AI Security Controls

By Victor D. Patterson Sr.

AI Security Strategist | SOC Architect | ISACA 2025 Speaker

“Critical infrastructure organizations face increasingly advanced AI-driven threats—from deepfake fraud and model poisoning to supply chain deception and adversarial identity spoofing. I developed an AI-powered security architecture prototype to enhance resilience, automate compliance, and counter AI-adversarial cyber risks. This framework is designed to secure high-risk, high-compliance environments where traditional controls are no longer enough.”

MITRE ATT&CK Tactic	***AI Adversarial Threat***	***Security Control Implementation***	***Compliance Framework Alignment***
🔹 ***Masquerading (T1036)***	***Deepfake Identity Spoofing (AI-generated faces, voices)***	***Zero Trust AI Identity Protection (Biometric validation, Adversarial ML detection)***	***ISO 42001 AI Risk Governance, NIST AI 600-1***
🔥 ***Phishing (T1566)***	***AI-enhanced deepfake phishing campaigns***	***SOC-driven AI deception detection, OSINT-based fraud analysis***	***ISO 27001, SOC 2, NIST 800-53***
⚡ ***Adversarial ML Attacks***	***Model poisoning, data manipulation***	***AI trust modeling (NIST AI 600-1), adversarial training pipelines***	***ISO 42001, AI RMF, CMMC***
🎭 ***Social Engineering (T1584.006)***	***AI-Generated voice scams, synthetic identity fraud***	***AI deception-based red teaming, deepfake-resistant IAM***	***NIST CSF 2.0, FS-ISAC, CIS Controls***

📌 ***Controls & Countermeasures***

Risk Category	***Business Impact***	***Recommended Security Control***	***Expected Outcome***

Third-Party Risk (Vendor Security)	***Vendor breaches, supply chain compromise***	***AI-driven Vendor Security Review (ISO 27001 & SOC 2)***	***40% faster vendor risk assessments, reduced supply chain vulnerabilities***
AI-Powered Cyber Deception	***Deepfake fraud targeting enterprise leadership and staff***	***Deepfake Detection & AI Adversarial Intelligence (Cerberus Shield)***	***Preemptive detection of AI-powered impersonation threats***
SOC Automation & AI-GRC	***Slow incident response, inefficient compliance reporting***	***DeepSecure AI-SOC (AWS SIEM, MITRE ATT&CK alignment)***	***50% faster threat detection & real-time compliance tracking***
AI Governance & Compliance	***AI regulation violations, lack of AI risk oversight***	***ISO 42001 AI Security Framework Implementation***	***Ensures regulatory compliance & AI governance resilience***

“This framework reflects next-gen cybersecurity thinking—designed to align with enterprise risk, operational resilience, and evolving AI-driven threats. By integrating adversarial intelligence, deception analysis, and compliance automation, this model empowers organizations to stay ahead of advanced synthetic threats.”

📚 *Source References*

- ***MITRE ATT&CK Framework***

- ***NIST AI Risk Management Framework***
- ***ISO/IEC 42001:2023 – AI Management Systems***

- ***NIST Cybersecurity Framework 2.0***
- ***NIST SP 800-53 Rev. 5***
- ***CMMC – Cybersecurity Maturity Model Certification***
- ***CMMCModel_V2_Mapping.xlsx***
- ***CMMC-v.-1.02-Audit-Spreadsheet.xlsx***

- ***CIS Controls v8***
- ***CIS_Controls_Version_8.1_6_24_2024.xlsx***
- ***FS-ISAC Threat Intelligence***

- ***SOC 2 – AICPA***