ATARC FORTINET FEDERAL

Beyond the Firewall: AI's Evolution in Cyber Defense

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Fortinet Federal, May 2024

During a recent roundtable, Federal experts discussed how agencies can begin integrating AI into cyber defense strategies. While there is immense need for AI in certain functions of cybersecurity, panelists highlight use cases where AI should not be a solution. Panelists also discussed the many challenges they foresee with the integration of AI into existing cyber defense systems.

Current Considerations

> **"What's the Pearl Harbor moment that's going to make everybody realize that cyber security is extremely important? That it's the number one priority in the nation?"**

The promise of AI's potential is well known and exciting for many end users. IT leaders at the roundtable are working to meet these high expectations while maintaining and enhancing cyber defenses. The two priorities often conflict, creating challenges with no apparent straightforward solution.

Roundtable participants remarked on the 'shiny object syndrome' plaguing the workforce, while noting that AI may not always be an appropriate solution to a problem. Several panelists shared use cases where a problem is better solved with updated operational workflows or robotic process automations than an AI program or system.

Integrating AI into cybersecurity strategies requires agencies to consider numerous factors including data accessibility, data protection, ATO frameworks, extending security perimeters into the cloud, and business needs. Several roundtable participants are concerned with the risks of embedded AI functions in new services. The challenge lies in verifying data sources, data access, and data storage of vendor products.

Because the risk to sensitive or classified data is so high, agencies typically fall into two categories: those who prohibit generative AI use and those who build their own large language models. While the latter allows for testing and validation of AI capabilities, the cost and complexity of building and maintaining in-house AI solutions is often too high.

Federal IT leaders are currently analyzing hundreds of AI use cases to understand where AI could be most effective. However, in approximately 90% of use cases, AI is not the most effective nor appropriate solution; rather automation workflows, data collection forms with branching logic, or a rudimentary chat bots are better applied solutions. This underscores a growing disconnect in awareness of the various technology solutions available to the end user, and reinforces the need for workforce training.

AI in Cybersecurity

> **“AI will give us the ability to make faster decisions dynamically based on context. And that’s exactly what we need.”**

Bringing Value to the Mission

Roundtable participants are encountering the same ‘shiny object’ challenges with AI in cybersecurity as well. Vendors are introducing assistive AI solutions designed to identify threats faster, when in most cases a solution already exists within an existing technology stack.

However, there are several areas where AI should be used in zero trust cybersecurity, particularly in the trust engine and policy enforcement points. Agencies need to move at the speed of the machine to keep pace with attackers.

Panelists also envision AI helping to manage Controlled Unclassified Information (CUI) in contextual situations. For instance, AI could identify CUI in a draft email based on the context and flag the user to encrypt the email before sending. Using AI in this manner has the potential to prevent breaches and better protect against user error.

Compared to rigid firewalls, the future of AI-powered cybersecurity can best be described as dynamic and contextual. AI will empower agencies to make contextual decisions at machine speed based on a much broader set of information. For example, an agency may choose to allow access to a user in one situation, but not another. Although agencies have this ability now, the difference is that these decision points will not be pre-programmed; rather, the AI will make real-time access decisions based on available data.

Data Integrity

> **There’s no humanly way to analyze all the data we're collecting.”**

Panelists note the potential for AI to enhance Security Operation Centers (SOCs) by analyzing data, identifying patterns, and flagging anomalies. However, before agencies tap into these capabilities they must normalize data, identify data sources, and implement proper security controls.

Roundtable participants also highlighted the challenges of trusting and verifying how data is used, stored, and protected in AI systems. Currently, there are few mechanisms to verify data sources and data use of AI-enabled services. Agencies must place considerable trust in the vendor to appropriately separate certain data from public domains.

Another concern is data poisoning, which is the slow and malicious manipulation of data fed to AI models to intentionally alter outputs. Panelists considered the challenges associated with data poisoning and hallucinations, while underscoring the critical role of humans to verify outputs.

Challenges with Integrating AI in Cybersecurity

- **Trust in AI Systems**- Trust in AI systems is a key challenge for agencies. Not only do agencies need to trust an AI model, but also the underlying hardware, software, and data sources. Panelists are looking to evidence-based assurances (EBAs) to evaluate specific hardware.

- **Interoperability** - Ensuring AI systems can integrate through systems architecture will be a significant challenge for agencies. In the current zero trust environment, the success of solutions depends on their ability to interoperate with other zero trust pillars and security layers.

- Panelists foresee a type of AI reference monitor to make decisions across an entire security system; however, this is only possible with full interoperability with all systems. Currently, no solution exists, but panelists see potential as the market matures.

- **API Security** - Panelists are also concerned with API security as agencies increasingly rely on cloud service providers and interconnected applications. Agencies must maintain a comprehensive inventory of APIs and implement security controls now to control risk.

- **Verifying Code** - Similar to mitigating the risks associated with open source code, agencies will also need methods to verify AI-generated code.

- **Ethical Considerations** - Government agencies collect public data, which must be stored, used, and managed ethically in order to maintain public trust.

- **Centralized AI Management** - One panelist suggests centralizing AI tools and models to help prevent fragmentation and system silos.

- **Shifting Mindsets** - Panelists anticipate challenges with changing the way the workforce thinks about problems. AI is an inherently different type of technology solution that requires people to think differently about a problem to be applied successfully.

FedRAMP Considerations

Applying FedRAMP requirements to AI systems will depend on the agency's mission, security posture, data inputs outside of security boundaries, and specific use cases. In some instances, agencies may need to develop custom frameworks exceeding FedRAMP criteria to address unique risks associated with AI. Panelists also highlighted the potential for AI to streamline the ATO process itself.

Final Thoughts

The prevailing sentiment among roundtable participants is that AI's value is its ability to process and analyze vast amounts of data to provide contextual cybersecurity solutions. However, the successful integration of AI into cybersecurity requires a holistic approach and careful evaluation. It's critical that agencies understand how AI interacts with other systems, processes, and data sources to ensure a comprehensive and cohesive approach to cybersecurity.

Learn more about Fortinet Federal here:
https://www.fortinetfederal.com