Joint Guidance on Deploying AI Systems Securely

Finished Intelligence Reports	TLP:WHITE	Alert Id: b95e8d97	2024-04-16 11:24:33

On April 15, 2024, multiple cyber agencies released a joint Cybersecurity Information Sheet Deploying AI Systems Securely with an aim to:

- Improve the confidentiality, integrity, and availability of AI systems.
- Ensure there are appropriate mitigations for known vulnerabilities in AI systems.
- Provide methodologies and controls to protect, detect, and respond to malicious activity against AI systems and related data and services.

Members who use AI systems in their operations are advised to get familiar with these guidelines. More information is available in the attached report.

Release Date: Apr 16, 2024 (UTC)

Tags: Guidelines, Artificial Intelligence

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments:

Please email us at toc@h-isac.org