קורס Cisco Certified Internetwork Expert (CCIE) Security

התמחות באבטחת מידע וניהול מתקדם של תשתיות Cisco

הקורס מספק את הידע והכלים הדרושים להתמודדות עם האתגרים המתקדמים ביותר בתחום אבטחת המידע.
המשתתפים ילמדו כיצד ליישם מנגנוני הגנה מתקדמים, למנוע התקפות, להקים חיבורים מאובטחים, ולנהל תשתיות תוך שימוש בטכנולוגיות Cisco המובילות בעולם. הקורס מתמקד באבטחת רשתות, פתרונות VPN, מנגנוני זיהוי מתקדם, ניהול זהויות ושליטה, והגנת תוכן מתקדמת. מטרת הקורס הינה הכנת המשתתפים להסמכת CCIE Security תוך רכישת מיומנויות פרקטיות שיסייעו להם להוביל בתחומם.

055-278-0865 • avishalomd@iitc.co.il • www.iitc.co.il

אודות מכללת IITC

מכללת IITC, שנוסדה בשנת 2007 על ידי יוני סלוקי – מומחה תקשורת נתונים בעל ניסיון רב בייעוץ, אינטגרציה והדרכה – היא מוסד מוביל להכשרה מקצועית בתחומי התקשורת וההייטק בישראל. המכללה משמשת כשותפת ההדרכה הבלעדית של Cisco בישראל (Cisco Learning Partner), והיחידה בארץ שמוסמכת להכשיר מדריכים מטעם סיסקו העולמית. בנוסף, IITC היא שותפה רשמית של Fortinet ומוכרת כמרכז ההדרכה הבלעדי של חברות התקשורת והאינטגרציה הגדולות בארץ.

IITC מתמחה בהכשרת אנשי מקצוע במגוון תחומים מבוקשים, כולל רשתות ותקשורת נתונים (CCNA ועד CCIE), פיתוח תוכנה (DevOps, Web), בדיקות תוכנה (QA) ועוד. בנוסף, מאז 2012, המכללה היא ספק ההכשרות הבלעדי של צה"ל ומשרד הביטחון בנושאי Cisco ותקשורת נתונים.

המכללה מציעה קורסים מותאמים אישית ללקוחות מהמגזר הציבורי והפרטי, בהם חברות מובילות כמו בזק, סלקום, ובינת, לצד קורסים היברידיים המתקיימים בקמפוס חדשני ומפואר במתחם הבורסה ברמת גן (רחוב החילזון 3), המאובזר בטכנולוגיה מתקדמת. IITC מתגאה במעמדה כמוסד מוביל התורם להכשרת אלפי אנשי מקצוע ומובילים טכנולוגיים בשוק ההייטק בישראל.

יתרונות מרכזיים

הדרכה מקצועית

צוות המדריכים של מכללת IITC מורכב ממומחי Cisco בעלי הסמכות מתקדמות (CCAI, CCSI) וניסיון מעשי עשיר. המדריכים מועסקים במשרה מלאה ומבטיחים לתלמידים חוויית למידה מקיפה, עדכנית ומעשירה.

מעבדות טכנולוגיות מהמתקדמות בארץ

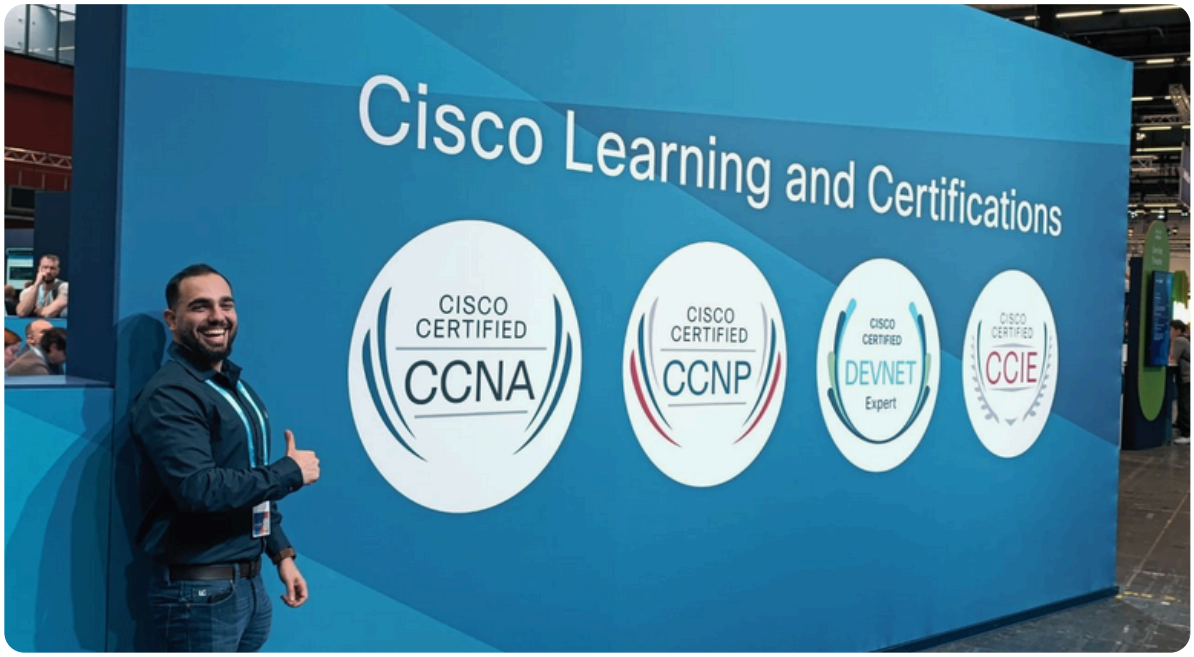
מעבדת Cisco במכללה מאפשרת התנסות מעשית בסביבות עבודה אמיתיות, במטרה להבטיח חיבור בין התיאוריה לפרקטיקה.

אחוזי מעבר גבוהים

אחוזי המעבר של תלמידי IITC במבחני ההסמכה של Cisco הם הגבוהים בארץ, עדות לרמה הגבוהה של ההכשרות והליווי האישי הניתן לכל תלמיד.

מוסד מוכר ומוסמך

מכללת IITC מוכרת על ידי האגף להכשרה מקצועית במשרד העבודה ומשמשת כמרכז בחינות מורשה של Pearson VUE ו- PSI.



אודות הקורס

הסמכת CCIE Security נחשבת לאחת ההסמכות היוקרתיות והמבוקשות ביותר בעולם בתחום אבטחת המידע והתקשורת. מהנדסי תקשורת ואבטחת מידע המחזיקים בהסמכה זו מצטיינים במומחיות, מיומנות ושליטה מעמיקה במגוון הציוד, הפתרונות והטכנולוגיות של Cisco.

במהלך השנים, קהילת ה- CCIE צברה מוניטין גבוה בתעשייה, בזכות רמת הידע הטכני המעמיק שלה והיכולת להתמודד עם האתגרים המורכבים ביותר בתחום אבטחת המידע והתקשורת. תוכנית ההסמכה מתעדכנת באופן תדיר כדי לשלב כלים, מתודולוגיות וידע חדשני, המבטיחים רלוונטיות, איכות וערך מקצועי גבוה.

המכללה מכינה אתכם הן לבחינה התיאורטית 350-701 SCOR (Security Core Technologies) אותה ניתן לבצע בארץ, והן לבחינה המעשית CCIE Security v6.0 המתבצעת במעבדות ייעודיות של Cisco בחו"ל.

משך הקורס

- כ- 40 מפגשים בשעות הערב (כחצי שנה)
- 200 שעות לימוד אקדמיות
- שעות הלימוד: 18:00–21:30
- מפגש אחד בשבוע, בימי שלישי

מיקום הקורס

- מכללת IITC, רחוב החילזון 3, רמת גן
- לנוחיותכם, ניתן לעשות את הקורס גם באופן מקוון

דרישות קדם

- הסמכת CCNP Security בתוקף או ידע מקביל
- ניסיון מקצועי של לפחות 3 שנים בתעשייה
- הקבלה לקורס מותנית בראיון אישי עם מנהל מקצועי

תעודות הסמכה

- תעודת גמר מטעם מכללת IITC
- תעודת הסמכה בינלאומית של CCIE Security
- **עלויות הבחינות אינן כלולות בעלות הקורס**

הכירו את מייסד מסלולי ה- CCIE בישראל

יוני סלוקי

מנכ"ל ומייסד מכללת IITC, הוא מדריך ה- CCIE הבכיר בישראל ומומחה בעל למעלה מ- 20 שנות ניסיון בתחום התקשורת. יוני מוביל את תחום ה- CCIE במכללה ואת צוות מדריכי התקשורת הגדול בארץ, ומשלב היכרות מעמיקה ומעשית עם כל הציוד של חברת CISCO.
דרכו המקצועית החלה כבר במהלך שירותו הצבאי, והפך לחלוץ בתחום התקשורת בישראל. לאורך השנים למד, חקר ופיתח ידע ייחודי שהוביל אותו להישגים גבוהים בהדרכה, בליווי מקצועי, ובניהול פרויקטים מורכבים. יוני מוכר כמוביל דעה ואחד המשפיעים המרכזיים בתחום התקשורת בארץ, וכמנכ"ל IITC הוא מחויב להכשיר את דור העתיד של מומחי הרשתות.

סילבוס

1	Perimeter Security and Intrusion Prevention
1.1	Deployment modes on Cisco ASA and Cisco FTD
1.2	Firewall features on Cisco ASA and Cisco FTD
1.3	Security features on Cisco IOS/IOS-XE
1.4	Cisco Firepower Management Center (FMC) feature
1.5	NGIPS deployment modes
1.6	Next Generation Firewall (NGFW) features
1.7	Detect, and mitigate common types of attacks
1.8	Clustering/HA features on Cisco ASA and Cisco FTD
1.9	Policies and rules for traffic control on Cisco ASA and Cisco FTD
1.10	Routing protocols security on Cisco IOS, Cisco ASA and Cisco FTD
1.11	Network connectivity through Cisco ASA and Cisco FTD
1.12	Correlation and remediation rules on Cisco FMC
2	**Secure Connectivity and Segmentation**
2.1	AnyConnect client-based remote access VPN technologies on Cisco ASA, Cisco FTD, and Cisco Routers
2.2	Cisco IOS CA for VPN authentication

2.3	FlexVPN, DMVPN, and IPsec L2L Tunnels
2.4	Uplink and downlink MACsec (802.1AE)
2.5	VPN high availability using (Cisco ASA VPN clustering, Dual-Hub DMVPN deployments)
2.6	Infrastructure segmentation methods
2.7	Micro-segmentation with Cisco TrustSec using SGT and SXP
3	**Infrastructure Security**
3.1	Device hardening techniques and control plane protection methods
3.2	Management plane protection techniques
3.3	Data plane protection techniques
3.4	Layer 2 security techniques
3.5	Wireless security technologies
3.6	Monitoring protocols
3.7	Security features to comply with organizational security policies, procedures, and standards BCP 38
3.8	Cisco SAFE model to validate network security design and to identify threats to different Places in the Network (PINs)
3.9	Interaction with network devices through APIs using basic Python scripts
3.10	Cisco DNAC Northbound APIs use cases

סילבוס

4	Identity Management, Information Exchange & Access Control
4.1	ISE scalability using multiple nodes and personas
4.2	Cisco switches and Cisco Wireless LAN Controllers for network access AAA with ISE
4.3	Cisco devices for administrative access with ISE
4.4	AAA for network access with 802.1X and MAB using ISE
4.5	Guest lifecycle management using ISE and Cisco Wireless LAN controllers
4.6	BYOD on-boarding and network access flows
4.7	ISE integration with external identity sources
4.8	Provisioning of AnyConnect with ISE and ASA
4.9	Posture assessment with ISE
4.10	Endpoint profiling using ISE and Cisco network infrastructure including device sensor
4.11	Integration of MDM with ISE
4.12	Certificate-based authentication using ISE
4.13	Authentication methods (EAP Chaining, Machine Access Restriction (MAR))
4.14	Identity mapping on ASA, ISE, WSA, and FTD

4.15	pxGrid integration between security devices WSA, ISE, and Cisco FMC
4.16	Integration of ISE with multi-factor authentication
4.17	Access control and single sign-on using Cisco DUO security technology
5	**Advanced Threat Protection and Content Security**
5.1	AMP for networks, AMP for endpoints, and AMP for content security (ESA, and WSA)
5.2	Detect, analyze, and mitigate malware incidents
5.3	Perform packet capture and analysis using Wireshark, tcpdump, SPAN, ERSPAN, and RSPAN
5.4	DNS layer security, intelligent proxy, and user identification using Cisco Umbrella
5.5	Web filtering, user identification, and Application Visibility and Control (AVC) on Cisco FTD and WSA
5.6	WCCP redirection on Cisco devices
5.7	Email security features
5.8	HTTPS decryption and inspection on Cisco FTD, WSA and Umbrella
5.9	SMA for centralized content security management
5.10	Cisco advanced threat solutions and their integration: Stealthwatch, FMC, AMP, Cognitive Threat Analytics (CTA), Threat Grid, Encrypted Traffic Analytics (ETA), WSA, SMA, CTR, and Umbrella