AI's Role in Cybersecurity Posture

As cyber exploits become more complicated and varied, artifical intelligence and machine learning can help organizations improve their posture and better resist attacks

Cybersecurity threats to every organization are growing. The proliferation of the Internet of Things (IoT) dramatically expands the number of potential internal targets and external points of attack. Ever-richer pools of organizational data remain juicy targets for criminals, who continue to launch attacks in record numbers and with increasing aggression and sophistication. An ongoing shortage in qualified cybersecurity personnel adds to the strain. Data from CyberSeek shows over 700,000 posted, open cybersecurity jobs as of August 2022[1] According to the 2021 (ISC)[2] Cybersecurity Workforce Study[2], the global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets.

Artificial intelligence and machine learning (AI/ML) capabilities can help mitigate some of these threats and workforce shortage challenges. AI bridges the gap between the speed and evolving nature of threats by providing continuous coverage, rapid analysis of large sets of behavioral data, and a growing ability to discern a wide variety of cyberattacks as they occur.

How AI Addresses Top Cybersecurity Challenges

Cyber defense teams aren't simply understaffed. They are under continuous pressure to assess and protect against an evolving slate of attacks—and attackers don't honor conventional work schedules. This can create a cycle in which talented practitioners are forced to spend a disproportionate amount of their time on the top of the funnel and lack the resources to investigate and respond appropriately elsewhere.

Cyber criminals are increasingly able to launch algorithmic attacks and are developing their own AI capabilities to explore targets and initiate attacks without human intervention or additional coding effort.

Organizations should be ready to match this escalation with AI of their own. By providing around-the-clock coverage and relieving trained employees of heavy data-sifting responsibilities, AI can help organizations address some of their most significant cybersecurity challenges, including:

Network traffic generates tremendous volumes of log data. AI helps make these logs digestible to human analysts and can flag cybersecurity-specific patterns for expedited review as they emerge.

Although not a complete substitute for trained personnel, AI can help organizations do more with available employees by freeing them for higher-value tasks.

Internal algorithmic surveys and probes can help identify network risks, including unmanaged or misconfigured devices and unpatched operating systems operating inside your network cordon.

Minimally used or obsolete network-connected devices can be flagged for remediation by experts.

With proper training against a dataset of normal and expected network activity, ML can build a picture of the range of typical network traffic and systems operations. Deviations from this range can be slowed, suspended, or escalated to professionals for further review. This capability helps free up professional hours formerly spent trying to monitor traffic in real time, an area where machines have a data-processing advantage. In addition, AI can also close gaps in accounts that are operating with improper credentials, logged in at unusual times, or not properly deprovisioned following an employee departure.

AI's primary strength is finding order in chaos by detecting patterns in vast volumes of data. AI can provide insights into the shape, intensity, and potential for damage caused by unexpected network contacts or prospective intrusions. This autonomous insight is critical for reducing response times and fighting the new generation of AI-enhanced cyber threats.

AI can mirror the workflow of a cybersecurity analyst, by monitoring unusual behavior and correlating disparate data over time. It can also use natural language processing (NLP) to generate reports on those investigations. These reports and response plans can then be folded into reinforcement for the AI model, which improves future waves of automated.

Challenges to Successful Deployment of Cyber-Aware AI

Adding AI capabilities to existing cybersecurity teams can pose significant and important challenges. Practitioners well versed in the intersection of AI/ML, change management, and cybersecurity—such as those at Guidehouse—can significantly ease the transition and ensure that algorithms and tools are deployed to best possible advantage.

For example, AI cybersecurity solutions are most successful when they have large volumes of properly labeled data to process for trends, patterns, and relationships. Access to that data in an AI-ready form is not available at every organization or would take significant analyst time to clean and prepare for ingestion. With an experienced team guiding the introduction of AI intro cybersecurity, all relevant data sources can be included early in the process. This decreases friction with model training, minimizes data drift, and reduces error rates in attack detection.

Ideally, the AI model will have real-time access to network traffic data in order to provide real-time threat detection. Implementing these real-time ingestion pipelines is different from preparing one-time or batch-training datasets, further complicating the rollout of cyber-aware AI. Real-time ingestion is also computationally expensive, beyond the practical reach of many organizations.

Developing and deploying cybersecurity AI is a significant investment of time, money, and expert resources. Developing and training an algorithm requires cybersecurity expertise as well as AI mastery. Change-management skills can help smooth the road to amassing enough real-time data to identify all points of vulnerability and all early-warning indicators of a potential attack. Refining models and datasets takes time, and additional computational resources are necessary to run the algorithm.

Over time, AI models will need to be tuned and retrained to reflect changing conditions and new sources of insight. As attacker patterns become clear and security advisory agencies identify new best practices, models may require additional access or lines of communication with live experts who can act on each new generation of emerging threats.

Conclusion

Cybersecurity teams need more support to quantify and assess present and future threats. Earlier warning and mitigation of suspicious network activity can prevent costly intrusions or denials of service. As workforces continue to operate in hybrid and increasingly complex conditions, better identity and access controls are needed to reduce exposure to mishandled or compromised credentials. Additionally, teams need stronger playbooks for coordinated action to minimize damage from previously undocumented weaknesses and automated attacks in progress.

AI can help with each of these goals. Implementation and deployment of AI cybersecurity solutions is an emerging discipline without a one-size-fits-all approach. Guidehouse's cyber-AI/ML experts can identify the best solutions to address gaps and vulnerabilities and bolster your security posture around the clock.

Talk to Guidehouse about how AI and ML can help your cybersecurity teams tackle threats, known and unknown, with greater agility, even in a constrained labor market.

1. "Cybersecurity Supply/Demand Heatmap", n.d, Cybersecurity Supply And Demand Heat Map (cyberseek.org).
2. "2021 (ISC)² Cybersecurity Workforce Study", 2021, ISC2_Cybersecurity_Workforce_Study_2021.pdf (iapp.org)

Contacts

April Fordyce, Director
Advanced Analytics and
Intelligent Automation
afordyce@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 17,000 professionals in over 55 locations globally. Guidehouse is led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit guidehouse.com.

https://guidehouse.com/services/cybersecurity

@GHTechSolutions https://www.linkedin.com/showcase/guidehouse-technology-solutions/