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
- Develop and apply VM metrics to measure program maturity, demonstrate risk reduction, and drive stakeholder support
- Design remediation strategies that include patching, compensating controls, and automation
- Communicate vulnerability risk effectively to executives, technology, security and other business units
- Align VM with frameworks like NIS2, NIST, HIPAA, GDPR, and CRA for sustainable governance

Business Takeaways

- Assess maturity and gaps in your organization's VM program
- Prepare for critical vulnerabilities and zero-day exposures
- Prioritize security investments using contextual risk models
- Translate technical findings into executive-level insights
- Use vulnerability grouping to uncover hidden risks and blockers
- Implement metrics and dashboards to drive compliance and performance
- Design proactive remediation workflows and future-ready programs

> **"This course is essential for both well-established and developing vulnerability management teams."**
>
> —Robert Adams, **CBC**

Strategic Vulnerability Management for Modern Enterprises

Whether you're starting from scratch or modernizing an enterprise-scale vulnerability management (VM) program, LDR516 provides the strategies, tools, and insights to make your efforts more impactful. This course helps you move beyond checkbox compliance and endless scan results, focusing instead on risk-based prioritization, stakeholder communication, and real-world remediation.

LDR516 equips security professionals with the ability to lead and evolve VM initiatives across traditional, cloud, and hybrid environments. With an emphasis on business alignment, threat modeling, and metrics that matter, you'll learn how to turn raw vulnerability data into clear decisions and measurable outcomes. Over five days, you'll complete 21 interactive exercises, including nine AI-enhanced hands-on labs and five strategic rounds of the Cyber42 leadership simulation, featuring 12 real-world decision challenges, giving you both tactical and strategic experience in risk reduction.

You'll explore modern frameworks such as Continuous Threat Exposure Management (CTEM), risk scoring using EPSS and threat intelligence (e.g., CISA KEV, MITRE ATT&CK), and context-aware prioritization based on asset criticality. The course also teaches you how to design metrics, influence executive stakeholders, and overcome challenges like limited resources, fragmented ownership, and culture resistance.

Hands-On Vulnerability Management Leadership Experience

LDR516 emphasizes applied learning through 21 hands-on labs, including nine AI-enhanced exercises and the immersive Cyber42 leadership simulation. Each activity is designed to mirror the real-world decisions security leaders face as they evolve vulnerability programs from reactive patching to measurable exposure reduction.

- **AI-Enhanced Labs—**Use AI to support executive communication, model attack paths, evaluate remediation trade-offs, and translate technical findings into business-aligned risk insights.
- **Threat-Informed Prioritization Exercises—**Apply exploit prediction (EPSS), MITRE ATT&CK mapping, asset criticality, and contextual analysis to defend prioritization decisions under pressure.
- **Governance and Policy Labs—**Develop vulnerability management policies aligned to regulatory requirements and risk tolerance, modernize workflows, and design defensible risk acceptance processes.
- **Communication and Executive Reporting Labs—**Craft audience-specific reports and board-level briefings that convert exposure data into strategic decisions.
- **Cyber42 Leadership Simulation—**Participate in five integrated rounds with 12 strategic challenge events. Navigate stakeholder resistance, cloud exposure scenarios, compliance pressures, and governance trade-offs in a realistic enterprise environment.

These labs reflect the complexity of modern enterprise environments—spanning traditional infrastructure, cloud, and hybrid systems—so you leave with practical frameworks, defensible decision models, and leadership confidence you can apply immediately.

> **"A great course to utilize if new to cloud vulnerability management."**
>
> —Amaan Mughal

sans.org/LDR516

- Watch a preview of this course
- Discover how to take this course: Online, In-Person

Section Descriptions

SECTION 1: Building the Blueprint for VM Success

This section covers the foundations of VM lifecycle, asset inventory, and attack surface visibility. Section 1 emphasizes leadership alignment and cloud-aware program design. It includes Cyber42 Round 1 and labs on defining VM values and communicating critical flaws.

TOPICS: Foundation of VM; Asset Management and Attack Surface Understanding; Assessment Techniques; Common Challenges and Pitfalls; Responding to Evolving Threats

SECTION 2: Mastering the Art of Prioritization and Remediation

Section 2 explores scanning strategies, tool integration, and modern discovery challenges across infrastructure and applications. It includes Cyber42 Round 2 and labs on scanning techniques, validation, and pipeline integration.

TOPICS: Prioritization Strategies; Remediation Approaches; Measuring and tracking success; Risk management and documentation; Governance and stakeholder engagement

SECTION 3: Communicating Risk and Driving Action in VM

Section 3 focuses on interpreting vulnerability data, prioritizing in context, and communicating with executives and stakeholders. The labs include contextual prioritization, executive translation, and board briefings. Cyber42 Round 3 is also included.

TOPICS: Risk-Based and Strategic Metrics; Reporting; Automation; Communications; Culture Change; Incident Response Integration

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

Section 4 balances compliance and risk-based strategies, strengthens VM programs through governance and policy, and prepares teams for zero-day events and audits. It covers real-world remediation, automation, and stakeholder engagement, with Cyber42 Round 4 and hands-on labs on gold image pipeline, culture change, and remediation.

TOPICS: Compliance and Regulations; Incident Preparedness and Response; Continuous Improvement; Roles and Responsibilities; Evolving VM with Technology

SECTION 5: The Future of VM – Proactive Defense and CTEM

Section 5 centers on future-proofing programs through CTEM, stakeholder mapping, and governance evolution. Labs focus on attack path modeling, CTEM design, and gaining executive buy-in. It concludes with Cyber42 Round 5.

TOPICS: Proactive VM; CTEM; Change Adaption; Emerging Risks and Technology; Future-Ready Governance

“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

“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**

Who Should Attend

LDR516 is designed for both technical practitioners and strategic leaders responsible for managing vulnerabilities across enterprise, cloud, and hybrid environments. Ideal participants include:

- Vulnerability analysts, engineers, and program managers
- Security architects, SOC leads, and CISOs
- IT operations, DevOps, and cloud platform professionals
- Risk, compliance, and governance officers
- Business continuity and disaster recovery planners
- Government and critical infrastructure cybersecurity teams (e.g., FedRAMP, NIST CSF)

NICE Framework Work Roles:

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