www.ijarp.com ISSN 2456-9992
Page 1 to 5
International Journal Advanced Research Publication

Review-Article
Volume: 02
Issue: 10

AI-POWERED SECURITY OPERATIONS CENTER AUTOMATION

Keerthana. Katkuri*

Dept. of Information Technology, RV College of Engineering, Bengaluru, India

Article Received	Article Revised	Published
11-09-2026	01-10-2026	21-10-2026

***Corresponding Author:** Keerthana. Katkuri
Dept. of Information Technology, RV College of Engineering, Bengaluru, India
DOI: https://doi-doi.org/101555/ijarp.2921

ABSTRACT

Security Operations Centers (SOCs) act as the primary defense for protecting businesses against the constant barrage of cyber threats we see today. However, the traditional way of running a SOC is essentially drowning under too many alerts, slow manual checks, and a serious lack of expert analysts to do the heavy lifting. Artificial Intelligence (AI) has stepped in as a real game-changer here, providing a way to automate workflows, spot threats with much better accuracy, and jump on incidents way faster than before. This paper breaks down a framework for an AI-driven SOC that brings together machine learning, behavioral tracking, threat data, and SOAR technology to modernize cybersecurity for the long haul.

Index Terms—*Artificial Intelligence, Cybersecurity, Incident Response, Machine Learning, SOAR, SOC Automation, Threat Detection.*

1. Introduction

Today most large companies rely on a Security Operations Centre (SOC) to keep their backs covered 24x7. But the issue is the traditional SOCs are already experiencing alert fatigue due to the increasing complexity of attacks and the manual, slow processes to prevent them. But AI-powered automation shifts the equation, by providing teams with smart detection tools, predictive analytics, and automated responses to incidents as they occur. Automating tasks to an AI power setup will reduce the grunt work, allow for quicker reactions when things go wrong and create a much stronger defense for an organization.

2. Challenges in Traditional SOC Operations

The old-school SOC model has basically hit a wall. Teams are dealing with way too many false alarms, investigations that take forever, and a massive shortage of people who actually know how to fight these digital battles. Analysts often spend their entire shift just sorting through notifications from a dozen different tools. When you have to do everything by hand, mitigation slows down, and the risk to the company goes up. Plus, simple rule-based systems usually miss the quiet, advanced threats like ransomware or insider attacks that do not follow a predictable script.

3. Role of AI in SOC Automation

AI tech makes a SOC actually smart by using things like machine learning and behavioral analytics. Machine learning models can go through mountains of security data and detect the unusual, that just doesn't fit. Behavioral analytics does that, by learning the profile of normal behavior for an individual user, it will be much easier to identify a hacked account or rogue employee. Then there are SOAR platforms that deal with the tedious, repetitive tasks such as the sorting of tickets, isolation of malware and even minor issues that require a solution without the need for a human to click a button.

4. Proposed AI-Powered SOC Automation Framework

Our suggested framework is built in several connected layers to keep things organized. The Data Collection Layer pulls info from everywhere: cloud apps, firewalls, and employee laptops. The AI Analytics Layer then uses predictive models to find threats and decide which ones are the most dangerous right now. The Threat Intelligence Layer adds outside info to give the system better context on what it is seeing. The Automation and Orchestration Layer is the actual layer to contain and fix problems in real time. Lastly, the Monitoring and Governance Layer oversees the system and ensures its compliance and visibility.

5. Comparative Analysis

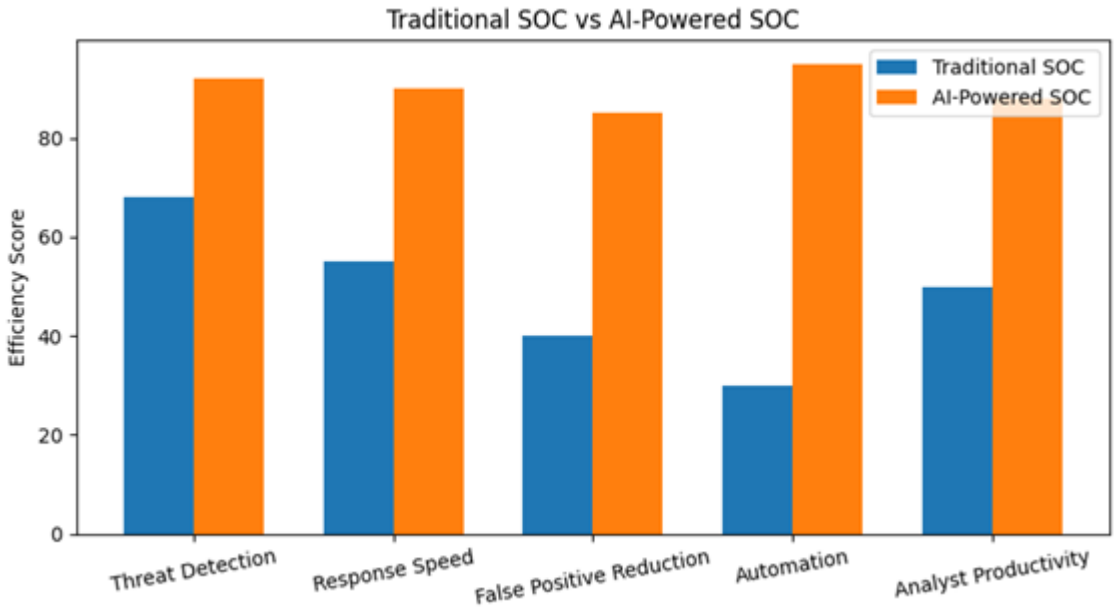
An AI-based SOC is a significant improvement over the traditional SOC approach. The automation of detection and response components equates to quicker fixes, less of the "false positive" noise, and a much more productive team. If you can get away from manual triage, analysts can now concentrate on the big picture instead of getting lost in the logs on a daily basis.

The following table compares traditional SOC environments with AI-powered SOC automation systems.

Feature	**Traditional SOC**	**AI-Powered SOC**
Threat Detection	Rule-Based	Predictive AI-Based
Response Time	Manual	Automated
Alert Analysis	Human Intensive	AI-Assisted
False Positives	High	Reduced
Scalability	Limited	High
Incident Prioritization	Manual	Intelligent Automation

6. Operational Efficiency Comparison

When you look at the numbers, the efficiency gains from AI automation are pretty clear. The speed at which a system can isolate a threat and start remediation beats human intervention every time, especially during off-hours or complex multi-vector attacks that happen all at once.



7. Enterprise Applications

Banks are already using AI-powered SOCs to catch fraud and watch for weird account activity as it happens. Hospitals are putting these systems in place to protect sensitive patient records from ransomware attacks. Even cloud providers use AI to monitor their massive networks and make sure they are hitting all their compliance targets automatically without manual audits.

8. Benefits and Limitations

Using AI to run a SOC makes a company much more resilient and takes a huge weight off the analysts' shoulders. It makes everything faster and smarter. But it is not a magic fix. There are costs to set it up, the integration can be a headache, and you have to worry about hackers trying to trick the AI itself. You also need really high-quality data to train these models in the first place, or they will not be much help.

9. Future Research Directions

Looking ahead, we need to focus on explainable AI so we actually understand why a system flagged a threat. We also need to look into autonomous response tools and security that can stand up to quantum computers. Researching the ethics and transparency of these systems will be just as important to make sure automated security stays accountable to the people using it.

10. CONCLUSION

AI automation is the biggest step forward for enterprise security in years. With the combination of machine learning and SOAR tech, businesses can now stay ahead of the curve and respond to threats within seconds, instead of hours. This framework provides a solid foundation to create a reliable and compliant smart SOC. With AI technology advancing constantly, these tools are becoming essential for any organization seeking to navigate the digital landscape safely.

REFERENCES

1. R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in Proc. IEEE Symp. Security and Privacy (SP), 2017.
2. B. Y. R. Thumma et al., "Agentic financial intelligence: A survey of LLM-powered agents for risk management, compliance, and financial analytics," *Indo Asian J. Management and Entrepreneurship*, vol. 13, no. 6, pp. 51–70, 2022.
3. M. Fredrikson, S. Jha, and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," in *Proc. ACM Conf. Computer and Communications Security (CCS)*, 2015.
4. I. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in *Proc. Int. Conf. Learning Representations (ICLR)*, 2015.
5. G. Tushar et al., "Enhancing digital payment security: A blockchain-based framework with multi-factor authentication and quantum-resistant cryptography," in *Proc. 38th Conf. Open Innovations Association (FRUCT)*, Nov. 2025, pp. 364–369.
6. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
7. A. R. Yadulla et al., "Development and integration of a privacy computing gateway for enhanced interoperability," *Indonesian J. Electrical Engineering and Computer Science (IJEECS)*, vol. 40, no. 2, pp. 1011–1022, Nov. 2025, doi: 10.11591/ijeecs.v40.i2.pp1011-1022.
8. National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, 2023.
9. C. Thumma et al., "Ethical considerations in AI-driven surveillance systems," in Proc. 2025 3rd Int. Conf. Computational Intelligence and Network Systems (CINS), IEEE, Nov. 2025, doi: 10.1109/CINS67018.2025.11412167.
10. IBM Security, "Zero trust architecture in enterprise security," IBM, 2024.
11. N. Deshai et al., "Rice grain quality analysis using deep learning," in Proc. Int. Conf. Smart Computing and Informatics, Springer Nature Switzerland, Apr. 2025, pp. 500–507, doi: 10.1007/978-3-032-08240-4_42.
12. A. Vaswani et al., "Attention is all you need," in Advances in Neural Information Processing Systems (NeurIPS), vol. 30, 2017.
13. Z. Liu and X. Li, "Privacy-preserving machine learning algorithms," IEEE Trans. Computational Intelligence, 2022.

14. S. Kadari et al., "Adaptive differential privacy-enhanced federated web shell detection with Text CNN and AST-based feature learning," in Proc. 2025 Int. Conf. Intelligent Computing, Information and Control Systems (ICOIICS), IEEE, Nov. 2025, doi: 10.1109/ICOIICS67115.2025.11390233.
15. European Commission High-Level Expert Group on AI, "Ethics guidelines for trustworthy AI," European Commission, 2019.
16. K. Saicharan et al., "Enhancing healthcare data security using PQ-ABE and verifiable secret sharing schemes," in Proc. 38th Conf. Open Innovations Association (FRUCT), Nov. 2025, pp. 377–382.
17. M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," IEEE Access, vol. 8, pp. 227756–227779, 2020.
18. B. A. Alahmadi, L. Axon, and I. Martinovic, "99% false positives: A qualitative study of SOC analysts' perspectives on security alarms," in Proc. USENIX Security Symp., 2022.
19. S. C. Sundaramurthy et al., "A human capital model for mitigating security analyst burnout," in Proc. Symp. Usable Privacy and Security (SOUPS), 2015.
20. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.
21. R. Banoth et al., "Evolving IoT botnet threats and practical honeypot observation: A summary review and experimental study," May 2026, Journal of Cybersecurity and Privacy (MDPI). doi: 10.3390/jcp6030082.
22. C. Islam, M. A. Babar, and S. Nepal, "A multi-vocal review of security orchestration," ACM Comput. Surveys, vol. 52, no. 2, Art. no. 37, 2019.
23. H. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber-attacks," Computers & Security, vol. 72, pp. 212–233, 2018.
24. S. Ayyamgari et al., "Authentication mechanisms in the Internet of Things: A comparative analysis across RFID, smart grids, vehicular networks, and smart homes," Sep. 2026, Sensors (MDPI). doi: 10.3390/s26185893.
25. B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognition, vol. 84, pp. 317–331, 2018.