IPS SecMLOps Framework v1.2

Updated March 2023 | www.secmlops.ai

SUMMARY

Common uses of Artificial Intelligence / Machine Learning (AI/ML) applications are focused on detection of cybersecurity vulnerabilities against malicious attacks to systems, whereas less focus is centered around the analysis of cybersecurity against the AI/ML application itself and the harm it may cause to our systems if Adversarial AI vulnerabilities go undetected. That brings us to a new beginning with SecMLOps. IPS provides strategic cybersecurity consulting geared to strengthen the cybersecurity posture of our client-base cybersecurity program with defense-in-depth solutions. Our implemented "IPS SecMLOps Framework" gears to bolster secure development and deployment of AI/ML models through a robust supply chain risk management methodology.

WHAT IS SECMLOPS

End-to-End repeatable cybersecurity processes for secure algorithmic software development and secure deployment of AI/ML models to the tactical edge.

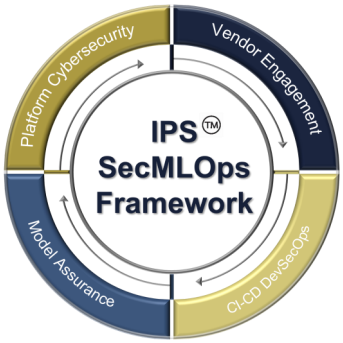
THE NEED

SecMLOps provide a robust supply chain risk management approach for mitigating the threat of Adversarial AI from the conception of algorithmic software development, through testing and evaluation (T&E), to the deployment of AI/ML models in operation.

SECMLOPS VS MLOPS

Differentiation between SecMLOps from MLOps, is SecMLOps is focused on the cybersecurity supply chain risk management of secure algorithmic operations, whereas MLOps is heavily concentrated on the DevOps framework for end-to-end ML application development.

Platform Cybersecurity: Focuses on continuous monitoring and ongoing assessment by applying vulnerability mitigation and remediation strategic methodologies on the AI Harness (Cloud/Hardware), instituting active threat modeling analysis, and executing secure configuration management implementation.



Vendor Engagement: Focuses on validating the vendor's secure environment against the NIST 800-171 compliance guidance, secure software development practices, software patch management methodology, and due care utilization of open-source software.

Model Assurance: Focuses on validating the vendor's AI/ML Program against the NIST AI Lifecycle Risk Management Framework, mitigation and remediation of Adversarial AI, protection of developed models in training, transit, and operations, and operational T&E methodology.

CI/CD DevSecOps: Focuses on validating the vendor's CI/CD pipeline against the OWASP Top 10 CI/CD Security Risks, measuring the effectiveness of the vendor's established static code and dynamic code vulnerability remediation methodology, verifying the software supply chain risk management approach, and code integrity implementation strategy throughout the CI/CD pipeline.

IPS SecMLOps Framework v1.2

Updated 29 March 2023 | www.secmlops.ai

SECMLOPS IMPLEMENTATION

The first and foremost importance of SecMLOps implementation is executing an effective stakeholder engagement analysis strategy within your respective AI/ML development and deployment project. Project Management Institute defined stakeholder engagement analysis as a method of systematically gathering and analyzing quantitative and qualitative information to determine whose interests should be taken into account throughout the project. Stakeholders are critical to the complete secure AI/ML development lifecycle from algorithmic software development to deployment of AI/ML models to the tactical edge users. Through an effective executed stakeholder engagement analysis strategy, key stakeholders are involved throughout the four critical domains of SecMLOps, consisting of Vendor Engagement, Continuous Integration/Continuous Delivery (CI/CD) DevSecOps, Model Assurance, and Platform Cybersecurity. Through stakeholder engagement, all parties are on one accord with the secure development and deployment of the AI/ML risk management supply chain process.

Key Benefits of SecMLOps:

⇒ Repeatable and Sustainable cybersecurity processes for AI/ML development and delivery through supply chain risk management.

⇒ Validation of data source and applied cybersecurity protection measures of the AI/ML development pipeline to mitigate the threat of Adversarial AI threats.

⇒ Engaged stakeholders on one accord with the unified goal of cybersecurity throughout the AI/ML lifecycle from development to the tactical edge.

CONTACT INFO

For more information contact:

Dr. Todd Chamberlain Sr., CISSP

secmlops@ips314.com

Adversarial AI Attack

Within the SecMLOps process, due care consideration is focused on where the data for the AI/ML model development and training is received, to include cybersecurity protections while the data is in transit from the data source to the AI/ML development environment. In this case, data should be obtained via a trusted source, then encrypted in transmission to ensure the integrity of the data. This encryption process shall be repeated throughout the integration and T&E processes. Of equal importance is executing vulnerability analysis of the data prior to data transmission, as well as throughout the AI/ML model training process to mitigate the threat of malicious poisoning attacks. The ultimate goal is to mitigate poisoned data from entering the AI/ML development and training supply chain pipeline. **After all, who wants to be responsible for allowing poisoned data in critical systems**?