CyberContego

Contego; to cover, shield, protect or defend

www.cybercontego.com

About CyberContego

CyberContego is a cybersecurity consultancy, support and monitoring company serving clients all over Ireland. Our focus is to provide digital defence solutions for SMEs. We provide a range of cybersecurity solutions including vulnerability assessments, penetration testing, endpoint detection & response and managed detection & response for Microsoft 365 to name but a few.

The team at CyberContego is led by Seamus Quinn. Seamus founded and ran an IT Managed Service Provider (called myITdepartment) from 2003 until 2021 when it was acquired by Intuity Technologies. From 2021 to 2024, Seamus served on the leadership team in Intuity and launched the cybersecurity service under the CyberContego brand within Intuity in 2023. In 2024, CyberContego was spun-off as a separate entity controlled and operated by Seamus.

Since 2003, Seamus has worked with numerous SME clients providing them with IT security focused solutions including cyber auditing, vulnerability assessments, penetration testing and general IT consultancy advice. This blend of technical skills, experience in multiple sectors, and 20+ years of running an SME allows Seamus to deliver a comprehensive, understandable and advice-driven cyber service to our clients.

At CyberContego we use best-in-class software solutions from the likes of Huntress Labs, Vonahi, RapidFire Tools and Sendmarc to deliver our services. We combine this world class software with a no-nonsense advisory service to deliver real, actionable outcomes for your organisation.

Our Services

- Managed Endpoint Detection & Response
- Penetration testing
- Managed Detection & Response for Microsoft 365
- DMARC compliance
- Managed SIEM
- DNS filtering
- Cybersecurity risk reviews and reporting
- Password management
- Vulnerability assessments

Website links

Please click on the links below to view our services and resources pages on our website.

Services page

Resources page

Managed Endpoint Detection & Response (EDR)

EDR is an advanced technology designed to continuously monitor your servers, PCs, and laptops, identifying and responding to cyber threats such as ransomware, malware, and other suspicious activities. Unlike traditional antivirus software, which only detects known threats, EDR proactively searches for emerging risks and suspicious behaviour, taking action before any damage occurs.

By combining cutting-edge software with expert analysis, EDR ensures that threats are addressed as soon as they are detected. Cybersecurity specialists are available around the clock to remove or contain risks, safeguarding your data from unauthorized access. With 24/7 monitoring, any breach is quickly contained or neutralized to protect your sensitive information, no matter when it happens.

Please click here to see detailed information about the EDR service on our website.

Managed Detection & Response for Microsoft 365 (MDR for M365)

MDR for M365 provides continuous monitoring of your Microsoft 365 accounts, detecting and responding to breaches or attempted breaches. If suspicious activity is detected, the service takes immediate action to either prevent the intrusion or lock out the attacker to avoid any damage. Like EDR, this service operates 24/7.

It also tracks unusual login locations or patterns that deviate from the norm and alerts cybersecurity teams for further investigation. For instance, if you're usually logging in from Ireland but the system detects a login from Spain, it could indicate you're traveling, or it may signal a compromised account. MDR sends alerts when such activity occurs, ensuring timely investigation.

Additionally, MDR detects and flags the use of Virtual Private Network (VPN) software, which hackers often use to disguise their location and mimic the typical login region of the target user.

Please click here to see detailed information about the MDR service on our website.

Managed SIEM

Security Information and Event Management (SIEM) is a security management approach that integrates the functions of Security Information Management (SIM) and Security Event Management (SEM) into a unified system.

A SIEM system operates by collecting relevant data from multiple sources, such as Windows event logs and firewall logs, to identify anomalies and take appropriate action. For instance, if a potential issue arises, the SIEM system may log additional details, generate an alert, or direct other security controls to halt an activity.

For example, a user account with 25 failed login attempts over 25 minutes might be flagged as suspicious but considered low priority, as it could be a case of forgotten login details. However, an account with over 100 failed attempts within five minutes would likely trigger a high-priority alert, as it could indicate an ongoing brute-force attack.

Please click here to see detailed information about the SIEM service on our website.

Partnership

To deliver the EDR, MDR and SIEM services described above we partner with one of the world's leading cybersecurity companies – Huntress Labs. Huntress operates a 24/7 Service Operation Centre (or SOC, for short) using the "follow-the-sun" method meaning that the technical staff in the SOC are always working during their daytime (i.e. no sleepy techs working a night shift!).

Huntress are dedicated to bringing cutting edge cybersecurity solutions to market at an affordable price-point for SMEs and their founder and CEO (Kyle Hanslovan) regularly says "Huntress is not cybersecurity for the Fortune 500, we're cybersecurity for the Fortune 5,000,000".

Huntress recently completed a $150m funding round valuing the business at $1.5b. They currently provide services to 120,000 customers worldwide and have been investing heavily in their Ireland / UK based teams in recent months.

Cybersecurity risk reviews and reporting

Our cybersecurity risk assessment encompasses all facets of cybersecurity within an organization and adheres to the NIST framework. Developed by the National Institute of Standards and Technology (NIST), a U.S. government agency, this framework consists of five key components: Identify, Protect, Detect, Respond, and Recover. These components provide a structured overview of all systems, ensuring that resources and budget allocations are not disproportionately concentrated on just one or two areas. For instance, while a firewall falls under the "Protect" category, an organization must first understand the current state of that firewall ("Identify") and monitor its logs for intrusion attempts ("Detect"). Without this knowledge, they may struggle to effectively respond to a network breach ("Respond") or to restore the system's functionality ("Recover").

During our audit, we will conduct a thorough examination of your systems, including discussions with you and your IT team or external IT provider, to leave no detail unaddressed. The final audit report will include a percentage-based score and employs a traffic light system to clearly indicate areas needing improvement.

We recommend conducting these reviews at least once a year, with more frequent assessments for larger or more complex systems, to account for emerging threats and technologies. Our review template is continuously updated to adapt to these evolving changes.

Vulnerability assessments

Continuous

Vulnerability assessments are used to detect software vulnerabilities in your systems so they can be mitigated in a controller manner before they can be exploited by hackers. Vulnerabilities are rated on a scale from "Low" to "Critical" and we will notify you and your IT department / IT provider immediately about any "High" or "Critical" vulnerabilities found.

Our vulnerability software scans all your devices (e.g. servers, PCs and laptops) on a daily basis and your network devices (e.g. firewall, routers, network switches etc.) on a weekly basis and reports its findings to us.

We will also present you with a report from the system twice annually and work with you your IT department / IT provider to resolve any persistent issues which pose a risk to your systems.

Point-in-time

A point-in-time vulnerability assessment uses the exact same technology and methodology as above but as the name suggests it is carried out once, generally over the course of 4-6 weeks. The is useful to diagnose unknown vulnerabilities in a system particularly after significant systems change e.g. moving from on-prem servers to the cloud etc. We recommend that vulnerability assessments be carried out on a continuous basis in order to keep pace with the ever-changing security landscape.

VULSCAN
by RapidFire Tools

Penetration testing (internal and external)

Penetration testing, often referred to as pen testing, is a security exercise designed to identify and exploit vulnerabilities in a computer system. This simulated attack aims to uncover weak points in a system's defences that malicious hackers might exploit.

You can think of it as a bank hiring someone to pose as a burglar to try to break into their premises and access the vault. If the 'burglar' successfully enters the bank or vault, the bank gains crucial insights on how to enhance its security measures.

There are various types of penetration tests, which are often confused with vulnerability assessments. One major difference is that a vulnerability assessment identifies and reports weaknesses discovered during a scan, while a penetration test attempts to exploit these vulnerabilities, much like a hacker would, to gain access to the system. Due to their nature, penetration tests can lead to system instability or downtime. Therefore, conducting a penetration test without first performing a vulnerability assessment is risky and may not provide a complete picture of cyber risks.

VONAHI SECURITY

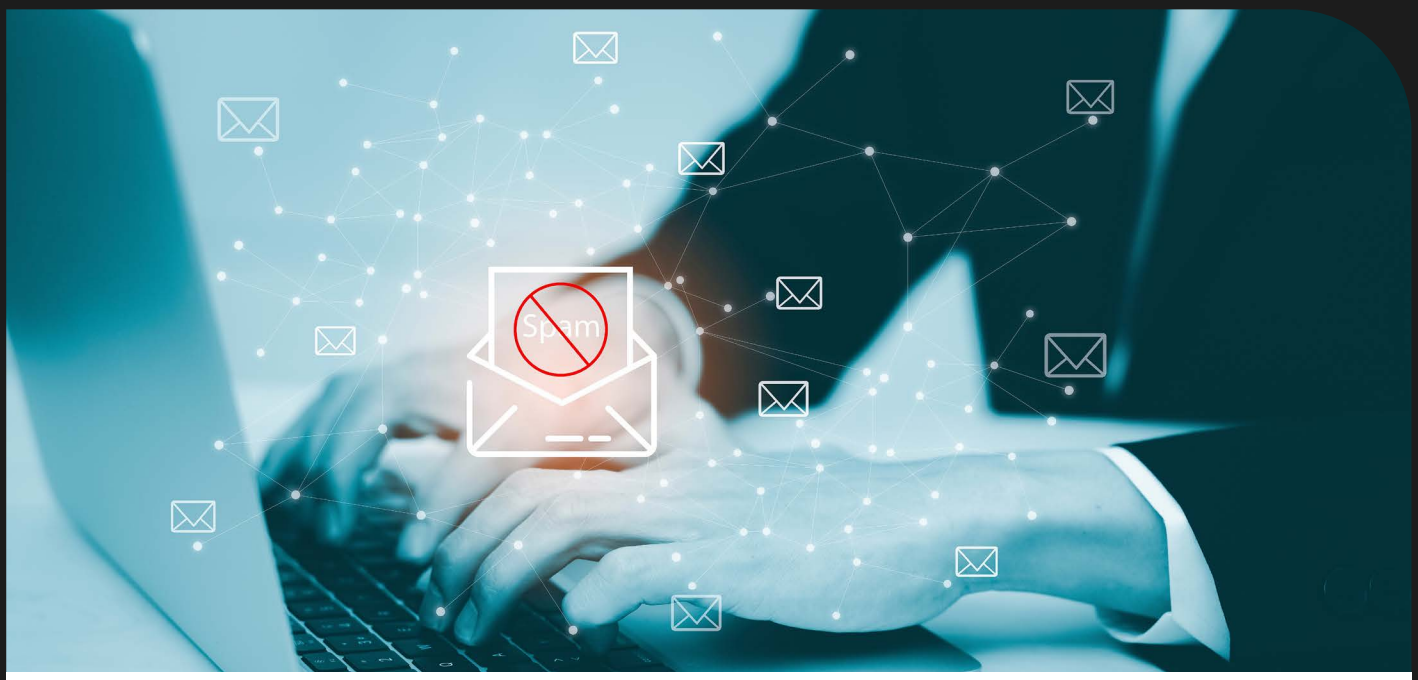
Combining a vulnerability assessment with a penetration test yields the best results by offering a thorough overview of the system's security posture. Many service providers claim to offer penetration tests, but they often only conduct vulnerability assessments, which leaves out a crucial element of the process.

Additionally, performing an external-only penetration test is unlikely to yield meaningful insights since scanning or attempting to penetrate a typical small or medium-sized enterprise's externally facing network (usually just a firewall) overlooks significant internal risks.

We recommend conducting multiple internal vulnerability assessments alongside a comprehensive internal and external penetration test. This approach delivers a true representation of your IT systems' security.

The results from our penetration tests are independently reviewed by external experts and certified by CREST (Council for Registered Ethical Security Testers).

DMARC Compliance



SENDMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a system for validating emails that aims to safeguard your company's email domain from misuse in spoofing and phishing attacks. It operates by verifying emails sent from your domain, ensuring that only authorized senders can utilize your domain name for outgoing messages. This process effectively prevents scammers from impersonating your domain. In simple terms, with DMARC compliance, recipients can be completely assured that any email claiming to come from your domain is legitimate and not fraudulent.

Implementing DMARC provides several advantages for your business:

- Protects your brand reputation: DMARC helps to prevent email spoofing scams, which could harm your brand image and erode customer trust.
- Enhances email deliverability: By ensuring proper authentication, your legitimate emails are more likely to reach recipients' inboxes rather than being diverted to spam folders.
- Offers valuable insights: DMARC reports provide detailed analytics, giving you visibility into how various recipients are managing your emails and helping you identify any potential issues.

DNS Filtering

What is DNS Filtering?

DNS filtering is the practice of using the Domain Name System (DNS) to block access to malicious websites and filter out harmful or inappropriate content. DNS acts as a translator, matching user-friendly domain names (like google.com) to numerical IP addresses (like 209.85.203.138). This process allows users to access websites without needing to remember complex numeric addresses.

DNS filtering plays an essential role in enhancing cybersecurity, acting as a safeguard against various online threats. However, it should be part of a comprehensive security strategy that includes multiple layers of defence to ensure maximum protection.

Why is DNS Filtering Important?

While DNS filtering is a crucial component of an organisation's cybersecurity strategy, it should not be relied upon in isolation. It often serves as the last line of defence against online threats.

Real-World Scenario

Consider a situation where a phishing email successfully bypasses your email security measures, and the recipient unknowingly clicks a link requesting their username and password. In such a case, a robust DNS filter can prevent the user from reaching the malicious website, thereby protecting their sensitive information and reducing the risk of a data breach.

Password management

The Importance of Password Management

In today's digital age, we're advised to create strong, unique passwords for each of our online accounts, especially for critical services like email, banking, shopping, and social media. However, managing numerous accounts with distinct passwords can be challenging, making it easy to fall into the trap of reusing passwords or opting for weaker ones.

A password manager is a valuable tool that helps address this issue. It securely stores all your passwords, so you don't have to remember each one individually. Instead, you only need to remember one strong password to access the password manager. This approach allows you to use unique, complex passwords for all your important accounts without the mental burden of recalling each one.

Risks of Browser-Based Password Management

While many modern web browsers come with built-in password management features, they can be risky. Hackers often target outdated web browsers to harvest saved passwords. Therefore, relying on browser-based password storage is generally not considered best practice for securing sensitive information.

Sharing Credentials in Businesses

In many organisations, sharing usernames and passwords for accessing various online portals is common. Password managers facilitate this process by allowing secure sharing of credentials while keeping the actual passwords hidden. This eliminates the need for insecure methods, such as writing passwords on post-it notes.

Password managers offer several beneficial features, including:

- **Synchronization Across Devices:** Easily log in from any device, as your passwords are accessible everywhere.
- **Strong Password Generation:** Automatically suggest strong passwords when signing up for new services or changing existing ones.
- **Password Reuse Alerts:** Notify you if you're using the same password across multiple accounts, helping you maintain uniqueness.
- **Breach Notifications:** Alert you if your password appears in known data breaches, prompting timely changes to protect your accounts.

CyberContego

Contact Us

Seamus Quinn
CEO

Phone: +353 (0)91 429 007
Mobile: +353 (0)87 825 0050
Email: seamus@cybercontego.com
LinkedIn: Seamus Quinn / CyberContego
Calendly: Book a meeting with me