BLACKBIRD FOR TRAINING

SANS – LDR553: Cyber Incident Management

SANS – LDR553: Cyber Incident Management

Introduction

SANS - LDR553: Cyber Incident Management is a structured and leadership-focused course designed to help organizations manage cyber incidents in a disciplined and systematic manner.

The course addresses preparation, response, coordination, and post-incident analysis to ensure operational continuity and risk reduction.

It connects incident management with risk governance, regulatory compliance, and business continuity frameworks.

This program is relevant for executives, department managers, information security leaders, technology supervisors, risk managers, compliance professionals, and project leaders.

It supports professionals across financial services, energy, telecommunications, public institutions, industrial organizations, and service sectors.

The practical value of this course lies in building a clear incident response structure, defining roles and responsibilities, strengthening crisis coordination, and improving root cause analysis.

Participants gain the ability to reduce downtime, improve decision-making under pressure, and enhance institutional resilience against cyber threats.

Course Objectives

The course aims to deliver measurable and practical outcomes, including:

- Understand the core principles of cyber incident management.
- Identify the stages of the incident lifecycle.
- Apply structured incident classification methodologies.
- Analyze the operational and financial impact of incidents.
- Develop a comprehensive incident response plan.
- Define roles and responsibilities within response teams.
- Establish structured communication procedures during crises.
- Coordinate with regulatory or supervisory bodies when required.
- Measure response effectiveness using performance indicators.
- Produce structured post-incident reports.
- Implement continuous improvement processes.
- Integrate incident management with business continuity strategies.

Course Outlines

Day 1: Foundations of Cyber Incident Management

- Definition and categories of cyber incidents.
- Overview of the incident lifecycle.
- Governance structure for incident response teams.
- Development of internal incident response policies.
- Organizational readiness assessment.
- Practical exercise to identify strengths and gaps.

Day 2: Detection, Classification, and Prioritization

- Early detection mechanisms for cyber incidents.
- Internal reporting channels and escalation procedures.
- Risk-based classification standards.
- Operational impact assessment methods.
- Prioritization aligned with organizational objectives.
- Case study analysis of a real-world incident scenario.

Day 3: Active Response and Crisis Coordination

- Establishing a crisis management structure.
- Task allocation between technical and leadership teams.
- Internal and external communication management.
- Coordination with affected stakeholders.
- Containment and mitigation strategies.
- Live simulation exercise of an incident scenario.

Day 4: Investigation and Root Cause Analysis

- Structured digital evidence collection.
- Root cause identification techniques.
- Review of response effectiveness.
- Identification of system and process weaknesses.
- Preparation of a comprehensive incident report.
- Analytical workshop on a complex scenario.

Day 5: Evaluation and Sustainable Improvement

- Full lifecycle incident review.
- Response plan effectiveness measurement.
- Development of an improvement roadmap.
- Policy and procedure updates.
- Presentation of applied exercises.
- Final case-based assessment.

Why Attend This Course? Wins & Losses!

- Strengthens organizational incident response capability.
- Reduces operational disruption and financial loss.
- Improves leadership decision-making during crises.
- Enhances cross-department coordination.
- Develops structured analytical and evaluation skills.
- Supports regulatory and compliance alignment.
- Reduces the likelihood of repeated incidents.
- Reinforces business continuity resilience.

Conclusion

SANS - LDR553: Cyber Incident Management provides a comprehensive framework for managing cyber incidents across their full lifecycle.

From early detection and structured response to investigation and continuous improvement, the course equips leaders with practical tools and governance structures.

By applying the methodologies covered, organizations can reduce operational risk, strengthen coordination, and improve resilience against evolving cyber threats.

Effective incident management is not only a technical necessity but also a strategic leadership function that supports institutional stability and long-term performance.