

LDR516: Strategic Vulnerability and Threat Management™

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Build and evolve vulnerability management programs across traditional, cloud, IoT, and hybrid environments
- Prioritize vulnerabilities using business-aligned context and threat intelligence
- Measure program maturity and risk reduction using metrics and maturity models such as VMMM and CTEMMM
- Validate real exposure through attack-path analysis and breach and attack simulation, then drive remediation at scale through VulnOps
- Use AI to accelerate analysis while applying the human judgment that tests and challenges its output
- Communicate vulnerability risk effectively to executives, IT, and business units through tailored reporting
- Align VM with regulatory frameworks (e.g., NIS2, NIST, HIPAA, GDPR, CRA) and board-level governance

Business Takeaways

- Assess organizational strengths, weaknesses, and maturity in vulnerability management programs
- Prepare for and respond to critical vulnerabilities and zero-day issues
- Prioritize security investments using data-driven decision-making and contextual risk models
- Translate technical VM findings into business impact to improve executive understanding and buy-in
- Uncover hidden obstacles by grouping and analyzing vulnerabilities
- Use program metrics and reporting to improve compliance posture and guide continuous improvement
- Implement proactive remediation capabilities

Strategic Vulnerability Management for Modern Enterprises

Whether you're building a VM program from scratch or leading a large-scale modernization effort, this course will transform how you think about managing exposures across your enterprise. You'll move beyond checklists and patch deadlines to tackle the real challenges: aligning with business priorities, managing risk acceptance responsibly, and driving remediation across siloed teams and complex infrastructure.

LDR516 blends tactical techniques and strategic leadership. You'll explore how to prioritize beyond CVSS using exploit prediction (EPSS), real-time threat intelligence (CISA KEV, MITRE ATT&CK), and asset criticality. You'll address challenges in cloud, container, and IoT environments—and learn to navigate resistance, resource constraints, and governance hurdles.

The course also dives into the principles of Continuous Threat Exposure Management (CTEM), breach and attack simulation (BAS), and VulnOps to help you plan for proactive, continuous improvement—but it does not require CTEM adoption. Instead, the focus is on building practical, scalable programs grounded in real-world constraints.

The course teaches two practical maturity frameworks, the Vulnerability Management Maturity Model (VMMM) v2 and the Continuous Threat Exposure Management Maturity Model (CTEMMM), to help leaders evaluate and evolve their programs.

Over five days, you'll complete 11 labs set inside one fictional company, ArctiqNova Industries, where the decisions you make early in the week carry into later labs. In most labs, AI produces the generic answer and your job is to find where it fails ArctiqNova; in others, the model argues against your position or attacks your own decisions. The Cyber42 leadership simulation game weaves through each day, putting you in realistic scenarios in 5 strategic initiative rounds with 10 decision challenges that test your ability to lead under pressure.

If you're ready to stop drowning in vulnerability data and start driving meaningful risk reduction, this course is your blueprint for building a future-ready VM program.

Hands-On Vulnerability Management Training

LDR516 uses the Cyber42 leadership simulation game, AI-driven scenario labs, and tool-based exercises to provide students with a dynamic, hands-on learning experience. These elements are woven throughout the course to reinforce core concepts, strengthen leadership and communication skills, and simulate the real-world decisions that vulnerability management professionals face. Students assume the role of a VM leader at the fictional ArctiqNova Industries, where they select strategic initiatives, respond to realistic operational challenges, and make prioritization and governance decisions that affect security outcomes and business risk. Decisions carry from section to section, in both the labs and Cyber42.

“It is excellent for people who are creating and implementing their VMP. The course is detailed, thorough, and sets clear expectations for a successful program.”

—Rachel Parkhurst

Section Descriptions

SECTION 1: Building the Blueprint for Vulnerability Management Success

Establish a strong foundation by understanding the VM lifecycle, aligning with business goals, and building the asset and discovery practices that power effective risk reduction.

TOPICS:

- Foundation of Vulnerability Management (VM)
- Asset Management and Attack Surface Understanding
- Business Alignment
- Asset Classification
- Configuration Flaws

SECTION 3: Communicating Risk and Driving Action In VM

Translate technical findings into business-relevant risk insights through metrics, reporting, storytelling, and executive communication that prompt real action.

TOPICS:

- Risk-Based Strategic and Maturity Metrics
- Effective Reporting and Communication
- Automation and Efficiency
- Driving Culture Change and Executive Engagement
- Integration with Incident Response

SECTION 5: The Future of Vulnerability Management – Proactive Defense and Continuous Exposure Management

Explore forward-looking practices like CTEM, attack path modeling, breach and attack simulation, VulnOps, and AI as you evolve from reactive patching to continuous, business-aligned threat exposure management. Students explore how maturity-based exposure management approaches help organizations transition from reactive vulnerability practices toward continuous exposure reduction.

TOPICS:

- Attack Path Modeling and Breach and Attack Simulation
- CTEM (Continuous Threat Exposure Management)
- Adoption Challenges and Solutions
- AI-Native Exposures
- VulnOps and Remediation Without Testing

SECTION 2: Mastering the Art of Prioritization and Remediation

Learn how to move beyond CVSS and prioritize vulnerabilities using context, threat intel, and business impact—while deploying smart, scalable remediation and risk acceptance strategies.

TOPICS:

- Prioritization Strategies
- Weighted Averages and Decision Trees
- Remediation Approaches
- Measuring and Tracking Success
- Risk Management and Documentation

SECTION 4: Navigating Compliance, Crisis, and Governance in VM

Balance regulatory obligations and risk-based strategies, build resilient VM programs with strong policies and governance, and respond effectively to zero-day events and audit demands.

TOPICS:

- Compliance and Regulatory Alignment
- Preparedness and Response
- Post-incident and Continuous Improvement
- Roles, Responsibilities, and Risk Ownership
- Evolving VM with Technology

Who Should Attend

LDR516 training is recommended for a diverse range of individuals, including:

- Vulnerability program managers and analysts managing vulnerabilities in the enterprise or cloud
- Information security managers, architects, analysts, officers, and directors
- Aspiring information security leaders
- Risk management, business continuity and disaster recovery professionals
- IT operations managers and administrators
- CISOs
- Cloud service managers, administrators, integrators, developers, and brokers
- Cloud service security and risk managers
- Government IT professionals who manage vulnerabilities in the enterprise or cloud (FedRAMP, NIST CSF) Security Control Assessor

NICE Framework Work Roles:

- Security Control Assessor (OPM 612)
- Vulnerability Assessment Analyst (OPM 541)

“Excellent labs. More fun than I thought possible with vulnerability management.”

—Page Jeffery, Newmont

“An understanding of vulnerability management and cloud security is becoming not only valuable but a necessity to keep one’s organization secure in this constantly changing and dynamic environment.”

—Kae David, EY