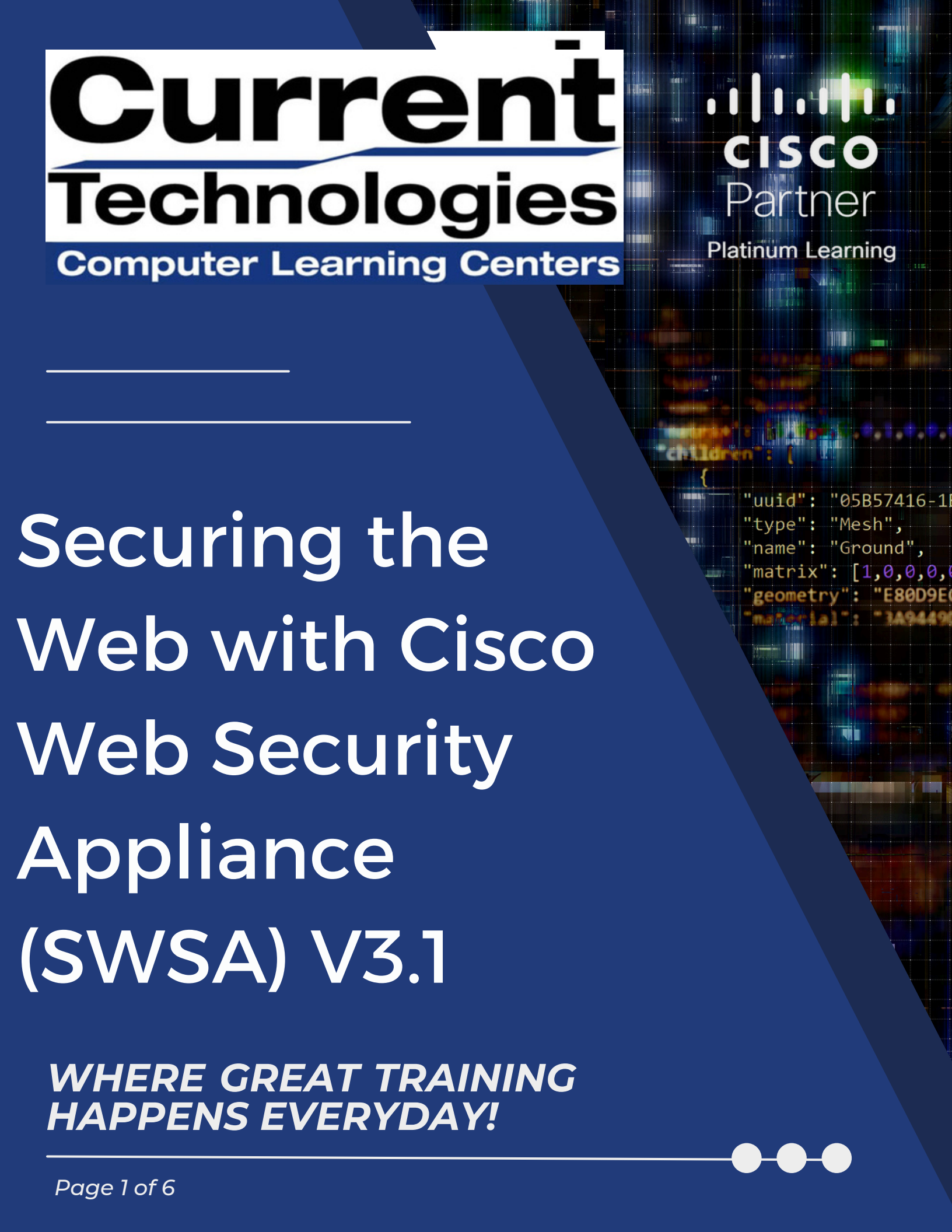
Current Technologies
Computer Learning Centers

cisco Partner
Platinum Learning



Securing the Web with Cisco Web Security Appliance (SWSA) V3.1

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Securing the Web with Cisco Web Security Appliance (SWSA) V3.1

Course Duration

2 Days

Course Price

$1,995.00
20 CLCs

Methods of Delivery

In-Person ILT
Virtual ILT
Onsite ILT

About this Class

The Securing the Web with Cisco Web Security Appliance (SWSA) v3.1 course shows you how to implement, use, and maintain Cisco® Web Security Appliance (WSA), powered by Cisco Talos, to provide advanced protection for business email and control against web security threats. Through a combination of expert instruction and hands-on practice, you'll learn how to deploy proxy services, use authentication, implement policies to control HTTPS traffic and access, implement use control settings and policies, use the solution's anti-malware features, implement data security and data loss prevention, perform administration of Cisco WSA solution, and more.This course helps you prepare to take the exam, Securing the Web with Cisco Web Security Appliance (300-725 SWSA), which leads to CCNP® Security and the Cisco Certified Specialist - Web Content Security. This course also earns you 16 Continuing Education (CE) credits towards recertification.

Securing the Web with Cisco Web Security Appliance (SWSA) V3.1

How you will benefit

This class will help you:

- Implement Cisco WSA to secure web gateways, provide malware protection, and use policy controls to address the challenges of securing and controlling web traffic
- Gain valuable hands-on skills focused on web security
- Earn 16 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

- Security Architects
- System Designers
- Network Administrators
- Operations Engineers
- Network Managers, Network or Security Technicians, and Security Engineers and Managers responsible for web security
- Cisco Integrators and Partners

Prerequisites

To fully benefit from this course, you should have knowledge of these topics:

- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- IP routing

Securing the Web with Cisco Web Security Appliance (SWSA) V3.1

Objectives

Upon completing this course, the student will be able to meet these objectives:

- Describe Cisco WSA
- Deploy proxy services
- Utilize authentication
- Describe decryption policies to control HTTPS traffic
- Understand differentiated traffic access policies and identification profiles
- Enforce acceptable use control settings
- Defend against malware
- Describe data security and data loss prevention
- Perform administration and troubleshooting

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Securing the Web with Cisco Web Security Appliance (SWSA) V3.1

Course Outline

- Module 1: Describing Cisco WSA
- Module 2: Deploying Proxy Services
- Module 3: Utilizing Authentication
- Module 4: Creating Decryption Policies to Control HTTPS Traffic
- Module 5: Understanding Differentiated Traffic Access Policies and Identification Profiles
- Module 6: Defending Against Malware
- Module 7: Enforcing Acceptable Use Control Settings
- Module 8: Data Security and Data Loss Prevention
- Module 9: Performing Administration and Troubleshooting
- Module 10: References

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Securing the Web with Cisco Web Security Appliance (SWSA) V3.1

Lab Outline

- Lab 1: Configure the Cisco Web Security Appliance
- Lab 2: Deploy Proxy Services
- Lab 3: Configure Proxy Authentication
- Lab 4: Configure HTTPS Inspection
- Lab 5: Create and Enforce a Time/Date-Based Acceptable Use Policy
- Lab 6: Configure Advanced Malware Protection
- Lab 7: Configure Referrer Header Exceptions
- Lab 8: Utilize Third-Party Security Feeds and MS Office 365 External Feed
- Lab 9: Validate an Intermediate Certificate
- Lab 10: View Reporting Services and Web Tracking
- Lab 11: Perform Centralized Cisco AsyncOS Software Upgrade Using Cisco SMA