LDR520: **Emerging Trends for Cyber Leaders – AI & Cloud™**

5 Day Course	30 CPEs	Laptop Required

You Will Be Able To

- Design secure AI strategies and implementation roadmaps
- Identify and defend against AI-specific vulnerabilities and adversarial attacks
- Architect secure cloud environments across IAM, workload protection, and DevSecOps
- Implement multicloud governance and SaaS security controls
- Build organizational readiness for cryptographic transition

"Team is collaborative. We are all able to bounce ideas off of each other comfortably and using AWS to get hands-on makes it feel more real than if we were answering questions on a quiz."

—Richard Sanders,
Best Western International

Adapt. Lead. Secure the Future of Cyber.

SANS LDR520 prepares strategic security leaders to confidently drive enterprise cloud and AI transformation while defending against tomorrow's threats. You will learn to govern AI systems, implement secure cloud architectures, mitigate advanced risks, and lead cryptographic modernization, all through battle-tested frameworks, real-world labs, and leadership simulations.

With escalating executive pressure to "move faster" on AI and cloud, this course bridges business imperatives with security strategy. Participants develop board-level communication skills, roadmap execution methods, and practical controls to safeguard high-value assets across multicloud and AI-powered environments.

Business Takeaways

- Lead enterprise-wide AI and cloud transformation securely
- Reduce risk exposure and regulatory impact from AI misuse
- Prevent deepfake and adversarial AI attacks
- Build governance frameworks aligned to NIST, ISO, and EU AI Act
- Strengthen multicloud resilience and data protection
- Prepare for post-quantum cryptographic threats

Hands-On Cloud Security Strategy Training

LDR520 includes daily hands-on labs and Cyber42 simulations to build strategic decision-making skills. Each session challenges students to manage budgets, prioritize risk, and lead cloud and AI security programs within a fictional enterprise. On Day 5, the course culminates in an executive-level capstone, where teams present a full security modernization strategy addressing AI, cloud, and post-quantum threats.

"I recommend this course thanks to the multi-cloud approach and cloud-agnostic strategy, where we learned to consider and ask the right questions related to the cybersecurity part."

—Madjid Kazi Tanoi

Section Descriptions

SECTION 1: AI Strategic Imperatives: Governance and Threat Assessment

This section delivers practical defensive strategies against AI-enabled threats and adversarial attacks while leveraging AI to transform security operations. Participants build comprehensive implementation roadmaps including vendor selection, resource planning, and measurable ROI targets for organizational deployment.

TOPICS: AI Security Business Case; NIST/EU AI Act/ISO Frameworks; Shadow AI Risks; OWASP LLM Top 10; AI-Enhanced Threats

SECTION 2: AI Defense and Enterprise Implementation

This section delivers practical defensive strategies against AI-enabled threats and adversarial attacks while leveraging AI to transform security operations. Participants build comprehensive implementation roadmaps including vendor selection, resource planning, and measurable ROI targets for organizational deployment.

TOPICS: Adversarial ML Threats; AI-Powered SOCs; Vendor Evaluation; Phased Implementation; Enterprise Outcomes

SECTION 3: Cloud Security Foundations, Identity, and Infrastructure

This section establishes the critical foundation for cloud security, covering fundamental adoption models, identity management, and core infrastructure protection. It provides the essential building blocks for creating a secure and resilient cloud environment from the ground up.

TOPICS: Cloud Models; IAM Segmentation; Multi-account Strategy; Config Management; Network Architecture

SECTION 4: Cloud Data Protection, Operations, and Governance

This section focuses on protecting your most critical assets and managing ongoing security operations, from data encryption and incident response to securing workloads. It also covers the strategic aspects of multicloud governance, compliance, and organizational alignment for a mature security posture.

TOPICS: Data Protection; Monitoring and Response; DevSecOps; Compliance; SaaS and Multicloud Governance

SECTION 5: Post Quantum Crypto and Capstone Exercise

This section addresses the modern crypto transition to post-quantum security management, a critical future-proofing strategy. It culminates in a capstone exercise where students apply all concepts and skills learned throughout the course in a practical, executive-level scenario.

TOPICS: PQC Risks and Strategy; Crypto-agility; Phased Transition; Capstone Exercise and Executive Strategy Brief

Who Should Attend

The primary target audience for this course is managers and directors who are in a position to lead or make key decisions on the IT transformation to cloud environments.

NICE Framework Work Roles

- Information Systems Security Manager (OPM 722)
- Program Manager (OPM 801)
- IT Project Manager (OPM 802)

Prerequisites

Students should have three to five years of experience in IT and/or cybersecurity. This course covers the core areas of security leadership in migrating workloads to the cloud environment and assumes a basic understanding of technology, networks, and security.

Notice to Students

This course will have limited overlap with the SANS SEC502: Cloud Security Tactical Defense course because it will provide foundational information on cloud services and cloud security to ensure that students are on the same page.

"Great way to break out of just the technical aspects of cloud and a step towards management-level learning."

—Joshua Rosetta, **Penn State Health**

"I loved the labs. They really helped emphasize what we are learning."

—Jana Laney