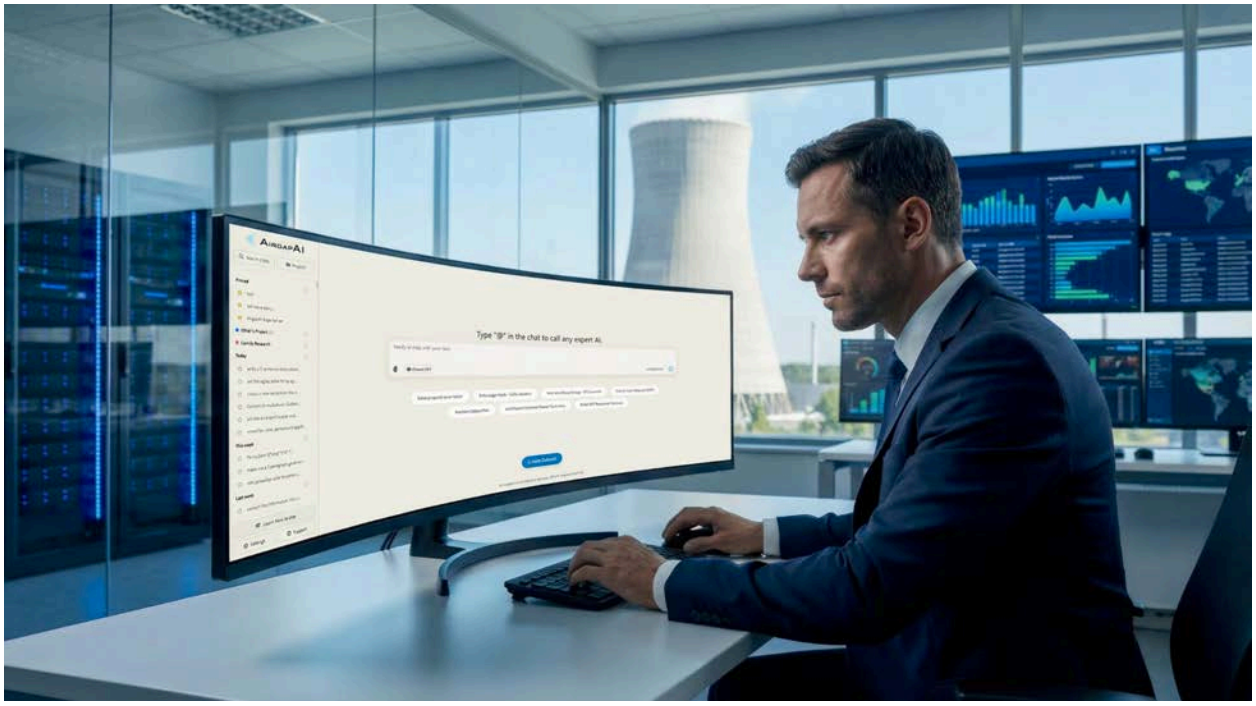
Strengthening Critical Infrastructure Cybersecurity for a Major Nuclear Energy Company through 100% Offline AI-Powered Security Analytics with AirgapAI and Intel Core Ultra



Executive Summary

Challenge: A Major Nuclear Energy Company operating more than 10 nuclear power plants across the United States needed to enhance IT security review capabilities for analyzing system access logs, credential management, logging anomalies, and complex JSON/YAML configuration datasets—all while meeting stringent NERC CIP cybersecurity requirements and maintaining complete isolation from external networks.

Solution: Intel and Iternal Technologies deployed AirgapAI™ powered by Intel Core Ultra AI PCs with OpenVINO optimization, enabling cybersecurity analysts to rapidly

query and analyze security data, identify anomalies, and correlate access patterns across multiple plant systems—all while maintaining 100% air-gapped operation with zero network dependencies.

Results:

- 78x improvement in AI accuracy versus traditional RAG pipelines
- 100% offline operation meeting NRC and NERC CIP cybersecurity mandates
- Up to 4.9x faster inference and 112x faster first-token latency with OpenVINO
- Security log analysis reduced from days of manual review to seconds per query
- Native JSON and YAML parsing enabling direct analysis of system configuration files
- Perpetual licensing model eliminating recurring subscription costs

Technology Stack: Intel Core Ultra 7 with NPU + OpenVINO | Blockify® + AirgapAI™

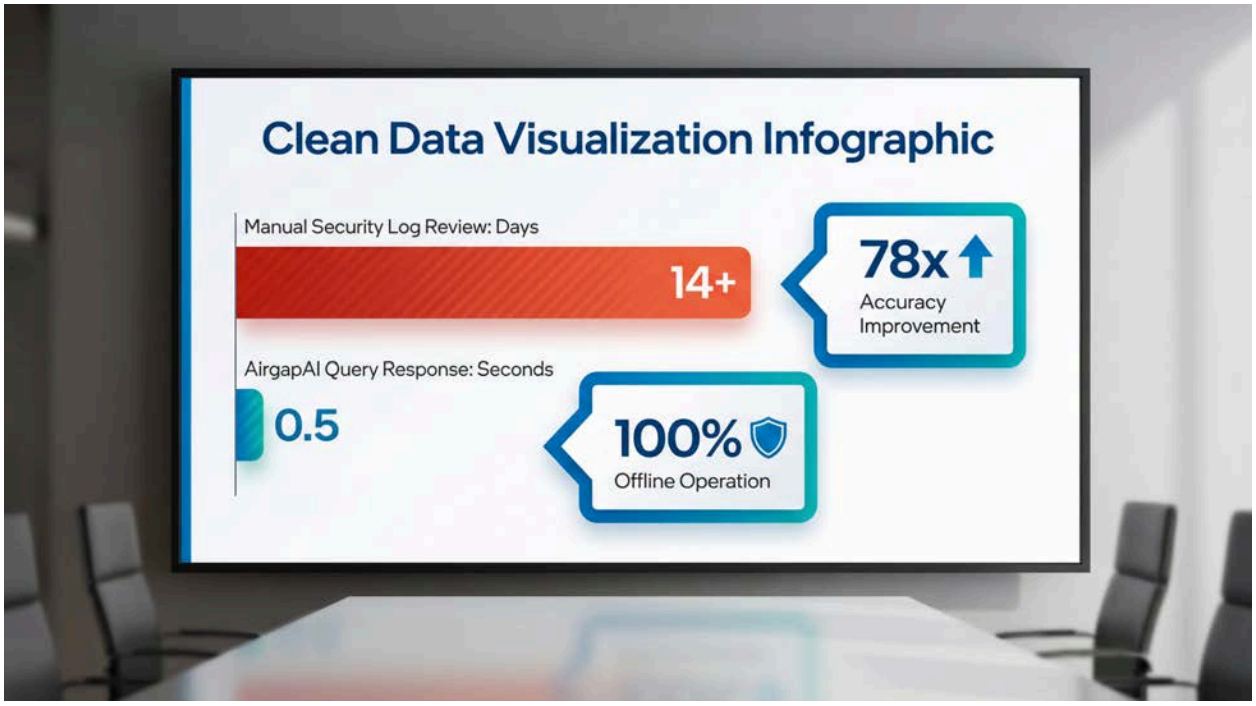
The Strategic Imperative: AI-Powered Cybersecurity for Nuclear Infrastructure

AI is rapidly becoming a strategic asset for critical infrastructure operators. To maintain the highest levels of cybersecurity and operational integrity, IT security teams must access the right information, at the right time, in a safe, secure, and trusted manner—while being absolutely certain every insight is factually correct and compliant with NRC regulations, NERC CIP standards, and federal cybersecurity mandates.

For a Major Nuclear Energy Company operating more than 10 nuclear power plants across the United States, the cybersecurity challenge is acute. IT security teams work in environments where accurate, fast, and secure data analysis isn't just nice to have—it's essential for protecting critical infrastructure that powers millions of American homes. Every security decision must reference current access policies, correlate patterns across multiple systems, and address regulatory requirements with precision.

Together, Intel and Iternal Technologies have partnered to provide a unique solution that supports this Major Nuclear Energy Company's IT Security teams via AirgapAI, transforming cybersecurity analytics while maintaining the ironclad data isolation that nuclear facilities demand.

The Challenge: AI-Powered Security Analytics in Air-Gapped Nuclear Environments



Why Traditional Cybersecurity AI Approaches Fall Short

Nuclear facilities present unique challenges for AI-powered security analytics that traditional cloud-based solutions simply cannot address:

Regulatory and Security Constraints:

- NERC CIP (Critical Infrastructure Protection) mandates strict controls on cybersecurity data flows
- NRC 10 CFR Part 73 requires complete isolation of security-related information systems
- Zero tolerance for data exfiltration—even encrypted cloud transmission is categorically prohibited
- Audit requirements demand complete transparency into AI processing of security data

Cybersecurity Operations Realities:

- Security analysts need instant access to access log patterns during incident investigations
- Configuration data scattered across JSON files, YAML configs, and multiple monitoring systems
- Time-sensitive security decisions cannot wait for cloud latency or connectivity issues
- Nuclear facilities operate in isolated network zones with no external connectivity permitted

The Traditional Approach Pain Points:

- Cloud-based SIEM and AI solutions immediately disqualified due to security requirements
- On-premise security AI requires expensive data center infrastructure
- Manual log analysis across 10+ plants consumes hundreds of hours per comprehensive audit
- Credential anomaly detection across multiple systems is error-prone and time-consuming
- JSON/YAML configuration drift analysis requires specialized tooling and expertise

Without an effective approach to content lifecycle, the organization risks relying on an AI that will never be fully accurate. It's a case of garbage in, garbage out—and if you can't trust your AI to continually be correct, you can't trust it at all because the mistakes are unpredictable.

Why AI Matters for Nuclear Cybersecurity Operations

Beyond simple log search and queries, cybersecurity professionals need AI that can synthesize information from access logs, credential databases, and system configuration files, identify anomalous patterns across multiple plants, and ensure compliance with regulatory standards—all without any network connectivity.

Traditional Process Pain Points:

- Days spent manually reviewing access logs for anomalies across 10+ plants
- Manual correlation of credential access patterns across disparate systems
- Risk of missed security indicators due to human fatigue during extended log reviews
- Inconsistent analysis approaches across different security team members and shifts
- Delayed incident response during critical security situations
- Sensitive security configurations requiring strict protection from any external exposure

The nuclear energy sector operates under constant scrutiny from regulators, with NERC CIP violations and NRC findings carrying significant penalties. Any AI solution must not only deliver productivity gains but do so while maintaining—or enhancing—the organization's cybersecurity posture.

The Solution: AirgapAI on Intel Core Ultra AI PCs

Blockify® Data Optimization for Security Data Retrieval

Blockify is Iternal's patented data ingestion and optimization system that improves AI accuracy by up to 78x (7,800%) for retrieval augmented generation (RAG) tasks. When security analysts need to search through massive volumes of logs, configurations, and credential records to find relevant information, Blockify's intelligent chunking and taxonomy creation ensures the AI retrieves precisely the right context—virtually eliminating hallucinations that plague traditional RAG pipelines.

Note: Blockify specifically enhances retrieval-based queries against large datasets. It does not apply to general LLM chat or one-off file analysis—it's designed for building searchable knowledge bases that analysts can query repeatedly.

For this Major Nuclear Energy Company, Blockify ingested and indexed:

- System access logs across 10+ nuclear facilities
- User credential and authentication records
- JSON-formatted configuration files from monitoring systems
- YAML-based infrastructure configuration data
- Security policy documentation and procedures
- Historical incident reports and remediation records

AirgapAI™ Edge Inference with Intel Core Ultra + OpenVINO

AirgapAI is a powerful, network-independent AI solution designed to run 100% locally on Intel Core Ultra-equipped AI PCs. By operating completely offline, AirgapAI upholds stringent data-protection standards—no external connection is required, minimizing potential vulnerabilities and ensuring sensitive security data, credential information, and infrastructure configurations never leave the organization's control.

Key Capabilities Requested and Delivered:

- **JSON File Support:** Direct ingestion of JSON-formatted log files and configuration exports—no conversion required
- **YAML File Support:** Native parsing of YAML infrastructure configurations and security policies
- **Anomaly Pattern Queries:** Natural language queries against security data to identify suspicious patterns
- **Cross-Plant Correlation:** Compare access patterns and configurations across multiple facilities
- **Role-Based Access Control:** Integrated permissioning supporting security data governance mandates
- **Perpetual Licensing:** One-time purchase model eliminating recurring subscription fees

Benchmark Results

Intel Core Ultra 7 265V (AI PC) Performance

Leveraging Intel Core Ultra 7 265V with OpenVINO optimization, AirgapAI processing achieves up to 4.9x faster inference speed and up to 112x faster first-token latency compared to generic implementations. The ability to process 4,860 pages of security content per month demonstrates the capability to start small and scale.

Processing Performance:

- **Total Security Content Processed:** ~200,000 words (access logs, configs, credential data)
- **Blockify Processing Time:** ≈27.8 hours on AI PC (one-time ingestion)
- **Total Optimized Blocks:** ≈143 chunks
- **Tokens per Second:** 2.66 tokens/second (AI PC baseline)
- **OpenVINO Optimized:** Up to 34.27 tokens/second with GPU acceleration
- **Vector Search Speed:** 10 million records in <1.5 seconds

Accuracy Improvements (for Retrieval-Based Queries): Beyond speed, Blockify's approach increased the precision of vector searches and RAG retrieval, virtually eliminating hallucinations when analysts query against the security knowledge base. Compared with a traditional RAG pipeline, Blockify improves retrieval accuracy by approximately 78x (7,800 percent)—ensuring analysts receive precisely relevant information from the indexed security data.

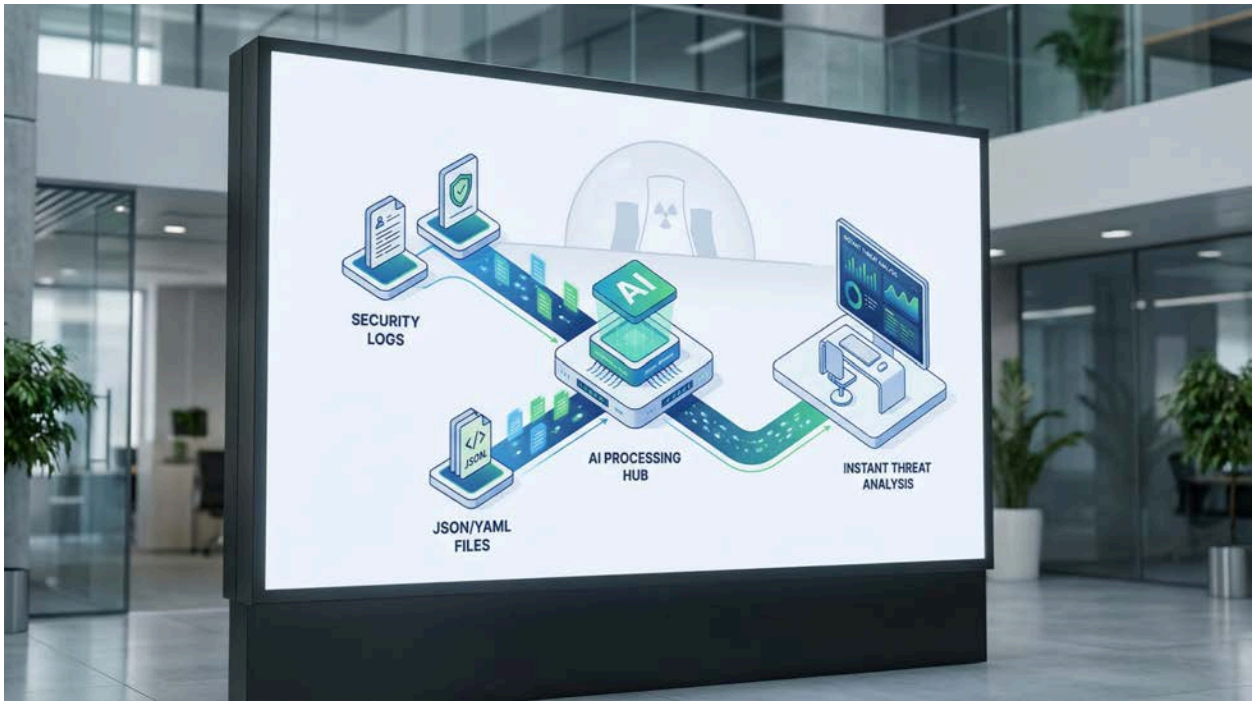
Intel OpenVINO Optimization

Intel's OpenVINO toolkit unlocks the true potential of Intel Core Ultra hardware, delivering:

- **Up to 4.9x faster inference speed** compared to generic implementations
- **Up to 112x faster first-token latency** for immediate responsiveness
- **Up to 9.2x higher ingestion throughput** for large log file processing

The OpenVINO optimization enables a "Better and Best" dynamic: the Intel NPU delivers efficient, high-performance processing for sustained security analytics workloads while preserving battery life, while the integrated GPU provides maximum burst performance for demanding incident investigations.

The Blockify Workflow: Building a Searchable Security Knowledge Base



Technical Process for Security Data Retrieval

Blockify prepares large-scale security datasets for intelligent retrieval. When analysts query the system, AirgapAI searches through this optimized knowledge base to find and return precisely relevant information—this is the retrieval augmented generation (RAG) pattern that Blockify enhances.

The Blockify workflow steps included:

1. **Chunking the Text:** Source data (access logs, JSON configs, YAML files, credential records) divided into smaller content chunks based on a proprietary algorithm. Chunks passed into specially configured LLM, outputting modular blocks with robust taxonomy optimized for retrieval.
2. **Embeddings:** Content blocks converted into embeddings (vector representations) capturing unique context and structure, enabling content-aware retrieval when analysts query against the knowledge base.
3. **Retrieval and Response Generation:** Based on user queries, the system searches the indexed content and retrieves relevant chunks from the

Context-Aware Retrieval Database, then generates accurate, contextually relevant responses grounded in the retrieved data.

Blockify's patented approach creates a single source of truth optimized for repeated querying. Distilling security content down to 2.5% of the original size allows for easy content lifecycle management and virtually eliminates hallucinations during retrieval-based queries.

Business Use Cases for Nuclear IT Security

The following use cases leverage Blockify-optimized retrieval to search through the indexed security knowledge base:

Access Log Anomaly Detection: Enable security analysts to query natural language questions against weeks of access logs—instantly retrieving unusual login patterns, off-hours access attempts, failed authentication clusters, and potential insider threat indicators across all 10+ facilities.

Credential Lifecycle Analysis: Analyze user credential data to identify dormant accounts, excessive privilege accumulations, shared credential usage patterns, and accounts that have not been properly deactivated after personnel transfers—ensuring compliance with NERC CIP access management requirements.

JSON Configuration Drift Detection: Ingest and compare JSON-formatted system configuration exports over time, automatically flagging unauthorized changes, configuration inconsistencies between plants, and deviations from approved baselines—critical for maintaining system integrity.

YAML Security Policy Verification: Query YAML-based infrastructure configurations to verify security policy implementation, identify misconfigurations, and ensure consistent security controls are applied across all nuclear facilities.

Incident Investigation Acceleration: During security incidents, surface relevant historical access records, related configuration changes, and similar past events—compressing investigation timelines from hours to minutes while ensuring complete documentation for regulatory reporting.

Regulatory Compliance Documentation: Generate comprehensive audit evidence by querying across all security data sources, demonstrating NERC CIP compliance, and preparing for NRC cybersecurity inspections with complete traceability.

Security and Compliance: Meeting Nuclear Regulatory Requirements

For an organization operating critical nuclear infrastructure, data security isn't optional—it's mandated by law and essential to national security.

AirgapAI's Security Architecture:

- **100% Local Processing:** All AI inference occurs on the Intel Core Ultra AI PC—no data transmission to cloud services
- **Zero Network Dependency:** Operates in fully air-gapped environments as required by nuclear facility cybersecurity standards
- **Complete Data Isolation:** Security logs, credential data, and configuration files never leave organizational control
- **NERC CIP Alignment:** Architecture designed to support Critical Infrastructure Protection cybersecurity requirements
- **NRC 10 CFR Part 73 Compliance:** Meets nuclear security information protection mandates
- **Audit-Ready Operations:** Complete transparency into AI processing for regulatory verification

By operating completely offline, AirgapAI upholds the stringent data-protection standards that nuclear critical infrastructure demands—no external connection is required, minimizing potential vulnerabilities and ensuring sensitive information remains strictly private.

Deployment Architecture Options

Phase 1: AI PC Edge Deployment (Current) Individual Intel Core Ultra AI PCs running AirgapAI locally, ideal for:

- Security Operations Center (SOC) analyst workstations
- Individual plant cybersecurity staff
- Incident response teams requiring portable security analytics
- Minimal infrastructure requirements with maximum security

Phase 2: Local Server Enhancement (Future Roadmap) AirgapAI clients connected to local GPU-powered servers for enhanced capability:

- Larger, more powerful language models for complex security analysis
- Centralized security knowledge management across all plants
- Still 100% air-gapped and on-premise
- Enterprise-wide security intelligence correlation

Maximizing AI Investment with The AI Strategy Blueprint

Technology alone doesn't guarantee AI success—85% of enterprise AI investments fail to deliver expected results. Iternal enhances its technology deployment with *The AI Strategy Blueprint*, a complete framework for AI transformation written by Iternal's CEO based on seven years of enterprise deployment experience.

The Blueprint addresses the 70% of AI success that depends on people and processes:

- **5x revenue gains** compared to competitors stuck in pilot programs
- **Governance frameworks** that enable speed rather than create barriers
- **Crawl-walk-run deployment strategies** that prove value before scaling risk
- **ROI quantification methodologies** that satisfy CFO scrutiny

This strategic foundation ensures the Major Nuclear Energy Company extracts maximum value from their AirgapAI deployment rather than joining the majority of failed AI initiatives.

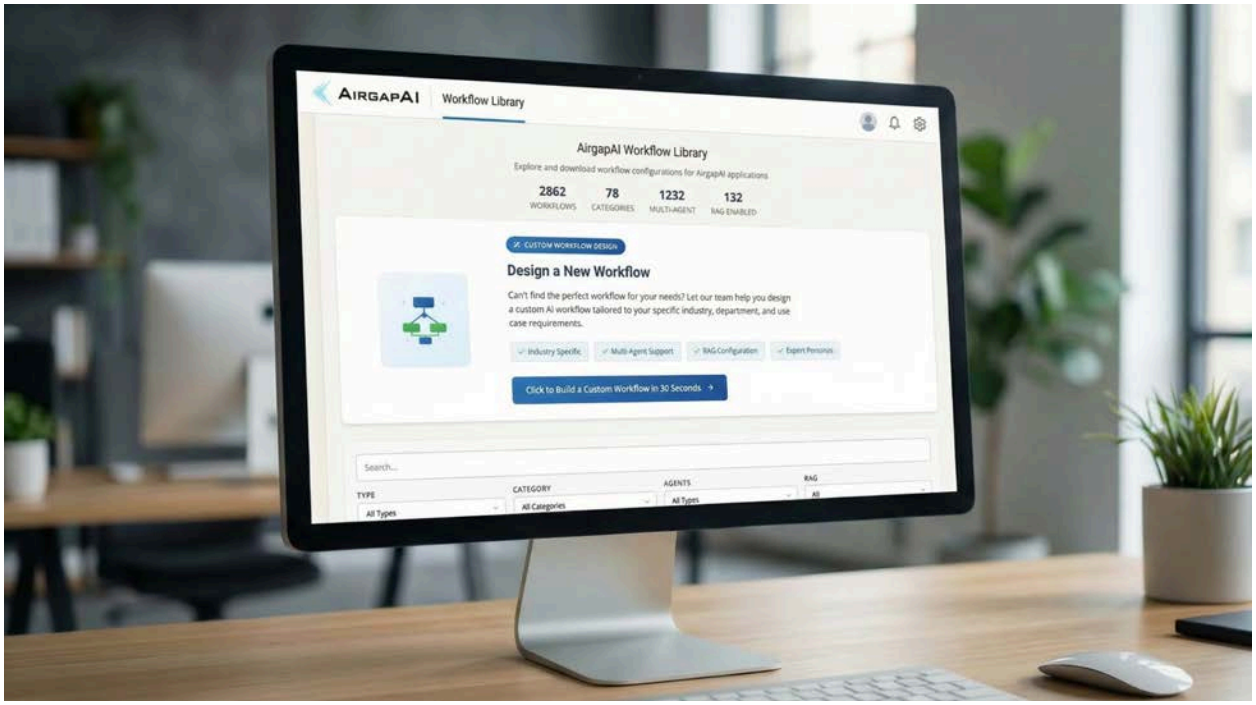
Accelerating Adoption with Iternal AI Academy

The fastest path to AI ROI is workforce capability. Iternal enhances its technology with the AI Academy (edu.iternal.ai)—comprehensive AI fluency training that accelerates how quickly cybersecurity professionals can leverage AirgapAI:

- **610+ courses** spanning every major industry and job role
- **Three proficiency tiers** - Beginner, Advanced, and Expert tracks
- **Real-time AI feedback** - Prompts scored and critiqued for immediate improvement
- **Verified certificates** - Independently verifiable credentials demonstrating competency
- **Universal application** - Skills transfer to any AI platform

By combining foundational education with interactive practice, AI Academy ensures the cybersecurity team can fully leverage their technology investment from day one.

Immediate Productivity with 2,800+ Quick Start Workflows



AirgapAI's technology is enhanced with more than 2,800 pre-configured Quick Start Workflows—enabling security professionals to achieve immediate productivity gains without a learning curve.

Pre-built workflows for cybersecurity operations include:

- Access log anomaly pattern detection
- User credential audit and compliance verification
- Configuration file comparison and drift analysis
- Security incident timeline reconstruction
- Regulatory compliance evidence generation
- Threat indicator correlation across systems

Custom workflow generation: Users can describe their security analysis process in natural language, and AirgapAI automatically creates a custom workflow tailored to their specific needs—no technical expertise required.

These workflows transform AirgapAI from a powerful tool into an immediate productivity multiplier for every member of the cybersecurity team.

Cost-Effective AI Deployment

Perpetual Licensing Model

Unlike cloud-based AI security solutions with recurring subscription fees, AirgapAI offers a perpetual licensing model that dramatically reduces total cost of ownership:

- **One-Time License Purchase:** No ongoing subscription fees per user or per query
- **No Cloud Costs:** Zero data egress charges, API fees, or usage-based pricing
- **Leverage Existing Hardware:** Runs on standard Intel Core Ultra AI PCs
- **No Mandatory Maintenance Contracts:** Professional services available but not required
- **Predictable Budgeting:** Fixed costs enable accurate long-term planning

Hardware Refresh Opportunity

The deployment of AI-capable workstations creates a natural opportunity to modernize cybersecurity infrastructure:

- **Strategic Replacement:** Prioritize AI PC deployment for SOC analysts and plant security staff
- **Gradual Rollout:** Start with 5-10 core security users, expand based on demonstrated value
- **Dual Benefit:** Productivity gains from AI plus general performance improvements
- **Future-Proofed:** Hardware capable of supporting evolving AI security capabilities

What This Means for You: Scalable AI Inference for Critical Infrastructure Security

By uniting Intel Core Ultra with OpenVINO optimization—delivering up to 4.9x faster inference and 112x faster first-token latency—and Iternal Technologies' Blockify and AirgapAI, nuclear energy operators can harness AI at the edge, turning years of security logs, configuration data, and credential records into actionable security insights without ever exposing sensitive information to third-party clouds.

Together, Intel and Iternal help Nuclear Energy Companies:

- **Automate Security Data Analysis:** Process massive volumes of access logs and configurations while achieving 78x accuracy improvement
- **Drive Compliance:** Ensure every AI-generated security insight respects NERC CIP, NRC, and federal cybersecurity requirements
- **Accelerate Incident Response:** Surface trusted security answers in seconds with OpenVINO-optimized inference
- **Protect Critical Infrastructure Data:** Keep all security information within organizational boundaries with 100% offline operation

Enhancing Technology with Complete AI Enablement:

- **Maximize Investment:** The AI Strategy Blueprint ensures your deployment succeeds where 85% of AI initiatives fail

- **Accelerate Adoption:** AI Academy training builds workforce capability for faster time-to-value
- **Immediate Productivity:** 2,800+ Quick Start Workflows eliminate the learning curve for security teams
- **White-Glove Support:** Optional AI Assist Bundle provides end-to-end deployment services

AI has moved from conceptual to operational in critical infrastructure cybersecurity. Whether detecting access anomalies, verifying credential compliance, or accelerating incident investigations, Intel and Iternal deliver the secure, accurate, and scalable framework nuclear energy companies need to protect the nation's power grid.

Summary: The Right Solution for Nuclear Cybersecurity

Security-First Architecture:

- 100% air-gapped operation with zero network dependencies
- NERC CIP and NRC cybersecurity regulation alignment
- Complete data isolation for all security-related information

Operational Excellence:

- 78x improvement in AI accuracy eliminating hallucinations

- Native JSON and YAML parsing for direct configuration analysis
- Instant security queries across multiple plant data sources

Cost-Effective Deployment:

- Perpetual licensing model with no recurring fees
- Runs on standard Intel Core Ultra AI PCs
- Scalable from individual analysts to enterprise SOC deployment

Future-Ready Platform:

- Support for JSON, YAML, and evolving log formats
- Local server enhancement path for larger models
- Rapid development cycle with continuous security feature updates

The Intel AI PC, powered by Iternal AirgapAI, delivers exactly what critical infrastructure cybersecurity requires—secure, accurate, and reliable AI that operates completely offline while maintaining the trust and compliance essential to nuclear energy operations.