hosts using non-destructive attack methods to gain entry to the network, escalate privileges and exfiltrate data where security weaknesses permit.

External infrastructure testing aims to highlight vulnerabilities and misconfigurations of systems which could allow for access into the supporting network.

Although the method for each test may vary, the goal is ultimately the same- to assess the organisation's security posture and understand how a threat actor could gain unauthorised access via exposed services.

Our consultants report on the technical vulnerabilities and provide guidance on activities to remediate, helping you to reduce the risk posed to your business and limit the likelihood of an attack.

Following the delivery of the report, the team are on hand for a follow-up call to clarify any areas of uncertainty.

ANALYSIS AND POTENTIAL EXPLOITATION

This testing is designed to assess security posture against best practices. Where permitted, attempts are made to safely exploit any vulnerabilities discovered.

OVERVIEW

The following is typically included within the assessment:

- Host discovery & port scanning.
- Open-Source Intelligence (OSINT) gathering.
- Fingerprinting of services.
- TLS/SSL analysis.
- Identify security misconfiguration.
- Exfiltration of vulnerabilities.

Following a vulnerability scan, the exposed services are further assessed for issues. Manual exploitation of weaknesses occurs where it is safe and practical to do so, and the consultant documents their findings.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

Web Application Security Testing

The internet means we're more connected than ever. It also means that we're exposed to more risk. How secure are your web applications?

Undergoing an app security test against any bespoke applications within your environment, including your website, e-commerce platform, or CRM solution, can help you to identify vulnerabilities that could lead to a data breach.

Our team provide a comprehensive assessments of the risks associated with your applications, ensuring that you have the knowledge you need to make tangible improvements in your security posture.

Using a combination of manual and automated techniques and tools, your application is assessed for vulnerabilities. Where it is permitted and safe to do so, we may exploit these vulnerabilities to understand the full scope of the potential risk.

These findings are verified to make sure no false positives are reported. No exploitation of vulnerabilities will be conducted without authorisation from the client.

OUR APPROACH

We follow accepted industry standards for testing both web applications and API interfaces. Leveraging methodologies from Open Web Application Security Project (OWASP), we ensure that your application is put to the test against a list of the most common attack vectors.

Any vulnerabilities found will be manually assessed and exploited where it is safe to do so. This allows us to verify our findings, removes the chance of reporting false positive results, and ensures the integrity of our assessment.

Our consultants provide recommended activities for remediation, which helps you to become more securely more quickly. We're also on hand following the delivery of the report for a debrief call to clarify any areas of uncertainty.

OVERVIEW

The following can be included within the application assessment:

- Web server configuration.
- Cryptography and communication mechanisms.
- Authentication and authorisation.
- Session management.
- Input and output validation.
- Business logic.
- Data storage security.

Applications are evaluated with manual walkthroughs designed to identify functionality and key areas of focus.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

Mobile Application Security Testing

More than half of the world's web traffic now comes from mobile devices. Ensure your mobile apps are secure.

As smartphone and tablet use increases, as does our use of mobile applications. With over 25% of apps containing at least one high-risk vulnerability, security testing is more important than ever.

Flaws within mobile apps can cause issues not only for the individuals using them, but also for application owners or developers too. Data exfiltration is a key concern, which could have a knock on effect on your organisation's finances and reputation.

Reference: https://cybersecurity.asee.co/blog/mobile-app-statistics-to-keep-an-eye-on/

METHODOLOGY

We categorise mobile applications into two areas:

- Web services/API based applications, which are responsive to compatible interfaces.
- Native applications which are developed for a specific platform i.e. iOS and Android.

Our assessment includes both the client and server elements used by the mobile app, in accordance with the OWASP mobile assessment framework.

For web service / API assessment, we perform a web application penetration test, in line with the OWASP application testing standard.

Our testing team also analyse the network communication protocols to ensure they follow best practices regarding the confidentiality and integrity of data in transit.

We identify the web service endpoints and assess privilege escalation opportunities, error handling problems, injection flaws, broken access controls, and other web application threats.

The application is further analysed to determine what information is stored locally on the device and could be recovered from a stolen device or malicious third-party applications.

The subsequent review of cached information checks for sensitive data in clear text, as insecure local storage is a concern if the device is lost or stolen.

Reverse engineering the application helps identify any sensitive information such as encryption keys, hard-coded database credentials, server IP addresses, or default credentials left behind by the developers within the binary.

The final deliverable contains detailed recommendations to help developers remediate the issues identified during the assessment. Where a problem cannot be quickly remediated, mitigation strategies will be presented, depending on the environment where the application is implemented.

OVERVIEW

Testing typically covers:

- Static analysis.
- Network Traffic Analysis.
- Authentication and Authorisation review.
- Tampering and Reverse Engineering.
- Storage Mechanism.
- Web Service / API Analysis.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

Cyber Security Review

Let us help you identify and recognise risk across your organisation’s people, processes and technology.

A comprehensive audit can help you to check that your information security controls are operational and effective, and build a roadmap for improvements to strengthen your security posture.

Undertaking a review will provide your organisation with an independent third-party assessment of your current state and our experts are there to help you develop a strategy to increased maturity in the future.

OVERVIEW

The following areas are included within the assessment:

- Security controls.
- Key cyber assets.
- Business continuity.
- Responsibilities and roles.
- Incident management.
- Staff awareness and current training.
- Risk register.
- Policies.
- Cyber risk governance.
- Any contractual, legal or regulatory obligations.

THE TECHNICAL AREAS

- How you monitor security.
- Your access controls.
- Perimeter controls – firewalls, IDS, IPS Proxy.
- What anti-malware is in place.
- An overview of user privileges.
- We review IT core infrastructure devices and sample endpoints.
- Data classification.
- Mobile Device Management (MDM), Multi-Factor Authenticator (MFA), and mobile working.

THE PHYSICAL AREAS

- How safe your perimeter is.
- Designated secure areas.
- The physical security of your IT systems.
- Any 3rd party access or policies.

WHY HAVE A CYBER SECURITY REVIEW?

Our cyber reviews give you a 360 degree view of your current state, providing objective guidance on the risk inherent in your business.

Reviews are non-intrusive, meaning that the day-to-day running of the business can continue, while we interview and discuss various areas of security with your team.

Creating a security baseline and targets for improvement means you have an actionable plan which can then be tracked and measured to provide you with attainable goals for improved maturity. .

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

Red Team Exercise

Test the true strength of your defences, technology, people and processes, by simulating the actions of a cyber attacker.

Penetration testing is a valuable part of your cyber security defences, however a Red Team Exercise goes a step further. Our exercises can test the full spectrum of organisation policies, processes, and technology defences.

Significantly more sophisticated than penetration testing, our cyber attack simulation accurately mimics advanced, covert, multi-phase attacks which occur in the real-world.

After agreeing specific targets, our ethical hacking team execute a program for achieving the compromise, which can include elements from a full scope of blended attacks, selected to give the best chance of a successful outcome.

TECHNICAL ELEMENTS

Once the targets and scope have been agreed, the service can include:-

- Open Source Intelligence (OSINT) gathering.
- Building, organisation, network, physical controls and system reconnaissance.
- Manual testing using the tactics, techniques and processes of a malicious actor.
- Attempted physical breach of the organisation's premises.
- Human targeting through social engineering.
- Hardware vulnerability exploitation.
- Wi-Fi network intrusion.
- Signal vulnerability exploitation e.g. RFID door-pass cloning.
- Business application exploitation.
- Zero-Day hunting and exploit development.
- Pivoting using compromised hosts for lateral movement through the network.
- Data insertion and exfiltration.
- Establish post-exploitation persistence.

Typical outputs include: results of reconnaissance, attack vectors chosen, attack methods, attack payloads used, attack results, short and long term mitigations, plus remediation.

KEY BENEFITS

- Improve your security posture. Go beyond typical pen testing to gain a deeper understanding of your likely attack vectors.
- Verify your security controls. Tests are against technology and employees, revealing your ability to detect and respond to attacks.
- Prioritise your risks. Understanding the most critical security issues to prioritise your remediation efforts.
- Reduce your risk. Modelling our exercise on real hacker behaviours provides greater visibility into your organisation's weaknesses.
- Achieve greater defensive agility. Use the outcomes to reduce the probability of a successful attack.

We're proud of our Red Team, which is made up of some of the most qualified people in the industry.

Our technical ability combined with our deep understanding of the techniques used by cyber criminals allows us to deliver a valuable service to protect you and your organisation.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

Phishing Simulation

How susceptible are you to phishing? Try a simulated attack and find out.

Cognisys can perform simulated phishing to determine the susceptibility of your people to this type of cyber risk.

Working with you to devise a range of scenarios, we will build a series of personalised phishing emails to target specific groups within your organisation.

Typically, the emails will invite recipients to take certain actions, such as giving away sensitive information or downloading malicious payloads allowing unathorised access to your environment.

Sophisticated to simple phishing tests are carried out to determine the security awareness of your employees and understand the strength of your security culture.

PHISHING, SPEAR-PHISHING AND WHALING

Phishing generally targets organisations or individuals at random, whereas spear-phishing is more focused on specific individuals. Whaling is a term describing the targeting of high-ranking executives in an organisation.

In the case of whaling and phishing, all employees, and not just high-level executives, should be trained about these attacks and how to identify them.

Preventing cybersecurity threat requires all employees to take responsibility for protecting the organisation's assets.

METHOD

The goal of a simulated phishing attack is to trick an individual into disclosing personal or corporate information through social engineering, email spoofing and content spoofing efforts.

For example, we may send the victim an email that appears to be from a trusted source, including links back to a customised malicious website that has been created especially for the attack.

Our emails and websites can be highly personalised and customised, incorporating the target's name, job title or other relevant information.

IDENTIFY

- Creation of easy, medium and difficult templates, so as to scale training.
- Identify existing security awareness.
- Training can be built-in to landing pages.

REMEDIATE

- Understand how to better defend your organisation using a layered defence approach.
- Provide cyber security awareness training for your employees.
- Build an effective cyber threat reporting culture, with a 'no-blame' approach for maximum uptake, throughout your organisation.

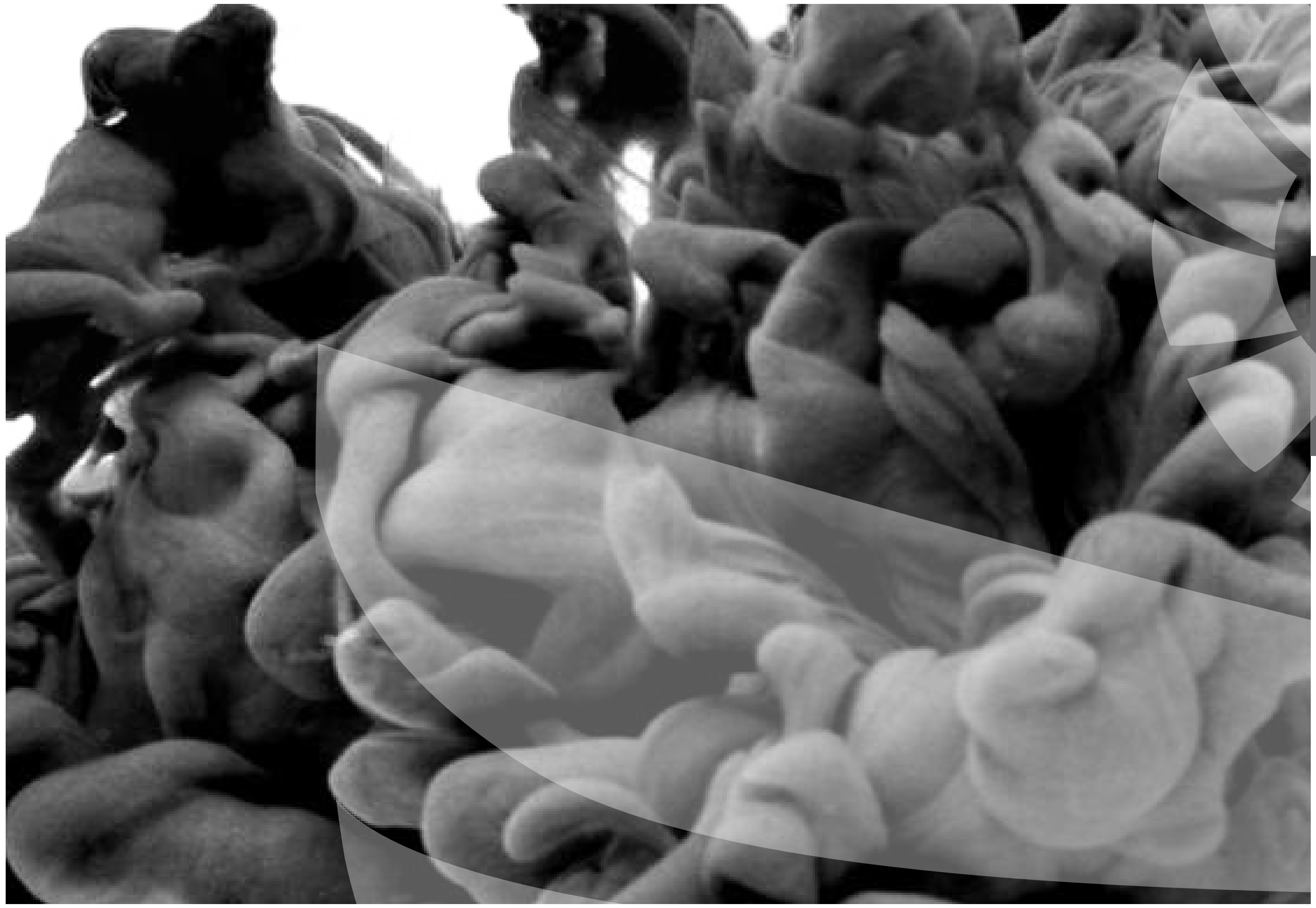
BENEFITS

- Quickly discover the status of internal security awareness.
- Discover which employees would benefit most from cybersecurity awareness training.
- We work alongside your team to raise awareness and increase cyber security maturity.

REPORT

Reports are provided, following each campaign, detailing the interaction levels and full metrics. All findings are delivered in a comprehensive yet simple report format.

BE SMART. BE SAFE. BE SECURE.



Dark Web Monitoring

We go into the dark web so you don’t have to.

Digital credentials such as usernames and passwords connect you and your employees to critical business applications and online services.

Unfortunately, criminals know this and that’s why digital credentials are among the most valuable assets found on the dark web.

Our dark web monitoring service detects compromised credentials in real-time on the dark web, notifying you immediately when your critical assets are discovered and allowing you to take action before your data is used against you.

Far too often, companies that have had their credentials compromised and sold on the dark web don’t know about it until they have suffered a costly cyber attack, but by then, it’s too late.

WHAT IS THE DARK WEB?

The dark web is made up of digital communities that sit underneath the internet. While there are legitimate purposes, it is estimated that over 50% of this type of site is used for criminal activities.

Sometimes referred to as the ‘underbelly of the internet,’ the dark web is a shrouded area, hidden from search engines and only accessible with a specialised web browser. It also masks IP addresses, which essentially allows fraudsters to operate undetected to commit crimes, including identity theft.

WHY WE’RE ALL VULNERABLE

Passwords are a 20th century solution to a 21st century problem. Unfortunately usernames and passwords, the most common digital credentials used today, are often all that stand between your employees and vital online services. This includes private networks, social media sites and e-commerce sites amongst many others.

Good security practice is to use a completely different password for every service, but the fact is that according to a survey conducted by Google nearly 65% of users replicate the same or very similar passwords for each service they use.

To make things worse, many employees use corporate email for personal use, often breaching IT Policy and compromising personal privacy and workplace security.

HOW TO PROTECT YOURSELF

There is no single solution that can protect against all possible attack vectors. However, you can take steps to mitigate the most common forms of attack. Statistically, these attacks are most likely to leverage passwords compromised on the dark web or leaked due to human error, often a result of phishing attacks or a lack of awareness around security best practices.

HOW DOES THE SERVICE WORK?

Our platform connects to thousands of dark web services, including Tor, I2P, Freenet, hidden chat rooms, ID theft forums, hacking sites, and C2 Servers. It searches for compromised credentials, without requiring you to connect to these high-risk services directly.

The platform is looking for breaches of your data 24/7/365 days and we can provide you with awareness of compromised credentials in real-time often before identity theft or data breaches can occur.

For a no-obligation free live scan, a demonstration of how the service works and to understand which of your company credentials may already be on the dark web, please contact us.

BE SMART. BE SAFE. BE SECURE.

Lost or Stolen Device Assessment

Mobile devices have proliferated since the start of the pandemic. Ensure you're not introducing additional risk alongside improved mobility.

When these devices are lost or stolen, it is vital that this cannot present a risk of data loss or unauthorised access to your network and data.

This service is a test to determine how much information can be gained from a lost device.

This ranges from almost nothing, which is unusual for laptops in particular, right up to all the information held locally, including details to achieve remote access to a company's internal infrastructure.

A Lost or Stolen Device Assessment is usually based on everything in a typical laptop bag, including all the information that would be found alongside the laptop.

The scope is something that can be discussed over a review call and tailored to each client's requirements.

The best test is to simulate a real-world scenario, rather than to analyse a laptop that has been separated from its owner, had its post-it notes removed, notebooks retained and anything else which would aid an attacker in trying to gain access to the device, network and data.

Smartphones and tablets usually present less risk than a laptop if properly secured but Cognisys check that the right configurations are in place.

ANALYSIS AND EXPLOITATION

The assessment commences, analysing the findings and attempts made, where safe and permitted, to exploit any vulnerabilities discovered.

If access is gained to the device, attempts may be made to access key systems on the internal network, over a VPN or any other discovered remote access gateway, using stored credentials.

OVERVIEW

The following are assessed in this exercise:

- Insecure storage or recording of passwords.
- Cached or unlocked credentials.
- Missing security patches.
- Boot process analysis.
- Device/disk encryption.
- Password brute force attack/weak password policies.
- Sensitive data disclosure.
- Information leakage.
- Local security policy circumvention.
- Multi-Factor Authentication (MFA).
- Mobile Device Management (MDM).

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

Wireless Security Assessment

Extending the scope of your testing to include any wireless networks is crucial. Hackers generally regard wireless as an ideal route into your systems.

The convenience and accessibility of wireless technology makes it an integral part of business today. No cords or cables, just radio waves between the device of your choice and the target data.

Wireless technology is unfortunately yet another attack vector which can be compromised and used for a malicious attack if not properly secured.

Is your network properly segmented from the public access network you give to guests and clients? How easy is it to compromise your network whilst sitting outside in the car park?

Wireless networks are often the primary method by which end-user devices access organisational data. It is therefore more important than ever to ensure the deployment and configuration of these networks is as secure as possible.

From flawed encryption schemes to badly configured networks, there is plenty for a malicious user to try and exploit.

Our wireless security assessments encompass all aspects of wireless infrastructure deployments and aim to uncover weaknesses that an attacker may leverage to remotely gain a foothold into the internal network.

METHOD

The assessment generally commences with reconnaissance to identify wireless networks, protocols used and technologies in use by the client, plus any other broadcast sources in the immediate vicinity, inside and immediately outside the premises.

Cognisys’ multi-faceted approach to wireless security testing assesses deployments against security best practices and can help ensure organisations adequately protect critical assets, whilst providing staff, contractors and guests the key flexibility that wireless offers.

OVERVIEW

The engagement is tailored to the client's particular topology and configuration and covers the following:

- Wireless security analysis of the premises.
- Identification of broadcast Service Set Identifiers (SSIDs).
- Identification of rogue/unauthorised wireless networks.
- Analysis of protocols and cryptography in use.
- Suitability review of authentication schema.
- Wireless radio configuration review.
- Network segregation testing.
- Analysis of wireless client protection mechanisms.
- Pre-Shared Key strength analysis including cracking exercises.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

Cloud Security Assessment

Uncover security vulnerabilities to ensure your public cloud deployments are secure and compliant.

As you move your workloads and services into the public cloud, you need to protect them. You may wish to take advantage of the cost and development benefits afforded by migrating from on-premise to public cloud environments, but securing these must be a key part of your considerations.

Our cloud security consultants can deliver cloud assessments for the following models:

- Infrastructure as a Service (IaaS).
- Platform as a Service (PaaS).

This helps you identify the risks to be minimised and protect your critical assets in the cloud.

INDEPENDENT VERIFICATION

Contrary to popular belief, it is not the responsibility of the cloud services provider (e.g. Microsoft, Amazon, Google) to implement and configure appropriate security controls within specific client environments.

MSPs often build functional environments which lack the required controls to properly secure your data. Gaining independent verification is a great way make sure you've identified any potential areas of risk.

An objective assessment of the configuration of your environment can highlight areas for improvement and help you to improve the security of your cloud assets

MINIMISE YOUR ATTACK SURFACE

With the myriad of security controls available across cloud platforms, it can often be confusing as to which is relevant for your business.

Let our team put the hard work in, so you don't have to. Using industry best practice and standards from the Center for Internet Security, our consultants review your configurations and prescribe the best course of action for minimising your attack surface in the cloud.

ONE STEP FURTHER

Our consultants can perform a basic configuration review of your cloud environment, however if this is an area of particular concern, we can go one step further.

A lot of organisations like to know the extent to which a vulnerability or misconfiguration could be exploited, and our team of experienced penetration testers are on hand to do just that.

Using the information obtained in the initial audit, as well as knowledge of common attack vectors for cloud environments, our team can attempt to safely exploit vulnerabilities to highlight the extent of the security risk.

PENETRATION TESTING/CONFIGURATION REVIEW

Testing is designed to uncover security flaws and weaknesses on systems hosted on cloud platforms, including:

- Amazon Web Services (AWS) .
- Microsoft Azure.
- Google Cloud Platform (GCP).

While the cloud providers platform, underpinning your solution is always outside our remit, it is our job to ensure that the platform configuration, application code, or any assets deployed within this environment, do not present security risks.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

Microsoft 365 Tenant Review

Microsoft 365 has become the platform of choice for organisations to share and store critical data.

Microsoft cloud services are built on a foundation of trust and security. Microsoft provides security controls and capabilities to help you protect your data and applications, however, these controls are often misconfigured or overlooked.

You also have the responsibility for protecting your own identities and corporate data. This includes the security of your on-premise resources and extends to the security of cloud components you control within Microsoft 365.

ANY FLAVOUR EXCEPT VANILLA

Sometimes, Microsoft 365 settings are left at default and in many cases left dangerously insecure, often by following a ‘vanilla’ MSP installation or without due security consideration during deployment.

Consequently, attackers are taking advantage of these poor deployments with alarming regularity. Malicious actors will commonly use phishing campaigns and leverage configuration weaknesses to maintain unauthorised access and exfiltrate data without detection.

MFA EVERYTHING

We recommend using Multi-Factor Authentication (MFA), Mobile Device Management (MDM), Azure Information Protection (AIP), Microsoft Information Protection (MIP) and we assess the risk of not using Data Loss Prevention (DLP).

MEASURE IT

The current configuration is correlated and analysed against Cognisys’ bespoke specification, based on Microsoft’s Secure Score and recommended best practices.

Appropriate recommendations can then be extrapolated. Our review aims to highlight the issues that allow attacks, breaches or losses to occur.

KEY BENEFITS

Tailored to your organisation and where appropriate, we undertake a review of the following areas:

- Authorisation and Access Management.
- Conditional Access Policies.
- Multi-Factor Authentication (MFA).
- Mobile Device Management (MDM).
- Azure Information Protection (AIP).
- Microsoft Information Protection (MIP).
- Application Protection Policies.
- Audit Logging.
- Document and Email Protection.
- Identity Protection.
- Detection and investigation of security incidents.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

Attack Path Management

Active Directory and Azure Active Directory are hot targets for threat actors.

In a world where identities are the new security perimeter, compromising identity platforms like AD and AAD provides the greatest payoff for attackers, ultimately giving them control of all users, systems and data within the organisation.

Misconfigurations in these services can create 'Attack Paths', or chains of abusable privileges and user behaviours, which can provide attackers with a route to sensitive data and / or administrator access.

The primary goal of our Attack Path Management service is to provide a way of highlighting potential vulnerabilities in identity services, which in turn will allow organisations to mitigate the associated risks.

Organisations often don't have properly defined identity management processes in place, which means that users and devices can end up accumulating unnecessary access permissions.

Using our Attack Path Management (APM) service, organisations can chart relationships and connections within Active Directory and Azure Active Directory to gain a comprehensive understanding of the permissions given to individual objects, computers, and users. We also assess the impact that specific privileges have on overall security posture.

METHOD

Our APM toolset is non-invasive, meaning we can run the assessment without interrupting any normal activities. Our aim is to discover attack paths towards domain administrator privileges.

We can tailor the service to identify methods of access to areas containing sensitive data and methods to access sensitive applications, including:

- Scoping to understand exact requirements.
- Analysis of AD and AAD environment including:
  - Users, groups, devices and properties.
  - Security groups and domain trusts.
  - Abusable rights on AD objects.
  - Group Policies and OU structure.
  - SQL admin links, active sessions and privileges.
- Vulnerabilities and misconfigurations.

As a result of the analysis, you will gain a thorough understanding your identity environment including misconfigurations, credentials and user activities, which attackers can combine to create attack paths. This allows you to foresee an attack, and mitigate against it, before it happens.

OVERVIEW

Key benefits:

- Comprehensive mapping of relationships and connections within Active Directory and Azure Active Directory.
- Empirical, or practical, measurement of the impact that particular privileges have on the security posture of your organisation, systems and network.
- Precise and safe remediation advice.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

OSINT Analysis

Personal data is the perfect starting point for cyber criminals.

Open-Source Intelligence (OSINT) gathers information from published or otherwise publicly available sources. Identifying unintentional leakage of sensitive data through social media networks and other platforms can help you plug the leaks and make it as difficult as possible for potential attackers.

The OSINT Analysis service demonstrates how much information a threat actor can find about an organisation quickly and easily online, without ever touching your system or running any scans.

Information discovered may include exposed data, breached work email credentials, personal staff data and other useful identity information.

Your public data footprint is probably much bigger than you think.
You can access electoral registers and telephone numbers through a regular web browser.
Companies House stores company data, including officers' data. Company websites often display hierarchical team structures. Platforms such as Facebook, Instagram, LinkedIn, TikTok and Twitter hold personal data on individuals, including friends, interests, hobbies, activities, pictures and events.

NOT HACKING, JUST LOOKING

It is not uncommon for threat actors to use open-source intelligence tools and techniques to discover potential targets and exploit weaknesses in networks. As soon as a vulnerability or a weakness is identified, it can be used to accomplish a breach.

OSINT is often initial reconnaissance for sophisticated social engineering campaigns using smshing, spear-phishing, whaling and vishing against a target. Social engineering campaigns use seemingly innocuous information shared in social networks or blogs to develop compelling campaigns and trick people into compromising their organisation.

The importance of OSINT Analysis becomes apparent when it uncovers weaknesses in your organisation's user network and helps you to remove sensitive information before it's used for exploitation.

METHOD

Using our OSINT Framework, the scope can be tailored to each organisation according to specific requirements. Searches utilise specialist tools to uncover the maximum results. Analysis typically includes:

- Search of the dark web for personal and company data.
- Search of social platforms including imagery.
- Assess common TLS/SSL issues.
- Search of the organisation's digital footprint for information and metadata.
- Web search for names, emails, addresses and phone numbers of staff.
- Search of DNS records and ensure they are configured correctly.
- Attempt to discover technologies used, e.g., on the website or infrastructure, which would provide a threat actor with useful information.
- Check for suspicious behaviour of the domain, website, and IP.

REPORT

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BE SMART. BE SAFE. BE SECURE.

Cyber Essentials Plus

Designed to help organisations of any size demonstrate their commitment to cyber security – while keeping the approach simple and the costs low.

THE REQUIREMENTS

Cyber Essentials Plus is an audited assessment, of your systems, and cyber security controls. The 5 controls examined are:

- Access control.
- Firewalls.
- Secure configuration.
- Patch management.
- Malware protection

Certification is only achieved when the essential levels of protection are assessed and passed by an independent IASME Certification Body such as Cognisys.

WHY GET CYBER ESSENTIALS?

Cyber Essentials helps you to guard against the most common cyber threats and demonstrates your commitment to cyber security. It enables your organisation to:

- Reassure customers that you are working to secure your IT against cyber attack
- Attract new business with the promise you have cyber security measures in place
- Ensure you have a clear picture of your organisation’s cyber security level
- Bid for government contracts which require Cyber Essentials certification

WHY USE COGNISYS?

Some of the Cyber Essentials self-assessment questions can be difficult to understand if you do not have a technical IT background or you have a complex company structure.

IASME has certified that Cognisys are able to help you understand the assessment questions, how they relate to your company and what steps you need to take in order to achieve certification.

Our experienced team helps you plot a route to success and work with you side by side to make sure your accreditation process is as simple as possible.

We provide all the expertise, guidance and knowledge to give you the very best chance of achieving the standard and all our consultants are qualified cyber security practitioners.

FOLLOWING ON FROM YOUR CERTIFICATION

Once you have achieved Cyber Essentials Plus, You’ll receive a certificate, which can be used to prove that you have essential Cyber security defences in place. You’ll also recieve a Cyber Essentials Plus logo, which can be displayed on your website.

Both of these items provide reassurance for your stakeholders and means that you are free to bid for certain local and national government contracts.

Additionally, Cyber Essentials certificates issued in the previous 12 months are displayed on the NCS and IASME website

Cyber Essentials is an annual process, and it’s vital to choose a partner who can make the recertification easier. Cognisys provides a number of tools, like SmartView, that make subsequent years audits, quicker and simpler.

In addition we have a dedicated internal support team, that can help improve your application process from start to finish.

BE SMART. BE SAFE. BE SECURE.

Governance & Compliance

Governance and compliance have never been more challenging or complex.

Legislation and regulation are becoming more stringent, obliging organisations to manage data securely in a landscape where cyber threat is increasing exponentially, whilst penalties for breach are becoming ever more punitive.

Organisations today manage more data than ever before, so making mistakes with data is almost inevitable. Anyone can make a Subject Access Request (SAR) for data that you may hold, and a data breach can sometimes be catastrophic.

This is why you need expert help to design the right processes, controls and systems to mitigate your risk and achieve the necessary compliance for your organisation. We help you do that and more.

WHY?

Organisations often don't invest in risk governance because it's considered a 'high level' service, only for corporate giants. If that describes you, we strongly suggest you reconsider.

Every public sector organisation has compliance obligations. In the commercial world your accreditations could be a competitive difference. Regardless of sector, size or scale, every organisation has a duty of care to its people, its partners and itself, to manage its data securely and effectively and limit risk.

Governance and compliance are generally linked to scale and complexity. Larger and more complex organisations invariably oblige more effort. Conversely, smaller organisations often find compliance easier to achieve but, in all circumstances, an independent, objective assessment of data, security and controls is an essential stepping-stone towards risk mitigation.

METHOD

Our Governance & Compliance service generally includes:

- Review of existing cyber security governance policies, risk register, security awareness training, audits and frameworks.
- Review of data structures.
- Gap analysis to identify changes required, against industry standards.

Based on the outcomes of the above, our experts help you develop cyber security governance measures including an effective security policy and cyber strategy in line with your requirements.

Cognisys helps you meet your Cyber Essentials, PCI, HIPAA, GLBA, IASME, ISO27001, NIST and other compliance requirements.

OVERVIEW

- Accredited expertise in Governance & Compliance.
- Independent and objective approach.
- Significant cross-sector experience.
- Active involvement in developing and maturing your cyber security posture.
- Multi-disciplinary team including experienced governance auditors and technical experts complementing our strategic consultancy service.
- Continuity of service.

REPORT

Cognisys provides regular reporting via dedicated Account Management, internal support and technical teams, as appropriate.

Additional information is available via our SmartView platform to keep you fully updated at all times.

BE SMART. BE SAFE. BE SECURE.

Virtual CISO

Add the right expertise to your organisation. Improve technical controls and achieve compliance objectives.

Our vCISO service allows you to take advantage of our expert knowledge, without needing to pay for a full-time Chief Information Security Officer.

Our senior staff integrate with your team, to lead, guide and help improve your cybersecurity strategy. Working with existing internal and third-party resources, we develop a programme of works that reduces your operational risk.

In addition, the knowledge and experience of our entire technical team is available, providing:

- A higher level of technical and governance expertise.
- Full support of an experienced cyber team.
- No single point of failure.

INITIAL REVIEW

The starting point is a comprehensive review, to discover the current cyber security status and objectives of your organisation.

A gap analysis is performed, which may include the following areas:

- IT network topology.
- Application estate.
- Security controls.
- Critical assets – hardware, software & data.
- Business continuity.
- Threat identification.
- Cyber security maturity level.
- Incident management processes.
- Roles and responsibilities.
- Capabilities and capacity.
- Third parties.
- Staff awareness training.
- Risk register.
- Policies.
- Cyber risk governance.
- Contractual, legal or regulatory obligations.

The output from this gap analysis typically informs the action plan to address and mitigate risks, then help move the organisation from its existing status, to its desired status.

PROJECT DELIVERY

Once the action plan is agreed, our Virtual CISO will work with your internal staff to implement any changes.

This is designed to improve the cyber security posture of your organisation, through a project with defined time scales, outputs and milestones, including:

- Security strategy - creation or revision.
- Business case and benefit realisation.
- Budget planning, phasing and time scales.
- People.
- Process.
- Technology.
- Training.
- Roles and responsibilities.
- Criteria for success.
- Security framework alignment (if appropriate).

OPERATION AND MONITORING

Following project completion, typically the service moves into the ‘business as usual’ phase, to:

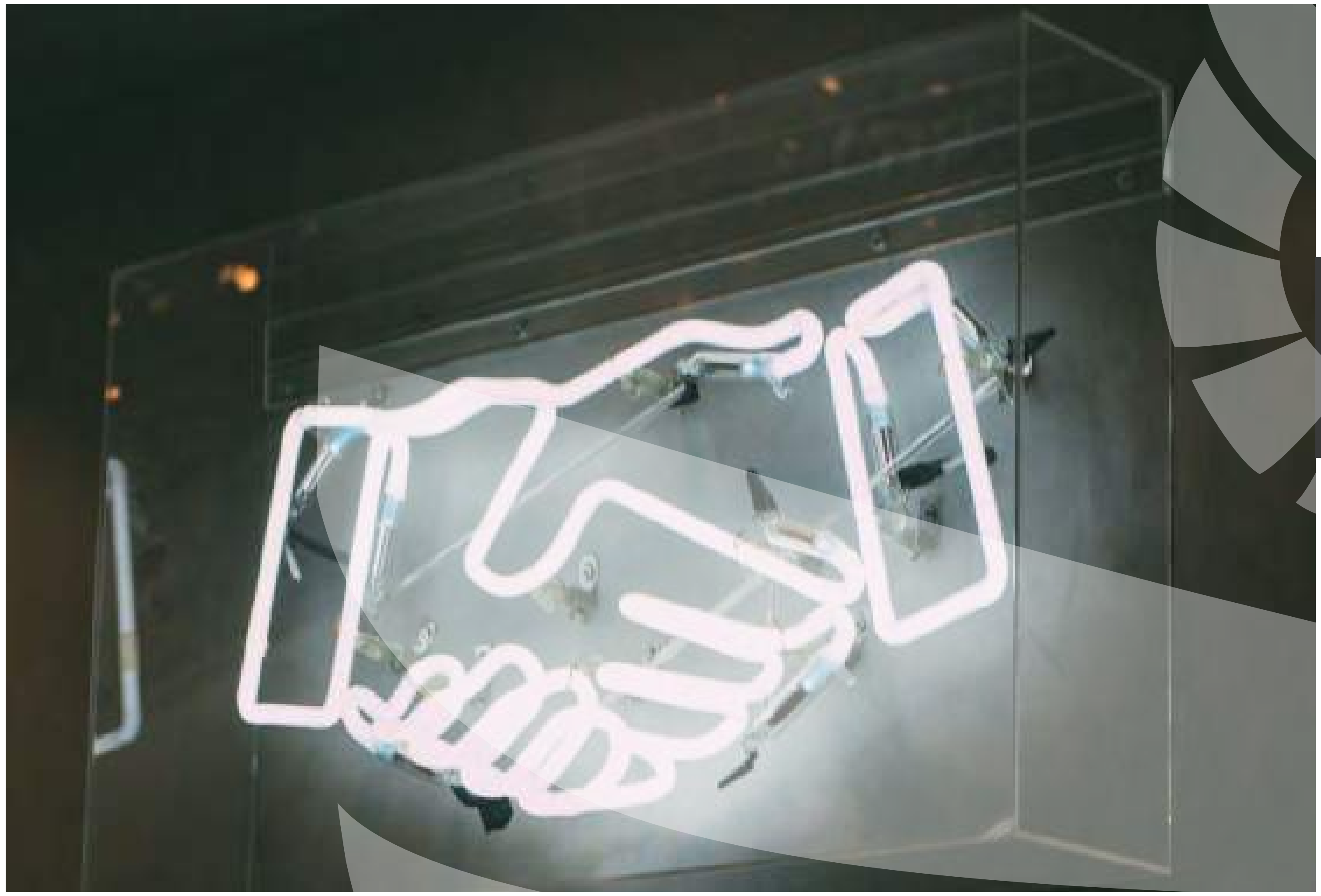
- Monitor and re-evaluate, refining continually.
- Setup and manage security forums.
- Provide regular updates on maturity, risk and threat landscapes, tailored to the relevant groups, typically executive, risk management committee and IT teams.

REPORT

Cognisys provides regular reporting via dedicated Account Management, internal support and technical teams, as appropriate.

Additional information is available via our SmartView platform to keep you fully updated at all times.

BE SMART. BE SAFE. BE SECURE.



Managed Security

New vulnerabilities are discovered daily, and attackers are more determined than ever.

Many organisations don’t have the available resources to staff a full-time security function. Instead, it is often left to IT staff who don’t have the time, the resources, or often the knowledge to properly secure an organisation’s environment.

We provide a service bundle that can be used over your contract period, meaning you can get help when you need it most.

Whether that’s because you’ve experienced a data breach and you need help understanding where attackers might have gained entry to your systems, or if you’re looking to mature your processes but need guidance with how to get started, we’re on hand!

THE KEY IS FLEXIBILITY

We’re keen to ensure that our Managed Security service provides value and meaningful improvements for you, which is why we allow you to tailor your contract to include the services that are most important to you, in a cost-effective and flexible way.

As a minimum, we include our SmartView service as standard, which provides regular vulnerability management reporting, giving insights into potential security risks in a simple to use dashboard.

You can then choose to add any or all of the following services:

- Internal Penetration Testing.
- External Penetration Testing.
- Web Application Security Testing.
- Mobile Application Security Testing.
- Cyber Security Review.
- Red Team Exercise.
- Phishing Simulation.
- Dark Web Monitoring.
- Lost or Stolen Device Assessment.
- Wireless Security Assessment.
- Cloud Security Assessment.
- Microsoft 365 Tenant Review.
- Attack Path Analysis.
- OSINT Analysis.
- Cyber Essentials.
- Governance & Compliance.
- Virtual CISO.
- SmartScan.

Your Account Manager will work closely with you to review your services year-to-year throughout your contract period. This ensures that you get maximum value and receive priority bookings in our consultant schedules.

KEY BENEFITS

- Regular monitoring of vulnerabilities within your environment to uncover potential risks earlier, allowing you to be more proactive.
- Flexibility with your services, meaning you can get the help and advice you need when you need it.
- Ongoing support from your designated account manager, who is on hand to provide guidance, coordinate resources and make sure you’re getting the security support you need.

REPORT

Cognisys provides regular reporting via dedicated Account Management, internal support and technical teams, as appropriate.

Additional information is available via our SmartView platform to keep you fully updated at all times.

BE SMART. BE SAFE. BE SECURE.

SmartScan

Reduce risk, improve your awareness and stay secure. Introducing SmartScan; our managed vulnerability service.

New vulnerabilities are discovered all the time, which means that the risk to your organisation is increasingly daily.

With more staff working remotely, it is vitally important that systems are effectively monitored to prevent potential breaches.

SmartScan from Cognisys provides visibility and management of all your systems.

Not just for your on-premise based IT estate, but also for remote users, and even cloud-based assets, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

SCAN

- Utilises multiple expert security tools along with proprietary code to analyse vulnerabilities.
- Perpetual analysis of internal and external network infrastructure for new vulnerabilities providing capability for you to to act and remediate quickly.
- Scans are conducted across all devices both within the network, remote and cloud locations.

IDENTIFY

- Categorisation of vulnerabilities into Critical/High/Medium/Low in order to prioritise and combat potential exploitation effectively.
- Identification of new vulnerabilities in real time.
- Validation of findings by experienced consultants reducing the potential for false positives and adding an expert human layer.

REMEDIATE

- Allows for your remediation of new security threats on an ongoing basis.
- Our consultants research remediation for vulnerabilities found, which allows for efficient action to be taken by your internal staff.
- Reports generated can be easily distributed to relevant asset managers for remedial actions.

CERTIFY

As this is a continual service, evidence is gathered on an ongoing basis that can be used to assist with Cyber Essentials Plus certification and other compliance aims.

SmartScan from Cognisys, powered by Qualys™, should only be considered as a single aspect of your cyber security strategy and does not remove the requirement for additional security services and assessments to be undertaken.

BENEFITS

- Helps meet your PCI, HIPAA, GLBA, ISO27001, NIST and Cyber Essentials compliance requirements.
- Reduces risk and provides evidence trails in the event of a breach/investigation.
- Works in conjunction with your team to raise awareness and increase cyber security maturity.
- Efficient, integrated and affordable service.

REPORT

Information is available via our SmartView platform to keep you fully updated at all times.

Cognisys provides additional regular reporting via dedicated Account Management, internal support and technical teams, as appropriate.

BE SMART. BE SAFE. BE SECURE.

SmartView

Enhance visibility of security information across your organisation.

SmartView from Cognisys centralises results from penetration testing, vulnerability scans, security assessments and managed cyber services into a simple and easy-to-use portal. Gain deeper insights, accelerate remediation, and achieve compliance faster.

BUILT BY SECURITY EXPERTS

SmartView has been designed by security experts as a single point of reference for identified vulnerabilities, helping to improve the understanding of risk in your environment.

Integrating with a variety of enterprise toolsets, SmartView allows organisations to easily view, sort and manage their threat vulnerability data, whilst also acting as a secure communications portal for sharing confidential or sensitive information, such as security test results.

Our intelligent dashboard shows your vulnerabilities, clearly and concisely, along with advice for their remediation. To improve efficiency, SmartView allows you to filter data so that you only see what's relevant for you, whether that's threats with a specific severity level, vulnerabilities related to a specific asset type, or other criteria.

SMARTER CYBER SECURITY

Security teams have never had it so tough. Threat actors are more determined. Vulnerabilities are more prevalent. Resources are more stretched. This means it is more important than ever to have all your security data in one, easily accessible place. Triaging and prioritisation of workloads should be simple and efficient. SmartView from Cognisys is the answer to this problem.

IMPROVED VISIBILITY

SmartView is a MFA controlled environment as standard, providing safe access to all your security engagement information.

Additional controls, such as automatic self-deletion, ensures that your highly sensitive information remains tightly controlled and only available to you and your team, as you need it

INFORMATION HELD

- Vulnerability Information.
- Penetration test results.
- Audit and review results.
- Feedback information for ISO27001 guidance.
- IASME governance information exchange.
- Cyber Essentials Plus.
- Dark web monitoring and OSINT Analysis results.
- Built-in live threat feeds.

OVERVIEW

- More comprehensive overview of your security vulnerabilities.
- Single point of reference for all your information and audit trails.
- Detailed issues and remediation advice.
- PTaaS (Penetration Testing As A Service).
- Compliance, governance, test results in one secured location.
- Validate remediation with subsequent testing.

REPORT

Cognisys provides additional regular reporting via dedicated Account Management, internal support and technical teams, as appropriate.

BE SMART. BE SAFE. BE SECURE.

COGNISYS
Smarter Cyber Security

Halifax Office
2.11 University Business Centre,
Piece Mill, 25-27 Horton Street,
Halifax, HX1 1QE

Manchester Office
Cognisys Group Ltd,
The Sharp Project,
Thorp Rd,
Manchester, M40 5BJ.

01422 416000
sales@cognisys.co.uk
cognisys.co.uk