cATO SCANNER

AI System Compliance Scanner for DoD Programs — v2.0

AIR-GAP COMPATIBLE | ZERO CLOUD DEPENDENCY

// OVERVIEW

The ATO Problem — Solved

The DoD Authorization to Operate process — a manual, document-intensive cycle producing 200-page static PDFs — is incompatible with the tempo of AI development and wartime operations. cATO Scanner v2.0 is a dual-purpose compliance platform: a dedicated AI/LLM compliance scanner for programs with AI systems, AND a full general-purpose IT compliance scanner for any Linux or Windows host — with or without AI.

KEY INSIGHT:
If the target has AI: 60+ AI-specific checks + full NIST 800-171/CMMC baseline. If no AI: complete NIST 800-171 / CMMC 2.0 / STIG-mapped scan with auto-generat

60+	NIST 171	CMMC 2.0	eMASS	XCCDF
AI-SPECIFIC CHECKS	COMPLIANCE BASELINE	LEVEL ALIGNMENT	AUTO UPLOAD	STIG VIEWER OUTPUT

// AI COVERAGE

What cATO Scans — AI Systems

RAG PIPELINE SECURITY
Scans Retrieval-Augmented Generation architectures: vector database access controls, document ingestion integrity, embedding model provenance, retrieval injection prevention, and PII/CUI in vector stores.

AGENT WORKFLOW ANALYSIS
Detects autonomous agent risks: tool call authorization, agent loop bounds, human-in-the-loop checkpoints, code execution sandboxing, inter-agent trust validation, and kill switch reachability.

AUTONOMOUS EVALUATOR SCANNING
Checks LLM-as-judge implementations: evaluator model independence, calibration documentation, human override on rejection, and hallucination-risk feedback loop detection.

LLM CONFIGURATION AUDIT
Validates model deployment: API key exposure, prompt injection surface, insecure execution paths, sensitive logging, error handling, and agent loop risk scoring.

// GENERAL IT COVERAGE

Dual-Use — No AI Required

NIST 800-171 / CMMC 2.0
Full baseline scan competitive with Vulnerator and OpenRMF. Auto-generated POA&M for any system, with or without AI components.

DISA STIG MAPPING
SCAP 1.3-compliant XCCDF XML output importable into STIG Viewer and OpenRMF. Direct eMASS API integration eliminates manual data entry.

WINDOWS / WINRM SUPPORT
Extends scanning to Windows Server AI systems via WinRM. No Linux requirement. Full NIST 800-171 coverage on Windows targets.

FLEET DASHBOARD
Multi-host scanning across an entire unit's systems. Aggregate compliance view across all hosts. Squadron/battalion CISO ready.

// OUTPUT FORMATS

Delivery Options

HTML REPORT	XCCDF / SCAP 1.3	EXCEL / POA&M	PDF EXPORT	eMASS API UPLOAD
Interactive browser-based report with full findings, risk scores, and remediation guidance.	STIG Viewer and OpenRMF compatible. Importable directly into existing RMF workflows.	Auto-generated Plan of Action & Milestones. eMASS-ready format.	Printable commander-ready report for environments without browser access.	Automatic upload of findings to eMASS. Eliminates manual XCCDF data entry for ISSOs.