ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 7/24 (July)

Security Operation Centres – the Backbone of Cybersecurity

INTRODUCTION

1. A Security Operation Centre (SOC) refers to a dedicated team of cybersecurity professionals that operate 24/7 to monitor an organisation's cybersecurity response to security incidents, as well as investigate cyber threats that can compromise critical infrastructures, systems and sensitive information. The SOC is an important part of the organisation's cybersecurity backbone and it provides continuous protection against cyber threats in an increasingly digital and interconnected world.

INCREASING PRESENCE OF SOCs

2. As organisations progressively integrate technology into their operations for efficiency and growth, we see the emergence of more sophisticated and illusive cyber threats as the cyber-attack surface also expands. As a result, more organisations are establishing SOCs to deal with such threats. A 2023 Gartner study predicted that 25% of all organisations would have a SOC function by 2024, up from 10% in 2020.

FUNCTIONS OF SOCs

3. SOCs carry out a wide variety of functions intended to increase an organisation's cyber defence capabilities and resilience against cyber threats. Some of these functions include:

a. **Threat Detection.** SOCs provide the first line of defence by detecting potential and active threats. The SOC actively monitors the organisation's IT infrastructure

through the use of various cybersecurity tools, including Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Endpoint Detection and Response Systems (EDR). The alerts and data generated by these tools are collated by Security Information and Event Management (SIEM) systems, which provide the SOC with a centralised platform from which alerts regarding potential security incidents can be received. Modern SIEM solutions may also include artificial intelligence capabilities that can automate these processes and identify suspicious activity quickly and accurately.

b. **Threat Analysis**. Modern SIEMs also provide threat analysis capabilities that SOCs can leverage. When a security incident occurs, the SOC utilise several methods such as behavioural analysis, threat intelligence integration and incident correlation, to assess the threat scope and cyber forensics, determine the root causes of the incident, and gather evidence. Larger organisations may encounter numerous incidents every day. As such, it is imperative that these incidents are sorted according to their severity, impact, and criticality to the organisation's operations, so that the SOC can prioritise its resources.

c. **Incident Response.** Upon the detection of a cybersecurity incident, the SOC will implement measures to mitigate the impact, contain the incident, and eradicate the threat. Thereafter, it will endeavour to recover affected assets such that the organisation is able to resume normal operations. One framework for incident response consists of the following steps (see Fig 1):

(i) **Identification of vulnerabilities and entry points.** The system is searched to identify the vulnerabilities and potential points of exploitation by adopting the mind-set of potential attackers

(ii) **Containment.** Compromised devices are isolated to prevent further spread of malware across the network, affecting other devices

(iii) **Eradication and Recovery.** Malicious components are removed from the system, and it is restored to a secure state through the use of tools such as backups. The focus is on mitigating the impact and restoring normal operations and services; and

(iv) **Post-incident Analysis.** A review will be conducted to refine future incident response procedures and current organisational policies.

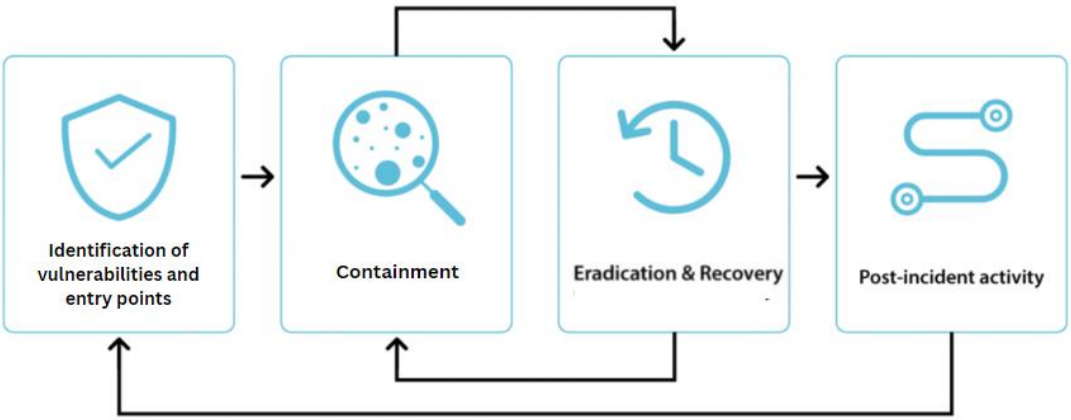

Fig 1: An infographic on the Cyber Incident Response Life Cycle (source: Devo)

TYPES OF SOC

4. While an effective SOC is an important element of a cybersecurity structure, the establishment of a SOC requires significant investments of money, time and employee resources. SOCs, if built in-house, can be costly, complicated to maintain and require deep expertise that is difficult to acquire. This is especially so for less mature organisations that may lack resources. Organisations will also have to strike a balance between cost and operational effectiveness. According to Gartner, there are several types of SOCs that can be implemented, each with varying levels of operational effectiveness and cost (see Fig 2):

Fig 2: The types of SOC (source: Gartner, ACICE)

ESTABLISHING A SOC

5. There are several key logistical considerations for establishing a SOC. Below are some of the factors:

a. **Manpower and Expertise.** A SOC cannot operate effectively without cybersecurity experts taking the lead; the experts are critical in making decisions on how to respond and what to prioritise, based on data available, in order to keep an organisation protected in both the short and long term. However, cyber experts can be difficult to find. According to a survey conducted by Artic Wolf, 41% of organisations listed “talent shortage” as their top concern for 2023.

b. **Infrastructure.** A SOC needs the right security tools in place to maximise its capabilities. Significant hardware and software investments must be made to ensure optimal security. These include network connectivity, power supply, cooling systems, physical storage for data and equipment, and various other tools that are required for monitoring, detection, analysis, and response.

c. **Time.** Standing up an internal SOC can take months or even years to hire staff, purchase security hardware and software, and then implement it throughout the enterprise. Even when established, it takes time to sift through alerts, prioritise threats and implement remediation.

d. **Protocols**. Protocols need to be established as well for coordinating with other teams within the organisation and external stakeholders during security incidents or breaches.

FUTURE TRENDS

6. The cyber threat landscape is constantly evolving. As a result, SOCs have begun to use AI to detect and respond to threats more efficiently. Here are some ways in which AI and machine learning are transforming the way SOCs function:

a. **Advanced Detection of Threats.** Large volumes of data can be analysed by AI and machine learning systems, and they can highlight patterns a human analyst may overlook. AI and machine learning also reduce the time needed for analysis. This improves threat detection and helps to avoid security breaches more efficiently. One such example is the IBM Security Guardium, which is a data security platform that leverages AI for outlier detection (see Fig 3).

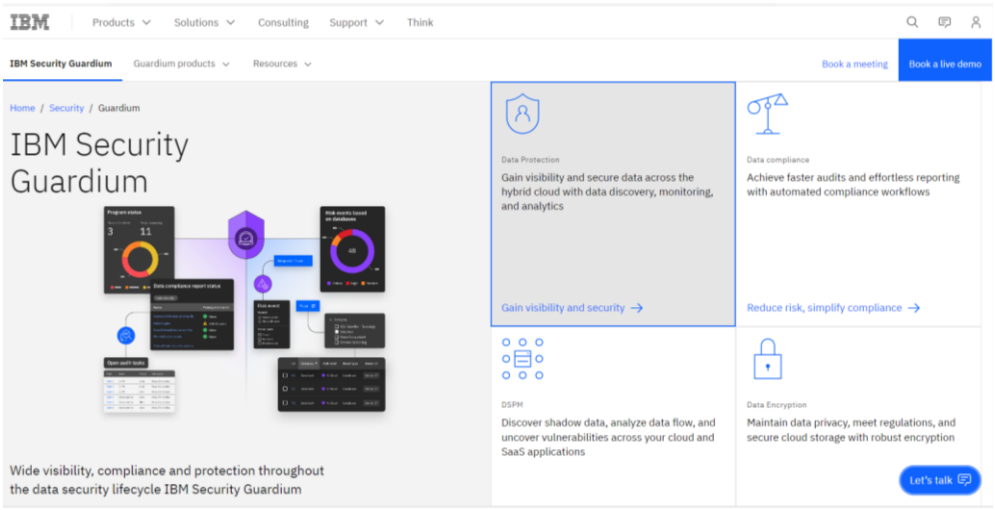

Fig 3: The IBM Security Guardium, a data security platform, and its functions (source: IBM)

b. **Reduction of Maintenance Costs.** Through real-time sensor data analysis, AI can forecast equipment breakdowns or maintenance requirements. SOCs can minimise maintenance expenses and prevent downtime by employing this proactive strategy.

c. **Optimisation of Resources.** Using AI, SOCs examine operational data and demand trends and optimise the distribution of resources, such as labour, energy, and transportation.

7. Besides AI and machine learning, it is expected that SOCs could acquire Zero Trust Architecture (ZTA) in the future. ZTA improves protection and visibility of an organisation by providing an adaptive security framework. The ZTA approach aims to reduce risk, enhance employee experience, and support remote and hybrid work.

a. **Embracing Zero Trust Security Models.** The ZTA is increasingly being integrated into SOCs to prevent insider threats and ameliorate security postures. For instance, Google implemented BeyondCorp, a Zero Trust security framework, which focused on device and user authentication and sought to deliver benefits to customers, such as providing a wide variety of solutions (see Fig 4). By eradicating the old security framework and embracing a new security model that monitors every request, SOCs will be able to significantly minimise the attack surface and reduce the risk of breaches.

Fig 4: Benefits provided while using BeyondCorp Enterprise (source: BeyondCorp Enterprise)

CONCLUSION

8. Just as organisations expand their utilisation of technology, cyber threats have also become widespread and common. If an organisation suffers a cyber incident, it is only through adequate and appropriate preparation that damage can be kept to a minimum. SOC establishment is one way an organisation can enhance protection and elevate its cyber incident strategy.

9. Recent developments in AI and machine learning have resulted in the considerable transformation of SOCs. AI and machine learning contribute to improvements in threat detection and data analytics, and increases overall productivity. In the coming years, AI and machine learning will become more deeply integrated within SOCs as they search for more effective ways to defend against the evolving threats in our digital environment.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

REFERENCES

1. What is a Security Operations Center (SOC)? – Checkpoint
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/

2. Security Operation Center (SOC) – IBM
https://www.ibm.com/topics/security-operations-center

3. Cyber Threat Intelligence: Strengthening Your Organisation's Security Posture – Institute of Data
https://www.institutedata.com/sg/blog/cyber-threat-intelligence-strengthening-your organisations-security-posture/

4. Security Operations Centers and Their Role in Cybersecurity – Gartner
https://www.gartner.com/en/newsroom/press-releases/2017-10-12-security-operations-centers-and-their-role-in-cybersecurity

5. Top Cybersecurity Concerns: A Global Perspective – Arcticwolf
https://arcticwolf.com/top-cybersecurity-concerns/

6. Will 2024 Be a Big Year for Job Cuts? – Nasdaq
https://www.nasdaq.com/articles/will-2024-be-a-big-year-for-job-cuts

7. IBM Security Guardium – IBM
https://www.ibm.com/guardium

8. Artificial Intelligence (AI) cybersecurity – IBM
https://www.ibm.com/ai-cybersecurity

9. Advancing The Security Operations Center (SOC): New Technologies and Processes Can Help Mitigate Cyber Threats – Forbes
https://www.forbes.com/sites/chuckbrooks/2023/04/26/advancing-the-security-operations-center-soc-new-technologies-and-processes-can-help-mitigate-cyber-threats/

10. 5 Key Elements of the Next-Gen Security Operations Center – TechBeacon
https://techbeacon.com/security/5-key-elements-next-gen-security-operations-center

11. IBM - What is a security operations centre (SOC)?
https://www.ibm.com/topics/security-operations-center

12. Zero Trust Architecture – NIST
https://www.nist.gov/publications/zero-trust-architecture

13. What is Zero Trust architecture? – Microsoft
https://www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture

14. BeyondCorp Enterprise: Introducing a Safer Era of Computing – GoogleCloud
https://cloud.google.com/blog/products/identity-security/introducing-beyondcorp-enterprise

15. A New Approach to Enterprise Security – BeyondCorp
https://beyondcorp.com/

16. Cybersecurity Incident Response Plan - Devo
https://www.linkedin.com/pulse/incident-response-life-cycle-devoinc