DATA SHEET

Skyhigh DSPM: Getting Started

Audience
Security Analysts, Admins, Deployment Partners

Recommended Pre-Work
Basic understanding of Skyhigh SSE, Data Classification methods, data exposure risks involving shadow IT, unsanctioned web destinations, and external sharing.

Course Overview

This is a story-driven course designed for security analysts, admins, and deployment partners. Learn to continuously discover, prioritize, and remediate data risks across SaaS, cloud, web, and AI tools like ChatGPT and Microsoft Copilot. Using Data Explorer (Chart and Table Views), you will master a repeatable Ask, Filter, Read, Act investigation playbook, interpret Object Risk Scores, track sensitive data movements, and link visibility findings directly to Skyhigh SSE policy enforcement controls.

Course Agenda

Module 0: Course Details and Objectives

Module 1: Why DSPM? - The Skyhigh Way

Module 2: Getting Started

Module 3: Tour Data Explorer

Module 4: Read the Object Risk Score

Module 5: Investigate with playbooks

Module 6: From insight to protection

Module 7: Wrap-up and your 30-day plan

Module P: Help your customer get value (Optional Partner Track)

Course Objectives

Course Details and Objectives

Introduces the course format, learning outcomes, and core framework. Follows a real-world enterprise investigation scenario to ground how analysts identify sensitive data sprawl, evaluate access risks, and prioritize remediation.

Module 1: Why DSPM? - The Skyhigh Way

Understand the fundamentals of Data Security Posture Management (DSPM), how it continuously discovers sensitive data across SaaS, cloud, web, and AI, and how it complements Skyhigh DLP enforcement.

Module 2: Getting Started

Learn how to access Data Explorer, verify active data feeds and scans, and apply key search practices to locate sensitive objects quickly.

Module 3: Tour Data Explorer

Master navigating Chart View for high-level risk triage and Table View for detailed file investigations, using powerful multi-attribute filters and detail panels.

Module 4: Read the Object Risk Score

Learn how the 1-to-9 Object Risk Score evaluates content sensitivity and user/service context to surface high-priority risks, and what triggers dynamic score recalculations.

Module 5: Investigate with Playbooks

Apply a repeatable Ask, Filter, Read, Act investigation playbook to address real-world scenarios, including unsanctioned cloud apps, risky user activity, and renamed file tracking.

Module 6: From Insight to Protection

Close the loop between visibility and enforcement by connecting Data Explorer findings directly to Skyhigh SSE policies, governing GenAI tools (ChatGPT and Microsoft Copilot), and streamlining remediation.

Module 7: Wrap-Up and Your 30-Day Plan

Consolidate your learning with an actionable 30-day rollout plan tailored to your industry's compliance needs.

Module P: Help Your Customer Get Value (Optional Partner Track)

Designed for deployment partners to run structured DSPM risk reviews, deliver tailored Sensitive Data Risk Reports, and lead outcome-focused conversations with customer stakeholders.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

Skyhigh Security is a registered trademark of Musarubra US LLC. Other names and brands are the property of these companies or may be claimed as the property of others. Copyright © 2026.