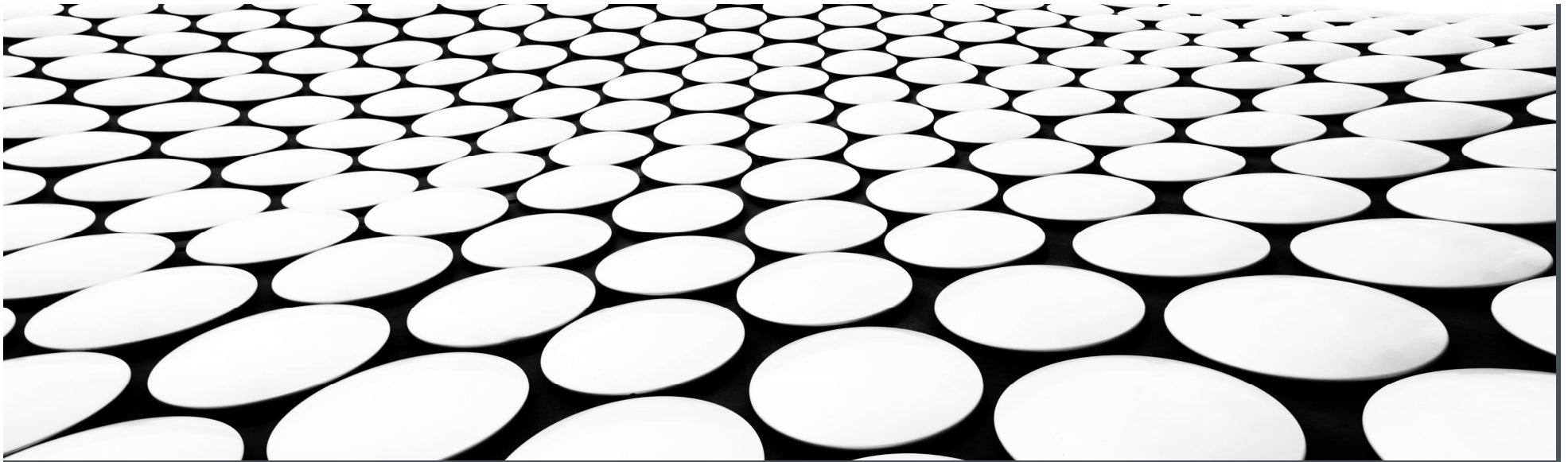




APPENDIX 3 - SOLARWINDS CYBERATTACK CASE STUDY





**APPENDIX 3 - AI
SECURITY THREAT
MANAGEMENT:
SOLARWINDS
CYBERATTACK CASE
STUDY**



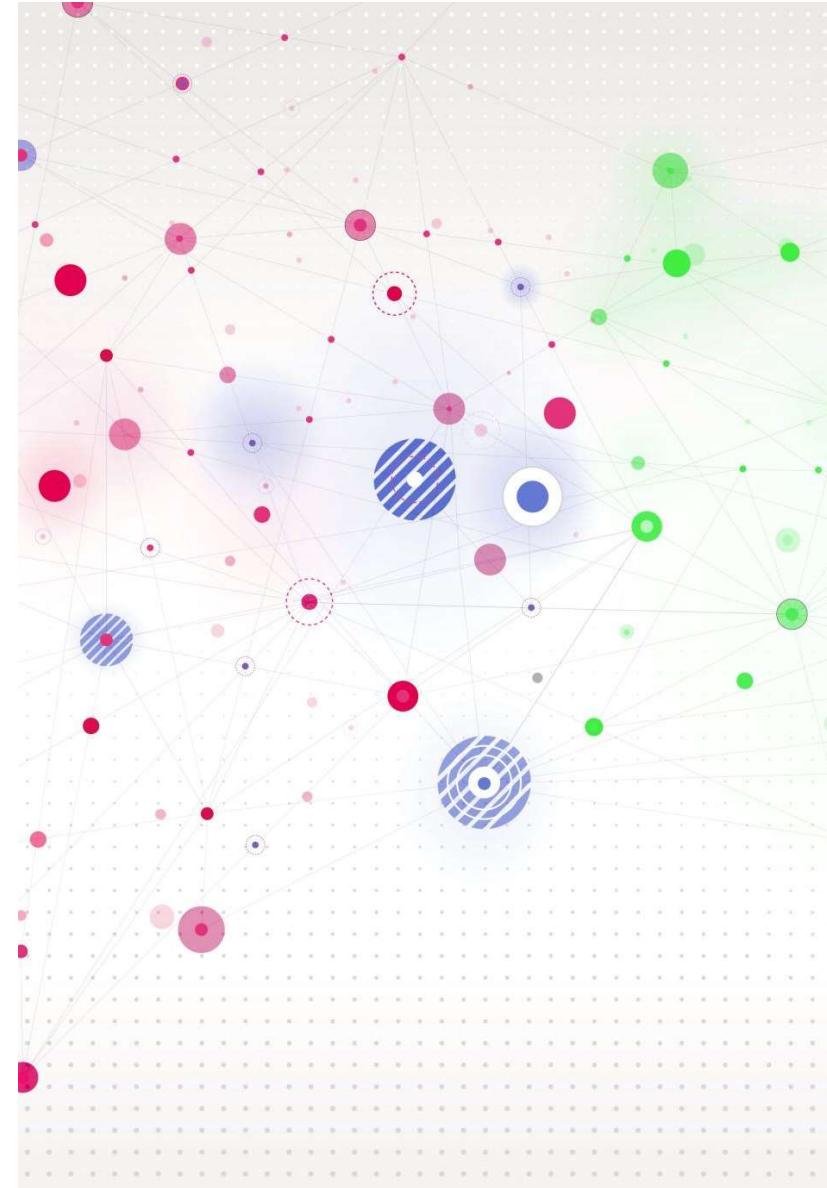
HOMEWORK: STUDY SOLARWINDS EFFECT ON AI SYSTEMS

Homework Description provided as a word document to complete.

<https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic>

AI, LLMS AND GENERATIVE AI APPLICATIONS

- Stages in the life cycle (including experimentation, training, or deployment), the data they process, and the personnel involved (both full time employees, government personnel, and contractors).
- Most AI applications and ML systems are highly dispersed and are typically reliant on very common open-source assets integral to the AI/ML lifecycle. This situation sets the stage for a major security vulnerability, akin to the ['SolarWinds incident'](#).



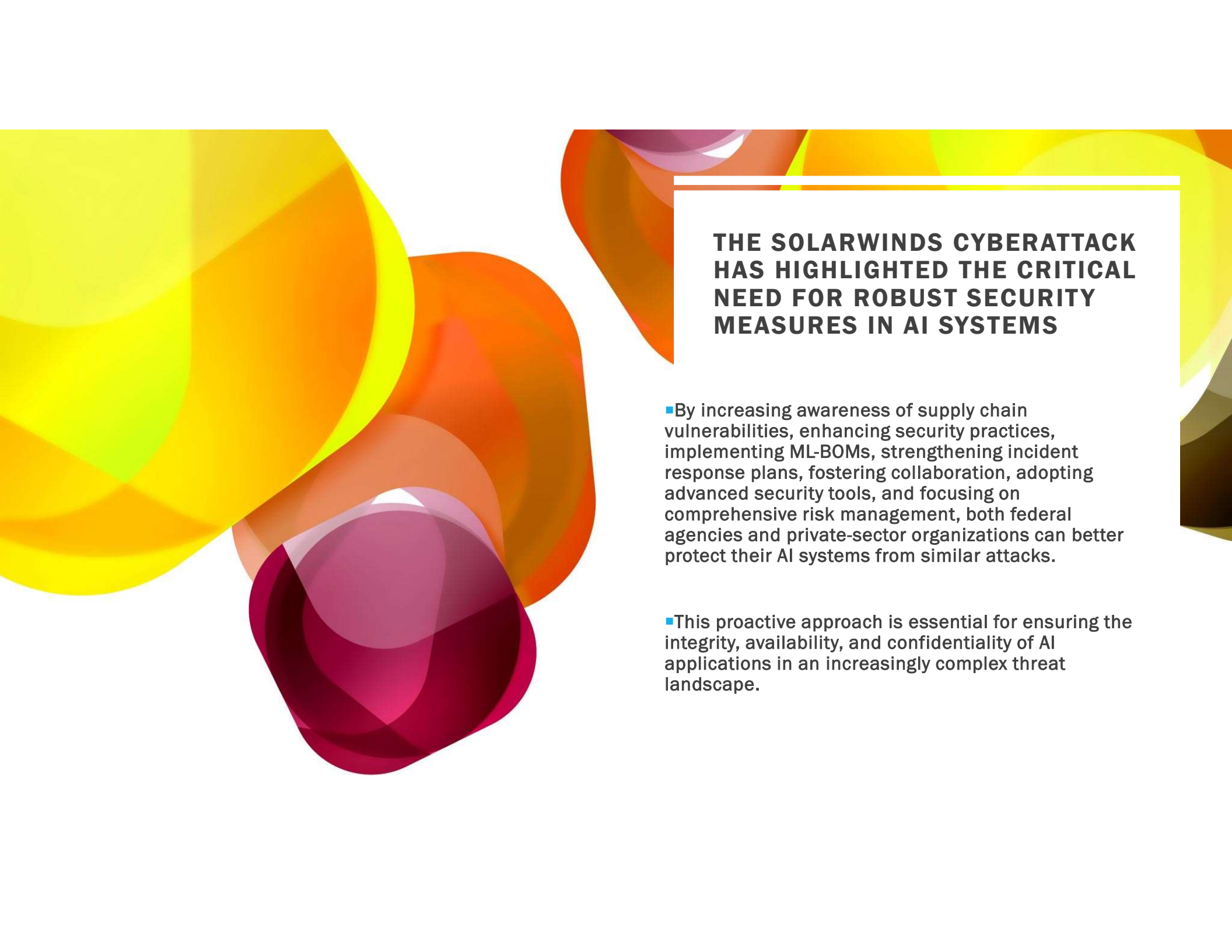


SOLARWINDS CYBERATTACK DEMANDS SIGNIFICANT FEDERAL AND PRIVATE- SECTOR RESPONSE

How the SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response and Its Impact on AI Security

Overview of the SolarWinds Cyberattack:

The SolarWinds cyberattack was a highly sophisticated and widespread breach that compromised numerous organizations, including federal agencies and private-sector companies. Hackers infiltrated the software supply chain, embedding malicious code in SolarWinds' Orion software updates, which were then distributed to thousands of customers. This attack highlighted critical vulnerabilities in software supply chains and the need for robust cybersecurity measures.

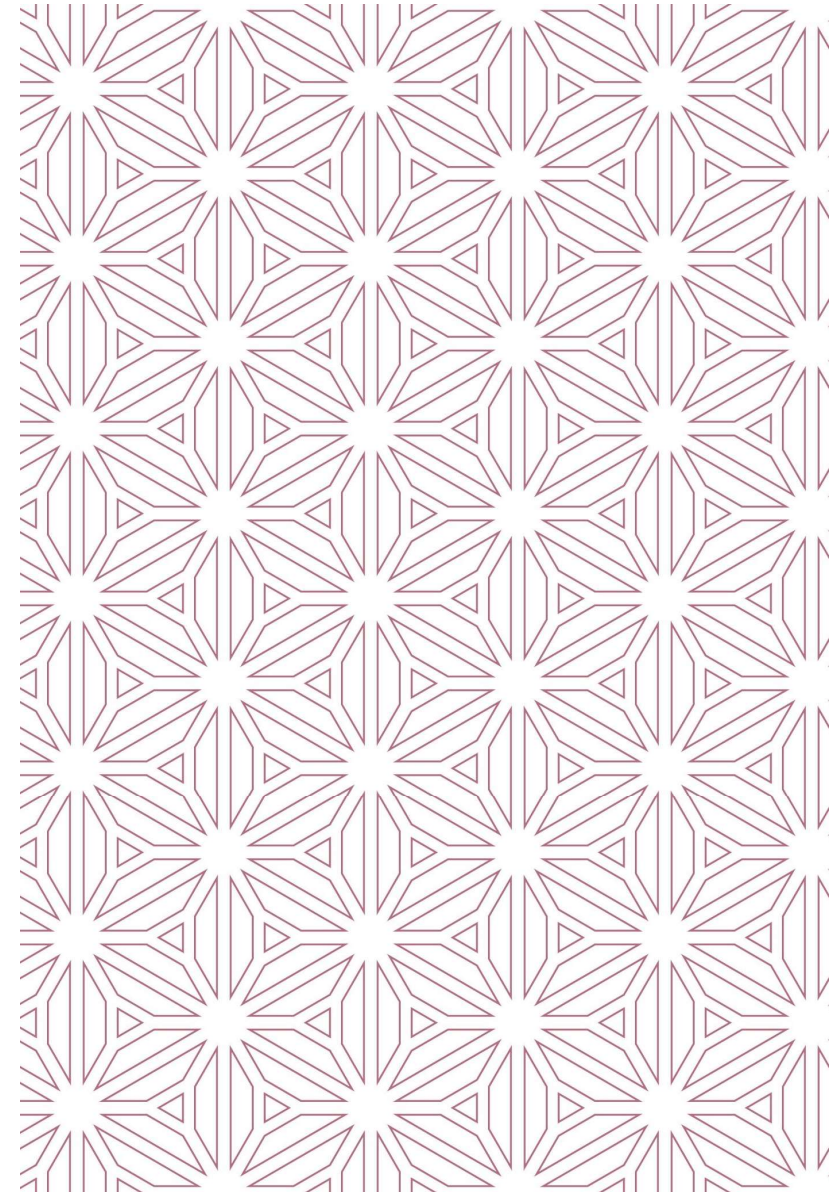


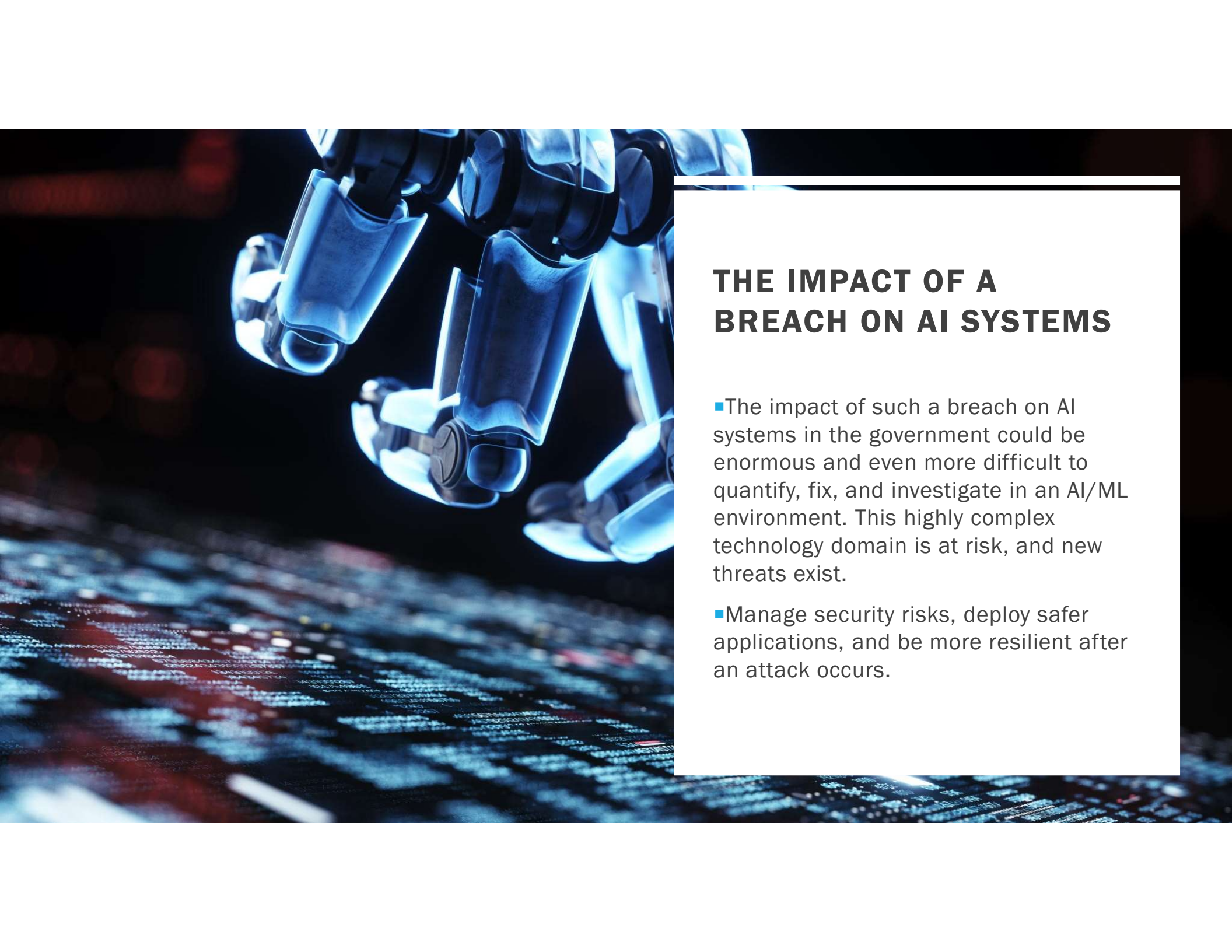
THE SOLARWINDS CYBERATTACK HAS HIGHLIGHTED THE CRITICAL NEED FOR ROBUST SECURITY MEASURES IN AI SYSTEMS

- By increasing awareness of supply chain vulnerabilities, enhancing security practices, implementing ML-BOMs, strengthening incident response plans, fostering collaboration, adopting advanced security tools, and focusing on comprehensive risk management, both federal agencies and private-sector organizations can better protect their AI systems from similar attacks.
- This proactive approach is essential for ensuring the integrity, availability, and confidentiality of AI applications in an increasingly complex threat landscape.

GOVERNMENT AND INDUSTRY COLLABORATION

- **Public-Private Partnerships:** The federal response to the SolarWinds attack has emphasized the need for collaboration between government and private sectors to enhance cybersecurity. This collaborative approach is essential for sharing threat intelligence and best practices related to AI security.
- **Regulatory and Policy Frameworks:** Governments are likely to introduce new regulations and policies to improve AI security. Organizations must stay compliant with these evolving standards to mitigate legal and operational risks.
- **Adoption of Advanced Security Tools:**
 - **Security Solutions for AI:** The development and deployment of specialized security tools tailored for AI systems will become more prevalent. Examples include tools for securing AI/ML pipelines, detecting adversarial attacks, and ensuring data integrity.
 - **Open-Source Contributions:** Encouraging contributions to open-source security tools can help improve the overall security posture of AI systems. These tools can provide practical solutions for managing AI-related risks.
- **Focus on Comprehensive Risk Management:**
 - **Holistic Approach:** Organizations will adopt a holistic approach to AI security, integrating it into their broader risk management strategies. This includes addressing technical, operational, and reputational risks associated with AI systems.
 - **Continuous Improvement:** Ongoing evaluation and improvement of AI security practices will be necessary to keep pace with emerging threats and technological advancements.





THE IMPACT OF A BREACH ON AI SYSTEMS

- The impact of such a breach on AI systems in the government could be enormous and even more difficult to quantify, fix, and investigate in an AI/ML environment. This highly complex technology domain is at risk, and new threats exist.
- Manage security risks, deploy safer applications, and be more resilient after an attack occurs.

IMPACT ON AI SECURITY

■ Increased Awareness of Supply Chain Vulnerabilities:

- AI Model Supply Chains: Just as the SolarWinds attack exploited vulnerabilities in the software supply chain, AI models often rely on numerous open-source and third-party components. This makes them susceptible to similar supply chain attacks.
- Dependency on External Libraries: AI systems frequently use external libraries and frameworks, which can introduce vulnerabilities if not properly vetted and secured.

■ Enhanced Focus on Security Measures:

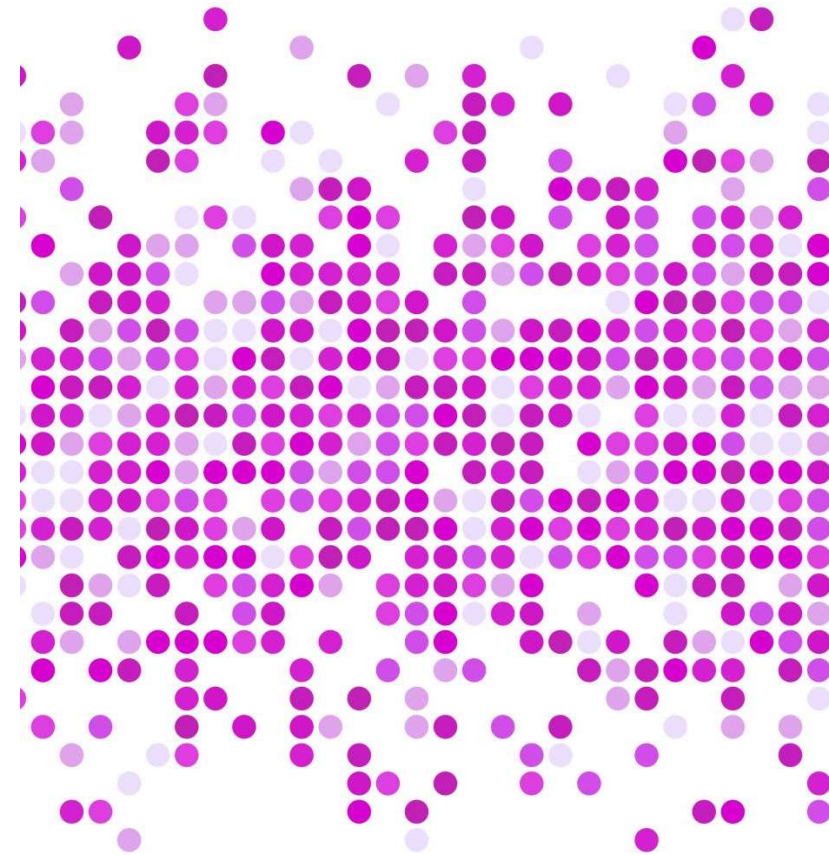
- Comprehensive Security Audits: In the wake of the SolarWinds attack, both federal and private sectors are likely to conduct more thorough security audits of their AI systems. This includes examining all components and dependencies within AI models.
- Rigorous Vendor Assessments: Organizations will increase scrutiny of vendors providing AI-related software and services to ensure they adhere to stringent security practices.

■ Implementation of ML-BOM (Machine Learning Bill of Materials):

- Visibility and Control: The attack has underscored the importance of having a detailed inventory of all components within AI systems. An ML-BOM can provide visibility and control over the entire AI supply chain, helping to identify and mitigate risks.
- Standardization of Practices: Encouraging the adoption of ML-BOM practices across the industry can lead to standardization, making it easier to detect and respond to vulnerabilities.

■ Strengthened Incident Response and Recovery Plans:

- Proactive Threat Detection: Organizations will need to enhance their threat detection capabilities to identify potential breaches in AI systems early. This includes monitoring for unusual activity and conducting regular security assessments.
- Resilience and Recovery: Developing robust incident response and recovery plans specific to AI environments is crucial. These plans should include steps for isolating affected systems, mitigating damage, and restoring normal operations swiftly.





MAJOR AI THREAT ISSUES

- You can't **SEE** the threats. AI/ML systems are fragmented, complex and dynamic. This creates hidden security risks that escape your current application security governance and control policies.
- You don't **KNOW** where the threats lie. The rapidly evolving adoption of AI/ML adds an entirely new challenge for businesses to ensure their applications are secure and compliant. Safeguarding against a potential "SolarWinds" moment in ML is business critical. Manufacturers and consumers of AI need to know where threats lie in their ML system so they can pinpoint and remediate risk.
- AI threats are difficult to **MANAGE**. AI/ML security vulnerabilities are difficult to remediate. When operational, technological, and/or reputation security risks are identified that could harm customers, employees, and partners, the business must quickly respond and mitigate them to reduce incident response times.

CRITICAL NEEDS FOR AI SECURITY

Organizations must be able to see, know, and manage AI threats effectively to ensure the security and integrity of their AI/ML systems. Here's a deeper look into each aspect:

■ See:

- **Complexity and Fragmentation:** AI/ML systems are inherently complex and often fragmented across various departments and functions within an organization. This complexity can obscure hidden security risks.
- **Invisible Threats:** The dynamic nature of AI models, which continuously evolve and adapt, can mask potential vulnerabilities that traditional security measures may not detect.
- **Current Security Gaps:** Existing application security governance and control policies might not adequately cover AI/ML systems, leaving blind spots where security threats can thrive undetected.

■ Know:

- **Threat Identification:** To secure AI/ML systems, it is critical to identify and understand where potential threats lie. This involves thorough risk assessments and continuous monitoring of AI models and their data inputs.
- **Rapid Evolution:** The rapid adoption of AI/ML technologies introduces new security challenges. Organizations must stay ahead of evolving threats to ensure their AI applications remain secure and compliant with regulatory standards.
- **SolarWinds Scenario:** Just as the SolarWinds incident highlighted vulnerabilities in software supply chains, AI/ML systems are susceptible to similar breaches. Knowing the specific points of vulnerability within AI systems is essential to preventing such scenarios.

■ Manage:

- **Effective Mitigation:** Once threats are identified, organizations must have robust mitigation strategies to address these vulnerabilities promptly. This includes deploying patches, updates, and other security measures to protect AI systems.
- **Incident Response:** Developing a comprehensive incident response plan tailored to AI/ML environments is crucial. This plan should outline steps to take when a security breach occurs, aiming to minimize damage and restore normal operations swiftly.
- **Stakeholder Protection:** AI security is not just about technology; it also involves safeguarding the interests of various stakeholders, including customers, employees, and partners. Effective management of AI security risks ensures that these groups are not adversely affected by

ML BILL OF MATERIALS (ML-BOM)

- Implementation of an ML-BOM for visibility and auditability of AI systems.
- Recommended adopting MLSecOps practices to identify, scan, and remediate AI/ML system risks.



GETTING AHEAD OF ML/AI ISSUES IN SEC- OPS

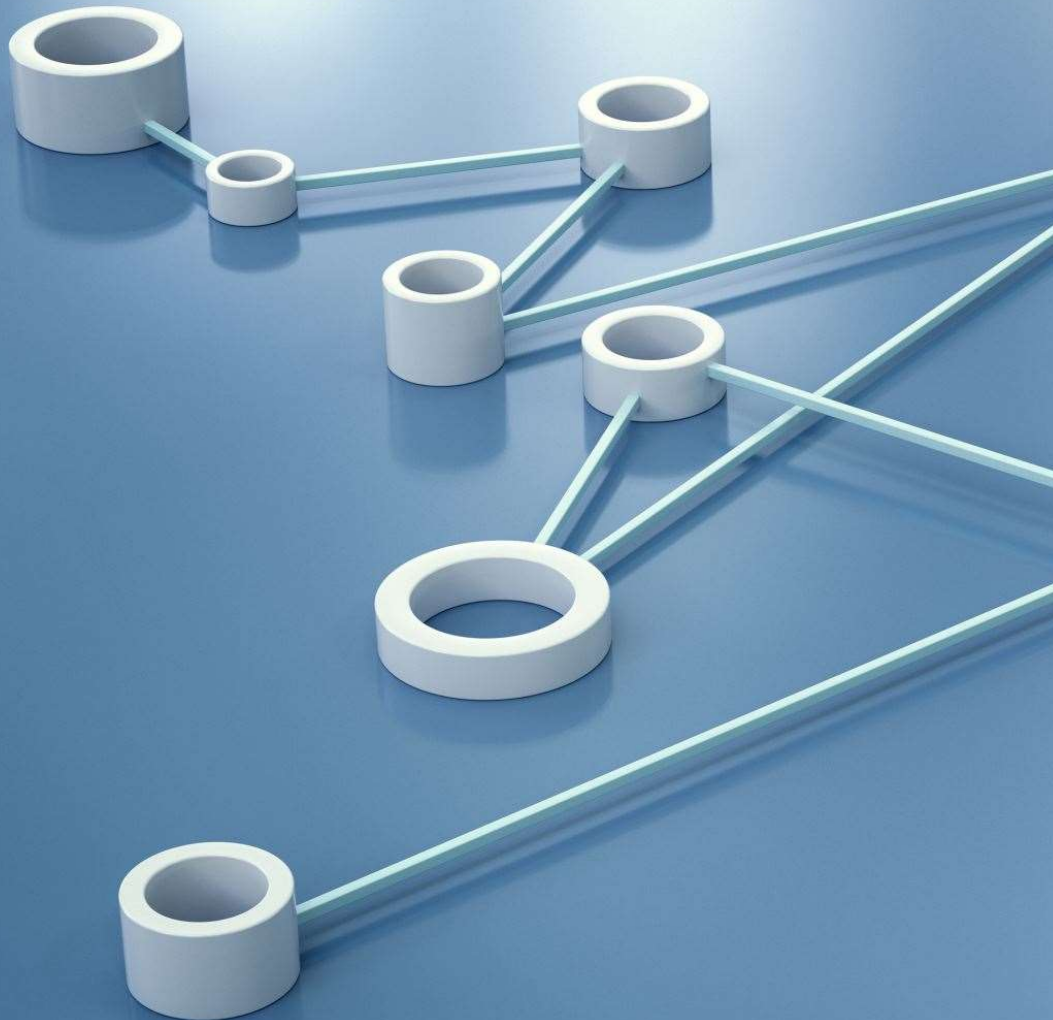
- Sec-Ops shops can get ahead by:
 - Proactive Engagement: Actively participating in AI/ML project discussions and development phases.
 - Education and Advocacy: Promoting the importance of MLSecOps and demonstrating how it can enhance innovation and development without being a hindrance.
 - Integration of MLSecOps Practices: Implementing MLSecOps frameworks and tools to monitor and secure AI/ML systems continuously.

ADVERSARIAL TESTING IN CYBER RESPONSE

- Yes, adversarial testing is part of cyber response. It involves simulating attacks on AI systems to identify vulnerabilities and improve their robustness against adversarial threats.
- Red Teaming for AI
 - Red Teaming for AI involves:
 - **Simulating Attacks:** Conducting offensive security tests to identify vulnerabilities in AI systems.
 - **Evaluating Defenses:** Assessing the effectiveness of existing security measures and identifying areas for improvement.

CRITICAL NEEDS

- Organizations must be able to see, know, and manage AI threats effectively:
 - **See:** AI/ML systems' complexity hides security risks.
 - **Know:** Identifying and understanding threats in AI/ML is essential for compliance and security.
 - **Manage:** AI/ML vulnerabilities require effective mitigation strategies to protect stakeholders.



ML BILL OF MATERIALS (ML-BOM)

- **Visibility and Auditability:** Implementing an ML-BOM provides comprehensive visibility into AI/ML systems, detailing all components, data sources, and stages in the lifecycle. This helps in recognizing and addressing security threats effectively.
- **Systematic Risk Management:** An ML-BOM enables organizations to systematically manage risks by pinpointing and remediating vulnerabilities within AI models and tools.
- **Policy Integration:** Coupling the ML-BOM with documented security policies enhances the overall security posture, ensuring compliance with regulatory requirements and improving incident response times.

QUESTION AND ANSWER

