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

5 Day Course	30 CPEs	Laptop Required

You Will Be Able To

- Build and defend the AI security business case
- Design governance structures including AI registries, oversight models, and third-party controls
- Counter OWASP LLM vulnerabilities and adversarial AI threats
- Architect secure multicloud environments using maturity-driven investment frameworks
- Govern SaaS operational security and workforce transformation
- Develop enterprise crypto-agility and post-quantum migration strategies

"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 equips security leaders to transform emerging technologies into strategic advantage. This course goes beyond cloud fundamentals to deliver structured AI governance, operational AI defense, multicloud modernization, SaaS security oversight, and post-quantum readiness.

As executive pressure accelerates AI adoption and cloud transformation, leaders must balance innovation with risk, regulation, and resilience. LDR520 bridges business imperatives with security strategy through governance frameworks, operational defense models, and executive-level transformation playbooks.

Participants build actionable roadmaps, board-level communication strategies, and modernization plans grounded in real-world frameworks and leadership simulations.

Business Takeaways

- Establish AI governance aligned to NIST AI RMF, EU AI Act, and ISO 42001
- Reduce exposure to adversarial AI, deepfake fraud, and Shadow AI risk
- Modernize cloud security across identity, infrastructure, and detection domains
- Strengthen SaaS governance and multicloud resilience
- Prepare for post-quantum cryptographic transition
- Lead enterprise-wide security modernization with executive alignment

Hands-On Cloud Security Strategy Training

LDR520 includes daily labs and Cyber42 simulations that place you in the CISO role. Participants manage budgets, mitigate AI and cloud risk, influence stakeholders, and build a full enterprise modernization strategy culminating in an executive capstone presentation.

"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

Build the foundation for responsible AI governance and regulatory alignment.

TOPICS: AI Business Case and Shadow AI Risk; NIST AI RMF, EU AI Act, ISO 42001; Governance Structures and Oversight Models; Executive Playbook for Influence and Resistance Management; Global Regulatory Strategy and Emerging AI Risks

SECTION 2: AI Defense and Enterprise Implementation

Shift from governance to operational AI security across three pillars.

TOPICS: Bias Detection and Safety Assurance; OWASP LLM Top 10 and Adversarial Attacks; AI-Powered Phishing and Deepfake Threats; MITRE ATLAS for AI Threat Intelligence; AI-Enabled SOC Capabilities and Investment Strategy

SECTION 3: Cloud Security Foundations, Identity, and Infrastructure

Apply the eight domain maturity framework to strengthen cloud posture.

TOPICS: Identity and Access Management Strategy; Secure Infrastructure and Configuration Guardrails; Detection, Response, and Analytics Modernization; Cloud Governance, Cost Management, and Vendor Risk; Maturity Assessment and Investment Prioritization

SECTION 4: Cloud Data Protection, Operations, and Governance

Extend modernization across workloads, assurance, and workforce readiness.

TOPICS: Data Protection and Encryption Strategy; DevSecOps and Workload Security; Security Assurance and Compliance Validation; Workforce Transformation and Operating Models; SaaS Operational Security and Shadow IT Governance

SECTION 5: Post Quantum Crypto and Capstone Exercise

Prepare for cryptographic disruption and integrate AI and cloud modernization into a unified enterprise strategy.

TOPICS: Post-Quantum Cryptographic Risks; Crypto Inventory and Agility Strategy; Phased Migration Planning; Executive-Level Modernization Capstone

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