CAPABILITY OVERVIEW

Sopra Steria Cyber Centres

Advanced Threat Detection And Protection Services

Delivering Transformation. Together.

sopra steria

The individuals and gangs that want to breach your organisation's security defences are becoming increasingly sophisticated and devious in the methods and tools they use. So it is vital that you are consistently monitoring your network to the highest standards and ensuring your defences keep pace with the latest detection and protection technology and processes.

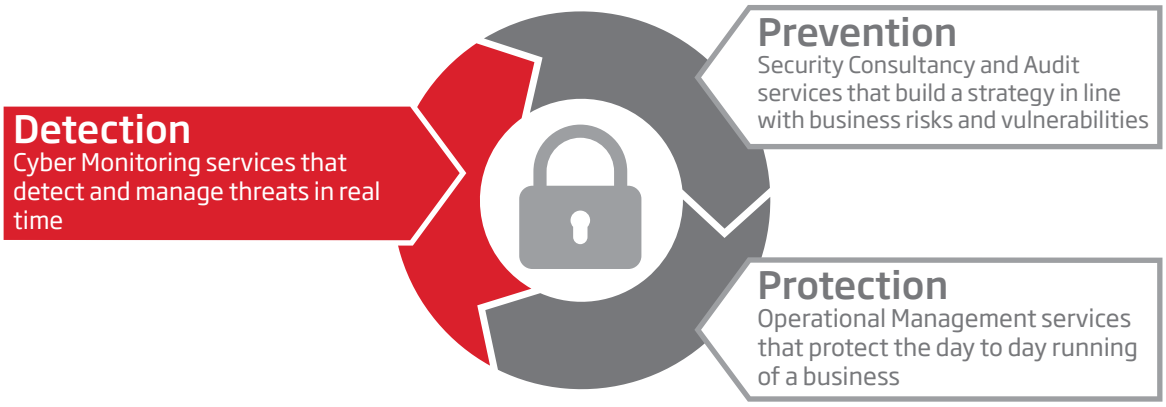
Sopra Steria Cyber Centres can help you do both these things. At our three centres in the UK, France and Singapore our experts combine the experience and knowledge of monitoring and analysing potential threats day-in, day-out with the most advanced technology and techniques available today.

They are continuously updating both the technology and their knowledge – as a result of protecting some of Europe's most targeted companies and government organisations. Our experts are also working with government security agencies like ANSSI in France, CSA in Singapore and CESG.

In addition, we subscribe to feeds from a wide range of advanced intelligence sources. All of these factors help us to continuously improve the services we provide. As a result, you can be confident Sopra Steria Cyber Centres can protect your organisation from even the most sophisticated internal and external threats.

Our service approach

Our offerings provide end-to-end cyber security capabilities



Based on strong foundations

At Sopra Steria we strongly believe that the first step to first-class threat protection is a solid security foundation. Consequently, as part of implementing our detection and prevention service, we help you assess the effectiveness of your current anti-virus, firewall, intrusion detection, intrusion prevention, and incident response capabilities and advise you if there are potential areas for improvement.

ADVANCED TOOLS

- AlienVault
- FireEye
- LogRhythm
- Nessus
- Qradar
- RSA
- RSA Envision
- Splunk

Designed for your organisation

Like all the services we provide, our Cyber Centre services are menu-driven, giving you the flexibility to choose what makes the most sense for your organisation. We can provide you with a fully outsourced detection and prevention service, fully integrated with your security and/or service management teams.

We can help you develop your own Security Operations Centre (SOC), using our expertise to advise on the most appropriate alerting and analysis tools and the best-practice processes we have developed around them.

Or you can choose a hybrid model, for example where we do the incident monitoring and hand off the investigation work to your team. Whatever works best for your organisation we can accommodate it.

Utilising the best tools and techniques

The key to successful protection is having a detailed understanding of the traffic flows within your network. The advanced alerting and analysis tools and techniques we use allowing us to sift through tens of millions of events per second and allowing us to detect malicious insider activity as well as external threats, something that is not possible using previous techniques and processes.

The tools we use automate the process of incident analysis, allowing us to sift through tens of millions of incidents a second and discard the false positives, so we only focus our attention on the small number of incidents that present a real potential danger. In addition, our sophisticated dashboards enable us to quickly drill down and reveal what is happening at the deepest levels. As a result, the time taken to detect and react to threats is minimised.

Integrated with system management

Security monitoring and management can be carried out in isolation. However, at Sopra Steria, we don't think this is the most efficient model. Instead we believe security monitoring and management should be integrated with system management, either as part of the service we provide or through your own internal team.

Running security monitoring and management in isolation results in two ticketing systems, which is inefficient and potentially counter-productive. Integrating it with system management ensures the impact of system changes on security is taken into consideration. Similarly the impact of any security actions on service level agreements can be assessed. In this way security monitoring and management becomes part of the wider IT decision making process.

Incorporating crisis management

When a major incident occurs it is vital to get on top of it quickly. Our additional crisis management service helps you respond swiftly and appropriately. We can rapidly put together a crisis management team that includes all the profiles and roles needed to handle the situation - from Sopra Steria, your organisation and third parties if needed.

Deployed in two war rooms - technical and governance - the team is backed by a comprehensive set of best practice methodologies and processes we have developed to handle a major incident through to remediation, including internal and external communications.

How can we help you?

High quality detection and prevention is essential to protect your organisations against increasingly sophisticated internal and external threats and putting the tools and processes in place is not a one-off exercise. You must be continually updating your defences as the threat landscape changes.

At Sopra Steria we have the expertise, advanced tools, threat intelligence and best practices to provide you with robust, evolving security monitoring and management services that protect your organisation to the highest possible standards.

OUR OFFERINGS

- Security Information and Event Monitoring (SIEM) Services
- Advanced Persistent Threat (APT) Detection
- Zero Day Attack Detection
- Forensic Investigation
- Crisis Management
- Security Watch and Threat Detection
- Threat Intelligence Gathering
- Vulnerability Management
- Security Operations Centre (SOC) Services
- Security Operations Centre Dashboarding

OUR CUSTOMERS

The customers that trust us to protect their IT environments include:

- Airbus
- Gloucestershire County Council
- MBDA
- RATP
- Stelia

KEY FACTS

In 2015 our three cyber security centres and 248 security professionals managed:

- 150,000 workstations
- 40,000 servers
- 5,000 applications
- 2,500 databases
- 400,000 user accounts
- 16 terabytes of SIEM log live
- 2,000 security incidents
- 300,000 EPS processed

About Sopra Steria

Sopra Steria, European leader in digital transformation, provides one of the most comprehensive portfolios of end to end service offerings in the market: Consulting, Systems Integration, Software Development and Business Process Services. Sopra Steria is trusted by leading private and public organisations to deliver successful transformation programmes that address their most complex and critical business challenges. Combining high quality and performance services, added-value and innovation, Sopra Steria enables its clients to make the best use of information technology.

To learn more about our services please:

Call: +44 (0)370 600 4466

Email: info.uk@soprasteria.com

Visit: www.soprasteria.co.uk/cybersecurity

SOPRA STERIA
Three Cherry Trees Lane, Hemel Hempstead, HP2 7AH
+44 (0)370 600 4466 - info.uk@soprasteria.com

PB044V02

www.soprasteria.co.uk

sopra steria