Information Security Forum

BUILDING A SUCCESSFUL SOC

DETECT EARLIER, RESPOND FASTER

Acutely aware of the adverse business impact of security incidents, organisations are seeking to reduce their exposure and keep their assets secure. Building a successful Security Operations Centre (SOC) can greatly enhance the ability to detect and disrupt cyber attacks, protecting the business from harm.

A SOC serves as the eyes and ears of an organisation, sounding the alarm when suspicious or anomalous activity is detected and enabling a rapid response to reduce the potential impact and severity of security incidents. Without a SOC, organisations lack real-time visibility of threats, impeding their ability to protect business critical assets and effectively manage information risks.

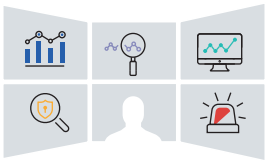
The ISF report, ***Building a Successful Security Operations Centre***, explores the key elements that are integral to optimising a SOC's performance, realising operational efficiency and pursuing innovation. It equips organisations with a practical understanding of how to design, establish and enhance a SOC that is both empowered by the business, and aligned with business requirements.

A successful SOC will demonstrate its worth to business by protecting the organisation's reputation, delivering on compliance obligations and embracing a proactive approach to risk management.

BUILDING A SUCCESSFUL SOC

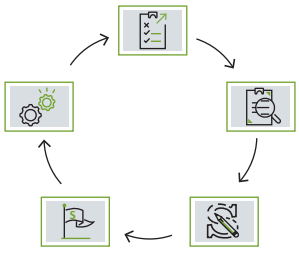
DETECT EARLIER, RESPOND FASTER

The ISF Approach for Building a Successful SOC incorporates three aspects, which enable organisations to plan for, create and evolve a high performing SOC that supports business objectives. By adopting the ISF Approach, organisations should be better positioned to detect threats earlier and respond faster to cyber attacks.



Based on business drivers, determine the set of capabilities your SOC will need to provide. The ISF Approach includes a detailed flowchart of SOC activities and highlights the fundamental skills, processes and tools required for a SOC to excel.

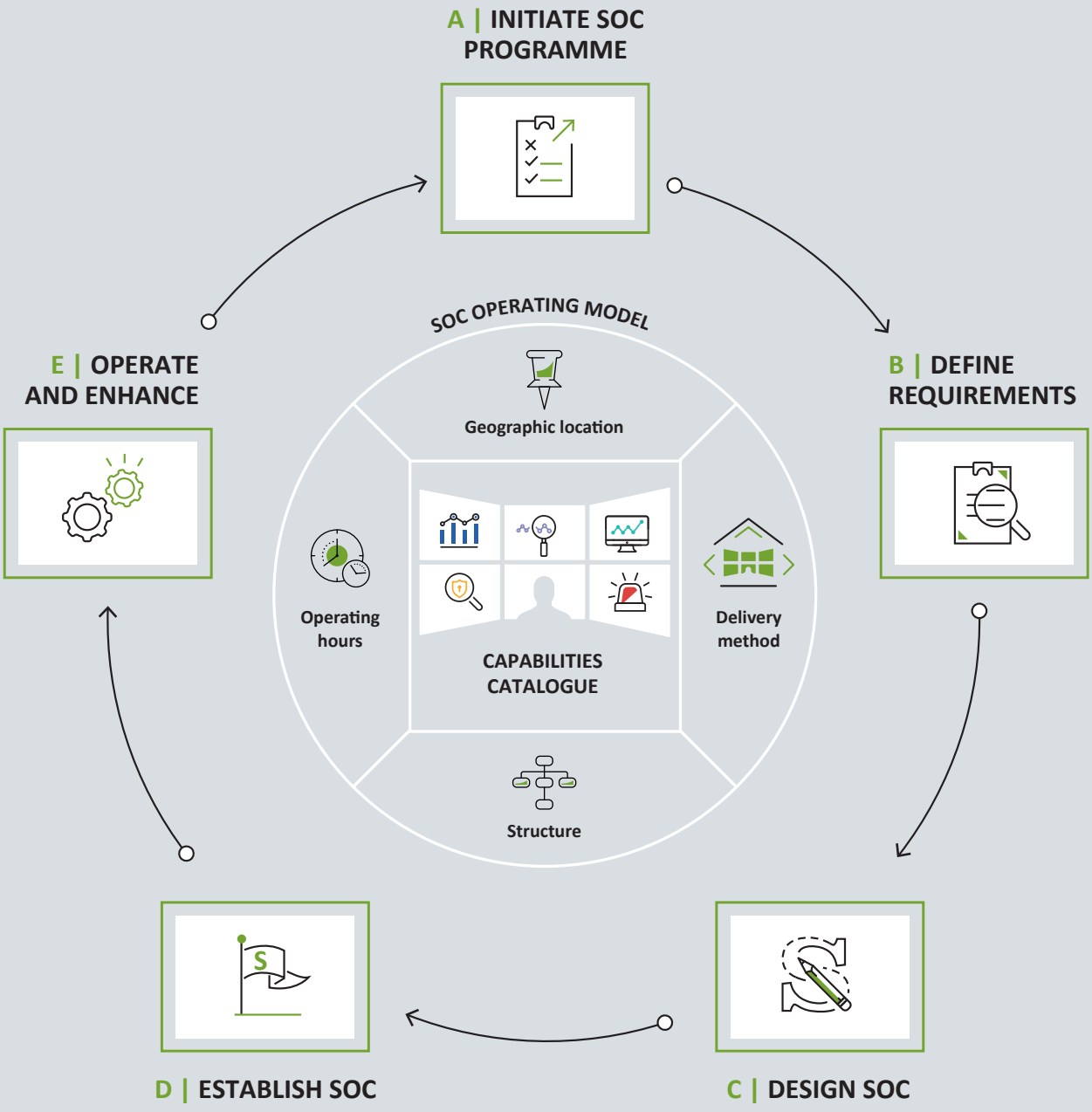
Determine the SOC operating model that is right for your business. It should be tailored to your organisational context to help drive success. The benefits and limitations of an internal, external or hybrid SOC are outlined in the report.



Follow the ISF framework – a pragmatic, systematic and structured approach to designing, establishing and operating a successful SOC that is continuously enhanced over time. Once the core capabilities are in place, incrementally add new functionality, innovate, improve processes and invest in people to optimise the SOC's performance.

"Understand that a SOC is not built overnight. Understand what you are trying to protect. Create proper processes around what the SOC is supposed to deliver. Be patient." – ISF Member

THE ISF APPROACH TO BUILDING A SUCCESSFUL SOC



WHERE NEXT?

Building a Successful SOC: Detect earlier, respond faster is aimed at those who are either creating a SOC or seeking to optimise their existing SOC. It equips an organisation to build and evolve a SOC of significant worth to the business by:

– describing the capabilities that a successful SOC can provide

– articulating the key considerations for selecting a suitable SOC operating model

– presenting a framework that provides practical guidance on how to design, establish and enhance a SOC.

This report reflects good practice, incorporating valuable and trusted advice, tips and recommendations from ISF Members with experience operating an effective and efficient SOC.

Organisations should also consider the ISF resources related to the report, including ***Threat Intelligence: React and Prepare, Protecting the Crown Jewels: How to secure mission-critical information assets, Building Tomorrow's Security Workforce (Briefing Paper) and Data Leakage Prevention (Briefing Paper)***.

The ISF encourages collaboration on its research and tools. Members are invited to join the **Building a Successful SOC** community on ***ISF Live*** to share their experiences and discuss the guidance in this report.

Consultancy services from the ISF provide Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products.

The report is available free of charge to ISF Members and can be downloaded from the ISF Member website www.isflive.org. Non-Members interested in purchasing the report should contact Steve Durbin at steve.durbin@securityforum.org.

CONTACT

For further information contact:

Steve Durbin, Managing Director
US: +1 (347) 767 6772
UK: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953800
steve.durbin@securityforum.org
securityforum.org

ABOUT THE ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

DISCLAIMER