Chapter 2
Cyber Security Centres for Threat Detection and Mitigation

Marthie Grobler
Council for Scientific and Industrial Research, University of Johannesburg, South Africa

Pierre Jacobs
Council for Scientific and Industrial Research, University of Johannesburg, South Africa

Brett van Niekerk
University of KwaZulu-Natal, South Africa

ABSTRACT

With the continuing evolution of cyber threats, it is only a matter of time before an organisation will suffer a major breach or there is an incident of national significance. This necessitates monitoring to detect possible incidents and mechanisms to respond and recover from breaches. This chapter provides an overview of structures to aid in threat detection and incident recovery. Security Operation Centres (SOCs), Computer Security Incident Response Teams (CSIRTs), and Security Intelligence Centres (SICs) will be covered, and the differences, benefits and limitations will be discussed. Guidance for the implementation of these security capabilities within organisations will be provided.
INTRODUCTION

Threats within the cyber domain are becoming more prominent. It is therefore imminent that threats need to be mitigated as far as possible. This chapter investigates how monitoring and incident response can be applied to assist cyber security centres to detect and mitigate threats. For the purpose of this publication, cyber security centres include the structures known as Security Operation Centres (SOCs), Computer Security Incident Response Teams (CSIRTs), and Security Intelligence Centres (SICs). This chapter indentifies the need for both monitoring and incident response, and the benefits that these actions bring about for organisations making use of the cyber security centre’s services. The chapter further looks at the benefits and challenges faced by cyber security centres in threat mitigation, and provides some guidance in terms of setting up these centres. The aim of the chapter is to assist cyber security centres in improving their threat detection and mitigation capabilities. The chapter investigates the need for and benefits of monitoring and incident response, and looks into the structures required to facilitate monitoring and threat detection, structures to facilitate incident handling, and structures to facilitate advanced threat detection and mitigation. The chapter concludes by providing guidance in terms of cyber security threat detection and mitigation.

THE NEED FOR MONITORING AND INCIDENT RESPONSE

Within the ever changing security environment, it is very important to adhere to constant monitoring. Not only is the security environment continuously changing, but new challenges arise daily in terms of new vulnerabilities and new attack types. Security attacks are now more likely to be targeted, purposeful and organised, posing a much more directed threat for an organisation. As a result of the increased level of connectivity between systems, sensitive data is faced with security, integrity and credibility issues (Gandotra, Singhal & Bedi, 2009).

In the view of the changing threat landscape, it is imperative that more attention be paid to system monitoring (Gandotra, Singhal & Bedi, 2009). In order to manage these aspects, all organisational systems should be monitored to such an extent that any incidents can be managed and appropriately responded to on a timeous basis. Thus, threat mitigation within an organisation needs to be planned and executed in an ordered way in order to enhance opportunities and reduce threats to the sensitive data within the organisation. As part of a holistic cyber security strategy, authorities will deploy security controls in supporting the improvement of their entity’s cyber security posture. The SysAdmin, Audit, Network, Security institute (SANS) groups these controls into technical security controls, administrative security controls and
On Experience of Social Networks Exploration for Comparative Analysis of Narratives of Foreign Members of Armed Groups: IS and L/DPR in Syria and Ukraine in 2015-2016
[www.igi-global.com/article/on-experience-of-social-networks-exploration-for-comparative-analysis-of-narratives-of-foreign-members-of-armed-groups/204417?camid=4v1a](www.igi-global.com/article/on-experience-of-social-networks-exploration-for-comparative-analysis-of-narratives-of-foreign-members-of-armed-groups/204417?camid=4v1a)

What Lawyers Want: Legally Significant Questions that Only IT Specialists can Answer
[www.igi-global.com/article/what-lawyers-want/105192?camid=4v1a](www.igi-global.com/article/what-lawyers-want/105192?camid=4v1a)