CyberTalk

BY CHECK POINT

SUPERCHARGING CYBER SECURITY
10 ESSENTIAL STEPS FOR AI INTEGRATION

Artificial intelligence (AI) promises to serve as a powerful cyber security force-multiplier. It can quickly parse through massive data sets, detect nearly indecipherable patterns, and dynamically respond at machine speeds.

In a world of endless digital hacks, AI is an essential ally. According to reports, 35% of CISOs report that they are already using AI for cyber defense. Think malware analysis, risk scoring and workflow automation.[1]

However, integrating AI into cyber security operations is not so easy. It requires strategic planning and careful execution. This 10-step checklist can serve as a brief AI roadmap for your organization; driving the effective and responsible use of AI in cyber security.

To future-proof your systems using AI, start here:

1. **Define objectives.** Clearly outline the specific cyber security objectives and goals that AI is expected to champion. These may include threat detection, vulnerability management or incident response.
2. **Assess data readiness.** If relevant, ensure that you have access to high-quality, diverse and representative data sets for training AI models and implement measures designed to protect sensitive data.
3. **Establish governance frameworks.** Develop policies, guidelines and oversight mechanisms to ensure the ethical, transparent and accountable use of AI in cyber security.
4. **Build cross-functional teams.** Assemble teams comprising cyber security experts, data scientists, AI engineers and domain experts to facilitate effective collaboration and knowledge sharing.
5. **Evaluate AI-based vendor solutions.** Conduct thorough assessments of their-party AI vendor solutions, their capabilities and security. Also, look at compliance with industry standards, ensuring that solutions align with organizational requirements.
6. **Implement robust testing and validation.** Rigorously test and validate AI models to ensure their accuracy, reliability and resilience against both adversarial attacks and data drifts.
7. **Integrate with the infrastructure.** Plan for a seamless integration of AI elements with existing cyber security tools, processes and workflows. This will help minimize disruptions while maximizing the AI's effectiveness.
8. **Develop AI incident response plans.** Establish comprehensive IR plans that account for potential adversarial attacks, AI system failures or other unintended consequences. Outline clear procedures for mitigation and recovery.
9. **Address interpretability and explainability.** Develop strategies to make AI models more interpretable and explainable. This will facilitate a higher degree of trust and understanding among cyber security staff and stakeholders.
10. **Continuous monitoring and adaptation.** Establish processes for monitoring the performance of AI systems and adapting them to evolving cyber threats and changing environments.

---

[1]The World Economic Forum, Cyber Security is on the frontline of our AI future. https://www.weforum.org/agenda/2024/01/cybersecurity-ai-front-line-artificial-intelligence/#:~:text=In%20the%20same%20CISO%20survey,digital%20systems%20secure%20and%20reliable.

Other items to note:

To ensure the effective use of your AI-based tools, establish clear benchmarks through which to assess performance, efficacy and ROI. Potential KPIs include:

- Time to detect/respond
- False positive rates
- Attack surface reduction
- Projected cost savings (from incidents prevented)

...

In optimizing your team's use of AI, consider providing or enrolling your staff in knowledge enrichment opportunities; workshops, company-developed tutorials, mini-courses or actual courses.

This will help ensure that your organization doesn't find itself in a constant cycle of poaching talent – rather, your business will develop its own talent, build competencies, and limit staff turnover.

...

Lastly, let's cover insurance. AI systems are becoming core to security operations. Do you know about whether or not your insurance policies cover AI-related incidents, like model corruption? Your organization may need to explore insurance updates.

...

Did you find this informative? For more of the latest insights pertaining to AI and cyber security, please see our recent whitepaper or visit CyberTalk.org.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com