Resources related to the AI-Enabled Vulnerability Discovery, Exploitation, and Remediation Series (May – June 2026)

Resources related to the AI-Enabled Vulnerability Discovery, Exploitation, and Remediation Roundtable Series organized by the Office of Security Management within the Maryland Department of Information Technology and hosted by the Maryland Cybersecurity Council. The series included presentations by the Cloud Security Alliance (CSA), the Microsoft Threat Intelligence Center, OpenAI, and Google/Mandiant.

- CSA roundtable presentation on AI (by permission)
- Cloud Security Alliance: Building a Mythos-ready Security Program
- Microsoft article: Defense at AI speed: Microsoft's new multi-model agentic security system tops leading industry benchmark
- OpenAI: Trusted Cyber Access Registration/ (Note: Maryland State Agencies in the executive branch should contact the Office of Security Management through their assigned information security officer.
- Google/Mandiant: Secure AI Framework (SAIF) and Google Cloud A
- Anthropic: Monthly Informational Briefing (registration form)
- CISA BOD 26-04: Prioritizing Security Updates Based on Risk