Skyhigh Security Cloud Fundamentals

Course Description Datasheet

Course Overview

The Skyhigh Security Cloud Fundamentals course is designed to introduce you to the concepts, architecture, user interface, and administration of Skyhigh Security Cloud and associated products. Skyhigh Security products and capabilities explained in this course include the Skyhigh Security Cloud Platform, Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Infrastructure as a Service (IAAS), Software as a Service (SAAS), Shadow IT, and Cloud Native Application Protection Platform (CNAPP). Each of these products and capabilities are integral to the Security Service Edge (SSE) product and security philosophy.

This eLearning course includes open topic navigation which allows students to move freely between any topics of interest to them at any time. Also, Skill Practice activities are included to help students practice the skills and concepts learned in their own Skyhigh Security environment. Course progress is saved each time a student exits the course so it does not have to be completed in a set time limit or within one session. Completion of the course is awarded when all topics are reviewed.

Example Course Objectives are provided in the next section of the datasheet. For a more complete outline of the course, register for the course in the learning portal.

Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with cloud asset security.

Recommended Pre-Work

- Knowledge of common cloud product administration including Microsoft Office 365, Amazon Web Services (AWS)
- Understanding of common security issues facing complex cloud environments including Shadow IT and Data Loss threats
- Knowledge of cloud infrastructure and service connection in order to connect cloud products

Example Course Objectives

Overview
Analyze key use cases and drivers for application of Skyhigh Security Cloud in a customer environment.

Interface
Perform configuration of a Saved View for use in a customer environment.

Administration
Evaluate critical infrastructure displays available in Skyhigh Security Cloud

Cloud Connector
Perform download and install of Skyhigh Security Cloud Connector

Connecting Services
Describe how Skyhigh Security Cloud integrates with Infrastructure-as-a-Service (IaaS).

Classifying Data
Define various data identifiers used in an Skyhigh Security Cloud environment.

Data Loss Prevention
Create a basic Data Loss Prevention policy for use in a customer environment.

Data Loss Prevention for Email
Summarize the Data Loss Prevention capabilities of Skyhigh Security Cloud in cloud email applications.

Cloud Access Protection
Summarize the Cloud Access Protection capabilities of Skyhigh Security Cloud.

Analytics
Identify uses of Analytics in a customer environment

Example Course Objectives

User Activity
Identify key activity monitoring information available, including users, activities, activity categories, and anomalies.

Threat Protection
Identify potential threat protection issues that Skyhigh Security Cloud will address in a customer environment.

Shadow IT
Summarize the Skyhigh Security Cloud features for "Shadow IT."

Anomalies
Explain the role of Cloud Trust Registry in identifying the Cloud Service Provider's risk scores

Incidents
Configure Incident Management controls for use in a customer environment

Configuration Audit
Construct a configuration audit for a cloud environment.

On Demand Scans
Identify potential data breaches for data that is stored cross CSPs and various IaaS platforms

Dashboard and Reporting
Construct a Dashboard scheme, which would be useful to various job functions in Skyhigh Security Cloud.

CNAPP and Container Security
Analyze the impact of Cloud Native Application Platform Protection (CNAPP) on a customer security environment

Advanced Topics
Describe supported application programming interface (API) calls to gather data from Skyhigh Security Cloud.