Chapter 6
Cyber Security Operations Centre Concepts and Implementation

Enoch Agyepong
Cardiff University, UK

Yulia Cherdantseva
Cardiff University, UK

Philipp Reinecke
Cardiff University, UK

Pete Burnap
Cardiff University, UK

ABSTRACT

Cyber security operations centres (SOCs) are attracting much attention in recent times as they play a vital role in helping businesses to detect cyberattacks, maintain cyber situational awareness, and mitigate real-time cybersecurity threats. Literature often cites the monitoring of an enterprise network and the detection of cyberattacks as core functions of an SOC. While this may be true, an SOC offers more functions than the detection of cyberattacks. For example, an SOC can provide functions that focus on helping an organisation to meet regulatory and compliance requirement. A better understanding of the functions that could be offered by an SOC is useful as this can aid businesses running an in-house SOC to extend their SOC capabilities to improve their overall cybersecurity posture. The goal of this chapter is to present the basics one needs to know about SOCs. The authors also introduce readers and IT professionals who are not familiar with SOCs to SOC concepts, types of SOC implementation, the functions and services offered by SOCs, along with some of the challenges faced by an SOC.

DOI: 10.4018/978-1-7998-3149-5.ch006

INTRODUCTION

Securing an organisation's network against cybercriminal activity remains one of the most challenging tasks for many businesses. In order for organisations to defend themselves against attacks, they need to understand current attack vectors and the specific threats that they face to put in place mitigation strategies. Traditionally, many organisations relied on security tools such as Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Anti-virus solutions to protect their networks, and secure their data against cyberattacks. However, recent cyberattacks have proven that deploying these defensive tools by themselves are no longer sufficient to fully protect an organisation and deal with the aftermath of a cyberattack (Chuan et al., 2019). For example, a Firewall can be hacked to behave differently by an attacker (Tuglular & Belli, 2008). Likewise, an Intrusion Prevention Systems (IPSs) can be evaded by some sophisticated attacks (Xia & Xu, 2017). The need to respond to such incidents in an efficient, coordinated and effective manner has led to organisations employing the services of a Security Operations Centre (SOC) (Majid & Ariffi, 2019).

A SOC can be defined as a centralised infrastructure, made up of people, processes and technology inside or outside an organisation that helps businesses to monitor their network and respond to cybersecurity threats and incidents (Mutemwa et al., 2019). A review of the literature shows that a SOC can also be referred to by other names, such as Security Intelligence Centre (SIC); Information Security Operations Centre (ISOC); Information Technology Operations Centre (ITOC) and Cyber Security Operations Centre (CSOC) (Brown et al., 2016; Miloslavskaya, 2018; Onwubiko & Ouazzane, 2019a). These terms are all used to denote the same meaning. In this chapter, we adopt and use the term SOC as it is the most commonly used term by many writers.

Since their inception in the '70s as coordinating centres for supporting governments or military organisations to protect their network against adversaries (Hewlett-Packard, 2013), SOCs have gradually evolved and are now being used in both the public and private sectors. According to Falk et al. (2017), the demand for SOC services is on the rise across all sectors. A threat report by researchers at McAfee, which surveyed over 400 companies in North America and across Europe found that 84% of commercial organisations and 94% of major companies use a SOC (Beek et al., 2016). Likewise, a publication by one of the world largest research store, Research and Markets on SOCs in 2019, reported that the global SOC market size is expected to grow from USD 372 million in 2019 to an estimated USD 1,137 million by 2024 US Dollars at a Compound Annual Growth Rate of 25% (Research and Markets, 2019). In fact, SOCs are being deployed by government agencies, universities and various corporations to defend their network and to identify malicious activities (Zhong et al., 2016). SOCs play a central role in the protection of an organisation's information communication systems and act as the custodian for monitoring, detecting and reacting to security incident (Onwubiko & Onwubiko, 2019). However, a SOC offers many more functions than the monitoring and detection of cyberattacks. For example, a SOC can be leveraged to support an organisation to address regulatory and compliance issues, like log retention and data privacy laws (Medeiros & Bygrave, 2015).

Similarly, a SOC can also offer a penetration testing function, which involves the simulation of an attack against an organisation's network to see how the business reacts (Schinagl et al., 2015). Other SOC functions include log collection and retention, policy management, compliance and vulnerability scans, risk management activities, performing business and technical audit through penetration testing, incident management activities, forensic and malware analysis, log analysis; threat identification and reporting of malicious activities. An understanding and appreciation of the functions of a SOC would be