NTT Security

Technical Insight

Exploring your choice of Security Operations Centre models

Closing the cyber intelligence gap with the right SOC investment

In most organisations, technical security implementation remains the responsibility of the IT function. However, CSOs, who normally sit outside the IT department, require business related information from the security technologies that standard Network Operations Centres do not deliver. This results in a drive to implement Security Operations Centres (SOCs) to gain greater visibility of risk.

Where establishing a Security Operations Centre is the next phase of your security roadmap, you will be making a number of critical business decisions to maximise this investment. Whatever the drivers for your decision – to transform threat visibility and analysis, consolidate your technology, react faster to breaches and mitigate the impact, or demonstrate greater risk management capability – we would like to share our wide experience of planning and delivering successful SOC infrastructures and operating SOC services.

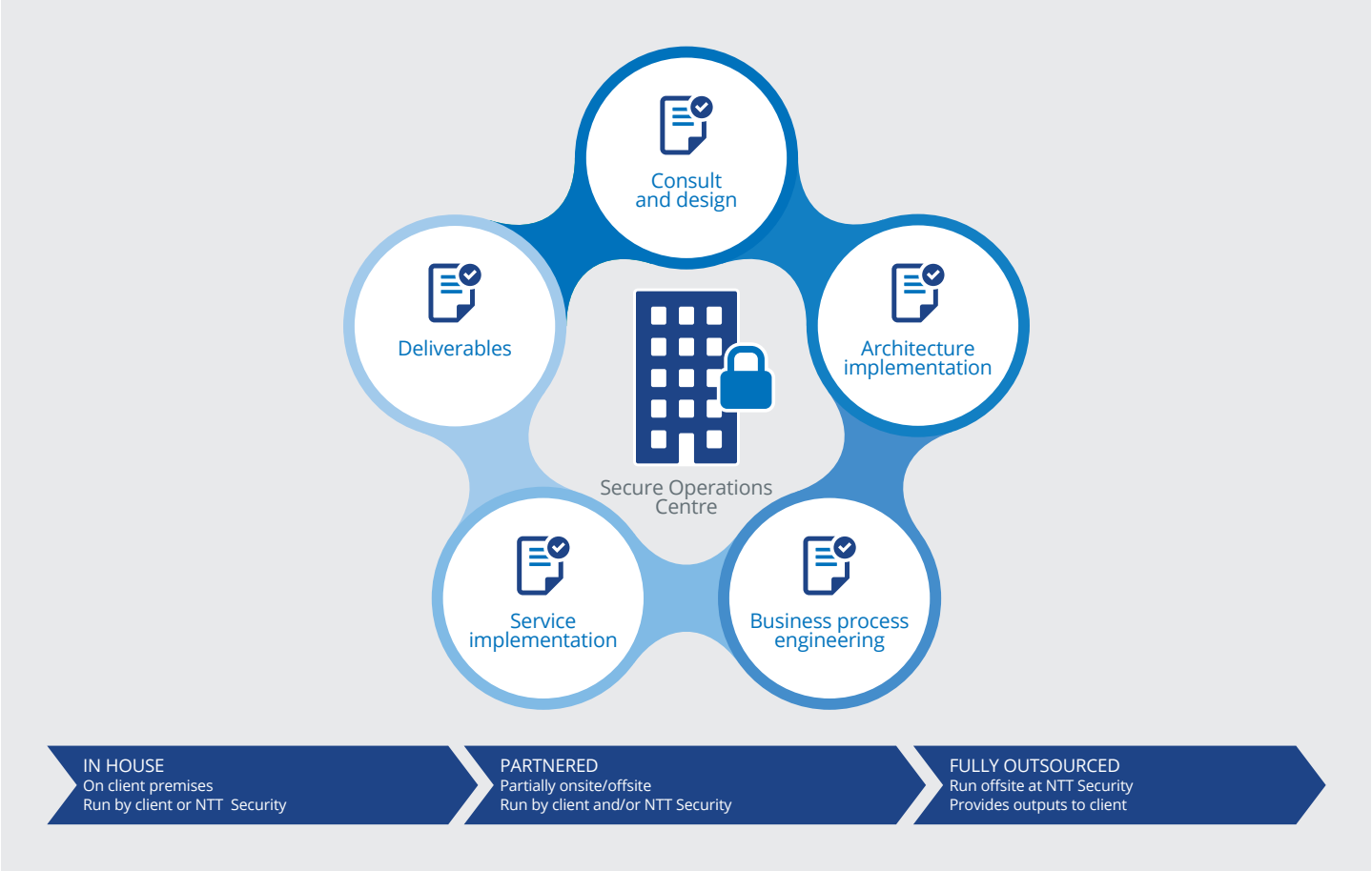
The value of a SOC to your business

Whether your organisation is considering investing in a SOC for the first time or seeking to evolve an existing SOC infrastructure, it's important to understand and communicate the objectives for the project. Being clear about the value of the SOC to your business is an important first step before any decisions are made around your approach and operating model.

In our experience, a successful SOC delivers the following business value:

- Protection of business critical information
- A single, consolidated view of all security information from every device
- Timely and meaningful security analysis based on correlated, contextual data
- Proactive risk reduction against highlighted threats and vulnerabilities
- Governance of IT policies
- Improved confidence and capability to manage security incidents and breaches

Figure 1: Illustrates the process NTT Com Security undertakes to advise a customer on the SOC options, whether the in house, partnered or fully outsourced model is chosen



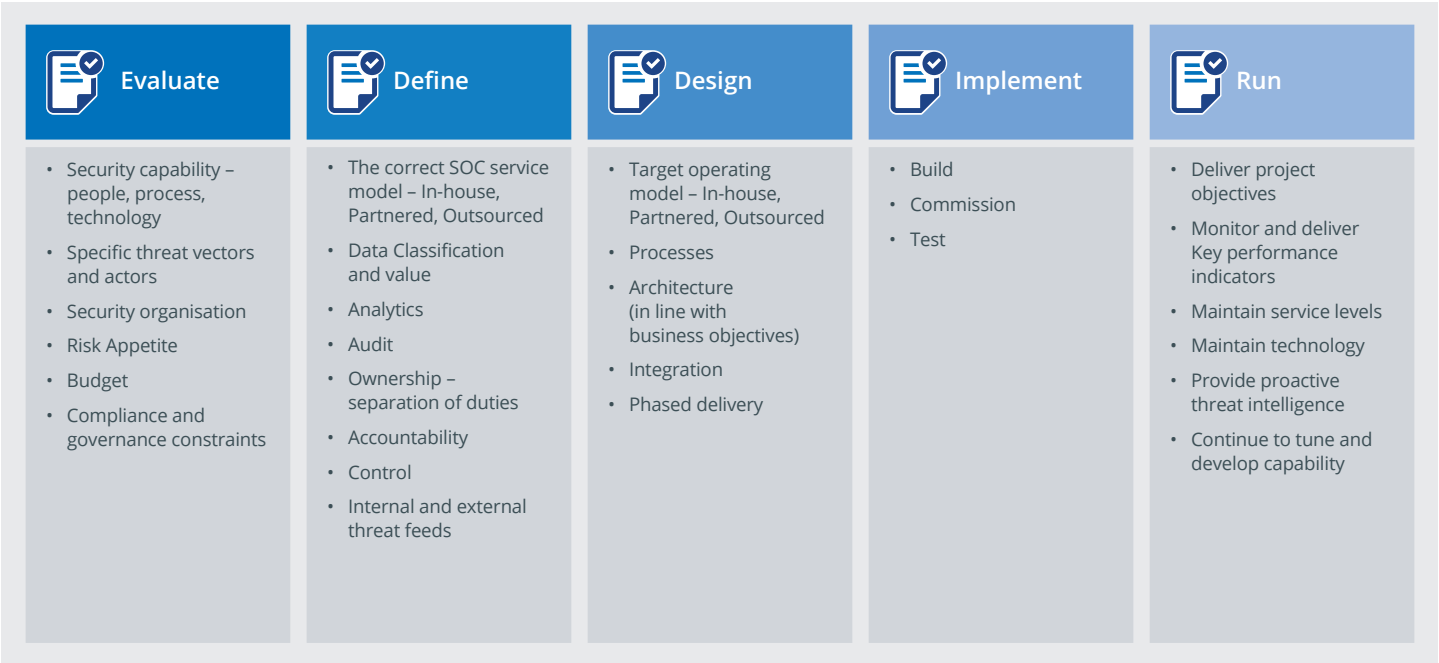
Closing the cyber intelligence gap

NTT Security is working with organisations across the globe to unify people, processes and technology into a coherent SOC service that focuses on continuous compliance and information risk management. These customers have very different business models and risk profiles with which the SOC must align, as well as a variety of existing technology investments, information security capabilities and governance and compliance requirements to satisfy. These factors all impact the SOC target operating model that the organisations choose to deploy. We are often asked to give advice in evaluating, defining and designing the SOC service. Some customers may then ask us to implement the design and in some cases, run some or all of the SOC as an outsourced service once it is operational. As in every project we undertake, we work with our customers every step of the way to help them take strategic, management and operational decisions to deliver a successful project.

Within just five years, we have witnessed organisations turning SOC investments from centralised sources of log data from network, infrastructure and security products, into a security nerve centre – driving proactive processes for threat, incident and vulnerability management. And this level of security maturity is just the beginning. Our customers are now extending the value of their SOCs to offer proactive risk management – closing the cyber intelligence gap by adding external threat intelligence to enhance the insights from existing internal data sources. We help organisations to correlate this information and most importantly, to unlock its value, placing these diverse sources in context so that they have absolute relevance to the specific business.

Any organisation considering an investment in a SOC must evaluate the choice of approach and implementation with a 360˚ perspective of the impact on the wider business. To do this, there are some common people, process and technology questions that we help our customers answer to inform their choice of approach and ultimate target operating model.

Figure 2: Evaluate/Define/Design/Implement/Run: the phases and outputs of establishing a SOC



Choosing the right SOC model for your business

Our experience has shown that there is no best practice SOC operating model to deliver maximum value. Every organisation must decide what will work best for them, having reviewed the growing number of successful operating and delivery models. Choosing the right SOC model will depend on the individual aims, circumstances, capabilities and constraints of the business. So what are the main models we have helped to create?

- **In house SOC model**
  An organisation may choose to create and run its SOC service in house. Organisations that choose to go down this route can typically exploit high levels of internal capability (maintaining the skills of staff needs careful consideration, however) or may decide this is the right course of action due to the type or value of data that must be protected. Taking this approach requires a significant budget, circa £3m and we are often asked to support the evaluation, definition and design phases of the project to ensure that the investment meets the needs of the business. Our customers use our knowledge of how to create a strategic vision and detailed plan for a SOC service, to avoid costly delays and U-turns, keep stakeholders on side and inform decisions around process, capability and technology improvement. Once the design is complete, customers may choose to build the SOC themselves or we can construct it to their design.
- **Partnered SOC model**
  Increasingly, organisations are choosing to outsource elements of SOC operation – creating a partnered model. This choice may help an organisation build additional capability in specific areas, introduce contextual external threat intelligence, or release internal resources to focus on other strategic initiatives. The partnered SOC approach uses a mix of in house and outsourced technologies, combined with NTT Security staff working hand in hand with your core business function and critical IT functions, such as resolver groups, to drive increased risk visibility and greater security maturity.
- **Fully outsourced SOC model (Managed Security Services)**
  As adoption of cloud services gains pace, some organisations may wish to fully outsource their SOC service from the outset. This model is particularly popular with organisations that do not have a large legacy estate or that have limited IT resources that are focused on running the business and are not security specialists. It is typically a more cost-effective service, with average yearly run costs circa £500k.

Whichever model organisations choose, in our experience high performing SOCs rarely stand still.

Summary

As an industry, we have come a long way in the last five years – focusing less on technology and more on identifying, understanding and managing risk. But there is still much to do. We are delighted that we have been able to help so many organisations restore information security control, confidence and compliance – closing the cyber intelligence gap by making the right investment in SOC for the business. Working with organisations at a local level, we share our global experience of SOC approaches and models to ensure businesses realign their focus and activities with corporate strategy and priorities, resulting in a more mature risk management approach. In our experience, a SOC is a critical component of the new business-led world of risk management and we have the capabilities and experience, global technology partnerships and flexible approach, to deliver solutions that unify people, processes and technology into a coherent central SOC service for the future.

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organisations to build high-performing and effective security and risk management programmes, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com**

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information