The Role of AI in Security:
Overcoming Challenges with Human Oversight

Artificial Intelligence (AI) is increasingly being embraced by organizations to enhance security operations, yet concerns surrounding its integration and effectiveness persist. Despite AI's growing presence in security workflows, human oversight remains a critical factor in ensuring its success. A report by Crogl, commissioned by agentic AI company Ponemon Institute, delves into the current state of AI adoption in enterprise security operations, revealing that while AI is a promising force in the field, its limitations must be addressed to maximize its potential.

The Growing Role of AI in Security Operations

The adoption of AI in security operations has been rising steadily, with 62% of organizations incorporating some form of AI into their security workflows. However, the effectiveness of AI in reducing security threats remains a matter of debate. According to Crogl's report, although AI is widely adopted, only 44% of enterprises believe AI alone is sufficient for securing their operations in real-time.

01

The report emphasizes the severity of the security challenge faced by businesses. On average, enterprises receive a staggering 4,330 security alerts daily. However, despite the massive volume of alerts, organizations can only manage to detect and investigate 37% of them. This gap in incident management underscores the importance of leveraging advanced technologies like AI to address the overwhelming workload of security teams.

02

Monzy Merza, CEO of Crogl, highlighted the operational pressure faced by security teams, stating, “They are managing thousands of alerts every day while defending against increasingly complex attacks.” AI’s role as a force multiplier in the Security Operations Center (SOC) is becoming clearer. However, Merza noted that while automation can assist in security tasks, it is not a panacea. Automation alone is insufficient without the guidance and expertise provided by skilled human analysts.

AI's Strengths and Weaknesses in Security Operations

AI's core advantages in security operations lie in its ability to quickly detect and automate tasks, particularly the management of security alerts. Respondents to the Crogl survey overwhelmingly cited speed as one of AI's most significant benefits, with 67% of organizations noting that AI helps resolve security alerts faster than traditional methods. Additionally, more than half of organizations with a dedicated SOC employ AI to automate documentation, streamline case management, and improve collaboration among security teams.

01

However, while AI can handle repetitive and time-consuming tasks, it faces inherent limitations. Human analysts are still considered the most effective last line of defense in an AI-enabled SOC. According to the report, 52% of respondents believe human analysts remain crucial to security operations, while only 44% trust AI to handle tasks on its own. The challenges of AI replicating human judgment and expertise in complex security scenarios are key factors in the ongoing reliance on human oversight.

02

Experts from the Gartner Security & Risk Management Summit, held last year, reinforced this perspective. AI agents are undeniably transforming SOCs by automating tasks and enabling faster response times. However, they are unable to replicate the critical human knowledge necessary to make nuanced decisions, especially in high-stakes situations. Thus, while AI agents can assist, their actions require careful monitoring by experienced human analysts.

Challenges in AI Integration and Data Oversight

While AI offers notable advantages, its integration into existing security workflows presents several challenges. According to the Crogl report, 50% of survey respondents cited integration issues as a barrier to AI adoption. Integrating AI into already-established security systems can be difficult, particularly when legacy systems are not compatible with modern AI tools.

01

Another significant challenge is the data dispersion within organizations. 49% of respondents indicated that the data they need to feed into AI systems is too fragmented and difficult to standardize. AI systems rely on vast amounts of data to function optimally, and without consistent, high-quality data, their effectiveness is compromised.

02

Oversight is also a growing concern. 36% of organizations reported that they lack the ability to detect whether AI tools might be introducing data leakage—a significant governance risk. As AI systems are deployed to handle sensitive data, the potential for breaches increases. Without adequate oversight, AI could inadvertently expose organizations to vulnerabilities that undermine their security posture.

03

Merza emphasizes that organizations can derive the most value from AI by combining agentic speed with strong human oversight, clear workflows, and rigorous data governance. "Organizations that combine agentic speed with strong human oversight, disciplined workflows, and clear data governance are positioned to see the greatest impact," Merza said.

Conclusion: The Future of AI in Security

The findings of the Crogl report reveal that AI is not a cure-all for the challenges faced by security teams. Its strengths in speed and automation make it a valuable tool, but AI cannot replace the nuanced understanding and judgment provided by human experts. As AI continues to evolve, organizations must find ways to integrate it effectively into their security operations while addressing concerns about data management, integration, and oversight.

The key to maximizing AI's potential in security operations is a balanced approach that combines AI's efficiency with the invaluable expertise of human analysts. With the right integration strategies, clear governance structures, and human oversight, AI can significantly enhance the capabilities of SOCs, enabling security teams to respond more effectively to the ever-growing array of cyber threats.