FEBRUARY 2024

MOORE NEWSLETTER

Prevent Financial and Reputational Loss with Effective Security Incident Management

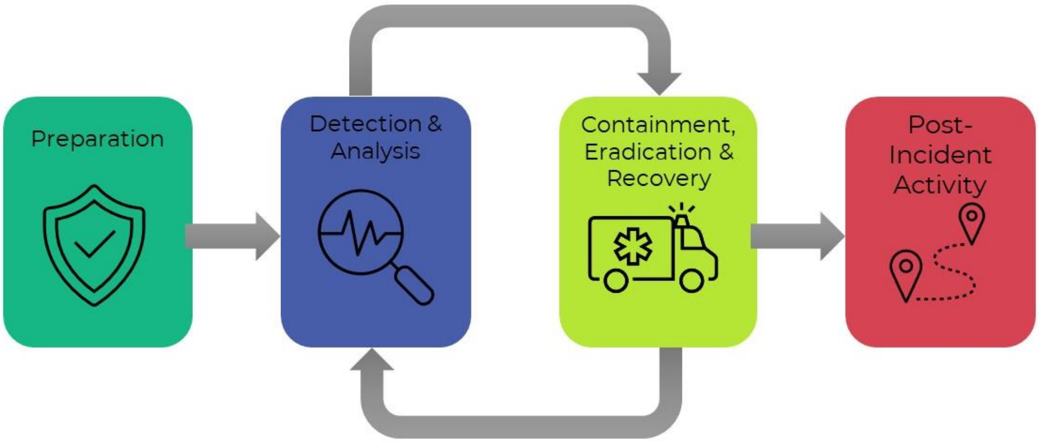
Introduction

The digital age has brought unprecedented convenience, but it has also given rise to a surge of new crimes. The anonymity and borderless nature of the internet make it easier for criminals to engage in illegal activities. Small and medium-sized enterprises (SMEs) are particularly vulnerable to cyber-attacks due to their limited IT resources. Cybercriminals often target SMEs as they perceive them as easier targets compared to larger corporations. Additionally, SMEs can inadvertently become a backdoor for cybercriminals to gain access to larger companies through their role as suppliers or business partners. As McKinsey predicts in their study, these damages from cyberattacks will amount to approximately US$11 trillion annually by 2025. To prevent financial loss, businesses are advised to prioritise effective security incident management.

The ability to promptly detect, respond to, and mitigate security incidents in real-time is crucial in minimising the potential financial and reputational losses resulting from cyber threats. Implementing advanced incident management tools such as **Security Information and Event Management (SIEM)** and **Security Orchestration, Automation and Response (SOAR)** has emerged as a vital strategy. According to IBM's 2023 Cost of a Data Breach Report, the utilisation of SIEM and SOAR could reduce the cost of data breaches by an estimated US$405,000. By harnessing the power of these tools, organisations can strengthen their incident management capabilities and establish a robust foundation for cybersecurity incident management.

Incident Response Framework

Swift and efficient incident response is paramount in the field of cybersecurity as organisations must be ready to promptly and effectively handle cyber threats, security breaches, or cyberattacks to mitigate devastating consequences. The National Institute of Standards and Technology (NIST) has developed a holistic incident response framework that provides a structured approach for organisations to effectively manage and tackle security incidents. The NIST incident response framework consists of four key phases:



Preparation

Encompasses four elements on preparing to handle incidents, including incident handler communication, incident analysis technology, incident analysis resources, and incident mitigation software. Also, preventive measures such as user awareness training and network security.

Detection & Analysis

Examine whether an incident has transpired, appraise its degree of severity, and categorise it accordingly. This encompasses elements such as attack vectors, indicators of an incident, sources of precursors and indicators, incident analysis, incident documentation, incident prioritisation, and incident notification.

Containment, Eradication & Recovery

The incident response team evaluates and selects the most suitable containment strategy to halt the spread of an incident and minimise its impact. The primary objective is to completely eliminate the threat and restore affected systems to their normal functioning state. This entails choosing a containment strategy, evidence gathering and handling, and identifying the attacking hosts.

Post-Incident Activity

Every incident response team should progress in line with evolving threats, enhanced technology, and knowledge gained from past incidents. A "lessons learned" meeting should be held with all involved parties after a major incident to review what occurred, what was done to intervene, and how well the intervention worked.

Incident Response Tools

In today's dynamic and rapidly changing threat landscape, organisations must equip themselves with effective strategies and tools to mitigate the impact and safeguard their digital assets. Some commonly used incident response technologies embraced by security teams worldwide include:

- **SIEM (Security Information and Event Management)**
  A security solution that merges real-time analysis of security alerts with AI and automation. Its purpose is to assist organisations in identifying and resolving potential threats and vulnerabilities by collecting data from various sources such as applications and servers, as well as recognising patterns or irregularities in user behaviour.

- **EDR (Endpoint Detection and Response)**
  A comprehensive endpoint security solution that combines real-time continuous monitoring and data collection from endpoints with automated response and analysis capabilities based on predefined rules. Its primary purpose is to identify potential threats and automatically respond to them by either removing or containing the threats. For instance, deleting malicious files and isolating compromised devices from the network. Additionally, EDR promptly notifies security personnel about the identified threats.

- **XDR (Extended Detection and Response)**
  A cybersecurity infrastructure that promotes openness by integrating various security tools and unifying security operations across all layers of the security infrastructure. This includes users, endpoints, email, applications, networks, and data. The purpose of XDR is to establish a unified and centralised enterprise system for comprehensive threat prevention, detection, and response. It assists security operations teams in prioritising threats and minimising alert volumes through the use of analytics and correlations. By doing so, teams can concentrate on the most crucial threat events and utilise automation to handle known or recurring incidents effectively.

- **ASM (Attack Surface Management)**
  A comprehensive and continuous procedure that involves the ongoing discovery, analysis, remediation, and monitoring of cybersecurity vulnerabilities, potential attack vectors, and exposures that collectively form an organisation's attack surface. This process entails systematically identifying and monitoring both internal and external internet-connected assets to evaluate their security posture and identify any potential weaknesses or areas of vulnerability. The goal of ASM is to narrow down the potential avenues and options that malicious actors can exploit to gain unauthorised access to an organisation's system and network.

What is SOAR?

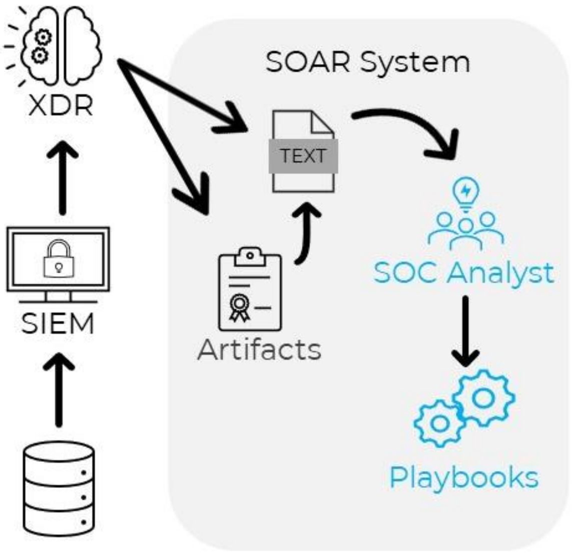
SOAR, also known as "security orchestration, automation and response", is a software system that empowers security teams to integrate and harmonise diverse security tools within cohesive workflows, resulting in effective and streamlined threat response. Security teams can leverage SOAR to establish and execute playbooks that automate the identification of compromised devices and initiate a series of actions to resolve potential threats without requiring human intervention. The software solution has predictive capabilities that enable the analysis and identification of recurring patterns of false detection and genuine threats, thereby enhancing the efficiency and effectiveness of security operations center (SOC) teams. Moreover, the software solution acts as a central console for SOC to integrate security tools and technologies into optimised threat response workflows and automate repetitive tasks in those workflows. To summarise, SOAR holds three main capabilities as follows:

1. Threat and vulnerability management
2. Security incident response
3. Security operations automation.

Integration between SOAR and other incident response systems

By seamlessly integrating with incident response tools like SIEM and XDR, SOAR establishes a strong synergy within the cybersecurity domain. This integration enhances the overall incident response capabilities of organisations, enabling them to effectively address and mitigate security incidents.

For instance, if a security breach occurs in a database, an alert is generated and sent to the SIEM system. The SIEM system then promptly forwards the alert to the XDR system in real-time, which communicates with the SOAR system to initiate a case or incident. The case is then tracked and managed from start to completion. Also, the SOAR platform obtains details about the attack, also known as artifacts, which include incident data, response playbooks and network traffic data. Afterwards, the case is delegated to a designated SOC analyst for additional investigation by employing preconfigured playbooks. These playbooks are scripted to automate precise actions tailored to the requirements of the security incident within the SOAR system. They are constructed to seamlessly connect and incorporate pertinent artifacts, thereby providing a comprehensive context for the analyst. Moreover, the software system features a live dashboard that offers the analyst a comprehensive understanding of the required actions. This could include information such as the incident timeline, attack graph and time to resolve that specific threat.



Benefits of SOAR

- **Facilitate Faster Incident Response**
  SOAR leverages security automation and incident response playbooks to create workflows that require minimal human intervention, resulting in reduced mean time to detect and mean time to respond for SOCs, thereby mitigating the impact of cyberattacks.

- **Simplified Incident Response Workflow**
  Security teams can efficiently manage multiple incidents and threats using a unified dashboard, customisable SOAR playbooks, and custom reports to track critical metrics and automate responses against sophisticated cyberattacks.

- **Integration with Tools**
  A range of security tools can be integrated with a SOAR platform to cater to the specific requirements of an organisation, potential tools include threat intelligence, SIEM and cloud security.

- **Improved Collaboration**
  SOAR promotes information sharing across internal security teams and enables task allocation based on team member's skills and availability.

- **Enhanced Decision-making**
  SOAR dashboards empower SOCs to gain network visibility and insights into the threats they encounter. This information assists in identifying false positives, improving alert prioritisation, and selecting the most appropriate response processes.

- **Continuous Advancement**
  Empower organisations to continuously improve their incident response processes by leveraging machine learning and artificial intelligence (AI) to capture and analyse data from previous incidents.

In summary, organisations can build a strong framework for managing cybersecurity incidents and protecting their digital assets by prioritising effective security incident management, utilising advanced tools such as SIEM, XDR, and SOAR, and integrating these technologies. This comprehensive approach enables organisations to respond quickly to incidents, automate workflows, and continuously improve their incident response processes. As a result, organisations are empowered to stay proactive in dealing with cyber threats, effectively safeguarding their crucial information and infrastructure.

Moore IT & Cybersecurity Services

Why work with us?

We are a global advisory network, with offices and member firms across the globe. Backed by our international network, we provide clients with comprehensive cybersecurity solutions and expertise from security vulnerability assessment to system penetration testing to protect them from modern cyber threats.

Our team is composed of professionals with practical and solid knowledge and experience. They are certified holders or members of professional bodies such as CISA, CISM, CRISC, CISSP, CIPP(A), CEH, OSCP and GPEN.

Our clients range from SMEs to listed companies from a wide variety of industry, and public sectors including government bureaus and authorities. Through our extensive sector knowledge, we provide comprehensive advice to suit each client’s goals.

Our IT & Cybersecurity Service Team

PATRICK ROZARIO
Advisory Services Managing Director

T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
IT & Cybersecurity Principal

T +852 2738 4631
E kevinlau@moore.hk

References

https://www.ibm.com/downloads/cas/E3G5JMBP

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

https://www.ibm.com/topics/incident-response

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

https://www.linkedin.com/pulse/implementing-soar-security-orchestration-automation-response-lpd8c?utm_source=share&utm_medium=member_ios&utm_campaign=share_via

Follow us on social media @moorehongkong

MOORE

www.moore.hk

We believe the information contained herein to be correct at the time of going to press, but we cannot accept any responsibility for any loss occasioned to any person as a result of action or refraining from action as a result of any item herein.