Building a Security Operations Centre (SOC)

Designing a security monitoring capability proportionate to the threats faced (and resources available).

Why have a Security Operations Centre?

Security Operations Centres (SOCs) can vary widely in scope, but most are responsible for detecting *and* responding to cyber attacks.

Whilst the primary goal of cyber security is to prevent attacks, this is not always possible. The role of a SOC is to limit the damage to an organisation by detecting and responding to cyber attacks that successfully bypass your preventative security controls.

Equally, a SOC can include a multitude of security activities, such as vulnerability assessment, compliance activities and system configuration.

This guidance is aimed at organisations that are considering investing in a SOC, or are looking at evolving a current SOC, as part of a wider approach to managing cyber risks.

What you will learn

This guidance doesn't prescribe the SOC you should build (there is no one-size-fits-all SOC). Instead, it helps you to decide what type of SOC your organisation needs and equips you with a firm understanding of the key concepts involved in SOC design.

By evaluating the threat that your organisation faces, understanding the assets you have and the resources at your disposal, this guidance will guide you in

developing a target operating model, which is the bedrock of a SOC.

Defining a target operating model will then allow you to develop proportionate SOC services, such as threat intelligence, content development, threat hunting and incident response.

The various functions that a SOC requires are huge subjects in their own right and some areas already have comprehensive guides available, these will be signposted where available.

This guidance attempts to remain technology agnostic. The goal is to equip you with a clear understanding of the fundamental considerations, which should guide the creation and operation of a SOC. This will enable you to go to market and identify the correct tools for your particular situation.

About this guidance

This guidance is split into five sections.

These are the common aspects of a SOC and whilst often linked, they are easier to address in turn. Where there are interdependencies, these will be signposted.

- **Operating Model** – discusses the various factors that need to be considered when designing a SOC.
- **Onboarding** – provides guidance on how to determine what logs/information should or could be made available to a SOC and introduces the use of attack trees to help you intelligently make decisions about log sources.
- **Detection** – discusses the various approaches in detecting cyber attacks.
- **Threat Intelligence** – touches on some of the common issues around threat intelligence and explores the value it adds to a SOC.
- **Incident Response and Management** – builds on existing guidance and discusses how it fits into the SOC as a whole.

It will take many iterations and a fair amount of investment to design and build a SOC that works for your organisation, you will not have all of the answers immediately or be able to pluck an appropriate SOC out of thin air. The hope is that this guidance provides a foundation and gives you an understanding of the questions you should be asking. Each subject of this guidance could be (and likely is) a book in its own right, which is why there is no one-size-fits-all SOC.

If there are any points that you need clarifying please do get in touch.

PUBLISHED

23 May 2022

REVIEWED

23 May 2022

VERSION

1.0

WRITTEN FOR

Large organisations

Public sector

Small & medium sized organisations

Cyber security professionals