



# Exabeam Academy

Course & Certification Catalog 2026





EXABEAM ACADEMY COURSE CATALOG

# Introduction

## How to Use This Catalog

This catalog provides a structured, role-based view of Exabeam Academy certifications and training. It is designed to help customers identify which certification paths apply to their responsibilities within specific product environments.

This catalog shows how certifications are organized by role and product, making it clear which paths apply based on what you are responsible for and the environment you work in. Certifications are defined by this combination, and the courses in this catalog exist to support those paths.

This structure reflects how security teams operate in practice—by role, product, and responsibility—not by browsing individual courses.

This catalog is not an entry-level cybersecurity curriculum, a course syllabus, or a sales or partner enablement guide. Channel partners and internal delivery teams should reference the Partner Catalog for role expectations and certification requirements specific to partner delivery.

## The Certification Model

Certifications validate readiness to perform a specific role within a specific product context. A persona defines responsibility, product lines define operational scope, and certifications are defined where role and product intersect. Courses support certification readiness but do not replace certification validation.

## Courses by Product Lines

### New-Scale Analytics (NSA):

Behavioral analytics focused on risk-based detection, prioritization, and investigation using user and entity context.

### New-Scale SIEM (NSS):

Cloud-native SIEM providing log ingestion, normalization, search, correlation, and investigation workflows.

### LogRhythm SIEM (LRS):

Self-hosted SIEM designed for organizations requiring direct control of deployment, scaling, and data residency.

### Network Monitor (NetMon):

Network traffic visibility and analysis that complements log-based telemetry.

## Accessing Training

Your access to training is determined by your organization's Customer Success package or training subscription. Each access level defines which training formats and learning experiences are available to your users, enabling the appropriate progression from foundational knowledge to applied product proficiency.

The sections below outline the training formats included at each access level.

### Training Consumption Model

All training access levels operate on an **unlimited consumption model**.

- There are no **credits or tokens**
- Learners may **access content at any time**
- Training may be **repeated as needed** to reinforce knowledge and skills

This model enables continuous learning without administrative overhead or consumption constraints.

### Access Levels and Included Training Formats

#### Basic Access

All customers receive access to:

- **Computer-Based Training (CBT)**

CBT modules are:

- Short, **introductory**, and informational
- Designed to provide **high-level product awareness**
- Not intended to support **hands-on product usage, workflows, or role-based task execution**

This level supports initial product familiarity and early-stage exploration.

#### Standard Customer Success Package

Organizations with a **Standard Customer Success package** receive access to:

- **Self-Paced On-Demand (SPOD)**

SPOD courses:

- Provide **structured, guided learning paths**
- Support **independent skill development**
- May align directly to instructor-led equivalents, allowing learners to complete the same course content in multiple formats where available

#### Enhanced Customer Success Package

Organizations with an **Enhanced Customer Success package** receive access to:

- **Self-Paced On-Demand (SPOD)**
- **Virtual Instructor-Led Training (VILT)**

VILT courses:

- Are live, **instructor-led sessions delivered remotely**
- Provide **guided instruction with expert facilitation**
- Include **applied workflows, use case-driven learning, and hands-on product interaction**

#### Signature Customer Success Package

Organizations with a **Signature Customer Success package** receive access to:

- **Self-Paced On-Demand (SPOD)**
- **Virtual Instructor-Led Training (VILT)**
- **Private Instructor-Led Training (Private ILT)** (virtual or in-person)

Private ILT enables:

- Organization-controlled **scheduling, audience, and delivery context**
- Alignment to **customer-specific environments, priorities, and use cases**
- Accelerated **team onboarding and operational readiness**

Note: In-person Private ILT may require additional fees for facility, travel, and related expenses.

#### Unlimited Enterprise Subscription

The **Unlimited Enterprise Subscription** provides:

- Access to all training formats and learning experiences

This subscription supports **broad, scalable enablement** across roles, teams, and use cases without format or access limitations.

#### How Access Works

Training access is **automatically provisioned** based on your organization's package or subscription.

- Users will see only the **training formats and courses included in their assigned access level** within the learning platform
- If a course or format is not visible, it is **not included in the current entitlement**

#### Key Takeaway

Your access level determines both the **training formats available** and the **depth of skill development enabled**—from foundational awareness (CBT) to guided, instructor-led, and hands-on expertise (VILT and Private ILT).



EXABEAM ACADEMY COURSE CATALOG

# Certifications, Roles & Delivery Modalities

## Exabeam Certification Pathways by Persona (SOC Role)

Find your certification path by role and product. Course-level requirements are defined at the beginning of each product line course descriptions.

Persona (SOC-Role)	<b>New-Scale Analytics (NSA)</b>  Certification  Cloud native analytics platform.	<b>New-Scale SIEM (NSS)</b>  Certification  Cloud native SIEM. Provisioned by Cloud Operations.	<b>LogRhythm SIEM (LRS)</b>  Certification  On prem SIEM with partner owned deployment and lifecycle responsibilities.	<b>NetMon (NET)</b>  No certification available  Network detection and forensics with deep packet capture and analytics.
Security Analyst	NSA-SA	NSS-SA	LRS-SA	—
Platform Administrator	NSA-PA	NSS-PA	LRS-PA	—
Deployment Engineer	NSA-DE	NSS-DE	—	—
Deployment Engineer 1	—	—	LRS-DE-1	—
Deployment Engineer 2	—	—	LRS-DE-2	—
Deployment Engineer 3	—	—	LRS-DE-3	—
Technical Support	—	—	LRS-TSE	—

### Training Delivery Modalities

Exabeam Academy courses are delivered using three primary modalities:

**Self Paced On Demand (SPOD), Instructor Led Training (ILT), and Instructor Led Bootcamps.**

The delivery modality determines **how learners access and experience training**, not whether a course is required for a role or certification.

#### Self Paced On Demand (SPOD)

**Self Paced On Demand courses allow learners to begin training immediately upon registration.**

- Courses are completed independently through the Exabeam Academy platform
- Access is available as soon as the learner enrolls
- Learners progress at their own pace, revisiting content as needed
- No scheduled session or instructor involvement is required

SPOD courses are commonly used for foundational knowledge, conceptual understanding, and role aligned readiness that does not require live instruction or hands on facilitation.

#### Instructor Led Training (ILT) / Virtual ILT (VILT)

**Instructor Led Training courses are scheduled sessions delivered by an instructor.**

- Availability depends on published training schedules
- Registration is completed for a specific scheduled session
- Training is delivered live with guided instruction

ILT courses are typically used for advanced topics, structured walkthroughs, or scenarios that benefit from real time interaction, explanation, and guided learning.

#### Instructor Led Bootcamps (Hands On)

**Instructor Led Bootcamps are a specialized form of instructor led training focused exclusively on hands on execution and real world application.**

- Bootcamps are scheduled, live sessions led by an instructor
- Learners participate in guided, hands on exercises and practical scenarios
- Content emphasizes execution, validation, and operational readiness rather than conceptual learning
- Bootcamps are commonly used as capstone or advanced experiences after foundational and professional level preparation

Bootcamps are most often associated with roles that require **direct operational execution** (for example, deployment, upgrade, advanced administration, or escalation level support).

**Course delivery format** does not determine whether a course applies to a certification.

Certification paths may include a combination of self paced courses, instructor led training, bootcamps, and exams, each serving a different purpose in building knowledge and hands on skills. The specific mix of delivery types depends on the role, product, and certification level.

### The Exabeam Advantage

Exabeam Academy has designed our offerings to remove friction from learning. **Our all-you-can-eat (AYCE)** model eliminates the need to pay separately for certifications, exams, or individual classes, and removes the administrative burden of managing tokens, credits, or budgeting for turnover and attrition.

Many courses are offered in both **Virtual Instructor-Led Training (VILT)** and **Self-Paced On-Demand (SPOD)** formats. These formats provide different learning experiences, but they are designed to deliver the same skill outcomes. Learners can move easily between formats based on their needs, whether starting with SPOD during onboarding or joining VILT later for live instruction and guided practice.

Most importantly, Exabeam Academy is designed to build real competency. Our SPOD and VILT courses are built to help learners do and perform—using Exabeam products to complete role-based tasks, support workflows, and apply skills on the job.



EXABEAM ACADEMY COURSE CATALOG

# Course Descriptions

Course Descriptions include delivery modality, estimated duration, prerequisites/assumed knowledge, and a concise description of what the course covers. Courses support role and certification readiness but do not define partner requirements.

## **New-Scale Analytics (NSA)**

Behavioral analytics focused on risk-based detection, prioritization, and investigation using user and entity context.

[Go to Courses >](#)

## **New-Scale SIEM (NSS)**

Cloud-native SIEM providing log ingestion, normalization, search, correlation, and investigation workflows.

[Go to Courses >](#)

## **LogRhythm SIEM (LRS)**

Self-hosted SIEM designed for organizations requiring direct control of deployment, scaling, and data residency..

[Go to Courses >](#)

## **Network Monitor (NET)**

Network traffic visibility and analysis that complements log-based telemetry..

[Go to Courses >](#)

# New Scale Analytics (NSA)

## Certification Path

New Scale Analytics offers persona based certifications where a defined certification outcome exists for a role.

### SOC Roles

- Security Analyst

### Platform & Technical Roles

- Platform Administrator
- Deployment Engineer

### Important Boundaries

Certification paths define the certification outcome for each persona and the courses and assessments required to validate readiness.

## NSA Learning Paths – Required Classes

Required classes for each certification

### Security Analyst

(NSA-SA)

**Required courses:**

- NSA-100
- NSA-101
- NSA-102
- NSA-103
- NSA-104
- NSA 201
- NSA 202
- NSA-206
- NSA-207

### Platform Administrator

(NSA-PA)

**Required courses:**

- NSA-100
- NSA-102
- NSA-103
- NSA-104
- NSA-201
- NSA-202
- NSA-203
- NSA-204
- NSA 205
- NSA-206
- NSA-207
- NSA-210
- NSA-211
- NSA-212

### Deployment Engineer

(NSA-DE)

**Required courses:**

Prerequisite: NSA-PA

- NSA-208-1
- NSA-208-2

## NSA-100 — New-Scale Analytics: NSA Advantage

**Delivery Modality:** Self-Paced On-Demand (SPOD)

**Estimated Duration:** 2 hours

### Prerequisites & Assumed Knowledge

No formal prerequisites. This course assumes general familiarity with security operations concepts such as alerts, detections, and investigations, but no prior experience with New-Scale Analytics is required.

### Course Description

This foundational course introduces the evolution of Exabeam's security analytics platform and explains how New-Scale Analytics (NSA) enables faster, more scalable, and more reliable threat detection. Learners explore the limitations of traditional static correlation rules, the principles of behavioral analytics, and the architectural advantages of NSA's cloud-native design. The course establishes a shared conceptual baseline for analysts, administrators, and support before moving into role-specific workflows.

### Learner Paths

- Security Analyst
- Platform Admin

## NSA-101 — New-Scale Analytics: Quick-Start Guide for Analysts

**Delivery Modality:** Self-Paced On-Demand (SPOD)

**Estimated Duration:** 0.5 hours

### Prerequisites & Assumed Knowledge

No formal prerequisites. General familiarity with security operations concepts such as alerts and investigations is helpful but not required.

### Course Description

This course provides a fast, analyst focused introduction to using New Scale Analytics for daily security operations. Learners become familiar with core navigation patterns, alert handling concepts, and how behavioral analytics surface risk for investigation. The course is designed to accelerate analyst onboarding and establish confidence before deeper investigative workflows.

### Learner Paths

- T1 Security Analyst

## NSA-102 — New-Scale Analytics: Introductory Guided Demos

**Delivery Modality:** Self-Paced On-Demand (SPOD)

**Estimated Duration:** 2 hours

### Prerequisites & Assumed Knowledge

Completion of NSA-101 or equivalent introductory familiarity with New-Scale Analytics is recommended.

### Course Description

This course walks learners through guided demonstrations of core New Scale Analytics capabilities, illustrating how behavioral analytics, alerting, and investigation concepts work together in practice. The focus is on conceptual understanding rather than execution, helping learners visualize real world usage before role specific training.

### Learner Paths

- Security Analyst
- Platform Admin

## NSA-103 — New-Scale Analytics: Attack Surface Insights

**Delivery Modality:** Self-Paced On-Demand (SPOD)

**Estimated Duration:** 0.5 hours

### Prerequisites & Assumed Knowledge

General familiarity with security detections and alert concepts is helpful.

### Course Description

This course introduces Attack Surface Insights and how behavioral analytics help identify exposure and anomalous activity across users and entities. Learners gain a conceptual understanding of how attack surface visibility supports triage, investigation prioritization, and risk awareness across security operations.

### Learner Paths

- Security Analyst
- Platform Admin

## NSA-104 — New-Scale Analytics: Threat Center Investigative Workflow

**Delivery Modality:** Self-Paced On-Demand (SPOD)

**Estimated Duration:** 1.5 hours

### Prerequisites & Assumed Knowledge

Basic understanding of alerts, cases, and investigative workflows is recommended.

### Course Description

This course establishes the core investigative workflow in Threat Center, guiding learners through alert triage, context evaluation, case progression, and defensible documentation. It builds repeatable investigative habits for analysts and support personnel responsible for validating and escalating suspicious activity.

### Learner Paths

- Security Analyst
- Platform Admin

## NSA-201 — New-Scale Analytics: Automation Management

**Delivery Modality:** Self-Paced On-Demand (SPOD)

**Estimated Duration:** 2 hours

### Prerequisites & Assumed Knowledge

Completion of foundational New Scale Analytics courses is recommended.

### Course Description

This course introduces automation concepts within New Scale Analytics and how automated actions support consistent and scalable security operations. Learners gain a conceptual understanding of how automation complements analyst workflows without focusing on detailed configuration.

### Learner Paths

- Security Analyst
- Platform Admin

## NSA-202 — New Scale Analytics: Threat Detection Management

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 4 hours

### Prerequisites & Assumed Knowledge

Foundational familiarity with detections and investigation concepts is recommended.

### Course Description

This course explains how detections are created, evaluated, and improved within New Scale Analytics. Learners explore detection logic at a conceptual level, enabling better interpretation of alerts, improved feedback loops, and alignment between detection outcomes and operational goals.

### Learner Paths

- Security Analyst
- Platform Admin

## NSA-203 — New Scale Analytics: Parsing with Log Stream

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 3 hours

### Prerequisites & Assumed Knowledge

Foundational understanding of logs and security telemetry is recommended.

### Course Description

This course introduces parsing concepts in Log Stream and explains how data normalization supports reliable analytics, investigations, and reporting. The focus is on understanding data readiness and quality rather than hands on engineering.

### Learner Paths

- Platform Admin

## NSA-204 — New Scale Analytics: Improving Security Posture with Outcomes Navigator

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 1.5 hours

### Prerequisites & Assumed Knowledge

General familiarity with detections and operational metrics is recommended.

### Course Description

This course explains how Outcomes Navigator supports visibility into security posture, coverage, and effectiveness. Learners gain insight into how outcomes based views help teams assess progress, identify gaps, and communicate security value.

### Learner Paths

- Platform Admin

## NSA-205 — New Scale Analytics: Enrichment

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 1 hour

### Prerequisites & Assumed Knowledge

Understanding of security telemetry and investigation context is recommended.

### Course Description

This course introduces enrichment concepts and how contextual data improves the accuracy and usability of analytics. Learners understand how enrichment supports analyst effectiveness and reliable investigation outcomes.

### Learner Paths

- Platform Admin

## NSA-206 — New Scale Analytics: Dashboards, Visualization & Reporting

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 3 hours

### Prerequisites & Assumed Knowledge

Foundational familiarity with analytics concepts and operational metrics is recommended.

### Course Description

This course introduces dashboards and reporting capabilities in New Scale Analytics. Learners understand how visualizations support situational awareness, trend analysis, and operational communication across teams.

### Learner Paths

- Security Analyst
- Platform Admin

## NSA-207 — New Scale Analytics: Making Threat Center Work for You

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 1.5 hours

### Prerequisites & Assumed Knowledge

Completion of Threat Center foundational courses is recommended.

### Course Description

This course focuses on optimizing Threat Center usage to support efficient, repeatable investigations. Learners gain insight into best practices for triage, prioritization, and collaboration.

### Learner Paths

- Security Analyst
- Platform Admin

## NSA-208-1 — NSA DE Part 1: Deployment Planning

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 3 hours

### Prerequisites & Assumed Knowledge

Platform and data architecture familiarity is recommended.

### Course Description

This course introduces deployment planning concepts for New Scale Analytics, focusing on readiness, dependencies, and handoff to operational teams. It establishes the conceptual foundation for deployment activities.

### Learner Paths

- Deployment Engineer

## NSA-208-2 — NSA-DE Part 2: Platform Configuration

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 4 hours

### Prerequisites & Assumed Knowledge

Completion of NSA 208 1 is recommended.

### Course Description

This course builds on deployment planning by introducing platform configuration concepts for New Scale Analytics. Learners understand how configuration choices impact analytics quality, investigations, and operational stability.

### Learner Paths

- Deployment Engineer

## NSA-210 — New Scale Analytics: Support Fundamentals

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 3 hours

### Prerequisites & Assumed Knowledge

General familiarity with security platforms and troubleshooting concepts is recommended.

### Course Description

This course prepares technical support personnel to identify, diagnose, and resolve common issues in New Scale Analytics environments. It reinforces structured troubleshooting and escalation practices.

### Learner Paths

- None

## NSA-211 — New Scale Analytics: Risk Scoring — Support Fundamentals

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 3 hours

### Prerequisites & Assumed Knowledge

Completion of NSA 210 is recommended.

### Course Description

This course explains risk scoring concepts as they relate to support and troubleshooting workflows.

Learners gain a conceptual understanding of how risk scores are calculated and interpreted when assisting customers.

### Learner Paths

- None

## NSA-212 — New Scale Analytics: Troubleshooting & Operations — Support Fundamentals

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 4 hours

### Prerequisites & Assumed Knowledge

Completion of NSA 210 and NSA 211 is recommended.

### Course Description

This course addresses advanced troubleshooting and operational scenarios in New Scale Analytics environments. Learners strengthen systematic problem solving skills and escalation readiness.

### Learner Paths

- None

# New Scale SIEM (NSS)

## NSS Certification Paths

New Scale SIEM (NSS) Persona based certifications are defined for the following roles.

### SOC Roles

- Security Analyst

### Platform & Technical Roles

- Platform Administrator
- Deployment Engineer
- Technical Support Engineer

### Important Boundaries

Certification paths define the certification outcome for each persona and the courses and assessments required to validate readiness.

## NSS Learning Path – Required Classes

Required classes for each certification

### Security Analyst

(NSS-SA)

**Required courses:**

- NSS-101
- NSS-102
- NSS-201
- NSS-202

### Platform Administrator

(NSS-PA)

**Required courses:**

- NSS-101
- NSS-102
- NSS-201
- NSS-202
- NSS-203

### Deployment Engineer

(NSA-DE)

**Required courses:**

Prerequisite: All NSS-PA courses

- NSS-204

## NSS-101 — New Scale SIEM: Exabeam Essentials — Log Journey & Common Information Model

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 0.5 hours

### Prerequisites & Assumed Knowledge

No formal prerequisites. General familiarity with logs and security events is helpful.

### Course Description

This course introduces the Common Information Model (CIM) and explains how events move through the New Scale SIEM platform. Learners gain a foundational understanding of how normalized data enables consistent investigation, detection, and reporting experiences across security operations.

### Learner Paths

- Security Analyst
- Platform Admin

## NSS-102 — New Scale SIEM: Overview of the Exabeam Security Operations Platform

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 1 hour

### Prerequisites & Assumed Knowledge

No formal prerequisites.

### Course Description

This course provides a high level overview of the Exabeam Security Operations Platform, including key components and how they support detection, investigation, and response. It establishes shared understanding for technical and operational personas before role specific training.

### Learner Paths

- Security Analyst
- Platform Admin

## NSS-201 — New Scale SIEM: Introduction to Exabeam Search

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 2 hours

### Prerequisites & Assumed Knowledge

Completion of NSS 101 and NSS 102 or equivalent foundational SIEM familiarity is recommended.

### Course Description

This course introduces search concepts within New Scale SIEM, focusing on how analysts and administrators query, filter, and interpret log data. Learners gain conceptual understanding of effective search practices without diving into advanced optimization or tuning.

### Learner Paths

- Security Analyst
- Platform Admin

## NSS-202 — New Scale SIEM: Creating Dashboards and Correlation Rules

**Delivery Modality:** Instructor Led Training (ILT) / SPOD      **Estimated Duration:** 6 hours

### Prerequisites & Assumed Knowledge

Foundational familiarity with SIEM concepts, searches, and log data is recommended.

### Course Description

This course explains how dashboards and correlation rules are designed and used to support detection and monitoring in New Scale SIEM. Learners understand how visualizations and correlations reinforce situational awareness and operational decision making.

### Learner Paths

- Security Analyst
- Platform Admin

## NSS-203 — New Scale SIEM: Log Collection & Parsing

**Delivery Modality:** Instructor Led Training (ILT)      **Estimated Duration:** 8 hours

### Prerequisites & Assumed Knowledge

General understanding of logs and event sources is recommended.

### Course Description

This course introduces log onboarding and parsing concepts in New Scale SIEM. Learners gain insight into how data ingestion and normalization impact detections, investigations, and reporting, without focusing on deep engineering execution.

### Learner Paths

- Platform Admin

## NSS-204 — New Scale SIEM: Deploy Overview — SIEM & SLM

**Delivery Modality:** Instructor Led Training (ILT)      **Estimated Duration:** 8 hours

### Prerequisites & Assumed Knowledge

Completion of foundational New Scale SIEM courses is recommended.

### Course Description

This course provides a conceptual overview of deploying New Scale SIEM and Security Log Management (SLM). Learners understand deployment considerations, responsibilities, and operational readiness rather than step by step installation.

### Learner Paths

- Deployment Engineer

# LogRhythm SIEM (LRS)

## LRS Certification Paths

LogRhythm SIEM (LRS) certification paths reflect the on premises operating model, including **level based deployment certification** and limited analyst and support paths.

### SOC Roles

- Security Analyst

### Platform & Technical Roles

- Platform Administrator
- Deployment Engineer: Level based (L1, L2, L3)

### Important Boundaries

Certification paths define the certification outcome for each persona and the courses and assessments required to validate readiness.

## LRS Learning Path – Required Classes

Required classes for each certification

#### Security Analyst

(LRS-SA)

**Required courses:**

- LRS-101
- LRS-102
- LRS-104
- LRS-105
- LRS-205

#### Platform Administrator

(LRS-PA)

**Required courses:**

- LRS-101
- LRS-102
- LRS-103
- LRS-201
- LRS-202
- LRS-225
- LRS-226

#### Technical Support Engineer

(LRS-TSE)

**Required courses:**

Prerequisite: LRS-SA & LRS-PA

- LRS-321

#### Deployment Engineer 1

(LRS-DE-1)

**Required courses:**

Prerequisite: LRS-SA & LRS-PA

- LRS-221
- LRS-311

#### Deployment Engineer 2

(LRS-DE-2)

**Required courses:**

Prerequisite: LRS-DE-1

- LRS-222
- LRS-312

#### Deployment Engineer 3

(LRS-DE-3)

**Required courses:**

Prerequisite: LRS-DE-1

- LRS-223
- LRS-313

## LRS-100 — LogRhythm SIEM: What Is a SIEM?

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 0.5 hours

### Prerequisites & Assumed Knowledge

No formal prerequisites. No prior SIEM or LogRhythm experience required.

### Course Description

This course introduces the core concepts of Security Information and Event Management (SIEM) and its role in modern security operations. Learners gain a foundational understanding of what a SIEM is, how it collects and analyzes security data, and why it is a critical component of an effective cybersecurity program.

### Learner Paths

- None

## LRS-101 — LogRhythm SIEM: Introduction to LogRhythm SIEM

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 0.5 hours

### Prerequisites & Assumed Knowledge

No formal prerequisites. No prior SIEM or LogRhythm experience required.

### Course Description

This foundational course introduces core SIEM concepts and explains how LogRhythm implements the SIEM lifecycle. Learners gain a shared understanding of how security data is collected, analyzed, and used to support detection, response, and compliance across security operations. The course establishes a common baseline before progressing to role specific training.

### Learner Paths

- Security Analyst
- Platform Admin
- Technical Support Engineer

## LRS-102 — LogRhythm SIEM: Introduction to LogRhythm SIEM – Administrators and Analysts

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 0.5 hours

### Prerequisites & Assumed Knowledge

General familiarity with security or IT concepts is helpful but not required.

### Course Description

This course establishes role clarity by differentiating Administrator and Analyst responsibilities within a SOC. Learners gain conceptual understanding of LogRhythm SIEM architecture, core components, and how consoles align to operational roles, preparing them for focused administrator or analyst training paths.

### Learner Paths

- Security Analyst
- Platform Admin

## LRS-103 — LogRhythm SIEM: Foundations of the Client Console

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 1 hour

### Prerequisites & Assumed Knowledge

Completion of LRS 101 is recommended.

### Course Description

This course introduces the LogRhythm Client Console and its role in platform administration. Learners become familiar with navigation concepts, system health views, and foundational administrative capabilities required for safe and effective platform operation.

### Learner Paths

- Platform Admin

## LRS-104 — LogRhythm SIEM: Web Console – A Day in the Life of an Analyst

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 0.5 hours

### Prerequisites & Assumed Knowledge

Completion of LRS 101 or equivalent SIEM familiarity is recommended.

### Course Description

This course introduces analyst workflows in the LogRhythm Web Console, focusing on alert triage, investigation flow, and situational awareness. Learners gain an understanding of how analysts use the Web Console to support detection and response activities.

### Learner Paths

- Security Analyst

## LRS-105 — LogRhythm SIEM: SecondLook in the Web Console & Automated Maintenance

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 0.5 hours

### Prerequisites & Assumed Knowledge

Completion of LRS 104 is recommended.

### Course Description

This course introduces SecondLook functionality and automated maintenance concepts in the Web Console. Learners understand how archived data access and automated cleanup support investigation continuity and operational stability.

### Learner Paths

- Security Analyst

## LRS-106 — LogRhythm SIEM: What's New in LR SIEM

**Delivery Modality:** Computer Based Training (CBT)

**Estimated Duration:** 0.25 hours

### Prerequisites & Assumed Knowledge

Prior exposure to LogRhythm SIEM concepts is recommended.

### Course Description

This update focused course highlights recent LogRhythm SIEM enhancements and changes. It helps learners stay current without revisiting foundational content, supporting ongoing operational awareness.

### Learner Paths

- None

## LRS-201 — LogRhythm SIEM: LR Administration Fundamentals

**Delivery Modality:** Self Paced On Demand (SPOD) / Instructor Led Training (ILT)

**Estimated Duration:** 24 hours

### Prerequisites & Assumed Knowledge

Completion of LRS 101 and LRS 102 is recommended. General familiarity with SIEM concepts is expected.

### Course Description

This course provides foundational administrative knowledge required to operate and maintain the LogRhythm SIEM platform. Learners gain conceptual understanding of core services, data flow, system health, and configuration principles necessary for stable, secure operations.

### Learner Paths

- Platform Admin

## LRS-202 — LogRhythm SIEM: LR AI Engine Fundamentals

**Delivery Modality:** Self Paced On Demand (SPOD) / Instructor Led Training (ILT)

**Estimated Duration:** 8 hours

### Prerequisites & Assumed Knowledge

Completion of LRS 201 is recommended.

### Course Description

This course introduces the LogRhythm AI Engine (AIE) and explains how detection logic, rules, and analytics operate within the platform. Learners understand detection structure and intent without focusing on advanced tuning.

### Learner Paths

- Platform Admin

## LRS-205 — LogRhythm SIEM: LR Analyst Fundamentals

**Delivery Modality:** Self Paced On Demand (SPOD) / Instructor Led Training (ILT)

**Estimated Duration:** 8 hours

### Prerequisites & Assumed Knowledge

Completion of LRS 101 through LRS 104 is recommended.

### Course Description

This course provides foundational analyst training for LogRhythm SIEM, covering investigative workflows, alert interpretation, and case handling concepts. It prepares learners for consistent, defensible investigation practices in production environments.

### Learner Paths

- Security Analyst

## LRS-221 — LogRhythm SIEM: LRS DE1 Pre Bootcamp Preparation

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 12 hours

### Prerequisites & Assumed Knowledge

LRS-SA and LRS-PA certifications are required.

### Course Description

This course prepares learners for deployment bootcamps by establishing baseline knowledge of deployment expectations, architecture considerations, and readiness topics.

### Learner Paths

- Deployment Engineer

## LRS-225 — LogRhythm SIEM: Custom MPE Rules Using Regular Expressions

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 10 hours

### Prerequisites & Assumed Knowledge

Completion of AI Engine fundamentals is recommended. Familiarity with regular expressions is helpful.

### Course Description

This course introduces custom MPE rule creation using regular expressions, focusing on detection flexibility and customization while reinforcing safe, structured rule design principles.

### Learner Paths

- Platform Admin

## LRS-226 — LogRhythm SIEM: Threat Detection with AI Engine

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 8 hours

### Prerequisites & Assumed Knowledge

Completion of LRS 202 is required.

### Course Description

This course expands on threat detection concepts using AI Engine, reinforcing how behavioral detections support operational security outcomes.

### Learner Paths

- Platform Admin

## LRS-311 — LogRhythm SIEM: LRS DE1 Bootcamp — Deployment & Upgrade

**Delivery Modality:** Instructor Led Training (Bootcamp)

**Estimated Duration:** 40 hours

### Prerequisites & Assumed Knowledge

Completion of LRS 221 and deployment fundamentals and exam are required.

### Course Description

This intensive bootcamp focuses on hands on LogRhythm SIEM deployment, upgrade, and validation scenarios. It prepares learners for real world deployment responsibilities under guided instruction.

### Learner Paths

- Deployment Engineer 1

## LRS-222 / LRS-312— LRS-DE-2 High Availability Pre Preparation & Bootcamp

**Delivery Modality:** SPOD / ILT

**Estimated Duration:** 8 hours (SPOD) / 32 hours (Bootcamp)

### Prerequisites & Assumed Knowledge

LRS-DE-1 certification is required.

### Course Description

These courses address high availability deployment concepts and validate learner readiness to design and support resilient LogRhythm architectures.

### Learner Paths

- Deployment Engineer 2

## LRS-223 / 313 — Disaster Recovery Preparation & Bootcamp

**Delivery Modality:** SPOD / ILT      **Estimated Duration:** 8 hours (SPOD) / 24 hours (Bootcamp)

### Prerequisites & Assumed Knowledge

LRS-DE-1 certification is required.

### Course Description

These courses focus on disaster recovery concepts and execution, preparing learners to design, deploy, and validate resilient DR environments.

### Learner Paths

- **Deployment Engineer 3**

## LRS-321 / 321-E / 321-PE — LogRhythm SIEM: Support Engineer Tier 1 Path

**Delivery Modality:** SPOD / Exam      **Estimated Duration:** 4 hours (SPOD) / 1.5 hours (Exam)

### Prerequisites & Assumed Knowledge

LRS-SA and LRS-PA certifications are required.

### Course Description

These courses prepare Tier 1 Support Engineers to diagnose, triage, and resolve frontline LogRhythm platform issues using structured troubleshooting workflows.

### Learner Paths

- **T1 Technical Support Engineer**

## NET-101 — Network Monitor: Intro to Network Monitor — Configuration & Management

**Delivery Modality:** Self Paced On Demand (SPOD)

**Estimated Duration:** 6 hours

### Prerequisites & Assumed Knowledge

General understanding of networking and security concepts is recommended.

Familiarity with SIEM platforms is helpful but not required.

### Course Description

This foundational course introduces Network Monitor (NetMon), Exabeam's network monitoring and security analytics solution. Learners gain practical knowledge for deploying, configuring, and managing NetMon to improve network visibility and integrate network telemetry with SIEM platforms. The course emphasizes operational readiness, including traffic ingestion validation, metadata analysis, SIEM integration, and basic maintenance and troubleshooting.

### Learner Paths

- **Deployment Engineer 3**