Chapter 5
Autonomous Defenders: Generative AI for Smarter Incident Response – AI-Augmented Security Operations in Modern SOCs

M. P. Rajakumar
St. Joseph's College of Engineering, India

M. Balasubramani
http://orcid.org/0009-0005-3706-0140
V.S.B. Engineering College. Karur, India

R. Balamurugan
New Prince Shri Bhavani College of Engineering and Technology, India

M. Navaneetha Krishnan
St.Joseph College of Engineering, India

M. Robinson Joel
http://orcid.org/0000-0002-3030-8431
KCG College of Technology, Karapakkam, India

Joel Jacson
http://orcid.org/0009-0006-3095-7024
Kings Engineering College, India

ABSTRACT

This chapter examines the transformative role of generative artificial intelligence in modern incident response, focusing on how AI-driven models enhance detection, triage, analysis, and remediation workflows within Security Operations Centers. The chapter outlines limitations of traditional human-centered response frameworks and demonstrates how large language models, reinforcement learning agents, and multimodal generative systems provide adaptive, context-aware decision support. A conceptual architecture for autonomous defenders is introduced, illustrating how generative AI integrates with SIEM, SOAR, and XDR platforms to enable semi-autonomous and fully automated security actions. Ethical, regulatory, and

DOI: 10.4018/979-8-3693-8397-1.ch005

governance considerations are discussed to ensure responsible deployment of AI-driven cyber defense capabilities. The chapter concludes by identifying emerging research directions and outlining future trends that will shape AI-augmented incident response ecosystems.

1. INTRODUCTION

1.1 Background

Cloud infrastructures and rapid digitalization within organizations are factors that add to today's complex cybersecurity operations. The attached distribution systems and IoT environments are further complicating the scenarios. The condition gets more complicated with flowing telemetry, event data, and threat signals that keep streaming into an enterprise network, causing strain in maintaining an instantaneous detection and management of cyber-incidents at Security Operations Center (SOCs) (Evans & Franks, 2023).Conventional cybersecurity channels like SIEM, EDR, IDS/IPS, and SOAR will basically meet the visibility requirement, but they rely heavily on their human experts to interpret a massive number of alerts and then put the pieces together to coordinate the actions of the response.

As a fallout, the cyber adversaries have begun to adopt automation, artificial intelligence, and adaptive techniques to bring up the lightning fast tempo and sophistication of their offensive operations (Thomas & Shrobe, 2024). The perpetrators are using automated exploit kits, AI-generated malware variants, multi-staged ransomware frameworks, and social engineering attacks empowered by synthetic content. These capabilities deepen the existing asymmetry between the attackers and defenders and impede any effective incident response.

New advancements in generative AI (GenAI) such as large language models (LLMs), generative adversarial networks (GANs), reinforcement-learning agents, and multimodal reasoning systems have given new potential towards improving the incident response functions in most parts involving partial automation. GenAI is proven to have the capability of analyzing logs, prioritizing alerts, simulating attack behavior, generating remediation playbooks, and supporting decision-making under uncertainty (Snyder & Malik, 2022). Thus far, overall, they provide an account of more autonomous and adaptive models of cyber defense, which this chapter refers to as autonomous defenders.