الاسم : - محسن علي شرهان

المرحلة : - رابع ذكاء صباحي

Artificial Intelligence in Cyber - : عنوان التقرير security

Using Artificial Intelligence in Cyber security

The enterprise attack surface is massive, and continuing to grow and evolve rapidly. Depending on the size of your enterprise, there are up to several hundred billion time-varying signals that need to be analyzed to accurately calculate risk.

The result?

Analyzing and improving cybersecurity posture is not a human-scale problem anymore.

In response to this unprecedented challenge, Artificial Intelligence (AI) based tools for cybersecurity have emerged to help information security teams reduce breach risk and improve their security posture efficiently and effectively.

AI and machine learning (ML) have become critical technologies in information security, as they are able to quickly analyze millions of events and identify many different types of threats – from malware exploiting zero-day vulnerabilities to identifying risky behavior that might lead to a phishing attack or download of malicious code. These technologies learn over time, drawing from the past to identify new types of attacks now. Histories of behavior build profiles on users, assets, and networks, allowing AI to detect and respond to deviations from established norms.

Applying AI to cybersecurity

AI is ideally suited to solve some of our most difficult problems, and cybersecurity certainly falls into that category. With today's ever evolving cyber-attacks and proliferation of devices, machine learning and AI can be used to "keep up with the bad guys," automating threat detection and respond more efficiently than traditional software-driven approaches.

At the same time, cybersecurity presents some unique challenges:

- A vast attack surface
- 10s or 100s of thousands of devices per organization
- Hundreds of attack vectors
- Big shortfalls in the number of skilled security professionals
- Masses of data that have moved beyond a human-scale problem

A self-learning, AI-based cybersecurity posture management system should be able to solve many of these challenges. Technologies exist to properly train a self-learning system to continuously and independently gather data from across your enterprise information systems. That data is then analyzed and used to perform correlation of patterns across millions to billions of signals relevant to the enterprise attack surface.

The result is new levels of intelligence feeding human teams across diverse categories of cybersecurity, including:

- **IT Asset Inventory** – gaining a complete, accurate inventory of all devices, users, and applications with any access to information systems. Categorization and measurement of business criticality also play big roles in inventory.
- **Threat Exposure** – hackers follow trends just like everyone else, so what's fashionable with hackers changes regularly. AI-based cybersecurity systems can provide up to date knowledge of global and industry specific threats to help make critical prioritization decisions based not only on what could be used to attack your enterprise, but based on what is likely to be used to attack your enterprise.
- **Controls Effectiveness** – it is important to understand the impact of the various security tools and security processes that you have employed to maintain a strong security posture. AI can help understand where your infosec program has strengths, and where it has gaps.

- **Breach Risk Prediction** – Accounting for IT asset inventory, threat exposure, and controls effectiveness, AI-based systems can predict how and where you are most likely to be breached, so that you can plan for resource and tool allocation towards areas of weakness. Prescriptive insights derived from AI analysis can help you configure and enhance controls and processes to most effectively improve your organization's cyber resilience.
- **Incident response** – AI powered systems can provide improved context for prioritization and response to security alerts, for fast response to incidents, and to surface root causes in order to mitigate vulnerabilities and avoid future issues.
- **Explainability** – Key to harnessing AI to augment human infosec teams is explainability of recommendations and analysis. This is important in getting buy-in from stakeholders across the organization, for understanding the impact of various infosec programs, and for reporting relevant information to all involved stakeholders, including end users, security operations, CISO, auditors, CIO, CEO and board of directors.

Some early AI adopters

Google: Gmail has used machine learning techniques to filter emails since its launch 18 years ago. Today, there are applications of machine learning in almost all of its services, especially through deep learning, which allows algorithms to do more independent adjustments and self-regulation as they train and evolve.

"Before we were in a world where the more data you had, the more problems you had. Now with deep learning, the more data the better. Elie Bursztein, head of anti-abuse research team at Google

IBM/Watson: The team at IBM has increasingly leaned on its Watson cognitive learning platform for "knowledge consolidation" tasks and threat detection based on machine learning.

"A lot of work that's happening in a security operation center today is routine or repetitive, so what if we can automate some of that using machine learning?" – Koos Lodewijkx, vice president and chief technology officer of security operations and response at IBM Security.

Juniper Networks: The networking community hungers for disruptive ideas to address the unsustainable economics of present-day networks. Juniper sees the answer to this problem taking shape as a production-ready, economically feasible Self-Driving Network™.

"The world is ready for autonomous networks. Advances in artificial intelligence, machine learning, and intent-driven networking have brought us to the threshold at which automation gives way to autonomy." Kevin Hutchins, Sr. VP of strategy and product management.

Balbix BreachControl (now called Balbix Security Cloud) platform uses AI-powered observations and analysis to deliver continuous and real-time risk predictions, risk-based vulnerability management and proactive control of breaches. The platform helps make cybersecurity teams more efficient and more effective at the many jobs they must do to maintain a strong security posture – everything from keeping systems patched to preventing ransomware.

"Enterprises need to build security infrastructure leveraging the power of AI, machine learning, and deep learning to handle the sheer scale of analysis" – Gaurav Banga, Founder and CEO.

AI Use by Adversaries

AI and machine learning (ML) can be used by IT security professionals to enforce good cybersecurity practices and shrink the attack surface instead of constantly chasing after malicious activity**.** At the same time, state-sponsored attackers, criminal cyber-gangs, and ideological hackers can employ those same AI techniques to defeat defenses and avoid detection. Herein lies the "AI/cybersecurity conundrum."

As AI matures and moves increasingly into the cybersecurity space, companies will need to guard against the potential downsides of this exciting new technology:

- Machine learning and artificial intelligence can help guard against cyber-attacks, but hackers can foil security algorithms by targeting the data they train on and the warning flags they look for
- Hackers can also use AI to break through defenses and develop mutating malware that changes its structure to avoid detection
- Without massive volumes of data and events, AI systems will deliver inaccurate results and false positives
- If data manipulation goes undetected, organizations will struggle to recover the correct data that feeds its AI systems, with potentially disastrous consequences

Conclusion

In recent years, AI has emerged as required technology for augmenting the efforts of human information security teams. Since humans can no longer scale to adequately protect the dynamic enterprise attack surface, AI provides much needed analysis and threat identification that can be acted upon by cybersecurity professionals to reduce breach risk and improve security posture. In security, AI can identify and prioritize risk, instantly spot any malware on a network, guide incident response, and detect intrusions *before they start*.

AI allows cybersecurity teams to form powerful human-machine partnerships that push the boundaries of our knowledge, enrich our lives, and drive cybersecurity in a way that seems greater than the sum of its parts.