FORTIFY EXPERTS

CISO FORUM: OWASP LLM and Enabling AI Securely Executive Summary:

Please note that individual names have been omitted, and the summary focuses on the collective discussion and key points.

Meeting Context:

The topic of discussion was AI in cybersecurity, with a focus on gathering insights from CISOs about their experiences with evaluating AI Risks and Securing AI.

Meeting Goals:

1. Identify security threats related to generative AI.
2. Discuss opportunities linked to AI in security.
3. Explore strategies for addressing AI-related security challenges.
4. Define a secure path for AI integration into organizations.

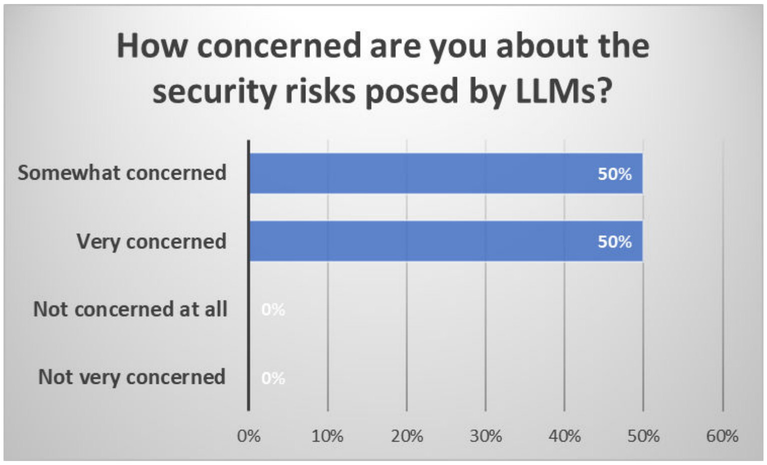
AI Defined:

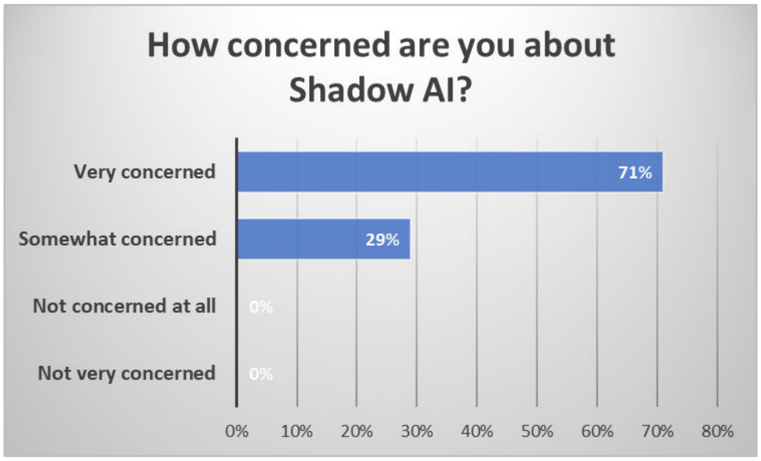
- Three types of AI
  1. Things that move (Robotics, Self-Driving Vehicles, etc.)
  2. Things that plan (Automated Schedulers, Navigation, Resource planning, etc.)
  3. Generative AI / Contextual / Language-based (LLMs - Chatbots, Image, Video, Music, etc.)

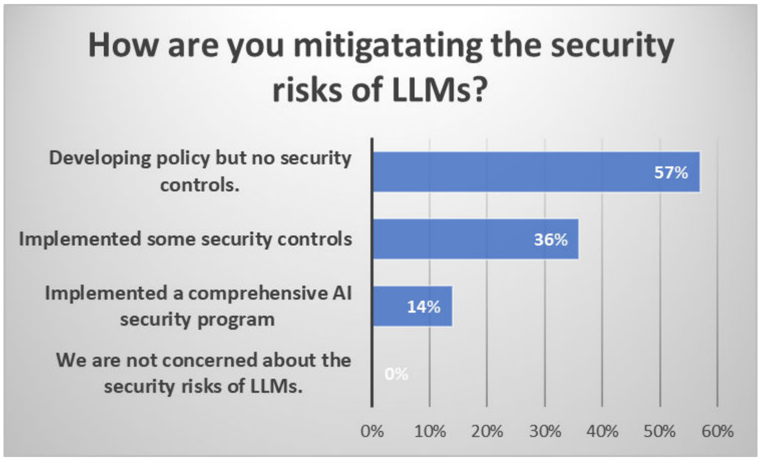
- Our discussion was focused on #3 Generative AI because that has been where the radical change has happened in 2023.

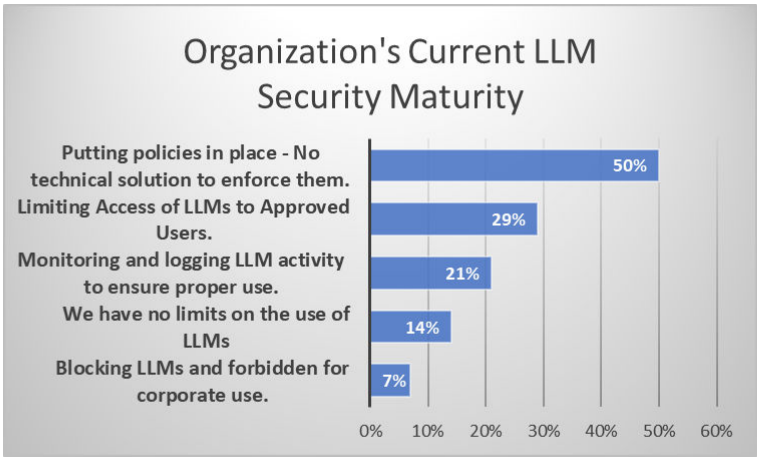
- Three ways it is Generative AI is implemented.
  1. Self-Developed Generative AI solutions - Requires the adoption of a strong SSDLC.
  2. Generative AI integration into an existing software product - Requires evaluation of data integrity and privacy.
  3. Public LLM’s - Requires a bubble of protection around it.

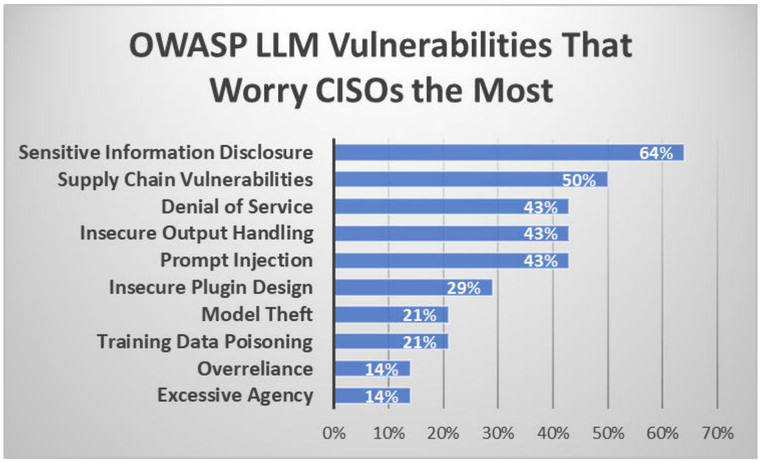
Poll Questions:

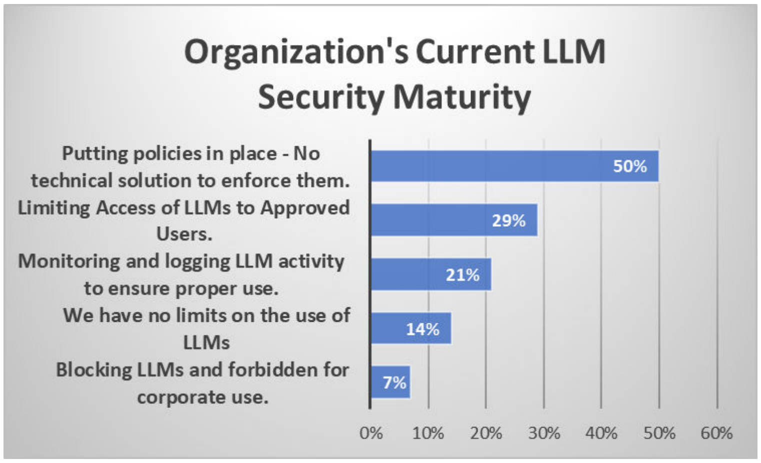












Generative AI Security Concerns:

1. Participants shared concerns and experiences with AI across various industries, including healthcare, insurance, and education.
2. Security concerns are raised, especially regarding the use of public AI models (i.e. LLMs - chatbots).
3. Concerns were expressed on data sharing, confidentiality, regulation, and AI's impact on decision-making.
4. AI is now embedded and integrated into most major software (i.e. Salesforce, Microsoft, Canva, etc.) so you can't shut it out completely.
5. Microsoft's Co-Pilot is a new integrated AI assistant tool integrated within Microsoft applications and will be released in Nov 2023. This will give AI capabilities to all Microsoft users directly. It does have some limitations and it is not claiming to be a security product.
6. Using AI for health diagnostics can be powerful, but accidentally exposing patient personal data is of very high concern in the medical field.
7. There is a big need for organizations to develop AI governance, policies, controls, and security strategies.
8. The challenge in distinguishing AI-generated content from real information will continue to grow.
9. Will the cost of implementing AI outweigh the ROI and the risk?
10. Participants express excitement about AI's potential for innovation but also concern about its impact on jobs.

Potential Solutions:

1. The current state of AI adoption and risk needs to be assessed in each organization for each use of AI.
2. Instead of shutting it out, which could lead to a leader being fired, AI should be embraced and enabled with proper security measures and guardrails.
3. To allow for AI adoption quickly, create and implement governance frameworks, policies, and procedures for proper use now, but then develop technical solutions to monitor and control.
4. Explore and adopt AI risk management strategies and frameworks. Implement security controls and risk management strategies for all AI initiatives.
5. Collaborate with legal and risk management teams to address AI-related challenges and ensure compliance.

6. Investigate state privacy laws that impact AI initiatives. As of 9/2023, 13 states have Privacy / AI laws, 11 more have proposed laws: https://www.bclplaw.com/en-US/events-insights-news/2023-state-by-state-artificial-intelligence-legislation-snapshot.html
7. AI incorporation must be addressed at a strategic enterprise transformation level to evaluate the ROI against the risks.
8. Organizations should also adopt a formal change management approach to address AI use and the resulting data.
9. Employees need to be extensively trained on the appropriate and inappropriate use of Generative AI and ways to get the most out of it without putting the company at risk.

Resources Mentioned:

- OWASP LLM
- NIST AI framework
- International Association of Privacy Professionals (IAPP) for privacy resources
- 2023 State-by-State Artificial Intelligence Legislation Snapshot
- OWASP AI Security and Privacy Guide
- Generative AI: Proposed Shared Responsibility Model - Cloud Security Alliance (CSA)

AI in Different Industries:

- Continue monitoring AI developments and security challenges in respective industries.
- Participants discuss whether guiding principles and policies for AI should be industry-specific.
- Healthcare and financial industries are highlighted as sectors where AI adoption and related challenges are significant.

Ethical AI and Standards:

- There is a growing need for ethical AI guidelines and standards to ensure responsible AI usage.
- Ethical AI guidelines are essential to address the ethical considerations of AI implementation.
- Standard topics include validity, reliability, safety, fairness, bias management, security transparency, and accountability.
- The challenge lies in adapting these standards to specific contexts.

Private Generative AI Solutions:

- Private Chatbot AI services were discussed as a potential solution to enhance control and security in AI usage.
- Consider implementing private GPT solutions to enhance control over AI models and data security.

Companion AI and Risks:

- The discussion touches on the rise of companion AI and the potential risks, such as manipulating individuals emotionally.
- Concerns are raised about creating AI characters that can deceive and form personal relationships with users.

Regulatory Oversight:

- The necessity of regulatory bodies in the tech industry, especially for AI, is mentioned.
- Self-regulation by major tech companies is deemed insufficient, and the need for external regulation is emphasized.

The discussion covered various aspects of AI in cybersecurity, including policy development, technical solutions, governance, and security considerations for AI models. Participants also emphasized the importance of understanding AI's capabilities, limitations, and the need for clear communication about AI-generated content.

Additionally, resources for AI and cybersecurity were mentioned, emphasizing the importance of staying informed in this rapidly changing field.

Overall, the meeting highlighted the evolving challenges and opportunities presented by AI in the field of cybersecurity.

Join us for **next month’s October’s CISO Forum on October 19th at 1:00 pm CST**.

Register here:
https://fortifyexperts.com/ciso-round-table-forums/