Skyhigh Security Service Edge Administration

Course Description Datasheet

Course Overview

The Skyhigh Security Service Edge Administration course provides in-depth training on Skyhigh Security Cloud and related cloud products. The course covers on configuration and administration of critical Security Service Edge (SSE) functions. It also walks through the components to help participants identify, define, and refine use cases based on specific scenarios. Products and capabilities covered in this course include the Skyhigh Security Cloud platform, Skyhigh Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Infrastructure as A Service (IAAS), Software as a Service (SAAS), Shadow IT, Remote Browser Isolation (RBI), Cloud Native Application Protection Platform (CNAPP), and Private Access (ZTNA).

Agenda At A Glance

Day 1

- Welcome
- Skyhigh Security Cloud Overview
- Skyhigh Security Cloud Interface
- Administration
- Cloud Connector
- Connecting Services
- SSE Principles
- Web Gateway Setup

Day 2

- Web Policy
- Web Policy Part 2
- Web Policy Part 3
- Remote Browser Isolation
- Web Analytics
- Cloud Access Protection
- Classifying Data
- DLP Policies
- Data Loss Prevention for Email

Day 3

- Analytics
- User Activity
- Threat Protection
- Shadow IT
- Anomalies
- Incidents

Day 4

- Configuration Audit
- On Demand Scans
- Dashboards and Reporting
- CNAPP and Container Security
- Private Access
- Advanced Topics

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

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

Skyhigh Security Cloud 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).

SSE Principles
Identify key customer concerns addressed by Security Service Edge

Web Gateway Setup
Construct a web gateway setup as per customer requirements

Web Policy
Identify concepts which apply to policy in Unified Cloud Edge and important feature configurations.

Web Policy Part 2
Analyze the impact of various web polices and features.

Web Policy Part 3
Analyze the impact of various web polices and features.

Remote Browser Isolation
Perform configuration of Remote Browser Isolation Rules in a simulated environment

Web Analytics
Create views to show priority information found in Web Analytics

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

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

Example Course Objectives

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

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

Private Access
Identify the steps required to configure Private Access

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

Skyhigh Security