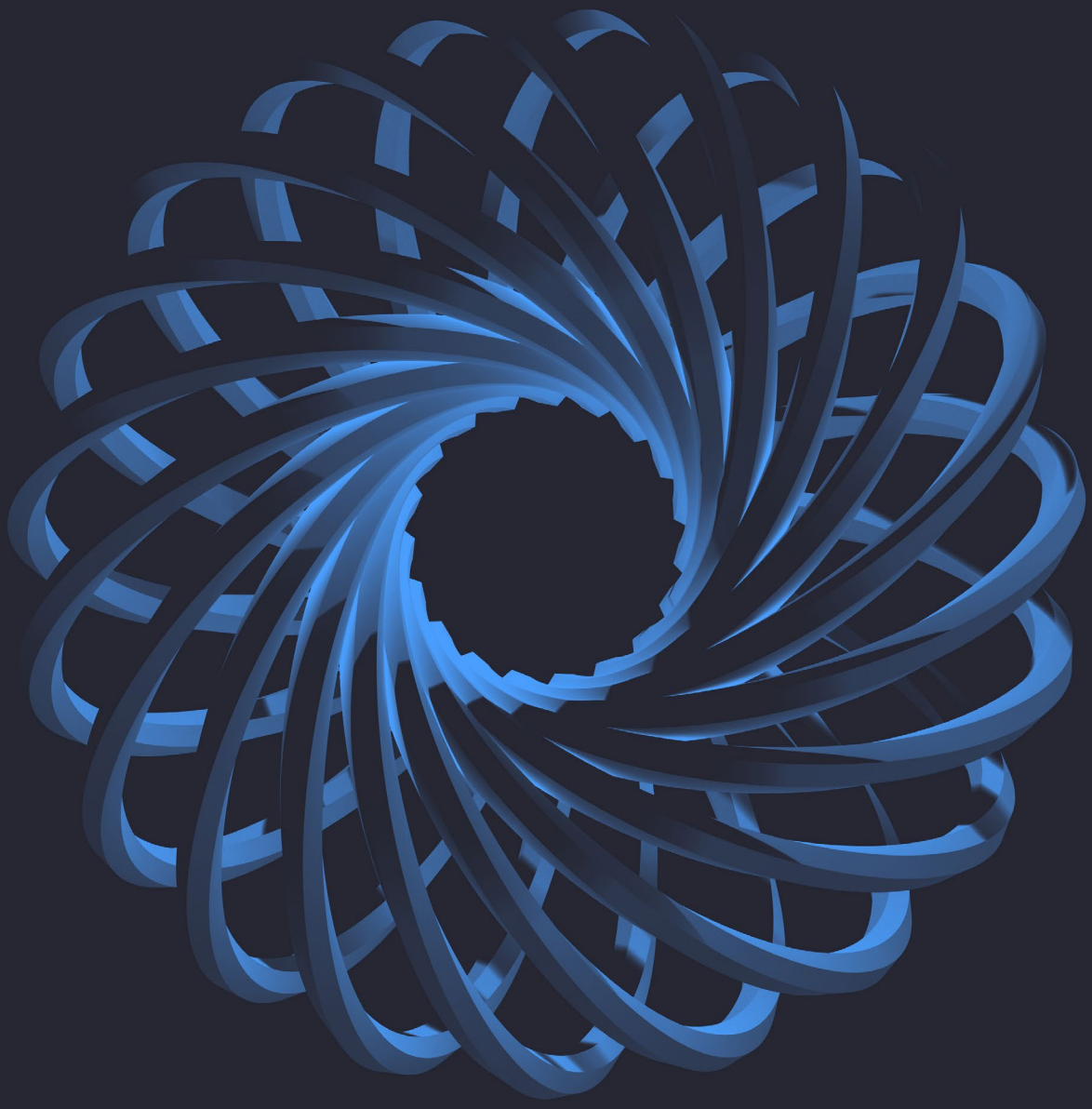
GF | GRASPAN FRANKTON®

COGNISYS
SMARTER CYBER SECURITY

Service Catalogue



Version 4.0

Spring 2024

Our partnership

We are thrilled to announce a ground breaking partnership between Graspan Frankton, a renowned specialist in security risk management, and Cognisys, a leading cyber security business. This collaboration represents a fusion of expertise and resources that promises unparalleled security solutions for our clients.

The synergy between Graspan Frankton's proficiency in holistic security risk management and the cutting-edge cyber security capabilities of Cognisys will create a comprehensive approach to safeguarding against evolving threats in today's digital landscape.

By leveraging Graspan Frankton's deep understanding of physical security risks alongside these advanced technological solutions, we are poised to offer tailored strategies that address both traditional and cyber threats with unparalleled effectiveness.

This partnership exemplifies our commitment to staying ahead of emerging security challenges and providing our clients with the highest level of protection. Together, we are confident in our ability to deliver innovative solutions that mitigate risks, enhance resilience, and safeguard the assets and operations of organisations across industries.

Paul Manning
Managing Director
Graspan Frankton

Penetration Testing

Governance, Risk and Compliance

Managed Services

It’s our business to make your business more secure

WHY COGNISYS?

It’s estimated that 88% of UK businesses suffered a security breach. From infrastructure and wireless network penetration testing to social engineering, red teaming and vulnerability scanning, we offer a range of penetration tests to help meet your business requirements and ensure your cyber security is fully functional and protects your assets.

WHO ARE COGNISYS?

Cognisys was formed with the ambition to improve the cyber security of every organisation it touches. We are an award-winning organisation that has helped keep secure over 430,000 people internationally from our offices in Leeds and Manchester.

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 ISO 27001 and Cyber Essentials, as well as via our vCISO and Governance, Risk and Compliance team.

STANDARDS AND ACCREDITATIONS

CREST | PEN TEST

Member CyberExchange

British Assessment Bureau – UKAS MANAGEMENT SYSTEMS 8289 – ISO 27001 INFORMATION SECURITY MANAGEMENT

British Assessment Bureau – UKAS MANAGEMENT SYSTEMS 8289 – ISO 9001 QUALITY MANAGEMENT

CERTIFICATION BODY – CYBER ESSENTIALS PLUS

TRUSTED BY BRANDS BIG AND SMALL

Quix

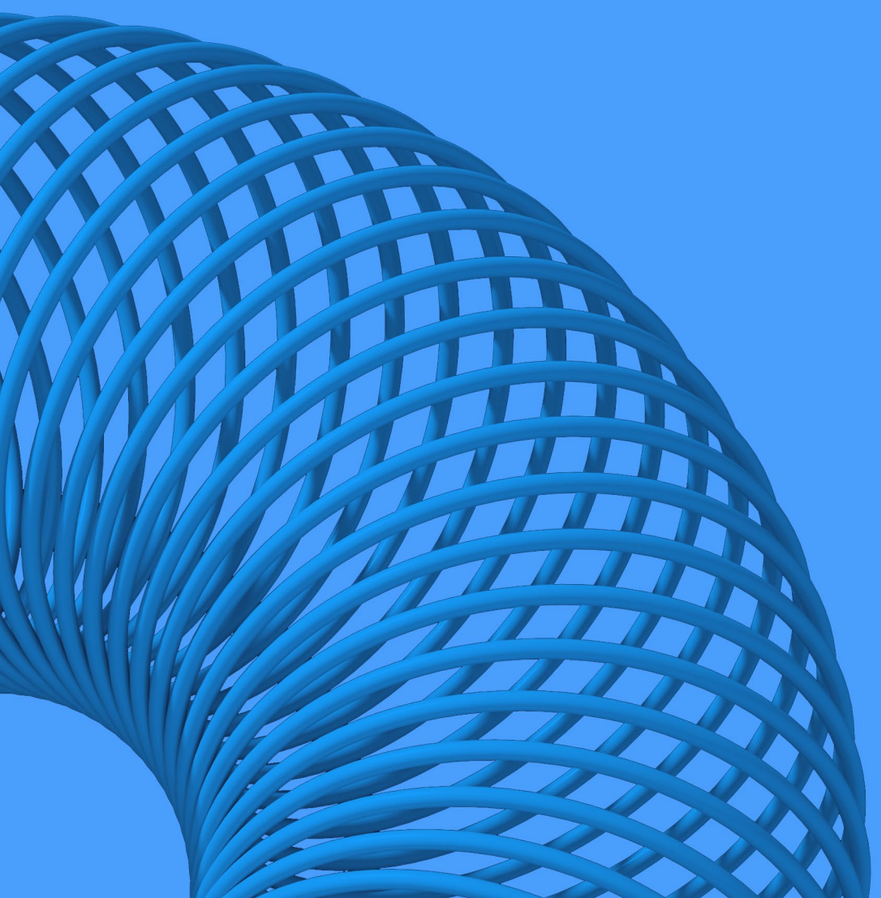
Edinburgh Leisure

Liaison Group

gch

Clarion

Penetration Testing



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.

Methodology

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 and 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.

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 and 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.

Methodology

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.

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 and 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.

Web application 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.

API penetration testing

APIs are critical components of modern web and mobile applications.

Their security is essential for protecting sensitive data and preventing unauthorised access. APIs are often used to access and manipulate data, including personal, financial, and other sensitive information. This makes APIs a prime target for attackers who are looking to steal this information, disrupt services, or perform other malicious activities.

Hence, API penetration testing becomes essential. This testing involves identifying vulnerabilities and weaknesses in the API that could be exploited by attackers to gain unauthorised access to sensitive data or perform malicious actions.

Methodology

We usually follow but do not limit our test cases to OWASP API Top 10. It is a list of the ten most critical security risks for APIs. These risks are ranked based on their likelihood of occurrence and the potential impact they could have on an organisation's security.

Our team utilises a range of cutting-edge methodologies and techniques to conduct a comprehensive and thorough evaluation of the API to identify all potential security risks. We use OWASP API Top 10 as a baseline for API testing but also go beyond it to uncover additional vulnerabilities and weaknesses in APIs.

Benefits

- Identification of vulnerabilities: An API penetration test helps in identifying vulnerabilities which could be exploited by threat actors to gain unauthorised access or perform other malicious activities
- Improved security posture: By identifying vulnerabilities early in the code base, this test can help improve the overall security posture of the API ecosystem, thus making it challenging for attackers to exploit
- Mitigation of risks: The vulnerabilities identified during the test can be addressed and mitigated, reducing the risks of a successful attack
- Compliance and regulations: Many regulations and standards require regular assessments to ensure compliance requirements are met and due diligence is followed
- Detection of anomalies: This pent can help identified anomalous behaviour such as unexpected data flows or excessive API calls, which may indicate an attack.

Overview

We perform an in-depth and thorough assessment of in-scope APIs to ensure that correct configuration and recommended practices have been followed to minimise the attack exposure. Following is a sample list of common tests that are performed during this test. It will vary depending on the technology and protocols that have been implemented. The tests are as followed:

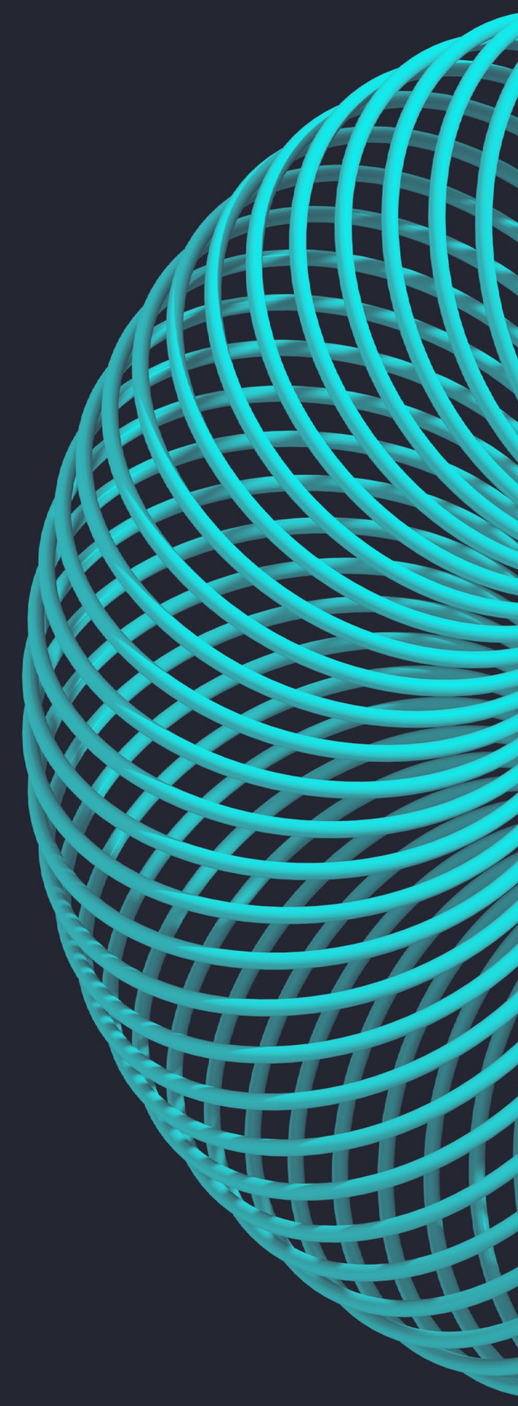
- Information Gathering
- Authentication and Authorisation Testing
- Input Validation Testing
- Error Handling and Logging Testing
- Business Logic Testing
- Fuzzing

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.



Get in touch: cognisys.co.uk | 0113 5311700 | info@cognisys.co.uk

Mobile application testing

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

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

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 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.

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 par

Methodology

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.

Get in touch: cognisys.co.uk | 0113 5311700 | info@cognisys.co.uk

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.

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.

Lost or stolen device assessment

Mobile devices are more prevalent in our lives than ever before. 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.

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.

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.

Attack path management

Active Directory and Azure 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 tool set 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 environm 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.

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.

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.

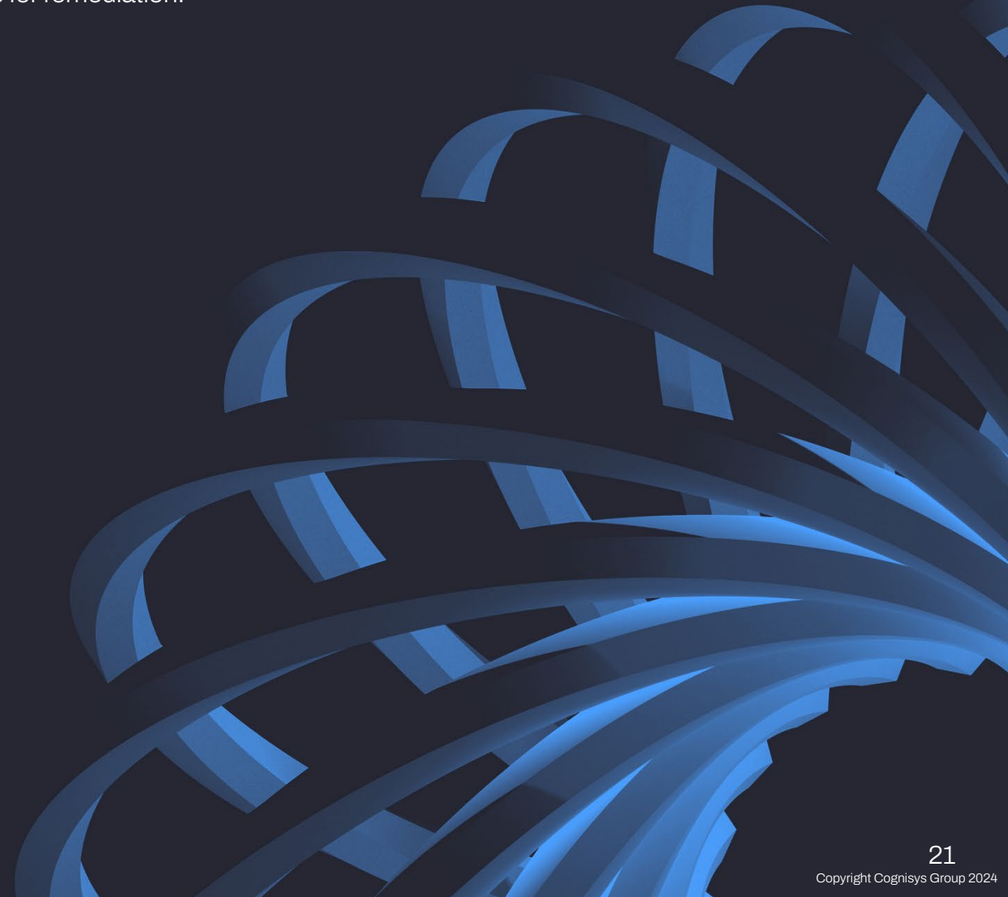
We're proud of our Red Team, which is made up of some of the most qualified people in the industry.

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.



Get in touch: cognisys.co.uk | 0113 5311700 | info@cognisys.co.uk

VoIP assessment

Penetration testing a VoIP network aims to identify vulnerabilities and potential attack vectors that can be exploited by a threat actor.

A VoIP (Voice over Internet Protocol) network is a system that transmits voice and multimedia content over the network. Penetration testing a VoIP network aims to identify vulnerabilities and potential attack vectors that can be exploited by a threat actor.

VoIP is vulnerable to many of the same issues as an internal network because it shares the same infrastructure. Due to the incorporation of emerging technologies and protocols, a VoIP network may expose additional security vulnerabilities. It is important to note that many VoIP implementations do not use encryption by default; this can allow attacks such as eavesdropping on calls.

VoIP testing is performed on-site, and assessments are undertaken from a network perspective. The areas of testing include:

- Supporting infrastructure – Servers, IP phones, routers, and switches
- Underlying protocols – SIP, SCCP, RTP, H.323, etc.

Cognisys will assess the VoIP infrastructure against the following type of attacks:

- **VLAN hopping** – this is a type of network attack where an attacker who is connected to an access port (which is attached to a particular VLAN) can gain access to network traffic from other VLANs. The attack mainly consists of spoofing devices on the network to gain access to the voice network from the data network.
- **Footprinting and enumerating SIP Services**
- **Man-in-the-Middle attacks** – Authentication to the SIP server without knowing the credentials by intercepting traffic.
- **VoIP authentication attacks** – capturing SIP authentication and cracking the SIP digest response hashes. Brute-force attacks against SIP accounts.
- **RTP injection attacks** – Inject audio into existing VoIP calls.
- **Caller ID spoofing** - Impersonating packets or the person transmitting the information. Several VoIP vendors' equipment is susceptible to common network-level issues such as ARP spoofing attacks.
- **Application-level attacks** – Identification of weaknesses that come from the web management interfaces of VoIP devices.
- **Eavesdropping** – Unauthorised interception of voice packets or Real-time Transport Protocol (RTP) media stream and decoding of signalling messages.
- **Replay** – The retransmission of a genuine session so that the device receiving it reprocesses the information.
- **Insecure services identification** – VoIP systems might contain services which are considered insecure, such as FTP and Telnet.
- **Voicemail attacks** – We will carry out attacks on the voice mail system for a given extension, testing the PIN security, lockout, and potential for call relaying.

Apart from the network review, we will assess your VoIP device and/or your softphone testing. e.g., With softphone software, we look at a device with the softphone configured on it and look for:

- DLL hijacking
- Insecure permissions
- Unquoted service paths for the VoIP software
- Check for the version of software being used

The team will assess your network infrastructure, VoIP components, and authentication methods to determine their effectiveness in preventing manipulation between the endpoints and VoIP server. Based on this assessment, we will provide you with a detailed report that identifies any issues or vulnerabilities and offer recommendations for remediation.

VPN assessment

Penetration testing a VoIP network aims to identify vulnerabilities and potential attack vectors that can be exploited by a threat actor.

At a fundamental level, VPNs safeguard the user's online privacy, preventing them from being targeted or discriminated against based on their location.

A virtual private network (VPN) is a service that assists individuals in maintaining their online privacy. It establishes a secure and encrypted connection between the user's computer and the internet, creating a private tunnel for data and communication transmission while utilising public networks.

Since the pandemic, the hybrid approach became lucrative giving rise to the use of VPNs which have now become an essential tool in a corporate environment.

The VPN assessment validates the security posture of all VPN types. The test ensures that the configuration does not allow information leakage or credential interception. Most VPN installations fall into one of the following types:

- IPsec
- PPTP
- SSL VPN

Zero Knowledge Assessment

Initial assessment of a VPN is performed with zero knowledge and with no information provided by the client other than the target IP address of the VPN server. When testing a VPN remotely, fingerprinting of the specific server and VPN type will be carried out, allowing appropriate test cases to be produced:

- **Encryption Cipher Analysis:** Weak encryption ciphers will be tested for, as these could lead to trivial decryption of the VPN traffic.
- **Username enumeration:** This would be attempted; if this is possible, and no lock-out policy is in place, Cognisys will attempt to compromise the VPN through a dictionary or brute-force attack. Often a username or credential set can be obtained while testing other targets throughout a wider external infrastructure assessment, providing that this is in scope.
- **Certification Authorities Check:** Certificates and local certification authorities are tested for potential information leakage and associated vulnerabilities.
- **Investigation of the challenge/response handshake:** The handshake would be assessed for any weaknesses, leading to the potential for offline passphrase cracking. In the case of IPsec VPNs, this may lead to the cracking of a pre-shared key through brute-force attacks if a valid Group name is guessed. Vendor-specific vulnerabilities are evaluated, such as man-in-the-middle attacks and cross-site scripting vulnerabilities in SSL VPN web frontends.

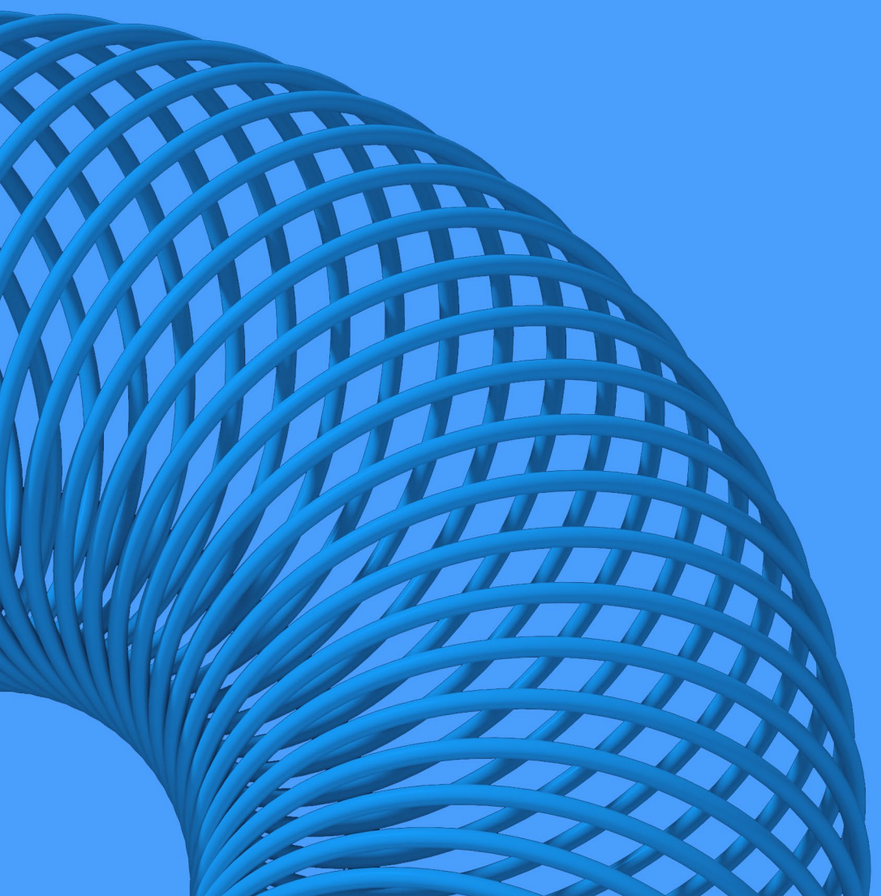
Testing using VPN Profile / Credentials

If compromise of the VPN is not achieved, we will proceed with a valid set of credentials/ profiles to establish the VPN session. This allows us to assess the risk presented by the theft of user credentials, such as through a social engineering attack against the helpdesk or by compromise from a stolen laptop with cached VPN credentials. An authenticated assessment of the VPN solution can determine a given user's visibility of internal network resources and, if in scope, attempt to escalate privilege through the network. User policy is also determined – for example lock-out and concurrent login policies.

Configuration review

As part of this check, we review the VPN's configuration settings, including the IKE phase 1 and phase 2 parameters, authentication methods, encryption algorithms, and key exchange protocols. For this, the configuration details should be made available to the consultant.

Governance, Risk and Compliance



Vanta

Vanta Implementation and Consultancy

Cognisys and Vanta have partnered to offer our clients unparalleled value. With our expertise in cyber security and compliance combined with Vanta's industry-leading technology, our clients can swiftly meet their security compliance objectives.

Cognisys are trusted by some of the brightest companies in the UK and across Europe, to help them achieve ISO 27001, SOC 2 (I &II), and Cyber Essentials Plus.

Businesses across Europe choose Cognisys as implementation and security testing partners to help speed up their journey and provide guidance to achieve certification.

We're 'Powered By Vanta' and typically we use the platform to help clients certify to a wide range of standards and frameworks throughout Europe.

CERTIFIED Vanta SERVICE PARTNER

How we work

Implementation phase:

We assist in installing the Vanta platform, ensuring deep integration, help develop tailored policies and procedures, aligning with ISO 27001/SOC 2 standards. Provide hands-on guidance for seamless integration and adoption within your organisation.

Assessment phase:

Cognisys conduct a thorough gap analysis, evaluating your current practices. We Identify vulnerabilities, compliance gaps, and prioritise areas needing improvement to ensure robust cyber security and readiness to begin your journey to compliance.

Audit preparation and guidance:

Finally we steer your organisation through audits, collaborating with a professional audit company. To ensure compliance, we offer strategic support in addressing audit findings, guaranteeing a successful ISO 27001/SOC2 certification process, wherever possible.

Get in touch: cognisys.co.uk | 0113 5311700 | vanta@cognisys.co.uk

ISO 27001

ISO 27001 is the international standard for Information Security Management Systems .

ISO 27001 sets the global benchmark for a risk-based approach to cyber security management. It establishes a comprehensive framework to ensure effective information security, cyber security, and privacy protection.

An ISO 27001 ISMS helps to make sure information is always appropriately protected to assist with the preservation of:

- Confidentiality – ensuring that access to information is appropriately authorised
- Integrity – safeguarding the accuracy and completeness of information and processing methods
- Availability – ensuring authorised users have access to information when required

Why ISO 27001?

This testing is designed to assess security posture against best practices and attempts are made, where safe and permitted, to exploit any vulnerabilities discovered. Improved information security: By implementing the controls outlined in the standard, your organisation will better protect its sensitive data and systems from cyber threats and other security risks.

Increased customer trust: ISO 27001 certification demonstrates to customers and clients that an organisation takes information security seriously and is committed to protecting its data.

Enhanced compliance: Many industries and sectors have regulatory requirements related to information security. ISO 27001 certification helps meet these requirements and demonstrate compliance.

Competitive advantage: In some cases, clients may only do business with organisations that have demonstrated their commitment to information security through ISO 27001 certification.

Improved risk management: The risk assessment and management process required for ISO 27001 certification can help an organisation identify and prioritise potential security risks and implement controls to mitigate them.

Improved business continuity: By implementing the controls outlined in the standard, an organisation can improve its ability to continue operating in the event of a security incident or other disruptive event.

ISO 27001 services

- GAP Analysis
- Development & Implementation
- Internal Auditing
- External Auditing (Stage 1, Stage 2, Surveillance)
- Management and maintenance (Continual improvement)

Why partner with Cognisys?

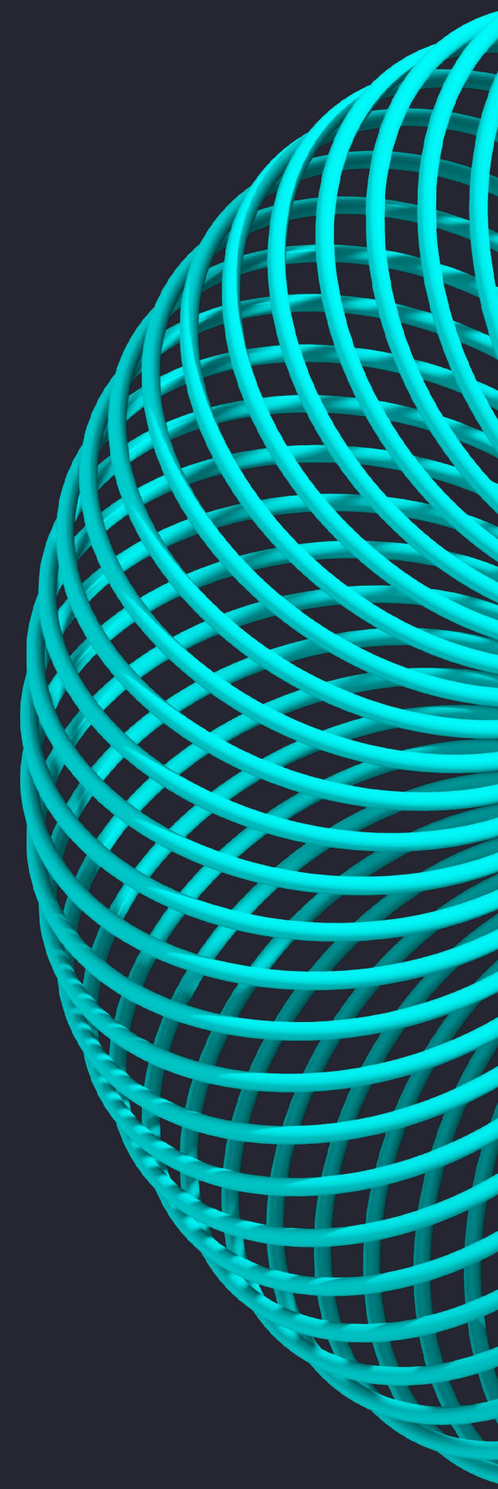
There are several reasons why an organisation should choose to use Cognisys to help with the development and implementation of an ISO 27001 ISMS:

- Expertise: Our team has extensive experience in ISO 27001 and holds all the relevant qualifications. We provide valuable expertise and guidance throughout the process of implementing an ISO 27001-compliant ISMS. We help the organisation understand the requirements of the standard and how to effectively implement them.
- Objectivity: We provide an objective perspective and help identify potential weaknesses or gaps in the organisation's current security practices.
- Time and resource savings: Developing and implementing an ISMS can be a time-consuming and resource-intensive process. We help streamline the process and ensure that it is completed efficiently.
- Independent verification: We provide independent verification of the organisation's ISMS, which is helpful in demonstrating compliance to regulatory bodies or clients.
- Ongoing support: We provide ongoing support to help the organisation maintain its ISMS and ensure ongoing compliance with the standard.

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.



Get in touch: cognisys.co.uk | 0113 5311700 | info@cognisys.co.uk

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 receive 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.

CYBER ESSENTIALS PLUS

Get in touch: cognisys.co.uk | 0113 5311700 | info@cognisys.co.uk

Microsoft 365 Tenant review

Microsoft 365 has become the method of choice for organisations to store and share 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 are often misconfigured or overlooked.

You own your data and identities and you also have the responsibility for protecting them. This includes the security of your on-premise resources, along with 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 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.

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-today 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.

Virtual CISO

Add the right expertise to your organisation. Maximise security and set your compliance direction.

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 cyber security 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 state, to its desired state.

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

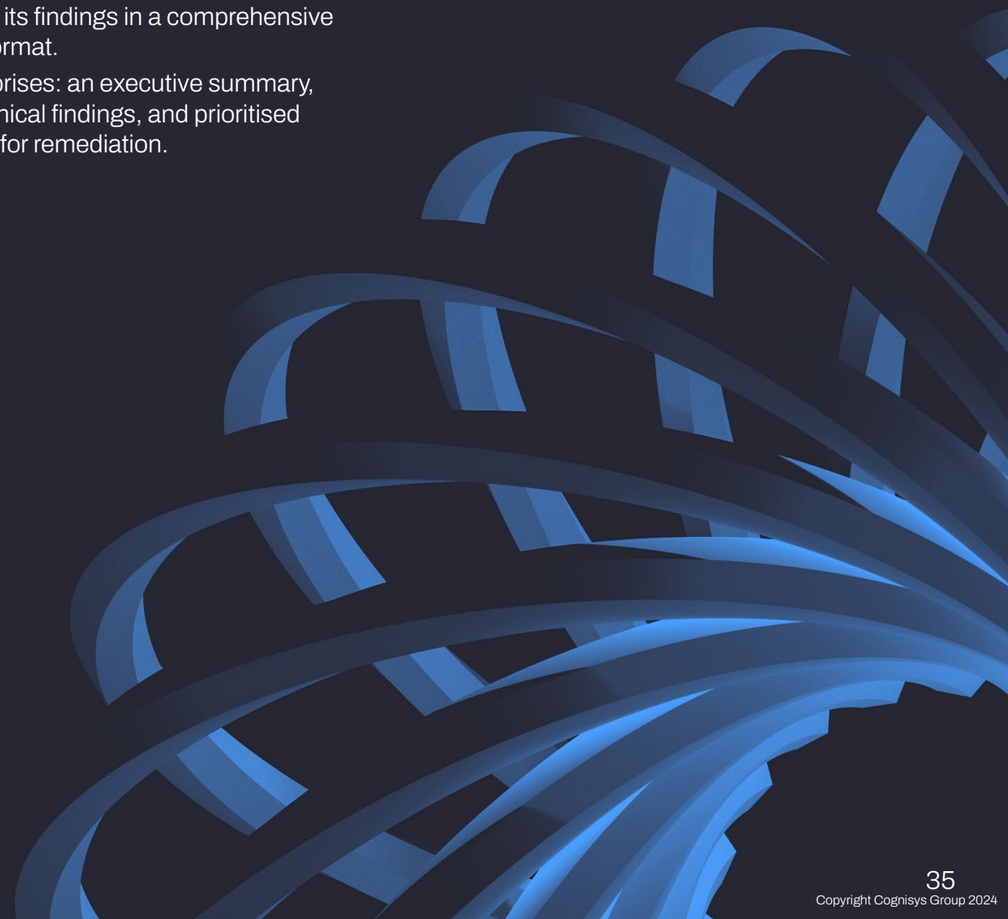
Following project completion, typically the service moves into the ‘business as usual’ phase, to:

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

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



Governance and 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.

Overview

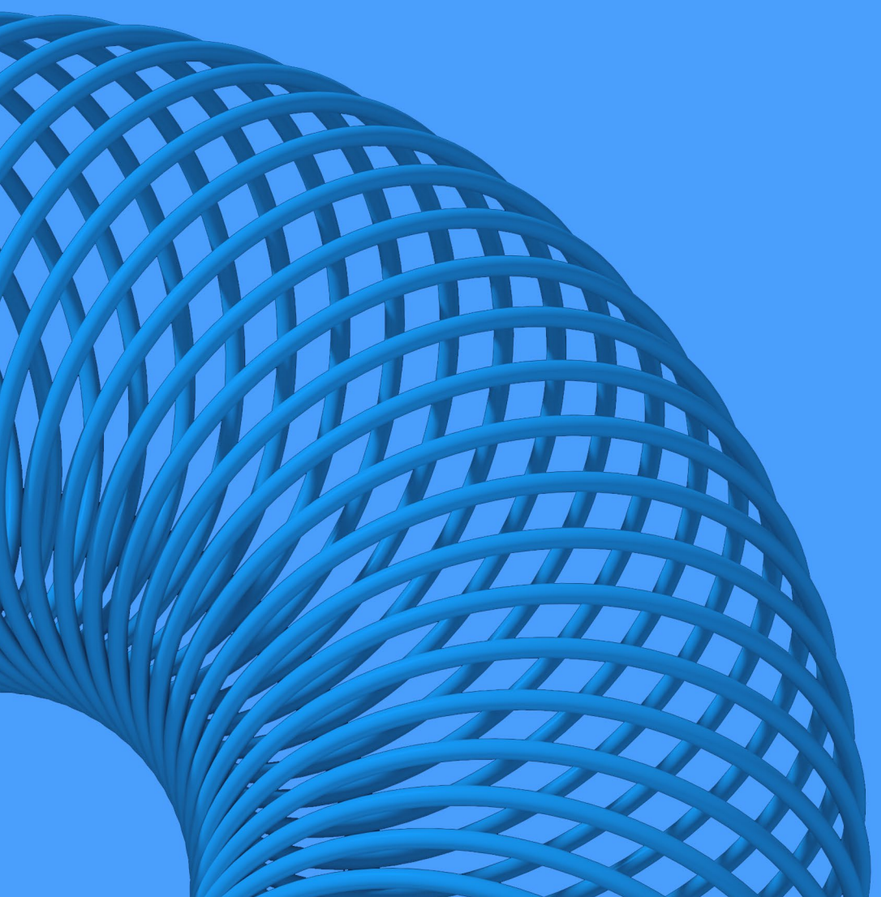
- Accredited expertise in Governance & Compliance.
- Independent and objective approach.
- Significant cross-sector experience.
- Active involvement in developing and maturing your cyber security posture.
- Multi-disciplinary team including experienced governance auditors and technical experts complementing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

Managed Services



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 Group 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 to act and remediate fast.

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 remediation of new security threats on an ongoing and immediate basis.

Our consultants research remediation for all 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

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.

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 tool sets, 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 ISO 27001 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.

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 unauthorised 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 cyber security 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 into 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 cyber security awareness training.
- We work alongside your team to raise awareness and increase cyber security 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.

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.

Get in touch: cognisys.co.uk | 0113 5311700 | info@cognisys.co.uk

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 the exposure of 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 smishing, 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.

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
- SmartView

Your Account Manager will work closely with you to vary 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.

Managed cyber security training

Fostering a cyber security culture is critical in the fight against cyber attacks.

Many organisations have turned to fully automated learning platforms for their cyber security training. These platforms typically start with a baseline survey and then send simulated phishing emails to test user behaviour. Based on their responses, users are enrolled in training.

While this approach provides a foundation, it falls short of delivering the complete benefits of a well-rounded cyber security training program.

A comprehensive cyber security training program must include interactive and personalised training, technical reviews and control analysis combined with regular follow-up and reinforcement, in addition to automated assessments and simulations.

Managed cyber security training elements:

- Automated training
- Phishing simulation
- Dark web monitoring
- Password auditing
- Bespoke cyber security training

Smarter cyber security training

Our Managed Cyber Security Training service provides a comprehensive wrap-around solution for organisations seeking to enhance their cyber security posture. Our focus is on mitigating the risks posed by threats targeting end users.

Our team of professionals provide cyber security consulting and technical support services which promote awareness and readiness throughout your organisation.

Our managed service includes:

- Bespoke end-user training, focused on repeat offenders
- VIP training, executives are the most targeted user group
- Security culture strategy development
- Risk assessments
- Policy development and implementation
- Ongoing monitoring

Benefits:

- Improved awareness, increased security: Providing employees with the knowledge and skills they need to better avoid cyber threats reduces the risk of data breaches and other security incidents.
- Help meet your compliance requirements: GDPR, ISO 27001, PCI DSS, HIPAA, SOC2, NIST, Cyber Essentials, IASME Cyber Assured.
- Early detection and response: Recognising and responding to cyber threats early reduces the impact of security incidents.
- Better threat intelligence: Gather valuable information on the types of threats that are most relevant to your environment and use this intelligence to better protect against future attacks.
- Limit liability: Providing training can reduce the risk of legal and financial liabilities associated with data breaches and other security incidents.

Report

Cognisys provides regular reporting via our GRC team, dedicated account managers, Internal support and technical teams. As appropriate.

DNS monitoring and brand protection

Fostering a cyber security culture is critical in the fight against cyber attacks.

DNS Security Monitoring involves the continuous monitoring of DNS traffic to detect suspicious activities, such as DNS hijacking, DNS tunnelling, or DNS cache poisoning. It also involves the monitoring of DNS servers to ensure that they are configured securely and are not vulnerable to attacks. This service helps organisations detect and prevent cyber attacks that exploit DNS vulnerabilities, protecting their data, network, and reputation.

Keeping DNS secure is crucial for several reasons:

- DNS is a common target for cyber attacks, such as DNS hijacking, DNS cache poisoning, or DNS tunnelling. These attacks can result in data breaches, malware infections, or other security incidents.
- Protecting against phishing: Cyber criminals can use DNS to create fake websites that mimic legitimate ones, tricking users into providing sensitive information such as login credentials or credit card numbers.
- Ensuring availability: A DNS outage can result in significant disruptions, such as the inability to access websites or receive emails.
- Maintaining trust: Any compromise in its security can erode users' trust in online services and commerce.

Brand Monitoring

Our Brand Protection Service helps organisations protect their digital assets and brand reputation from cyber threats. It includes a range of services such as domain name, trademark, and social media monitoring.

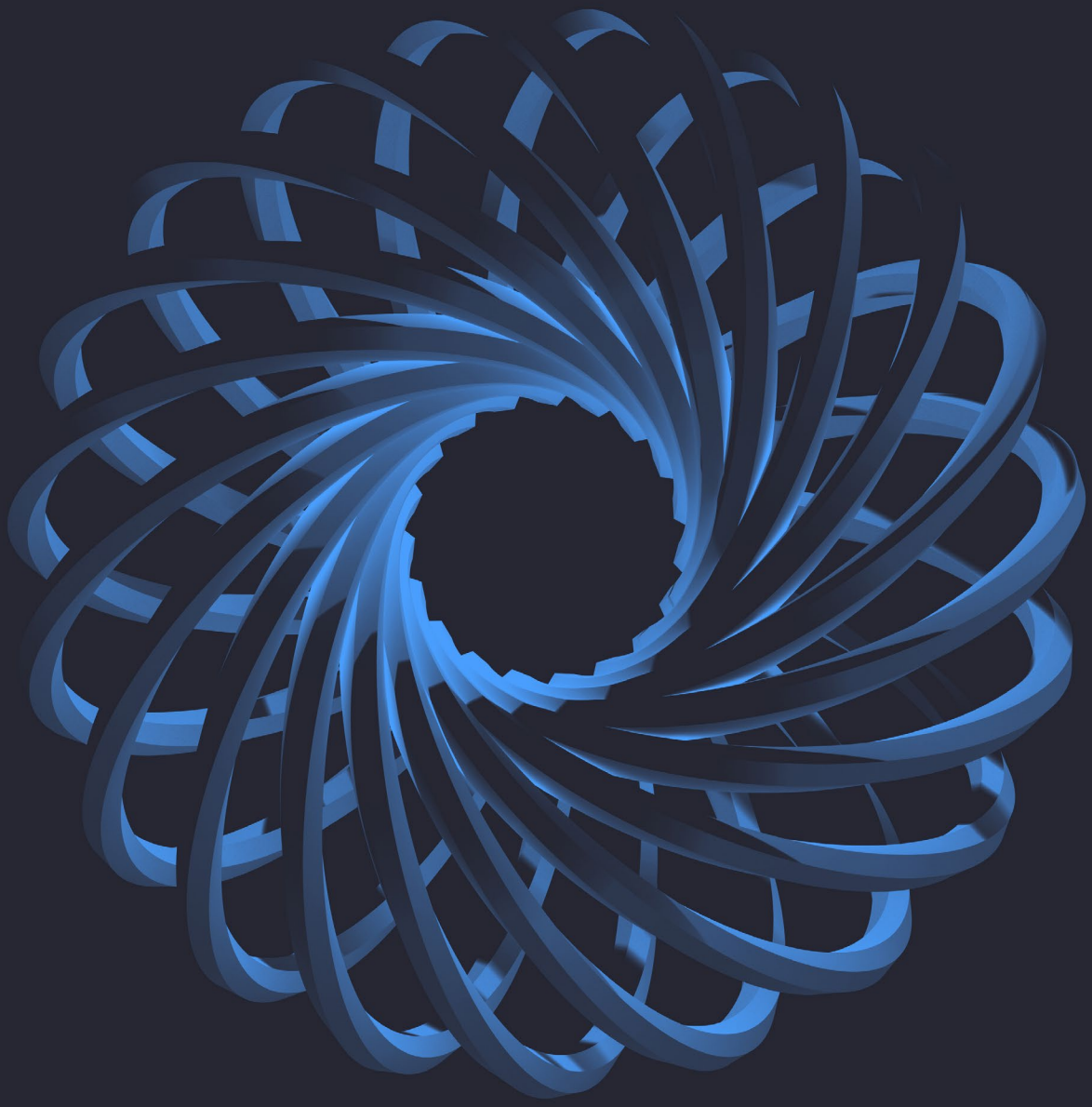
It helps organisations monitor and protect their brand reputation by detecting and mitigating online threats such as domain name squatting, phishing, counterfeiting, or impersonation that can harm their reputation or customer trust.

What is monitored as part of the service?:

- DNS server availability and performance: If response times exceed a predefined threshold or the server does not respond, this could indicate a possible DNS server outage or performance issue.
- DNS resolution: We verify that the IP addresses are correct and authoritative. Otherwise, a possible DNS hijacking or cache poisoning attack could have occurred.
- DNS record changes: If a change is detected, it could indicate an unauthorized DNS record modification.
- DNS server security: Ensuring the DNS server is configured securely.
- Zone transfer settings: Ensure that unauthorised zone transfers are not possible.
- Start of Authority (SOA) record: Changes to this record may indicate unauthorised changes to the DNS zone.
- DNS TTL (Time to Live) values: An abnormal TTL value could indicate a possible DNS cache poisoning or a DNS amplification attack.
- Squat domains: Domains that are like legitimate domains but with minor variations, such as misspellings, use of internationalized domain name homograph character set or different TLDs. which can be used for phishing, spamming, or malware distribution.
- DNSSEC: A set of security extensions to DNS that provide data integrity and authentication which helps prevent DNS cache poisoning and other DNS-based attacks.

Report

Cognisys provides regular reporting via our GRC team, dedicated account managers, Internal support and technical teams. As appropriate.



Improve your cyber security.
Let us find the gaps before the bad guys do.

GF | GRASPAN FRANKTON®

COGNISYS
SMARTER CYBER SECURITY

Leeds Office
Cognisys Group Ltd,
5 Park Place,
Leeds, LS1 2RU

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

Lets keep in touch
0113 531 1700
info@cognisys.co.uk
cognisys.co.uk