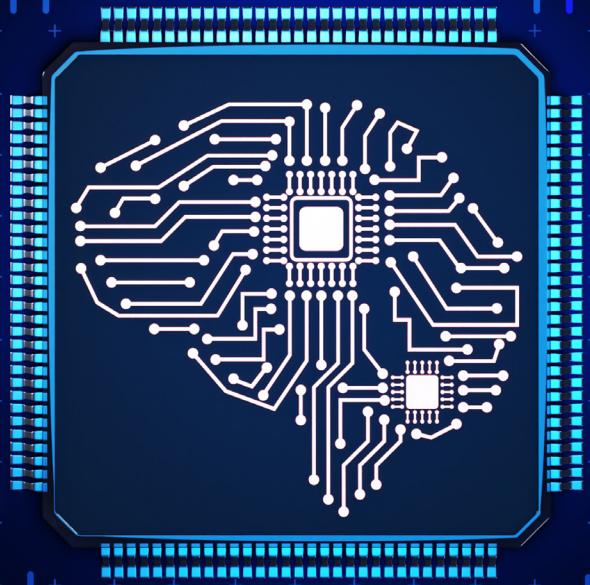
european electronique

in partnership with **SOPHLEE**



ELITE CYBER SECURITY SOLUTIONS

Secure Today, Secure Tomorrow

ABOUT US

At European Electronique, we are the architects of secure digital transformation. With a bold vision and commitment to innovation, we provide cutting-edge IT services and infrastructure solutions that safeguard your business's future.

Our Mission

To empower organisations with advanced cybersecurity and IT infrastructure solutions that protect, enhance, and drive success. We believe in a proactive approach to security, ensuring your data and operations are always a step ahead of emerging threats.

What We Do

We offer a comprehensive suite of services designed to strengthen your digital landscape and drive business efficiency:

- **IT Services & Infrastructure:** Crafting resilient, scalable, and secure IT environments tailored to your business needs.
- **Cybersecurity Solutions:** Implementing state-of-the-art security measures to protect against cyber threats and ensure data integrity.
- **Digital Transformation:** Leading your business through seamless integration of digital technologies to enhance operations and drive growth.
- **Cloud Services:** Delivering flexible and robust cloud solutions for dynamic business environments.

Why Choose Us?

- **Innovative Solutions:** We harness the latest technologies to provide forward-thinking, reliable solutions.
- **Customer-Focused:** Your security and success are our top priorities. We tailor our services to meet your unique needs.
- **Expert Team:** With decades of experience, our experts deliver unparalleled knowledge and insights.
- **Dependability:** We are a trusted partner dedicated to excellence and reliability in every project.

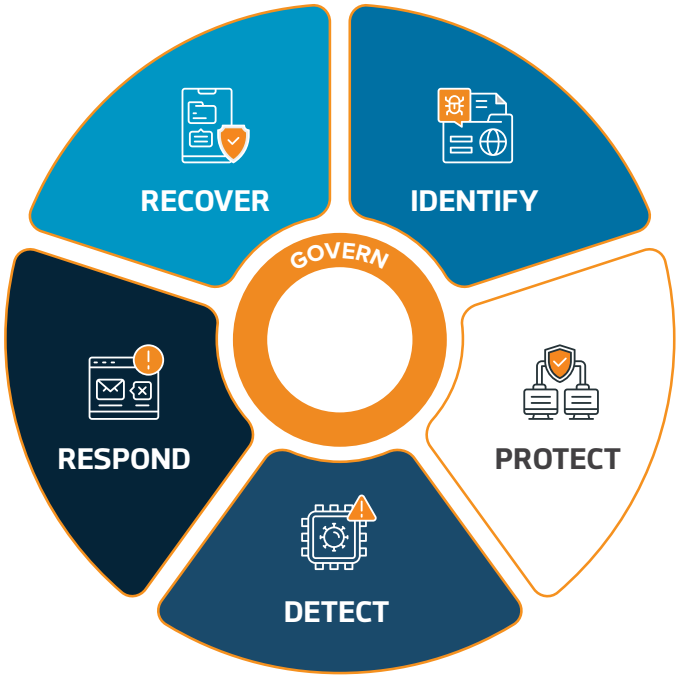
Our Vision

To lead the IT industry in cybersecurity and infrastructure, continually setting new standards for innovation and excellence. We aim to protect and empower organisations , ensuring a secure and prosperous digital future.

Join us in shaping a secure, innovative future. Together, we'll protect your business, secure your future, and unlock limitless possibilities.

OUR APPROACH

OUR APPROACH



IDENTIFY

The organisation's current cyber security risks are understood. Understanding the organisation's assets (e.g., data, hardware, software, systems, facilities, services and people), suppliers, and related cyber security risks enables an organisation to prioritise its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organisation's policies, plans, processes, procedures, and practices that support cyber security risk management to inform efforts under all six Functions.

PROTECT

Safeguards to manage the organisation's cyber security risks are used. Once assets and risks are identified and prioritised, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cyber security events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.

DETECT

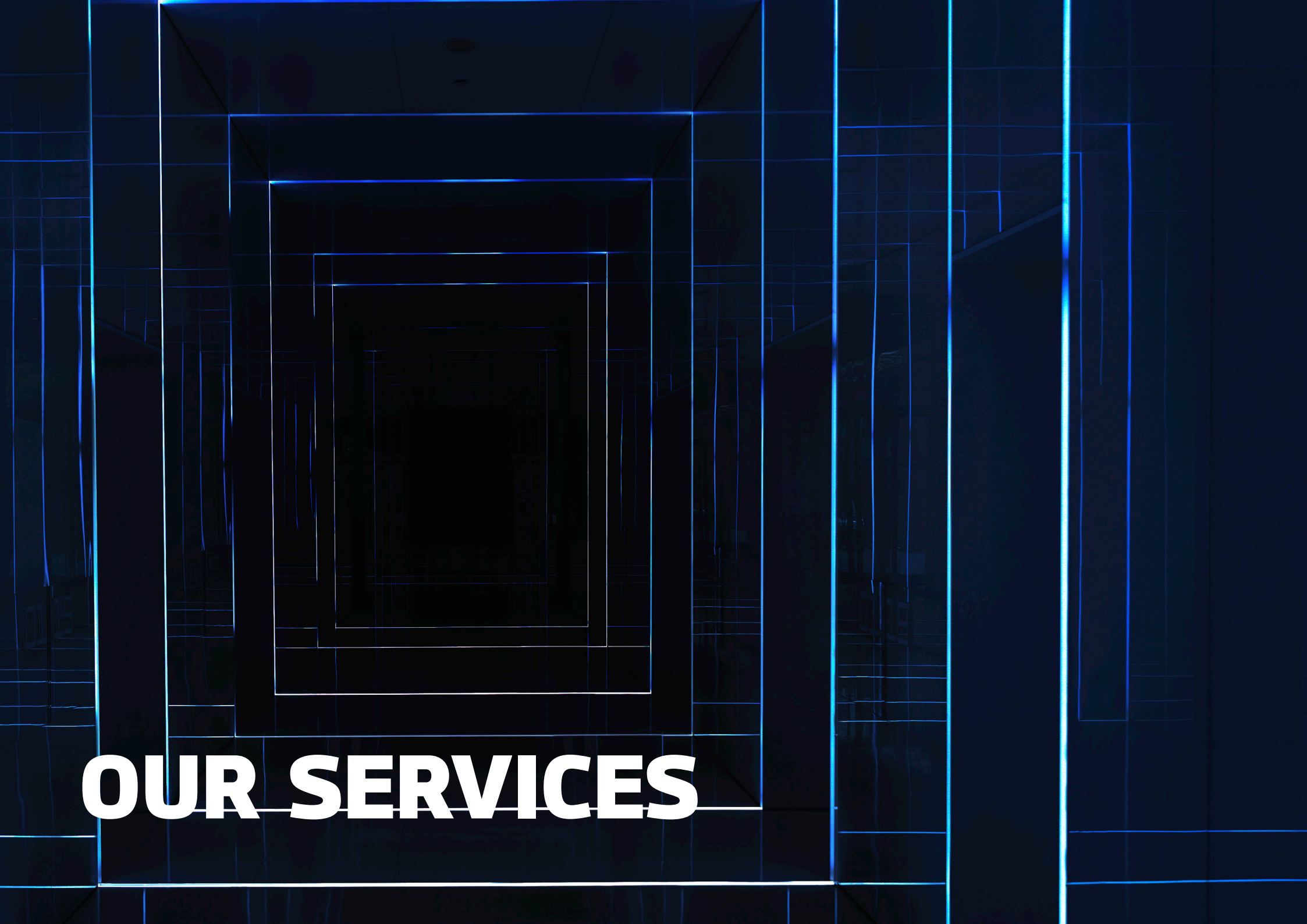
Possible cyber security attacks and compromises are found and analyzed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cyber security attacks and incidents are occurring. This Function supports successful incident response and recovery activities.

RESPOND

Actions regarding a detected cyber security incident are taken. RESPOND supports the ability to contain the effects of cyber security incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

RECOVER

Assets and operations affected by a cyber security incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cyber security incidents and enable appropriate communication during recovery efforts.


OUR SERVICES

OUR SERVICES

Safeguarding your organisation from cyber threats is more critical than ever. European Electronique is at the forefront of providing comprehensive cyber security solutions designed to defend, protect, and ensure the resilience of your digital infrastructure. Our services are tailored to meet the dynamic needs of today's businesses, spanning across various domains of cyber security.

EE DEFENCE

Endpoint Security | Vulnerability Management Service | Phishing | Training & Awareness | Disaster Recovery | Media Hygiene | Secure Remore Access

EE OFFENCE

Penetration Testing | OSINT Gathering Analysis & Reporting | Vulnerability Assessments | Incident Response | Computer Forensics

EE ASSURE

Cyber Essentials | Cyber Essentials Plus | IASME Governance | DFE Compliance | NIS Compliance

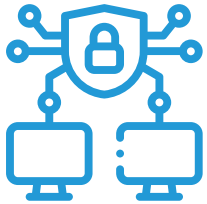
EE OT

Network & Asset Visability | Log Management | Incident Response | Backup Recovery | Media Hygiene | Secure Remote Access | 62443 Risk Assessments | ICS Penetration Testing


EE DEFENCE

01

EE DEFENCE



Endpoint Security

In the face of increasing attack sophistication, volume, and pace, driven by AI, organisations require a complete security framework – to identify, protect, detect, respond, and recover.

Phishing

A large part of keeping your business safe is making sure that employees avoid online threats. Simulated phishing is a great way to give your employees hands-on, risk-free experience with scam emails. And we'll get it all set-up and configured for you.

Media Hygiene

Protect your critical network and assets against removable media threats any time portable media accesses your environment. Software updates, reporting, audits, and more all require external data sources and as threats evolve, so too must the means necessary to protect your organisation from them.

Vulnerability Management

New vulnerabilities emerge daily. VMaaS lets you stay on top of them through a risk-based approach to vulnerability management, which includes vulnerability scanning, analysis and prioritisation.

Disaster Recovery

Advanced Disaster Recovery enables you to restore operations in a few clicks, without any upfront investments, so you can rapidly recover workloads or services in the event of ransomware, hardware failure, and any other disruption.

Secure Remote Access

Safeguard your environments against evolving cyberthreats. Implementing a secure remote access platform within a day and without disrupting operations to enable professionals to safely connect from anywhere in the world.

Protective Monitoring

Network monitoring is the systematic process of observing and analysing network traffic to ensure its smooth operation, security, and performance. It involves the continuous surveillance of network components, such as routers, switches, servers, applications and endpoints, to gather data on their behaviour and status. This data is then analysed to detect anomalies, identify potential issues, and optimise network performance.

EE OFFENCE

EE OFFENCE

Penetration Testing

Penetration testing, also known as pen testing, is an ethical cyber security assessment method aimed at identifying and safely exploiting vulnerabilities in computer systems, applications, and websites. By employing the tools and techniques used by real cyber adversaries, pen testing accurately replicates the conditions of a genuine attack, providing valuable insights for remediation.

Incident Response

In today's digital landscape, cyber threats lurk around every corner, ready to disrupt your operations and compromise your valuable data. Our cutting-edge Cyber Security Incident Response solutions are here to safeguard your organisation against the unexpected.

Computer Forensics

Our computer forensics service involves the collection, preservation, analysis, and presentation of digital evidence stored on computers and digital storage media. It encompasses techniques and methodologies to investigate and uncover evidence related to cybercrimes, data breaches, unauthorised access, and other digital incidents.

OSINT Gathering & Reporting

Our OSINT Gathering And Reporting (OGAR) service can monitor where cyber criminals are active on the open, deep, or dark web. We can identify threats to your company and executives, detect dark web data leakage and uncover exposed credentials.

Vulnerability Assessment

A vulnerability assessment is a systematic process of identifying, quantifying, and prioritising vulnerabilities in a system, network, or application. It involves analysing various aspects such as software, hardware, configuration settings, and user practices to determine potential weaknesses that could be exploited by attackers.


EE ASSURE

EE ASSURE

Cyber Essentials

Cyber Essentials certification demonstrates a base-level appreciation of cyber security within your organisation. The assessment process comprises of an online questionnaire being completed by the organisation, which captures information that supports the five controls being in place.

Cyber Essentials Plus

Cyber Essentials Plus builds on the requirements that are mandated by the Cyber Essentials certification and includes an active assessment that is conducted at your organisations premises.

IASME Cyber Assurance

The IASME Cyber Assurance standard provides an affordable and achievable alternative to other international standards. It allows small and medium enterprises in a supply chain to demonstrate their level of cyber security for a realistic cost and indicates that they are taking good steps to properly protect their customers' information.

NIS Compliance

Since May 2018, essential services providers have been subject to the Network and Information Systems Regulations 2018, also known as the NIS Regulations. There are 14 key principles for NIS compliance, split across four objectives. Your business must be able to manage security risk, protect against cyberattack, successfully detect cyber security events and minimise the impact of any cyber security incident.

DFE Compliance

The Department for Education (DfE) introduced its Cyber Security guidance publication as part of its 'Meeting digital and technology standard in schools and colleges' advice in 2023. As of May 2024, this guidance has been updated to reflect the current threat landscape the education sector is facing.


EE OT

EE OT

Log Management

In the world of Operational Technology, every minute counts. That's why seamless performance, robust security, and streamlined operations are non-negotiable. At European Electronique, we understand the unique challenges facing OT environments, and we're here to revolutionise the way you manage logs.

Network & Asset Visability

Network monitoring is the systematic process of observing and analysing network traffic to ensure its smooth operation, security, and performance. It involves the continuous surveillance of network components, such as routers, switches, servers, applications and endpoints, to gather data on their behaviour and status.

Secure Remote Access

Safeguard your environments against evolving cyberthreats. Implementing a secure remote access platform within a day and without disrupting operations to enable professionals to safely connect from anywhere in the world.

Backup & Recovery

Performing repetitive yet crucial tasks on sensitive systems – like full disk image and file-level backup – is a daily reality for technical personnel. So let our hardened backup solution make your job easier and your systems more resilient to attack.

Media Hygiene

Protect your critical network and assets against removable media threats any time portable media accesses your environment. Software updates, reporting, audits, and more all require external data sources and as threats evolve, so too must the means necessary to protect your organisation from them.

62443 Risk Assessments

Our IEC 62443 implementation services offer unparalleled protection for your industrial control systems (ICS) and operational technology (OT) infrastructure. By following the rigorous guidelines set forth by the standard, we ensure that your assets are fortified against cyber threats.

ICS Penetration Testing

Our penetration testing goes beyond surface-level evaluations. We conduct thorough assessments of your OT infrastructure, including industrial control systems (ICS), SCADA systems, and embedded devices, to identify vulnerabilities across the entire attack surface.

CONTACT US

Phone :
Office 01865 883300
Sales 08453 458340

Mail & Website :
sales@euroele.com
www.euroele.com

Address :
Forward House
Oakfields Industrial Estate
Eynsham, Oxfordshire, OX29 4TT