SECACC - Administering and Troubleshooting Cisco Secure Access Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Build practical skills to implement, operate, and optimize Cisco Secure Access, zero trust and SASE solutions across hybrid networks with visibility automation and security analytics.

This comprehensive 5 Day training program provides an end-to-end understanding of Cisco cloud security, with Cisco Secure Access as the central platform supporting Secure Internet Access, Secure Private Access, Zero Trust Access, and traditional VPN services. The course begins by establishing foundational knowledge of cloud security, the evolution of networking and security architectures, SASE concepts, and zero-trust principles, then transitions to hands-on management using Cisco Security Cloud Control. Learners gain deep exposure to Cisco Secure Access architecture, deployment planning, protocols, authentication, and core services such as SIA and SPA, followed by structured onboarding, subscription management, and initial configuration workflows. The curriculum expands to include managing virtual appliances across on-premises and cloud environments, implementing DNS Defense, and integrating identity via directories, Active Directory, and SAML providers to enable identity-driven access decisions. Advanced integrations with Cisco ISE, Catalyst SD-WAN, Meraki MX, and Cisco Secure Firewall demonstrate how Secure Access operates within hybrid enterprise networks. Learners then build operational expertise by configuring network connections, tunnels, Cisco Secure Client for Zero Trust Access, and VPN use cases, and managing networks, objects, and security settings, including posture, IPS, malware protection, decryption, and data loss prevention. The course culminates in in-depth policy creation for SIA, SPA, and ZTA; visibility through Digital Experience Insights and ThousandEyes; extensive monitoring, logging, reporting, and troubleshooting workflows; and, finally, automation and intelligence using Secure Access APIs and AI. By the end, learners are equipped to design, deploy, secure, monitor, automate, and optimize Cisco Secure Access in real-world enterprise environments while supporting modern zero-trust and SASE strategies at scale.

Who Should Attend?

Highly recommended attendees include:

- **Network Engineers:**
  Those engaged in designing, implementing, and maintaining security infrastructures. This encompasses the integration of SASE components to achieve a secure, streamlined network architecture that supports both traditional and cloud-based applications while meeting operational standards.
- **System Administrators:**
  Key players in the day-to-day operations, configuration, and management of network systems. Their pivotal role extends to ensuring the seamless operation of SASE configurations across different departments, contributing to the overarching network security.
- **IT Professionals:**
  A diverse group of IT staff within Companies needing a comprehensive grasp of SASE for secure, reliable cloud security systems. Their responsibility lies in maintaining network compliance with strict regulations and standards.
- **Technical Support Staff:**
  Frontline support personnel who address and resolve technical issues within SASE-enabled network systems in network settings. Their proficiency is vital in upholding network integrity and security, ensuring uninterrupted service.
- **Cisco Certified Professionals:**

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Individuals holding Cisco certifications and aspiring to deepen their SASE knowledge and skills. This course offers an opportunity to specialize in SASE solutions, significantly enhancing their capabilities in addressing network security requirements.

Training Outline

Module 1: Introduction to Cisco Cloud Security

- Lesson 1: Cloud Security Overview
- Lesson 2: Evolution of Networking and Security
- Lesson 3: Overview of SASE (Secure Access Service Edge)
- Lesson 4: Umbrella vs Secure Access vs Secure Connect
- Lesson 5: Zero Trust Access (ZTA) / Zero Trust Network Access (ZTNA)

Module 2: Introduction to Cisco Secure Access

- Lesson 1: Introduction to Cisco Secure Access
  - Platform Architecture
  - Secure Access Licensing
  - Network Requirements for Secure Access
  - Service Levels and Support:
  - Secure Access Regions
- Lesson 2: Secure Access features
  - Clientless Zero Trust Access (ZTA)
  - Client-Based Zero Trust Access (ZTA)
  - VPN as a Service (VPNaaS)
  - Unified Private Access
  - Firewall as a Service (FWaaS)
  - Intrusion Prevention System (IPS)
  - Experience Insights: Digital Experience Monitoring (DEM)
  - Domain Name System (DNS) Security
  - Secure Web Gateway (SWG)
  - Multimode Malware Protection
  - Cloud Access Security Broker (CASB)
  - Multimode Data Loss Prevention (DLP)
  - Remote Browser Isolation (RBI)
- Lesson 3: Cisco SD-WAN Integration Overview
- Lesson 4: Cisco Meraki Integration Overview
- Lesson 5: Secure Private Access
  - Via VPN
    - Via ZTNA (Client Based)
    - Via ZTNA Clientless
    - Branch to RA user
  - Secure Intemet Access
    - VPN full tunnel
    - Branch traffic
    - Roaming
- Lesson 6: Cisco Secure Client Integration Overview

Module 3: Secure Cloud Control

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Lesson 1: Security Cloud Control Overview
  - Mission and Objectives
  - Customer Benefits
  - Strengths & Differentiators
  - Core Services
  - Managed Products
  - Platform Navigator
- Lesson 2: Secure Cloud Control Organizations
  - Organization Overview
  - Organization Creation
  - Multiple Organizations Use Cases
  - Organization Management
- Lesson 3: Secure Cloud Control Subscriptions
  - Claiming and Activation Process
  - Customer Onboarding
  - Enterprise and Region Selection
  - Claim Process Walkthrough
  - Activation and Provisioning
- Lesson 4: Secure Cloud Control User Management
  - Unified User Management
  - Granular Control
  - Administrator Access
  - Identity Provider (IdP) Integration
- Lesson 5: Network Connectivity
  - Connectivity requirements for SCC operations
  - Secure flows and policy enforcement
  - Integration of network infrastructure with SCC
- Lesson 6: Integrating Identity Providers
  - Unified User Experience
  - Login Security
  - IdP Setup Process

Module 4: Onboarding and Initial Configuration of Cisco Secure Access

- Lesson 1: Accessing Cisco Secure Access
- Lesson 2: Security Cloud Sign-On
  - Multi-factor authentication (MFA) for enhanced security
  - Find Your Organization ID
- Lesson 3: Secure Access Single Sign-On Authentication
  - Configure Single Sign-On Authentication
  - Troubleshoot Single Sign-On Authentication
- Lesson 4: Secure Access Initial Workflow
  - Configure Network Connections
    - Task 1 - Add Network Connections
    - Task 2 - Provision Users and Groups
    - Task 3-Configure Integrations with SAML Identity Providers
  - Configure Access to Resources
    - Task 1-Set Up Private Resources
    - Task 2- Configure Rule Defaults and Global Settings
    - Manage Rule Defaults
    - Manage Global Settings
    - Task 3 - Add a Policy Rule

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

    - Configure End User Connectivity
        - Task 1 - Configure Zero Trust
        - Task 2- Configure Virtual Private Networks
        - Task 3 - Configure Intemnet Security
    - Configure Endpoints and Network Sources
        - Add Networks to Secure Access
        - Set Up the Cisco Secure Client
        - Add IPS Profiles
        - Configure Rule Profiles
    - Secure Access Overview Dashboard
        - Experience Insights
        - Connectivity
        - Data Transfer
        - Security
        - Users and Groups
        - Private Resources

Module 5: User Management and Authentication

- Lesson 1: Manage Users and Groups
    - View User Details
    - View Group Details
    - View Organizational Unit Details
    - Unenroll Devices for Client-Based Zero Trust Access
    - Disconnect Remote Access VPN Sessions
- Lesson 2: Manage User Directories
    - Configure User Directory Integrations
    - Manage Cloud Identity Providers
    - Import Users and Groups from CSV File
    - Manage Active Directory Integration
    - Manage Google Workspace Account
    - Manage Imported Users and Groups
    - Learn to enhance security with contextual factors like geolocation, device posture, and user behavior analysis
- Lesson 3: Provision Users and Groups from Active Directory
    - Prerequisites for AD Connectors
    - Connect Multiple Active Directory Domains
    - Manage AD Components
        - Add AD Components in Secure Access
        - Manage Sites for AD Components
        - View AD Components in Secure Access
        - Delete AD Components
    - Manage AD Connectors
        - Configure Authentication for AD Connectors and VAs
        - Configure Updates on AD Connectors
        - Connect Active Directory to Secure Access
        - Deploy LDIF Files for AD Connector
        - Change the Connector Account Password
        - AD Connector Communication Flow and Troubleshooting
    - AD Integration with Virtual Appliances
        - Prerequisites for AD Connectors and VAs
        - Prepare Your AD Environment

BILGINC IT Academy
info@bilginc.com
bilginc.com

        - Connect Active Directory to VAs
        - Multiple AD Domains with Secure Access Sites
- Lesson 4: Manage User Authentication Profiles
    - Add User Authentication Profiles
    - About Single Sign-On for Users
    - Edit User Authentication Profile
    - Delete User Authentication Profile
- Lesson 5: Configure Integrations with SAML Identity Providers
    - Prerequisites for SAML Authentication
    - Configure Microsoft Entra ID for SAML
    - Configure Okta for SAML
    - Configure AD FS for SAML
    - Configure Duo Security for SAML
    - Configure Ping Identity for SAML
    - Configure OpenAM for SAML
    - SAML Certificate Renewal Options
    - Test SAML Identity Provider Integration

Module 6: DNS Forwarders

- Lesson 1: Virtual Appliances Overview
    - Prerequisites for Virtual Appliances
    - Virtual Appliance Deployment Guidelines
    - Virtual Appliance Sizing Guide
- Lesson 2: Manage VAs in Secure Access
    - Configure Authentication for Virtual Appliances
    - Manage DNS Forwarders
    - Manage Site for Virtual Appliance
    - Configure Updates for Virtual Appliances
- Lesson 3: Deploy Virtual Appliances
    - Deploy VAs in Hyper-V for Windows 2012 or Higher
    - Deploy VAs in VMware
    - Deploy VAs in Microsoft Azure
    - Deploy VAs in Amazon Web Services
    - Deploy VAs in Google Cloud Platform
    - Deploy VAs in KVM
    - Deploy VAs in Nutanix
- Lesson 4: Configure Virtual Appliances
    - Configure Settings on VAs
- Lesson 5: Local DNS Forwarding
- Lesson 6: Test Virtual Appliance Deployments
- Lesson 7: SNMP Monitoring for Virtual Appliances
- Lesson 8: Troubleshoot Virtual Appliances

Module 7: Network Connections

- Lesson 1: Network Connection Overview
- Lesson 2: Network Requirements
    - Secure Access DNS Resolvers
    - Secure Access Encrypted DNS Queries
    - Secure Access DNS - Block Pages
    - Secure Access DNS and Web - Client Configuration Services
    - Secure Access DNS and Web - Client Sync Services

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

    - Secure Access DNS and Web - Client Certificate Revocation Services
    - Cisco Secure Client and Captive Portal Detection
    - Cisco Secure Client and Device Hostnames
    - TLS Protocol Requirements
    - Secure Access Secure Web Gateway Services
    - Secure Access Realtime DLP Secure ICAP
    - Secure Access SaaS Tenants
    - Secure Access SAML Gateway Services
    - Secure Access SAML Identity Provider Domains
    - Secure Access SAML Gateway Client Certificate Revocation Services
- Lesson 3: Secure Access VPN Services
    - Secure Access VPN Client Certificate Revocation Services
    - Secure Access Zero Trust Client-Based Enrollment Services
    - Secure Access Zero Trust Client-Based Proxy Services
    - Secure Access Zero Trust Client-Based Proxy - Client Certificate Revocation Services
    - Secure Access Zero Trust Proxy Services - Unmanaged Devices
    - Secure Access Resource Connectors
- Lesson 4: Secure Access NAT as a Service
    - Web Traffic and NATaaS
    - Non-Web Traffic and NATaaS
    - Reserved IP
    - Best Practices
- Lesson 5: Manage Network Connections
    - IPsec Network Tunnels
    - Resource Connector Groups
        - Resource Connectors (Deployed in Connector Groups)
        - Network Tunnels (Deployed in Network Tunnel Groups)
- Lesson 6: Manage Network Tunnel Groups
    - Device Compatibility and Network Tunnels
    - Add a Network Tunnel Group
    - Delete a Network Tunnel Group
    - Edit a Network Tunnel Group
    - View Network Tunnel Group Details
    - Supported IPsec Parameters
- Lesson 7: Network Tunnel Configuration
    - Establish a Tunnel
    - Tunnel Size
    - Maximum Transmission Unit Size
    - Client Reachable Prefixes
    - Throughput and Multiple Tunnels

Module 8: SD-WAN Integration

- Lesson 1: Cisco SD-WAN Overview
- Lesson 2: Catalyst SD-WAN Security
- Lesson 3: Configure Tunnels with Cisco Catalyst SD-WAN
    - Cisco Catalyst SD-WAN SD-WAN Prerequisites
    - Configure Tunnel in Secure Access
    - Configure Cisco Catalyst SD-WAN Templates
    - Configure Cisco Catalyst SD-WAN Configuration Groups
    - Configure Static Routes
    - Verify Tunnel Status

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Lesson 4: Configure Tunnels with Meraki MX
  - Meraki MX Prerequisites
  - Caveats and Considerations
  - Supported Use Cases and Requirements
  - Add a Network Tunnel Group in Secure Access
  - Configure a Tunnel in Meraki MX
  - Verification and Troubleshooting

Module 9: Managing Secure Access Networks and Objects

- Lesson 1: End-User Connectivity
- Lesson 2: Traffic Steering for Zero Trust Access Client-Based Connections
  - Using Wildcards to Configure Traffic Steering for Private Destinations
- Lesson 3: Remote Access Virtual Private Networks
  - FQDNs for Network Connections
  - Manage IP Pools
  - Add an IP Pool
  - Manage VPN Profiles
  - Add VPN Profiles
  - Add a RADIUS Group
  - Manage Machine Tunnels
- Lesson 4: Internet Security
  - Set Up Internet Security on User Devices
  - Manage Internet Security Bypass
    - Add Destinations for Internet Security Bypass
    - Edit Destination for Internet Security Bypass
    - Delete Destination for Internet Security Bypass
  - Configure Cisco Secure Client Settings
- Lesson 5: PAC Files
  - Deploy the Secure Access PAC File for Windows
  - Deploy the Secure Access PAC File for macOS
  - Customize the Secure Access PAC File
  - Upload Custom PAC Files to Secure Access
- Lesson 6: Proxy Chaining
  - Forwarded-For (XFF) Configuration
- Lesson 7: Registered Networks
  - Add Network Resources
  - Point Your DNS to Cisco Secure Access
  - Clear Your DNS Cache
  - Update a Network Resource
  - Delete a Network Resource
- Lesson 8: Internal Networks
  - Add Internal Network Resources
  - Update an Internal Network Resource
  - Delete an Internal Network Resource
- Lesson 9: Sites
- Lesson 10: Destination Lists
  - Add a Destination List
  - Upload Destinations From a File
  - Edit a Destination List
  - Download Destinations to a CSV File
  - Control Access to Custom URLs

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

    - Wildcards in Destination Lists
    - Add Top-Level Domains to Destination Lists
    - Add Punycode Domain Name to Destination List
    - Troubleshoot DNS Destination Lists
- Lesson 11: Application Lists
    - Add an Application List
    - Application Categories
    - Delete an Application List
- Lesson 12: Content Category Lists
    - Available Content Categories
    - Add a Content Category List
    - Request a Category for an Uncategorized Destination
    - Dispute a Content Category
    - View Content Categories in Reports
- Lesson 13: Tenant Control Profiles
    - Add a Tenant Controls Profile
    - Control Cloud Access to Microsoft 365
    - Control Cloud Access to Google G Suite
    - Control Cloud Access to Slack
    - Control Cloud Access to Dropbox
    - Use Tenant Controls in Access Rules
    - Review Tenant Controls Through Reports
- Lesson 14: Roaming Devices
    - View Internet Security Settings for Roaming Devices
    - Edit Internet Security Settings for Roaming Devices
    - Delete a Roaming Device
- Lesson 15: Private Resources
    - Add a Private Resource
    - Add a Private Resource Group
    - Private Resource Configuration Examples
- Lesson 16: Connections to Private Destinations
    - Comparison of Zero Trust Access and VPN
    - Comparison of Client-Based and Browser-Based Zero Trust Access Connections
    - Requirements for Zero Trust Access
    - Network Authentication for Zero Trust Access
    - Manage Branch Connections
    - Allow SSH and RDP Access to Private Resources
- Lesson 17: Network and Service Objects
    - Network Objects
        - Add Network Objects
        - Edit a Network Object
        - Manage Details of a Network Object
        - Delete a Network Object
    - Network Object Groups
        - Add Network Object Groups
        - Edit a Network Object Group
        - Manage Details of a Network Object Group
        - Delete a Network Object Group
    - Service Objects
        - Add Service Objects
        - Edit a Service Object
        - Manage Details of a Service Object

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

        - Delete a Service Object
    - Service Object Groups
        - Add Service Object Groups
        - Edit a Service Object Group
        - Manage Details of a Service Object Group
        - Delete a Service Object Group

Module 10: Configuring Access Policies and Access Rules

- Lesson 1: Secure Access - Access Policies
    - Access Policy Overview
    - Show Additional Data on Your Access Rules
    - Edit the Order of the Rules in Your Access Policy
    - Rule Defaults: Default Settings for Access Rules
    - Global Settings for Access Rules
    - Edit Rule Defaults and Global Settings
    - Edit the Default Access Rules
    - Using Wildcard Masks on Access Rules
- Lesson 2: Internet Access Rules
    - Components for Internet Access Rules
    - Default Settings for Internet Access Rules
    - Add an Internet Access Rule
    - About Configuring Sources in Internet Access Rules
    - About Configuring Destinations in Internet Access Rules
    - Ensure Rule Matching for Encrypted Internet Traffic
    - Block Internet Access to Geographic Locations
    - Advanced Application Controls
    - Global Settings for Internet Access Rules
    - About Isolated Destinations
- Isolate Downgrade
    - Troubleshoot Internet Access Rules
    - Zero Trust Access to Internet Destinations
- Lesson 3: Private Access Rules
    - Components for Private Access Rules
    - Default Settings for Private Access Rules
    - Add a Private Access Rule
    - About Configuring Sources in Private Access Rules
    - About Configuring Destinations in Private Access Rules
    - About Endpoint Requirements in Access Rules
    - Allowing Traffic from Users and Devices on the Network
    - Global Settings for Private Access Rules
    - View Rules Associated with a Private Resource
    - Troubleshoot Private Access Rule

Module 11: Cisco Secure Client

- Lesson 1: Cisco Secure Client Overview
- Lesson 2: Managing Client-based Zero Trust Access from Mobile Devices
    - Set up the Zero Trust Access App for iOS Devices
    - Set up the Zero Trust Access App for Android Devices
    - Set up the Zero Trust Access App for Android on Samsung Devices
    - Monitor and Troubleshoot the Zero Trust Access App from Mobile Devices
- Lesson 3: Cisco Secure Client on Windows and macOS Devices

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

    - Download Cisco Secure Client
    - Install the Root Certificate for All Browsers
    - Install the Cisco Secure Client
- Lesson 4: Internet Security on Cisco Secure Client
    - Download the OrgInfo.json File
    - Umbrella Roaming Security Module Requirements
    - Domain Management
    - Interpret Internet Security Diagnostics
    - IPv4 and IPv6 DNS Protection Status
    - Customize Windows Installation of Cisco Secure Client
    - Customize macOS Installation of Cisco Secure Client
- Lesson 5: Manage Zero Trust Access using Cisco Secure Client on Windows and macOS Devices
    - Requirements for Secure Client with Zero Trust Access
    - Invite Users to Enroll in Zero Trust Access for Secure Client
    - Troubleshoot Client-Based Zero Trust Access
    - Completely Remove Zero Trust Access from a Device
- Lesson 6: Manage Virtual Private Networks on Cisco Secure Client
    - Download the Virtual Private Network XML Profile
    - CA Certificates for VPN Connections
- Lesson 7: Cisco Security for Chromebook Client
    - Cisco Security for Chromebooks
    - Prerequisites for Cisco Security for Chromebooks Client
    - Deploy the Cisco Security for Chromebooks Client
    - Enable Reporting for Private IP Addresses of Chromebook Device
    - Verify Cisco Security for Chromebook client Deployment
    - Troubleshoot Cisco Security for Chromebooks Client Deployment
    - View Protection Status of Chromebook Devices
    - Add Policies to a Chromebook Device

Module 12: Managing Secure Access Security Settings

- Lesson 1: Endpoint Security Settings
    - Endpoint Attributes
- Lesson 2: Zero Trust Access Posture Profiles
    - Add a Client-Based Zero Trust Access Posture Profile
    - Add a Browser-Based Zero Trust Access Posture Profile
- Lesson 3: VPN Connection Posture Profiles
    - Add a VPN Connection Posture Profile
- Lesson 4: IPS Profiles
- Lesson 5: Security Profiles
    - Security Profiles for Internet Access
    - Add a Security Profile for Internet Access
    - Enable SafeSearch
    - Security Profiles for Private Access
    - Add a Security Profile for Private Access
- Lesson 6: Threat Categories
    - Threat Category Descriptions
    - Add a Threat Category List
    - Dispute a Threat Categorization
- Lesson 7: File Inspection and File Analysis
    - Enable File Inspection
    - Enable File Analysis by Cisco Secure Malware Analytics

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

    - Test File Inspection for Internet Access
    - Monitor File Inspection and Analysis Activity
    - Troubleshoot File Inspection and Analysis
- Lesson 8: File Type Controls
    - Enable File Type Controls
    - File Types to Block
    - Review File Type Controls Through Reports
- Lesson 9: Notification Pages
    - Preview Notification Pages
    - Create Custom Block and Warn Pages
    - Allow Users to Contact an Administrator
- Lesson 10: Traffic Decryption
    - Important Information About Do Not Decrypt Lists
    - Add a Do Not Decrypt List for Security Profiles for Internet Access
- Lesson 11: Certificates
    - Certificates for Internet Decryption
    - Install the Cisco Secure Access Root Certificate
    - Add Customer CA Signed Root Certificate
    - View the Cisco Trusted Root Store
    - Manage Certificates for Private Resource Decryption
    - Certificates for Private Resource Decryption
    - Certificates for SAML Authentication
    - Manage SAML Certificates for Service Providers
    - Manage SAML VPN Service Provider Certificate Rotation
    - Manage SAML Certificates for Identity Providers
    - VPN Certificates for User and Device Authentication
    - Manage CA Certificates for VPN Connections
- Lesson 12: Data Loss Prevention Policy
    - Add a Real Time Rule to the Data Loss Prevention Policy
    - Understand Exclusions in a Real Time Rule
    - Supported Applications
    - Add a SaaS API Rule to the Data Loss Prevention Policy
    - Discovery Scan
    - Edit a Data Loss Prevention Rule
    - Delete a Data Loss Prevention Rule
    - Enable or Disable a Data Loss Prevention Rule
    - Supported File and Form Types
    - Best Practices for the Data Loss Protection Policy
- Lesson 13: Data Classifications
    - Create a Data Classification
    - Copy and Customize a Built-In Data Classification
    - Delete or Edit a Classification
    - Create an Exact Data Match Identifier
    - Index Data for an EDM
    - Exact Data Match Field Types
    - Create an Indexed Document Match Identifier
    - Built-In Data Classifications
- Lesson 14: Built-in Data Identifiers
    - Copy and Customize a Data Identifier
    - Create a Custom Identifier
    - Custom Regular Expression Patterns
    - Individual Data Identifiers

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Lesson 15: SaaS API Data Loss Prevention
  - Enable SaaS API Data Loss Prevention for AWS Tenants
  - Enable SaaS API Data Loss Prevention for Azure Tenants
  - Enable SaaS API Data Loss Prevention for Box Tenants
  - Enable SaaS API Data Loss Prevention for Dropbox Tenants
  - Enable SaaS API Data Loss Prevention for Google Drive Tenants
  - Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants
  - Enable SaaS API Data Loss Prevention for ServiceNow Tenants
  - Enable SaaS API Data Loss Prevention for Slack Tenants
  - Enable SaaS API Data Loss Prevention for Webex Teams
- Lesson 16: Cloud Malware Protection
  - Enable Cloud Malware Protection
  - Revoke Authorization for a Platform
  - Enable Cloud Malware Protection for AWS Tenants
  - Enable Cloud Malware Protection for Azure Tenants
  - Enable Cloud Malware Protection for Box Tenants
  - Enable Cloud Malware Protection for Dropbox Tenants
  - Enable Cloud Malware Protection for Google Drive
  - Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants
  - Enable Cloud Malware Protection for ServiceNow Tenants
  - Enable Cloud Malware Protection for Slack Tenants
  - Enable Cloud Malware Protection for Webex Teams

Module 13: Monitoring and Troubleshooting Cisco Secure Access

- Lesson 1: Monitoring Secure Access
  - Monitoring Remote Access Client
  - Monitoring Networks
  - Monitoring Network Path
  - Monitor Application Performance
- Lesson 2: Secure Access Logging
  - Enable Logging
  - Enable Logging to Your Own S3 Bucket
  - Enable Logging to a Cisco-managed S3 Bucket
  - Change the Location of Event Data Logs
  - Stop Logging
  - Delete Logs
  - Log Formats and Versioning
    - Reports and CSV Formats
    - Admin Audit Log Formats
    - Cloud Firewall Log Formats
    - Data Loss Prevention (DLP) Log Formats
    - DNS Log Formats
    - File Events Log Formats
    - IPS Log Formats
    - Remote Access VPN Log Formats
    - Web Log Formats
    - Zero Trust Access Log Formats
- Lesson 3: Cisco AI Assistant
  - Add Rules with the Cisco Assistant
  - Cisco Assistant Rule Examples
  - Find Documented Answers with the Cisco Assistant

    - Messages Generated by the Cisco Assistant
- Lesson 4: Experience Insights with ThousandEyes
    - Experience Insights
    - Onboard Experience Insights
    - Set-Up Experience Insights
    - Generate OAuth Bearer Token
    - Configure Experience Insights
    - Cisco AI Assistant for Experience Insights
    - View Endpoint Performance Map
    - View Summary of Endpoints
    - Wi-Fi Descriptions
    - View Common SaaS Applications
- Lesson 5: Reports
    - Monitor Secure Access with Reports
    - Export Report Data to CSV
    - Bookmark and Share Reports
    - Report Search Window & Retention
    - Report Scheduling
    - Schedule a Report
    - Update a Scheduled Report
    - Remote Access Log Report
        - View the Remote Access Log Report
    - Activity Search Report
        - View and Customize the Activity Search Report
        - View Firewall Events in Activity Search Report
        - View Zero Trust Events in Activity Search Report
        - View Activity Search Report Actions
        - Schedule an Activity Search Report
        - Use Search and Advanced Search
    - Security Activity Report
        - View Activity and Details by Filters
        - View Activity and Details by Event Type or Security Category
        - View an Event's Details
        - Search for Security Activity
    - Total Requests Report
    - Activity Volume Report
    - App Discovery Report
        - View the App Discovery Report
        - View the Highest Risk Apps
        - Review Apps in the Apps Grid
        - View App Details
        - Change App Details
        - Control Apps
        - Control Advanced Apps
        - View Traffic Data Through SWG Service
    - Top Destinations Report
        - Destination Details
    - Top Categories Report
        - Category Details
    - Third-Party Apps Report
    - Cloud Malware Report
    - Data Loss Prevention Report

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

    - Admin Audit Log Report
        - Export Admin Audit Log Report to an S3 Bucket
- Lesson 6: Troubleshooting and Scalability
    - Troubleshooting Common Issues
    - Troubleshooting Clients
    - Troubleshoot Client-Based Zero Trust Access
    - Troubleshoot Failure in Accessing Private Resources
    - Troubleshooting Network Connectivity
    - Troubleshoot Secure Access Roaming Clients
    - Cisco Secure Client Diagnostic and Reporting Tool (DART)
    - Packet Captures
    - HTTP Archive (HAR) Captures

Module 14: Experience Insights with ThousandEyes

- Lesson 1: Experience Insights Overview
    - Purpose, key concepts, data flow (endpoint -> network/Wi-Fi -> cloud/SaaS), and benefits within Cisco Secure Access
    - Architecture with ThousandEyes integration: data sources, collectors/agents, and correlation points
    - Real-world scenario: diagnosing 'Teams is slow' by correlating device Wi-Fi, WAN path, and SaaS endpoint
- Lesson 2: Onboard Experience Insights
    - Tenant readiness checks and required roles/permissions
    - Connecting Cisco Secure Access to ThousandEyes: account scoping, API enablement, least-privilege considerations
    - Lab: verify tenant linkage; confirm agent inventory and accessible measurements
- Lesson 3: Set Up Experience Insights
    - Core settings: regions, identity provider alignment, endpoint tagging standards, and privacy controls
    - Generate OAuth Bearer Token: register API client (client ID/secret), scope selection, token lifetime hygiene
    - Token generation flow, secure storage, and rotation practices
- Lesson 4: Configure Experience Insights
    - Link ThousandEyes tests to Experience Insights (HTTP Server, Page Load, Network/Path Visualization)
    - Endpoint group definitions, thresholds, and alerting policies
    - Dashboards & widgets: building role-specific views for NOC vs. help desk
- Lesson 5: Cisco AI Assistant for Experience Insights
    - Capabilities: natural-language queries, root-cause suggestions, and remediation prompts
    - Guardrails: data scope, auditability, and explainability of AI-generated insights
    - Real-world workflow: 'Why are logins slow in Chicago?'-AI Assistant surfaces Wi-Fi RSSI issues plus CDN edge degradation
- Lesson 6: View Endpoint Performance Map
    - Map layers: endpoint health, local network, WAN/ISP, cloud path, and SaaS reachability
    - Reading hop-by-hop visualizations and identifying chokepoints
- Lesson 7: View Summary of Endpoints
    - Fleet health roll-ups: top impacted users, devices, and locations
    - Drill-downs: per-endpoint KPIs (CPU, memory, Wi-Fi signal/noise, driver/version), recent incidents
- Lesson 8: Wi-Fi Descriptions
    - Key Wi-Fi metrics: RSSI, SNR, PHY rate, retries, roaming behavior, band/channel utilization

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

    - Common pitfalls: sticky clients, misconfigured band steering, power/channel planning
    - Real-world fixes: targeted AP tuning vs. client driver updates
    - Lab: classify issues from Wi-Fi descriptions and match each to a remediation action
- Lesson 9: View Common SaaS Applications
    - Catalog of monitored SaaS (M365, Webex by Cisco, Salesforce, Google Workspace, etc.)
    - Interpreting service status vs. user experience; distinguishing local vs. provider-side incidents
    - Lab: compare two SaaS apps across sites; set alert thresholds and notification routing

Module 15: Secure Access APIs

- Lesson 1: Secure Access Overview
    - Secure Access API Resources
    - Base URI
    - Authorization
    - Rate Limits and Response Codes
    - OAuth 2.0 Scopes
- Lesson 2: Secure Access API Authentication Keys
    - API Key Use Cases
    - Sign in to Secure Access
    - Managing API Keys
- Lesson 3: API Reference
    - Auth
    - Admin
    - Deployments
    - Investigate
    - Policies
    - Reports
- Lesson 4: Secure Access Postman Collection