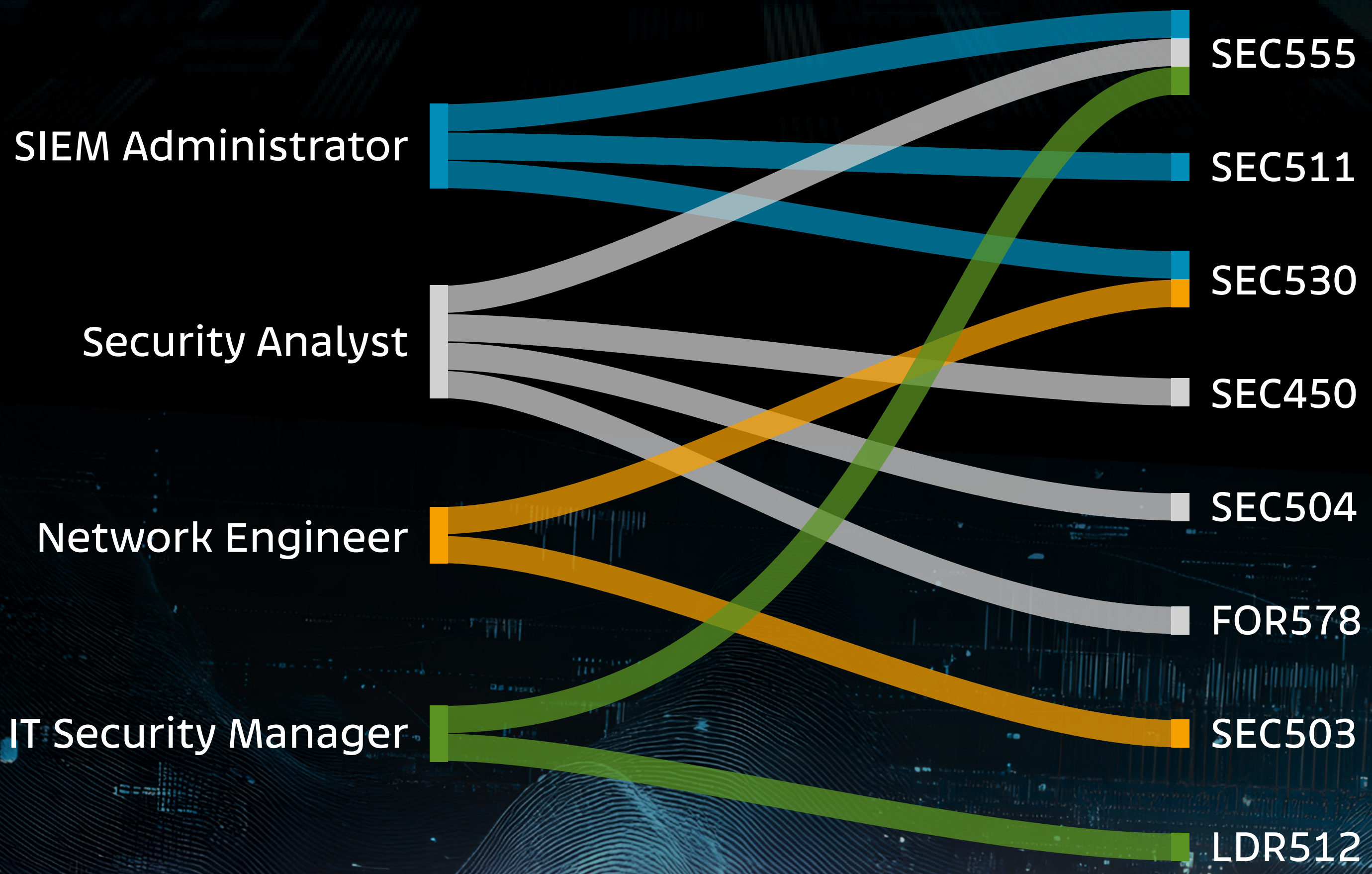
SANS

From Chaos to Clarity: Your SIEM Training Roadmap

Find the Right SANS Training Based on Your Role and Goals

Strong SOCs don't rely on tools alone—they build cross-functional teams where each role plays a part in turning noise into signal. Whether you're tuning rules or leading strategy, your contribution shapes the value of your SIEM investment.

Use this guide to find your optimal training path and turn your SIEM investment into a competitive advantage.



SIEM Administrator

Security Analyst

Network Engineer

IT Security Manager

SEC555

SEC511

SEC530

SEC450

SEC504

FOR578

SEC503

LDR512

Roles

SIEM Administrator

I am a: SIEM Administrator (SIEM Engineer, Detection Engineer)

I report to: Security Operations Manager or SOC Lead

My duties include: Managing SIEM rule tuning, log ingestion, and platform stability.

Security Analyst

I am a: Security Analyst (SOC Analyst, Incident Responder)

I report to: SOC Manager or Threat Detection Lead

My duties include: Triaging alerts, investigating threats, and feeding insights into detection tuning.

Network Engineer

I am a: Network Engineer (Network Security Engineer, Infrastructure Engineer)

I report to: a Network Operations Manager or a Director of IT

My Duties Include: Supporting secure network architecture and ensuring SIEM visibility into traffic.

IT Security Manager

I am a: IT Security Manager (SOC Manager, Security Program Manager)

I report to: a Chief Information Security Officer (CISO) or a Director of Information Security

My duties include: Overseeing SOC operations and aligning detection priorities with business risk.

Courses

SEC450: SOC Analyst Training: Applied Skills for Cyber Defense Operations™ *(GSOC)*:

Strong starting point for analysts—teaches alert triage, threat prioritization, and practical SOC workflows.

SEC503: Network Monitoring and Threat Detection In-Depth™ *(GCIA)*:

Teaches detailed traffic analysis, log interpretation, and visibility enhancement—key foundations for effective SIEM signal.

SEC504: Hacker Tools, Techniques, and Incident Handling™ *(GCIH)*:

Adds attacker mindset and incident response depth to boost SOC performance and threat context.

SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring™ *(GMON)*:

Teaches hybrid visibility across endpoint, network, and cloud with emphasis on threat-informed detection strategy.

SEC530: Defensible Security Architecture and Engineering™ *(GDSA)*:

Shows how to design security architectures that enable visibility, support Zero Trust principles, and enhance detection capabilities.

SEC555: Detection Engineering and SIEM Analytics™ *(GCDA)*:

Teaches how to design, build, and optimize detection rules and pipelines that transform raw log data into high-fidelity alerts.

FOR578: Cyber Threat Intelligence™ *(GCTI)*:

Teaches how to validate and contextualize alerts using intelligence, shifting from reactive triage to proactive hunting to reduce alert fatigue.

LDR512: Security Leadership Essentials for Managers™ *(GSLC)*:

Provides security managers with the essential leadership, governance, and communication skills to align cybersecurity operations—including SIEM efforts—with organizational priorities and risk goals.

Your SIEM Has More to Give—Learn to Unlock It

Your SIEM reflects what your people put into it. Skilled teams with the right processes turn raw alerts into actionable detection, aligned to real threats and real risks.

Explore the SANS SIEM Resources Hub
www.sans.org/mlp/siem-optimization

SANS