OUR CYBER SECURITY SERVICES

The ITC mission is to be trusted experts, providing customers with cyber solutions and confidence to operate in an otherwise uncertain digital world.

About ITC Secure

Formed in 1995, ITC Secure has over two decades of experience delivering cyber security solutions to organisations in over 180 countries.

At the heart of ITC's cyber services is a London based, 24-hour, manned Security Operations Centre. From this centre of excellence, ITC's teams deliver high quality managed security services to help organisations manage the growing complexity of cyber threats and securely support their digital transformation.

ITC's cyber advisors support customers from our London and Washington DC offices, driving cyber security change inside organisations and helping them make the right security investment choices.

ITC is making the digital world a safer place to do business.

Investing in People

At ITC we are passionate about our people, we value diversity and invest in the tools needed to ensure we attract the best talent from around the world.

OUR CYBER SECURITY SERVICES

ITC Cyber Advisors

CISO AS A SERVICE

CYBER ASSESSMENTS

CYBER DUE DILIGENCE

PENETRATION TESTING

ITC Managed Security Services

BEHAVIOURAL ANALYTICS

EMAIL PHISHING PROTECTION

ENDPOINT DETECTION AND RESPONSE (EDR)

FIREWALL AND INTRUSION PREVENTION

LOG MANAGEMENT

NETWORK ACCESS CONTROL (NAC)

SECURITY INCIDENT EVENT MANAGEMENT (SIEM)

SENTINEL SIEM

SENTINEL MDR

THIRD-PARTY RISK MANAGEMENT

THREAT INTELLIGENCE

VULNERABILITY INTELLIGENCE

Use this navigable tool to view each of our cyber security services.

Click on the buttons (left) to find out about each of our services – why you might need it and the key benefits associated with it.

At the foot of each services page you'll see buttons which will either return you to this portfolio page or take you to the end of the presentation.

FINISH

ITC CISO AS A SERVICE

As cyber threats continue to increase in frequency and complexity, successful organisations consider information security their key priority. Chief Information Security Officers (CISOs) are sought-after individuals who have the experience and skills to bridge the gap between the C-level leaders and information security professionals within an organisation.

Why you might need this service

With the cyber security talent gap widening – 53% of organisations wait over 6 months for qualified candidates – mid-tier businesses are struggling to find experienced (and certified) personnel who are both knowledgeable cyber professionals and leaders with a high degree of business acumen.

However, hiring the right CISO is not the only challenge. Long-term retention of good CISOs is also difficult as they are often being poached by other companies. So, for many mid-tier enterprises, attracting and retaining a full-time CISO is simply not cost effective.

Key benefits

Utilising CISO as a service will enable you to bridge the gap between senior leadership and information security. When the right CISO is placed within an organisation, they use their field experience and leadership skills to develop information security to not only support the business cyber security needs, but to enable an organisation to keep winning in their marketplace. This service provides:

- Security leadership at a cost tailored to your organisation's needs
- Direct access to a selection of experienced and highly skilled candidates that can competently drive your organisation towards achieving mature, sustainable information security defences

Why ITC Cyber Advisors

The advisory team will ensure you are paired with a CISO that is right for your business. ITC has been providing CISO as a service for many years and can draw on experience of working with various high-profile organisations.

ITC CYBER ASSESSMENTS

The crucial first step in managing cyber risk is to understand it. An ITC Cyber Assessment will provide you with this understanding. We assess every aspect of your organisation: technology; culture; governance; and people, to give you a clear, comprehensive and independent understanding of the specific levels of risk you face. This puts you in the optimum position to address and lower your cyber risk.

Why you might need an assessment

To manage your organisation's cyber security and ensure the safety of your most valuable data assets. You need to understand the levels of cyber risk you are carrying, to know where you are most vulnerable and to determine how best to prioritise your security budget.

Key benefits

An ITC cyber assessment covers:

- ■ Governance (strategy, accountability, board oversight)
- ■ Identification (asset inventory, third-party risk, user access)
- ■ Situational awareness (threat intelligence, collaboration)
- ■ Protection (patch management)
- ■ Detection (continuous monitoring, incident response)

What we deliver

Following the assessment, we deliver a report that highlights the vulnerabilities you carry in each area of your organisation. This will include a management-level executive summary of the identified issues and their potential business impact, together with a detailed technical appraisal.

We will also ensure you consider any relevant regulatory standards.

Why ITC Cyber Advisors

Our advisory team includes former members of National Intelligence and has access to some of the world's leading security experts. Using a proven methodology to show organisations their current cyber maturity, we deliver clear, outcome-based recommendations that assist organisations in making the right cyber investment choices.

BACK TO PORTFOLIO FINISH

ITC CYBER DUE DILIGENCE

This is a non-invasive review that assesses an organisation’s current cyber security (controls and practices), IT architecture and protection status. It identifies high-risk areas, red flags and cyber vulnerabilities to deliver a clear and easy to understand security ratings report.

Why you might need this service

It’s critical you have a qualified view of the cyber risks your organisation is exposed to. Whether it’s a point-in-time view of your own cyber security maturity, that of a current third-party supplier, vendor or partner, or that of a business you are considering investing in, trading with or acquiring, this service will provide you with the information needed to make informed decisions.

Key benefits

We provide a straightforward report that rates the cyber security of your business or that of a third party, giving comparisons with industry peers.

The ratings report provides data on:

- Compromised systems (evidence of any communication with known malware-associated IP addresses)
- Diligence (the configuration of public facing services, such as emails and encryption)
- User behaviour (potentially insecure practices such as the use of peer-to-peer file sharing)

Why ITC Cyber Advisors

We partner with leading private equity and international law firms to promote cyber due diligence. Our credible and confidential reporting enables better, fact-based, decision-making which helps prevent financial loss and reputational damage.

ITC PENETRATION TESTING

Regular penetration (or pen) testing is an important step in hardening an organisation’s cyber security posture. Under controlled conditions it will highlight vulnerabilities and enable them to be fixed before they are exploited. By identifying vulnerabilities, predicting their likelihood and quantifying the possible impact, pen testing enables proactive management and the implementation of corrective measures which can be used to shape an organisation’s cyber security strategy.

Why you might need this service

In an age of threat actors with advancing sophistication, a growing number of breaches are achieved or leveraged using application vulnerabilities. Regular pen testing is therefore a crucial aspect of any robust cyber security solution. It will enable vulnerabilities to be identified before they can be exploited. Pen testing also provides the initial vulnerability assessment that is an essential part of any cyber security strategy.

Key benefits

Following the pen test we deliver a report highlighting identified vulnerabilities and recommend the remediation steps necessary to mitigate these vulnerabilities. The report will include an executive summary of the identified concerns and their potential business impact.

An ITC pen test will help you to:

- Uncover critical vulnerabilities in your environment
- Prioritise and tackle risks based on their exploitability and impact
- Meet compliance with industry standards and regulations such as ISO and PCI-DSS
- Protect your brand and market reputation
- Provide assurances to information security and senior management

Why ITC Cyber Advisors

Our pen tests are delivered by professionals with a history of handling complex, large-scale vulnerability assessments across a wide range of clients and industry sectors. The advisory team uses a proven ITC methodology to assist organisations with achieving cyber security maturity.

BACK TO PORTFOLIO

FINISH

ITC BEHAVIOURAL ANALYTICS

Insider threats to your cyber security are potentially the most devastating. They are founded on familiarity with your organisation and privileged access to your data. If Edward Snowden can undermine the NSA, what are the chances an individual could wreak havoc with your business?

Why you might need this service

Based on machine learning and artificial intelligence, it observes and monitors user devices and network activity to learn your organisation's way of life. It can then detect threats and anomalies in real time – and act on them.

This will help you manage the evolving risk of cyber attacks and ever-present insider threats, meet increasing regulatory expectations, and make best use of finite resources.

Key benefits

It is an automated process that provides 24x7x365 security risk reduction and real time remediation of incidents that may have gone undetected in traditional event-driven alerting platforms.

In addition it:

- Frees-up existing staff (entire network monitoring reduces reliance on security maintenance)
- Brings greater visibility of network traffic (maintains regulatory compliance)
- Increases flexibility and cost-effectiveness (additional benefits through integration with existing services)

Why ITC

From our Security Operations Centre we monitor logs, incident reports, anomaly threats and insider risks, alerting you through prioritised, consumable reports for both technical and executive audiences.

ITC EMAIL PHISHING PROTECTION

Phishing attacks are a daily occurrence. Recent stats indicate that over 90% of cyber attacks start with a phishing email. Phishing is becoming more widespread and, as it develops in sophistication and effectiveness, its impact is growing year on year. To help organisations prepare for and counter such attacks, ITC delivers simulated phishing campaigns that target the organisation's employees. These simulations are also important to help raise awareness around these types of attacks.

Why you might need this service

It is crucial to understand the exposure your organisation has to phishing, spear phishing, or even whaling attempts. Knowing what these types of attacks look like is the first step in ensuring the safety of your network and, ultimately, the reputation of your business. In raising awareness of these threats, this service strengthens a key part of your cyber security – your people.

Key benefits

Using statistics from a simulated phishing campaign we are able to produce an in-depth executive summary identifying areas within an organisation that would benefit from increased or additional cyber awareness training.

The service provides:

- Sophisticated and safe simulated phishing campaigns run on a quarterly basis
- Increased awareness of phishing attacks within an organisation
- An understanding of the responsive actions employees should take

Why ITC

The advisory team uses a proven ITC methodology to help organisations achieve security maturity and ensures their employees are aware of cyber risks. Our credible and confidential reporting enables better, fact-based, decision-making which helps prevent financial loss and reputational damage.

BACK TO PORTFOLIO

FINISH

ITC ENDPOINT DETECTION AND RESPONSE (EDR)

ITC delivers a quick-to-deploy, fully managed, 24x7x365, EDR service that is the next generation in antivirus and endpoint detection and response. We ensure key endpoints are monitored, cyber threats are detected and breaches, should they occur, are contained.

Why you might need this service

If malicious software is introduced to your network it can wreak havoc with your systems, devices and data. But with an increasing number of users and entry points, and the ever-present risk of malware emails, how can you provide a sufficient detection and response service?

Key benefits

- 24x7x365 monitoring (via our Security Operations Centre in London)
- Response to critical incidents on all endpoint devices
- Cloud processing of endpoint agent data
- Automated updates (for software and cyber threats)
- Prioritised endpoint actions (from containment to disconnection)
- Real time protection in support of digital/cloud transformation
- A collaborative on-boarding process
- Remediation advice and support
- Replaces and extends traditional signature-based antivirus

ITC's managed EDR service optimises the use of automation, threat intelligence and our Security Operations Centre resources. It enables rapid predictive data gathering, defence updating and corrective action.

Why ITC

Our best-in-breed EDR solution is supported by a team of expert analysts who are on hand 24x7x365 to deliver forensic cyber threat intelligence that will help detect threats, ensure relevant response and protect your endpoints if, and when, the worst-case scenario actually happens.

ITC FIREWALL AND INTRUSION PREVENTION

Network intruders, who could come from inside as well as outside the network, will look to exploit your vulnerabilities. They'll launch distributed denial-of-service attacks, or attack Internet connections. This has the potential to release worms and viruses that can spread across worldwide networks in a matter of moments. There is often no time for human intervention – the network itself must possess the intelligence to recognise and mitigate these dangers.

Why you might need this service

This is a cost effective, entry-level cyber protection service that guards against network intruders and attackers. Allowing you to be sure your network perimeter is secure, and to know that anyone accessing it, from outside or inside, will not pose a risk to your cyber security. It's an essential part of the cyber security basic hygiene that all businesses should adopt, and it ensures compliance with the growing demands from tighter regulation.

Key benefits

The service ensures that, in spite of an ever-evolving threat landscape, your critical infrastructure is protected and you have control and visibility of all applications.

ITC delivers:

- 24x7x365 proactive monitoring and management
- Rapid deployment of preventative measures
- Protection against advanced persistent threats
- Actions to stop malware entering your network
- ISO 20000:1 change control processes
- Easy integration with other ITC services

Why ITC

We have more than two decades' experience of delivering firewall and intrusion protection for some of the UK's best-known organisations and a number of major global brands. The service is managed by expert analysts from our state of-the-art Security Operations Centre in London.

ITC LOG MANAGEMENT

This service logs the activity on your network and uses the data to identify cyber threats – actual and potential. It also supports the regulatory requirement for businesses to retain user logs which can be forensically analysed.

Why you might need this service

How do you know who's using your network, when and for how long? Can you compare usage to identify suspicious behaviour? And do you have records that confirm your regulatory compliance?

Key benefits

This service simplifies your security arrangements by providing:

- 24x7x365 monitoring (via our Security Operations Centre in London)
- Time-synchronised logs across your multiple platforms (infrastructure, servers, endpoints and applications)
- Scalable secure storage for the multiple terabytes of data logged each day
- A centralised repository which ensures regulatory compliance

The service also enables better risk management and decision-making, as logged data can be used in sophisticated 'what ifs?' to evaluate, and plan for, possible future intrusions. This means appropriate recovery plans can be designed around likely scenarios.

Why ITC

We provide automated/scheduled reporting, access to security experts, and the cost certainty associated with continual, resilient management and platform support. Our managed security services have been providing visibility, control and assurance to major global brands for more than two decades.

BACK TO PORTFOLIO

FINISH

ITC NETWORK ACCESS CONTROL (NAC)

NAC reduces cyber risk by establishing and enforcing security policies that control/restrict the users and devices that can access your network.

Why you might need this service

How can you provide a mobile workforce or a diverse customer base with access to your network while ensuring security and complying with data regulations?

And with BYOD and the IoT can you really police who, and what, uses your network without limiting creativity, reducing productivity and potential excluding new business?

Key benefits

Through a process of simplifying, identifying, controlling and remediating, our NAC service enables seamless interaction, while ensuring compliance.

The service provides:

- 24x7x365 proactive monitoring and management across your entire network (wired and wireless)
- Visibility from any device, anywhere, at any time
- Processes for guest access and onboarding
- Assurances to keep pace with ever-evolving cyber threats (patch management policies)
- Automated containment of rogue or compromised devices

Why ITC

We partner with technology specialists to provide continuously managed NAC services that protect corporate networks. We incorporate centralised access control, user and device visibility, enforced endpoint compliance and holistic network protection, all of which helps alleviate the pressure on your already-stretched internal resources.

BACK TO PORTFOLIO FINISH

ITC SECURITY INCIDENT EVENT MANAGEMENT (SIEM)

Our SIEM service provides 24x7x365 proactive security to protect an organisation’s most precious data assets. It incorporates centralised logging, threat monitoring and vulnerability management. Our UK-based team of security analysts supports the service.

Why you might need this service

In an ever-evolving threat landscape, with increasing corporate risk responsibilities, more regulated compliance rules and hefty breach fines, how do you manage your cyber risk, your critical data and protect your brand reputation?

Key benefits

The main benefit associated with ITC’s SIEM service is peace of mind. We deliver this through a constant process of monitoring known areas of risk and analysing dynamic threat feeds, which we review against your logging data, asset model and vulnerability management rules.

The service provides:

- 24x7x365 protection
- Access to expert analysts
- Real time threat and response advice
- Straightforward threat reports

In a world where cyber resource is scarce and most businesses require around ten full-time staff to provide 24-hour network monitoring, our experts take the pressure off your security team and help you make the most of your IT budget.

Why ITC

We have more than two decades’ experience of delivering SIEM for some of the UK’s best-known organisations and a number of major global brands. The service is managed from our state-of-the-art Security Operations Centre in London.

ITC SENTINEL SIEM

ITC's SOC and Microsoft's Azure Sentinel platform provides a comprehensive approach to data collection, threat detection, incident investigation and rapid response. Our London-based expert analysts manage and support the service 24 hours a day, 365 days a year.

Why you might need this service

To address evolving cyber threats, businesses need to be proactive rather than reactive. Increased responsibility on internal IT teams and manual processes divert the focus of budgets and resources.

A partnership with ITC will alleviate internal pressures, provide access to security experts and industry-leading automated tools and technology so your business can focus on the bottom line.

Key benefits

Through built-in machine learning and artificial intelligence, ITC's Sentinel managed service brings automation and orchestration to multiple security tasks. Adhering to a range of compliance rules and regulations, the need for centralised logging is addressed, allowing data to be collected at cloud-scale, providing unlimited compute and storage capability.

The service provides:

- 24x7x365 management, detection and response
- Access to expert analysts
- Automation of common tasks and incident response
- Easy integration into behavioural analytics tools, workflow management systems (ServiceNow etc.)
- Simple and scalable pricing

Why ITC

ITC has over 25 years of experience delivering managed security services for a number of global brands. Delivered and managed through our world-class, London-based, Security Operations Centre, we utilise the industry's first cloud-native technology to automate and orchestrate an all-encompassing security information and event management solution.

ITC SENTINEL MDR

As businesses and the technical architectures that support them evolve, perimeter-less security is becoming the new normal. With this comes new risk requiring alternative strategies for response and mitigation.

ITC Sentinel Managed Detection and Response (MDR) is a complete endpoint security solution that delivers preventative protection, post-breach detection, automated investigation, and response.

Why you might need this service

To minimise cyber security risk to your business, it is essential to gain visibility of and rapidly identify and shut down cyber threats. Being able to do that 24/7 is another challenge.

By seamlessly integrating Microsoft Defender Advanced Threat Protection and Microsoft's cloud-native SIEM tool, Azure Sentinel, this sustainable and all-encompassing solution delivers protection across the entire kill chain, and therefore business.

Why ITC

ITC has over two decades of experience delivering cyber security solutions to organisations in over 180 countries. Delivered and managed from our world-class, London-based, Security Operations Centre, we utilise the best in breed technology and combine it with the finest talent in the industry. This ensures we can provide your business with consistent, high-quality managed security services.

The service provides:

- Unparalleled Visibility
- Exceptional Threat Detection
- Expert Response
- Security recommendations and best practice advice for improved cyber security posture
- Empower in-house teams with access to ITC's security expert oversight and assistance
- Seamless integration across Microsoft Security portfolio and ITSM tools (ServiceNow etc.)
- 24x7x365 management, detection and response

BACK TO PORTFOLIO FINISH

ITC THIRD-PARTY RISK MANAGEMENT

This is a fully managed service that helps organisations measure, manage and reduce their exposure to third-party and supply chain-related cyber threats. We provide continuous daily monitoring of third parties, using an industry recognised scoring system to identify where risk is highest and to alert customer and third party on the actions needed to improve their cyber security position.

Why you might need this service

It's estimated that over 60% of breaches are linked to third parties. So, understanding and mitigating this risk is a business imperative. Whether it's vendors, clients, partners or acquisitions you're dealing with, continuous visibility of their security performance is critical. Poorly rated third parties carry a significantly higher risk of cyber breach.

Key benefits

Using externally observable data, our analysts can rate all the third parties you interact with.

The service provides:

- A stress-free onboarding process
- 24x7x365 monitoring
- Industry recognised ratings from expert analysts
- Risk identification and advice for remediation
- Peer and industry comparisons
- Frees up time for your valuable internal resources

Why ITC

From our London-based Security Operations Centre we constantly monitor the world of cyber security, ensuring that all relevant threats are identified, and our customers are given the right advice to reduce risk exposure.

In addition, our cyber experts deliver a comprehensive onboarding process that ensures a complete understanding of your risks and priorities.

BACK TO PORTFOLIO FINISH

ITC THREAT INTELLIGENCE

It’s virtually impossible to maintain a view of all threats across the surface web and the dark web that could impact your business. Which is why threat intelligence services are becoming a major element in most cyber defence strategies.

Why you might need this service

Constant monitoring is needed to track current and potential cyber threats, which may be specific to your organisation or a global trend. Threat actors are varied and many.

Information is disparate, and difficult to find, mine and interpret. The time it takes to identify threats and react during incidents is critical. And resource constraints, limited data sets and data overload are a challenge.

Key benefits

ITC’s managed Threat Intelligence is a professionally-deployed and maintained service that ensures your key information is protected. It alerts you to relevant information, filters out false threats, spots future threats and enables a proactive response. And by using prediction and prevention, rather than detection after the event, you can make the best cyber security decisions for your business.

The service provides:

- Broad visibility, including areas such as brand monitoring
- Business risk-aligned reporting
- Alerting with context triggered by new threats or data leaks
- Real time threat identification through machine learning
- Sensitive projects support
- Security operations access to the threat intelligence platform
- Integrated risk scoring

Why ITC

ITC utilises a highly-stable commercial platform chosen for its breadth and depth of information. We ensure constant feedback and tuning, together with monthly reporting and de-brief sessions. We also provide support with intelligence goals and special projects that require critical fine tuning.

ITC VULNERABILITY INTELLIGENCE

Businesses face hundreds of malicious attempts to break their cyber defences every day, and nearly half of all UK firms have suffered breaches or attacks in the last 12 months. Our Vulnerability Intelligence service helps you cope with this threat. It identifies your overall exposure to cyber attacks, ascertains the dangers inherent in your network, and enables you to prioritise your security spend.

Why you might need this service

It will help you to understand the threat to your business, and enable you to take control of, and manage your level of risk. It does this by establishing where you are most vulnerable to cyber attacks, identifying precisely what's on your network, where your key data is housed, what should be patched and how effective your patching process is.

It also considers the cyber threats to your business – what they are, which are a priority and where you are most vulnerable to the attacks that will inevitably occur.

Key benefits

You will obtain visibility of all your assets (known and unknown), and gain an understanding of those that are critical to your business.
To make this possible we:

- Provide visibility of disparate systems and applications
- Identify your critical data
- Show you where you are most vulnerable
- Review the effectiveness of your current patching process

Why ITC

We are proven vulnerability experts, delivering global visibility, control and assurance, supported by 24x7x365 monitoring and management from our London-based Security Operations Centre.

CREDENTIALS

Operating from our state-of-the-art Security Operations Centre in London, we have more than two decades' experience in monitoring and securing data networks for some of the world's best-known brands.
A few examples are shown here.

Our advisory team includes former members of National Intelligence and has access to some of the world's leading security experts. Using a proven methodology to show organisations their current cyber maturity, we deliver clear, outcome-based recommendations that assist them in making the right cyber investment choices.

All information we provide is credible and confidential, enabling better, fact-based, decision-making.

British American Tobacco
Coller Capital
Coca-Cola
ABInBev
BM Brooks Macdonald
Schroders
MIZUHO
photobox
DeepMind
TeamViewer
VANQUIS BANK
PERMIRA
3i

Making the digital world a safer place to do business

10th Floor
5 Churchill Place
London E14 5HU

itcsecure.com
Tel: +44(0) 20 7517 3900
enquiries@itcsecure.com