Volume 11, Issue 8, August– 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug301

Bridging the AI Security Skills Gap: An Approach to Preparing the Cybersecurity Workforce in the AI Era Threats

Sreenivasa Rao Basavala[1]; Prudhvi Raju Mudunuri[2]

[1]Marymount University/Department of BuILT, Arlington, USA
[2]Independent Researcher, Montgomery Village, USA

Publication Date: 2026/08/17

Abstract: The rapid growth of Artificial Intelligence (AI) is having a profound impact on Cybersecurity. The means by which organizations will protect their networks, systems and applications is undergoing rapid transformation as are how Cyber adversaries design, plan and attack. What was once a purely human-led discipline is increasingly influenced by automated and intelligent technologies, including those that can learn, self-optimize and process enormous volumes of data. Cyberattacks are becoming more sophisticated, more frequent, faster and more covert and the tools and technologies required to counter them are evolving at pace to keep up with the attackers. The information security workforce is quickly getting familiar with new AI-driven technologies. However, there exists a skills gap as most of the current IT staff are trained in more traditional information security practices and not prepared to handle the specific security needs for AI and Deep Learning, analyze potential risks of malicious use of machine learning, and respond to AI powered attacks. Organizations are rapidly deploying new technologies that rely on AI and are in dire need of a skilled workforce to defend them. This paper discusses current challenges and advancements in the use of AI/ML (Machine Learning) in cybersecurity to help address the current cybersecurity skills shortage. It then translates these insights into practical advice for organizations looking to strengthen their cybersecurity workforce through upskilling, cross-functional work, and the use of secure AI within established security processes and procedures.

Keywords: *AI Security, Cybersecurity Workforce, Skill Gap, Threat Modelling, MLOps Security, Data AI Security.*

How to Cite: Sreenivasa Rao Basavala; Prudhvi Raju Mudunuri (2026) Bridging the AI Security Skills Gap: An Approach to Preparing the Cybersecurity Workforce in the AI Era Threats. *International Journal of Innovative Science and Research Technology*, 11(8), 590-596. https://doi.org/10.38124/ijisrt/26aug301

I. INTRODUCTION

Cybersecurity is changing from something that people do by hand to something where bad people use AI to launch smart and automatic attacks. AI can really help with cybersecurity by making it easier to find and understand problems and to predict what might happen next. Bad people are using AI to do bad things like constantly looking for weaknesses in computer systems and sending fake emails that can change and get smarter based on how the security system responds. On the other hand, AI can be used for good, it can do tasks that used to take people hours or days to do and now it can be done in just seconds by organizations. A lot of organizations are getting excited about using AI for cybersecurity even though it still has a lot to show us. Organizations are using AI for security tasks like finding threats and responding to incidents, managing weaknesses in computer systems and preventing fraud, and more than 90% of organizations are using AI now or will be using it soon. Most organizations do not really understand how AI works, how it can be attacked and how to protect it. Not knowing enough about AI is a problem for almost half of the organizations that want to use it. Computer system breaches are getting worse fast. As organizations start using AI, they are not taking the time to teach their employees the skills they need to deal with the new threats [4]. This lack of knowledge about AI security puts organizations, computer networks and important, sensitive assets at high risk because bad people are ready to take advantage of the weaknesses.

II. EVOLUTION OF CYBER THREATS IN THE AI ERA

AI is transforming the cyber threat landscape in the era. In the past, cyberattacks were typically planned and executed over a long period of time by an individual using manual, laborious methods to search for and exploit vulnerable targets. Today's cybercriminals are vastly more automated, intelligent and adaptive than their predecessors, using vast amounts of data to identify and target organizations and individuals of value, and exploiting newly discovered vulnerabilities in a matter of hours or even minutes as shown

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug301

in Figure 1. Moreover, because they are highly automated and possess the ability to learn and adapt at speed, threats can be distributed via social media in hours, sweep through an organization's network in the time it takes to type an exploit, or have a phishing email generated by a computer in the time it takes to type a command line. The reality is that hackers are getting smarter, and the entry barriers to launching intelligent threats are decreasing for less skilled hackers [9]. It is therefore time for organizations to rethink their security approach to keep pace with today's intelligent cybercriminals.

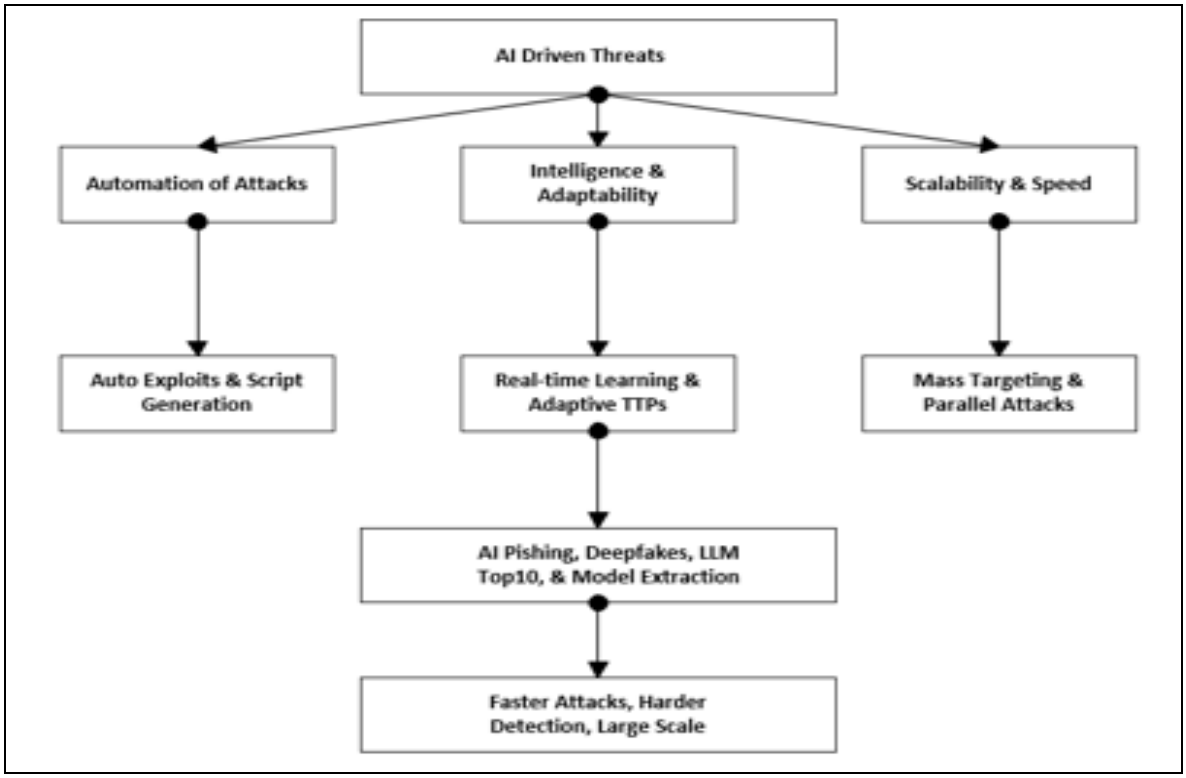

Fig 1 AI Driven Cyber Threats

➢ *AI as an Offensive Weapon*

The power of AI in cyber warfare is growing as a formidable tool in the adversary's arsenal. With current AI-powered tools, misconfigurations can be identified easily. But more importantly, these tools can also automatically generate, optimize and combine exploit code and specially crafted scripts to maximize impact. AI is also starting to change the game when it comes to cyber-attacks. While intelligence gathering and some aspects of an attack can be automated, the creative part of an attack like developing highly personalized, context-specific phishing e-mails (including audio and video deepfakes) can also be done by AI. And these emails can be used for a large-scale impersonation campaign that is hard to detect for end users and security tools alike including users who are highly aware of phishing attempts. With AI in the mix, what were once the domain of highly skilled nation-state actors and top cyber criminals can now be carried out by a far broader range of cyber adversaries.

Cyberattacks can now be carried out automatically but that's not the worst of it. In addition to the initial automation, attackers can use that gained time to test, evaluate, learn from their previous attempts, and refocus their efforts in real time, and as the attack is powered by AI, it becomes increasingly intelligent. Before they reach that level, AI also greatly enhances the capabilities of those launching attacks by enabling massive parallel execution, allowing a single adversary to amplify efforts and attack thousands of targets with only a modest increase in effort. The line between a human powered attack and a machine powered attack will continue to blur as the threat continues to evolve at a breakneck pace, becoming faster, more sophisticated, and even more autonomous.

➢ *Acceleration of Attack Speed and Scale*

The usage of artificial intelligence (AI) in cyberattacks is on the rise. Manual, labor-intensive, time-consuming network scanning, vulnerability detection and exploitation testing can now be performed in seconds by threat actors. This new breed of cyber threats is learning based, self-sufficient, highly adaptable and in real time, the threats are improving their tactics and techniques to evade detection. The job of an information security professional has never been more challenging. Most attacks must be neutralized within seconds, not hours or days. The use of AI in malicious activity is growing exponentially [1]. With a single individual able to launch tens of thousands of or even hundreds of thousands of threats per day against large, mid-market and other organizations, detecting, responding to, and preventing advanced, distributed threats has become an exponentially more difficult task for security professionals. So, how do you stop these things? This is what security teams are facing daily. With the attackers now utilizing AI in

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug301

their attacks, security teams are faced with a challenge of scale, dealing with not only an increased volume of attacks but also multiple concurrent attacks at the same time, requiring different skill sets and resources to mitigate. The security teams are struggling to keep up. How can organizations keep up?

➢ *The AI Security Skills Gap: Current State*

There is a well-established and growing "skill gap" between the AI that vendors are integrating into security solutions and the skill set needed to manage and administer that technology. The shortage of qualified individuals already appears to be severe with many organizations reporting trouble finding candidates with meaningful AI security experience [2]. The lack of knowledge required to safely integrate and manage current AI systems is a growing burden on security teams already operating on thin budgets and with limited personnel. The training organizations and various certifications in the industry are only just beginning to develop curricula and programs aimed at increasing the number of individuals who can manage these complex systems. There are model poisoning and other so-called "white box" attacks that need to be defended against, adversarial samples generated by deep learning models that require detection, and data leakage from the generative models used in data loss prevention and other systems. As AI is quickly being integrated into many different aspects of security, the world is currently operating in a temporary state of chaos while the necessary skills are brought online.

➢ *Skills Gap vs. Talent Shortage*

In the cybersecurity world, we commonly bandy about the terms "talent shortage" and "skills gap," and on the surface, they seem to be synonymous. However, to the cybersecurity leader facing a staffing conundrum, these two terms mean very different things. A talent shortage exists in the workforce at large, and it refers to a shortage of professionals who are qualified to fill specific, open cybersecurity job vacancies. A skills gap, on the other hand, exists among those who are qualified to perform the role and already are working in the profession, but simply lack the skills needed to address the unique and problematic threats that are faced by organizations, many of which are employing artificial intelligence as part of their assaults. Cybersecurity may be facing a shortage of professionals with the right skills, but there's one skillset that may be in even greater demand: the ability to battle AI with AI [14].

As AI becomes a huge threat vector, there's already a lot on security teams, when it comes to threat investigation daily. But the growing list of AI threats, which now apparently includes models themselves, is pushing the industry to wonder if security teams will be able to keep up. Threat investigators already have tough job juggling networks, endpoints, and a host of other security challenges, all while keeping an eye on regulations, compliance, and security operations. But machine learning, and particularly the non-standard use cases, interesting data pipelines, and 'black box' models, are an emerging challenge for security teams. Will their existing experience and skills be enough? Additionally, advanced threats such as prompt injections and data poisoning demand specialized knowledge and skills. There is a big difference between a "talent shortage" and a "skills shortage." A talent shortage is typically addressed by hiring more people. A "skills shortage," however, is addressed by reskilling or upskilling the employees the organization have already. To address the AI security workforce challenges facing organizations today require more than just hiring more professional bodies. Those employees also need hands-on experience with AI and the practical application of knowledge about the AI-specific security techniques in their everyday work. An organization can have all the personnel it needs, but if they don't have the skills needed to address AI security challenges, it won't make any difference [18].

➢ *Impact on Security Outcomes*

Unlike skills gaps in AI security that future workers will have to address, the AI security skills gap is currently faced by the very security practitioners and SOC teams tasked with defending their organizations today. Organizations rolling out security tools, automation, and processes are counting on these security practitioners and SOC teams to deliver near term gains in their ability to quickly detect and respond to advanced threats. AI-powered security tools are having a significant and rapid impact on the way that security teams work, shifting from a siloed, manual approach to one that is automated, distributed, and dependent on processes and tools that can scale to handle unprecedented volumes of data. However, while processes and tools can handle volume and velocity of attacks for a time, at some point, humans will be needed to triage, analyze, contain, and recover from a threat. Without the necessary AI security skills, security practitioners will either miss or make very poor decisions in their fight against cyber threats.

The emergence of AI is dramatically reshaping the threat landscape faced by the security professional [14][15]. AI-powered threats are fueling increased breaches, longer durations of time that attackers remain within a network, and greater damage to an organization following a breach. AI-enabled attacks are typically fast, multi-vector, and highly destructive as they quickly move from system to system, exploiting vulnerabilities before traditional security processes can respond. While traditional security professionals are still getting familiar with the features and operation of AI, many lack experience in AI threat modeling, adversarial testing, and model risk management. As a result, there is a general lack of understanding of how AI can be used for malicious intent, how it can be manipulated or abused for harmful purposes, and organizations that rely heavily on generative AI technologies are particularly vulnerable to unknown risks. The biggest issue is security posture and maybe the lack of AI security skills. What began as an aggressive, proactive and risk-managed security approach is slowly being devoured by a reactive one. That reactive approach will suck money out of the organization, erode trust in the security programs and ultimately cost big in terms of money and reputation. As threats become more intelligent and adaptive, the outcome of your security efforts will be limited by the skills of the workforce to deal with them.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug301

III. KEY AI SECURITY SKILLS GAP

There is much concern in the industry about how AI can be used to attack organizations and businesses. But there are also new threats to AI itself. As more AI models are deployed across more industry sectors and applications, IT professionals will need to understand emerging threats such as adversarial examples, prompt injection attacks, and model extraction attacks. They will need a deep understanding of how an AI model learns, and how and why it fails, to defend against these threats on scale. Professionals begin to adopt automated decision support to run their day-to-day operations, and it will need a solid understanding of the basics of AI/ML security to maintain network security and gain trust in automated decision processes.

AI security skills gaps stem from the rapid adoption of AI outpacing the ability to secure it, leaving shortages in areas like protecting ML systems from attacks, safeguarding sensitive data, managing risks and compliance, explaining model decisions, monitoring and responding to incidents, securing deployment pipelines, handling generative AI or Large Language Models (LLM) threats (like prompt injection), and ensuring safe use of third-party tools, highlighting a broader need for combined expertise in cybersecurity, risk, governance, and compliance as shown in Figure 2.

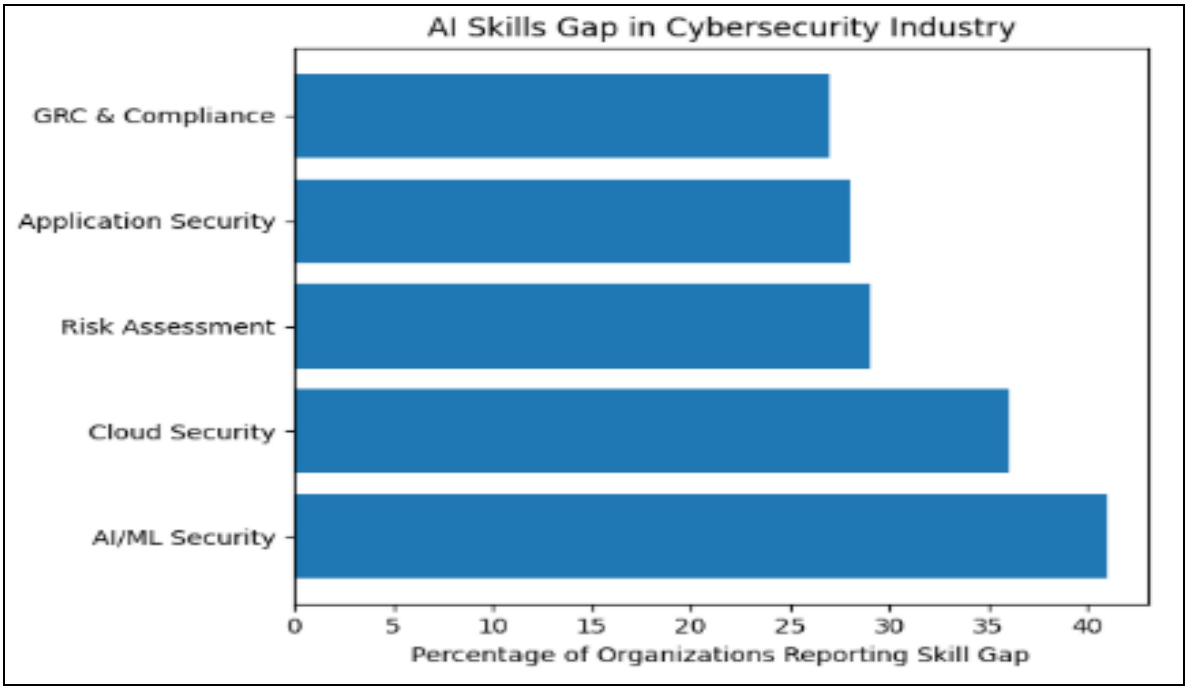

Fig 2 AI Security Skills gap in Cybersecurity Domain

Future is going to be shaped significantly by the adoption of AI and machine learning. This in turn means that we will have to adapt our view on security in Information Technology (IT). Currently organizations are focusing on protecting the IT-infrastructure and applications but protecting artificial intelligence (AI) and Machine Learning (ML) models is so much more than that. In addition to protecting the model itself, all data that is input to the model, the results of the model and the data that is used to train the model all need to be protected [16]. Each phase of the ML lifecycle offers an attacker a potential attack surface, for poisoning of data, manipulation of a model or harvesting of data. Current monitoring and threat detection tools for traditional IT do not extend to monitoring the performance and accuracy of AI/ML models. Tools for traditional IT monitoring are designed to provide a human centric visual representation of current IT operations. As AI/ML models are inherently probabilistic and can be affected by low frequency, high impact events that the human eye is not even able to detect, monitoring tools must evolve as well.

- *AI Threat Modeling & Adversarial Thinking*

Securing AI systems is important and that is why threat modeling and adversarial thinking are crucial [3]. When organizations build AI systems must think about the threats to these systems just like with traditional systems. As AI moves from the research stage to being ready for use, security professionals need to start thinking like attackers when they make threat models for Artificial Intelligence. They need to check the training data to see if it has been tampered with thinking about how someone might reverse-engineer a model to use it for things that could be used to cause harm. This means security professionals must be more proactive and think about threats before they happen than just reacting to them after they happen. To do this the security team that makes threat models has to think like an adversary. If they do these organizations will be able to find weaknesses, in their AI systems discover weaknesses that they had not thought of before and develop ways to protect against both technical problems and people trying to manipulate the system. This will help build Artificial Intelligence systems that're safe and secure.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug301

➢ *Secure AI Development (MLOps Security)*

Enterprises are struggling to secure their AI development pipelines, which are growing in complexity and depth. The challenge of securing training data is particularly acute as compromised or biased training data can cause a model to act in ways that are unforeseen and un-intentional. Ensuring that models have not been subverted during development and deployment is also critical. In addition, managing AI supply chain risks from 3rd party models, open-source data and pre-trained components is increasingly important as unknown security vulnerabilities can be introduced into the pipeline if these components are not properly validated and managed [4].

➢ *Data Security in AI Systems*

As organizations adopt AI systems, they will encounter new challenges to the security of information data that goes beyond typical information security concerns with legacy IT systems. This includes reviewing content generated by AI models for inadvertent exposure of sensitive or proprietary content as well as intentional exposure for malicious purposes. There is also growing concern for data poisoning, where AI models are trained on poisoned or manipulated data with the intent to produce specific and potentially damaging results. While most current AI workflows lack sufficient data lineage and integrity controls, today's organizations require effective information governance policies and data security measures to ensure accurate, trustworthy, and secure use of data within AI workloads.

➢ *Human–AI Collaboration Skills*

Artificial intelligence (AI) is transforming the work of security analysts. As AI assumes new functions in cybersecurity, analysts must acquire skills to effectively interact with AI tools. Two critical skills involve constructing effective input for AI (for example, developing insightful prompts to natural language processing or machine learning) and critically evaluating the accuracy, completeness, and correctness of AI output [6]. Analysts must also be able to recognize how AI can automate biases that analysts then rely upon to make security decisions, a phenomenon known as automation bias. To effectively wield AI in the security analyst role, individuals must understand how to utilize technology as a complementary tool to, not substitute for, analysts' skills.

➢ *AI Governance, Risk, and Compliance (GRC)*

Governance, Risk, and Compliance (GRC) must transform dramatically to address the impact of artificial intelligence on organizations. This includes identifying and managing risks from AI across the entire AI lifecycle and understanding and managing new compliance requirements that are more complex to address the growing number of laws and regulations that demand more transparency, accountability, and control over how AI is developed and used [12]. Finally, there are new ethics-related issues that must be managed including bias, model explainability, and end-user trust in and buy-in from regulators.

➢ *Causes of the Skills Gap*

The AI security skills gap exists because organizations are rushing to deploy AI and lock down data-intensive workloads before their security teams have developed the necessary skills to evaluate risk. The timeframe from proof-of-concept (POC) to production-ready AI workloads is too fast for security teams to keep up [8]. The lack of integrated training for security professionals, data scientists, and software engineers is also driving a shortage of skills required to address AI-specific threats and countermeasures. As threats to AI and automated systems continue to grow, the skills gap is likely to continue to grow unless there is a unified approach to security and skills training.

There is a lack of emphasis on practical skills training for AI security, and this is worsening the skills gap in the field. While there are many established training programs for cybersecurity that concentrate on theoretical models and best practices, there is a pressing need for more practical experience designing, testing, and managing of AI systems to counter threats such as model manipulation, data exfiltration, generation of adversarial examples, and malicious prompts injection into large language models [7]. The training offered by academic programs for AI security is not adequately aligned with the AI security skills that organizations need their employees to possess. Many organizations are having difficulties finding qualified candidates to fill entry-level positions related to AI security.

IV. WORKFORCE UPSKILLING AND RESKILLING

To struggle with these emerging AI threats, organizations will need to invest in AI security training helps to enable their existing cybersecurity workforce through upskilling and reskilling. Security professionals and teams will need to have a deep understanding of how AI works. Despite significant investment in training the security professionals that will fight against AI, there will be a rapid transition in the industry to focus on cross-functional training and knowledge sharing between security, data science, and engineering teams against AI powered threats. Security professionals will need deep knowledge of how AI models are trained and deployed, as well as deep understanding of the specific vulnerabilities and weaknesses in those models [12]. As importantly, they will need to learn to detect, mitigate, and manage AI powered threats targeted at their own AI models.

➢ *Integration of Secure AI Development (Secure MLOps)*

Security must be embedded in the model development lifecycle and good secure Machine Learning Operations (MLOps) practices such as protecting data pipelines from corruption, misuse or degradation, adequate testing prior to deployment into production, and ongoing monitoring for anomalies must be adopted. Companies must consider the potential risks and challenges early on, quickly detect vulnerabilities in their AI systems as new threats are emerging and as attack patterns are evolving over time.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug301

➢ *AI Threat Modeling and Red Teaming*

As more organizations adopt AI and ML to enhance their security posture, those organizations taking a proactive security approach will also need to implement AI specific threat modeling and red teaming. This means simulating out attacks where the AI/ML model is the defender of the system. Testing of Large Language Models will also require unique evaluation techniques to ensure there are no vulnerabilities to attacker abuse for prompt injection or other manipulations. As with traditional defensive controls, ongoing validation and verification of not only the AI/ML models but the defensive controls surrounding them will also be crucial [10].

➢ *Adoption of AI Governance and Security Frameworks*

When integrating AI security into existing governance and organizational processes and policies, it is crucial to consider consistency and accountability across the organization. To assist organizations, identify, assess and manage potential risks of AI, NIST recently published an AI Risk Management Framework (AI RMF) as well as OWASP (Open Web Application Security Project) recently published the Top 10 for Large Language Models called OWASP LLM Top 10 risks. These documents are then translated into security controls and organizational policies to manage the risk identified.

➢ *Hands-on Learning and Simulation*

There is little room for lectures and traditional classroom instruction on how to defend against AI, because AI is rapidly evolving. To adequately train future network defenders, CTFs (Capture the Flag) and AI security labs where defenders can practice using new skills to defend against the latest AI threats must play a much larger role in security education and training [11]. In fact, this type of training will resemble the training of future AI models, which will evolve rapidly in the coming years. New studies reveal that "AI is already better than humans in certain areas of battling current cybersecurity threats and competitions" but battling against future AI powered cyber threats will require training students and employees to defend computer networks in simulation labs and hands-on environments.

➢ *Strengthening Human–AI Collaboration*

With the new AI companion, professionals will need to learn how to leverage the technology effectively in their daily security operations. Security professionals will need to critically evaluate the AI generated data, accept ownership of the accuracy of the information and utilize a strategic, methodical and thorough approach to decision making when utilizing the AI as an augmentation to their existing workload. AI should be used as a powerful assistant, not as a quick fix to fill skills gaps.

➢ *Building a Sustainable Skilled Workforce*

CISOs and other leaders in the cybersecurity organization should be thinking beyond the next patch cycle. They should be thinking about building cybersecurity readiness over the long haul. This means building a pipeline of future talent with appropriate skills and knowledge for dealing with AI and systems that incorporate AI. Enterprises can build future ready cybersecurity talent by participating in or hosting apprenticeships / internships, funding training and industry accepted certifications like those provided by ISC2, ISACA, CompTIA, AIOps Exchange, collaborating with other enterprises, and working with academic organizations and training providers to support students entering the workforce as well as to develop curriculum that addresses these emerging challenges to securing AI systems.

V. CONCLUSION

The global cyber security industry faces a major talent gap as organizations battle to keep up with the latest AI-powered threats, as well as those that are utilizing the technology to accelerate, amplify or transform their operations in a bid to infiltrate and exploit systems that also incorporate AI-powered security solutions. As organizations face off against a new type of threat, many are grappling with a growing skills shortage between their security teams and the threat they face. But, given the nature of cybersecurity work is changing as attackers use AI for malicious purposes, traditional learning and development practices are not enough.

REFERENCES

[1]. Arif, A., Khan, M. I., & Khan, A. R. A. (2024). An overview of cyber threats generated by AI. International Journal of Multidisciplinary Sciences and Arts, 3(4), 67-76.

[2]. Ball, J., Lyons, M., & Evans, K. (2025, April). Bridging the Cybersecurity Skills Gap: Aligning Educational Programs with Industry Needs. In Journal of The Colloquium for Information Systems Security Education (Vol. 12, No. 1, pp. 9-9).

[3]. Basavala SR. *AI Security/Designing Effective Defenses for Large Language Models (LLM) in Adversarial Settings*. Order No. 32741550 ed. Marymount University; 2026.

[4]. Basavala, S. R., & Mudunuri, P. R. (2026). Emerging LLM Threats: A Comprehensive Analysis of Attacks and Mitigation. *International Journal of Innovative Science and Research Technology (IJISRT)*, *11*(05), 2136-2145.

[5]. Calefato, F., Lanubile, F., & Quaranta, L. (2024). Security Risks and Best Practices of MLOps: A Multivocal Literature Review. ITASEC.

[6]. Cichocki, A., & Kuleshov, A. P. (2021). Future Trends for Human-AI Collaboration: A Comprehensive Taxonomy of AI/AGI Using Multiple Intelligences and Learning Styles. Computational Intelligence and Neuroscience, 2021(1), 8893795.

[7]. Falco, G., Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A master attack methodology for an AI-based automated attack planner for smart cities. IEEE Access, 6, 48360-48373.

[8]. George, A. S., Baskar, T., & Srikaanth, P. B. (2025). Bridging the Security Skills Gap: A Comprehensive Framework for Developing Application Security Competencies in Modern Software Engineering.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug301

Partners Universal Innovative Research Publication, 3(3), 96-123.
[9]. Graham, C. M. (2025). AI skills in cybersecurity: global job trends analysis. Information & Computer Security, 33(5), 673-689.
[10]. Grosse, K., Bieringer, L., Besold, T. R., & Alahi, A. M. (2024). Towards more practical threat models in artificial intelligence security. In 33rd USENIX Security Symposium (USENIX Security 24) (pp. 4891-4908).
[11]. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence, 36(1), 2037254.
[12]. Karpatou, P. A. (2025). The evolution of cybersecurity threats & the rise of artificial intelligence.
[13]. Lau, D., Samy, G. N., Rahim, F. A., Maarop, N., & Hassan, N. H. (2023). Review of the governance, risk and compliance approaches for artificial intelligence. Open International Journal of Informatics, 11(2), 25-35.
[14]. Oladimeji, S., Egon, A., & Broklyn, P. (2024). Cybersecurity workforce development: Bridging the skills gap in the age of automation. Available at SSRN 4904939.
[15]. Smith, G. (2018). The intelligent solution: automation, the skills shortage and cyber-security. Computer Fraud & Security, 2018(8), 6-9.
[16]. Upadhyaya, N. (2023). AI-Powered Secure Software Development: The Future of Safe and Efficient Coding. ESP Journal of Engineering & Technology Advancements, 3(2), 148-152.
[17]. Vogel, R. (2016). Closing the cybersecurity skills gap. Salus journal, 4(2), 32-46.
[18]. Zakkiya, S. A., Selviandro, N., & Utomo, R. G. (2025, August). A Guideline for the Adoption of Generative AI to Support Secure Software Development Life Cycle (SSDLC): A Case Study of ChatGPT. In 2025 IEEE International Conference on Artificial Intelligence for Learning and Optimization (ICoAILO) (pp. 62-68). IEEE.