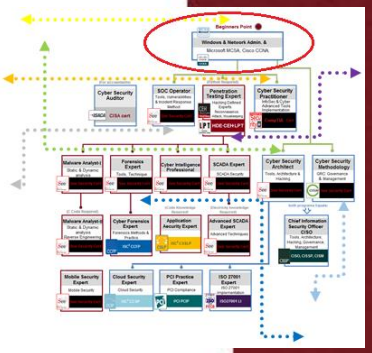
מאושר משרד העבודה לפקדונות
ולשוברים לחיילים משוחררים



התכנית ללימודי ניהול רשתות
ומבואות הגנת סייבר
(הכנה על-פי חוק אסדרת מקצועות הסייבר בישראל,
ותכנית מוכרת לצורך שימוש בפקדון חיילים משוחררים)

(MCSA, CCNA, CCSA, LPI Linux, Python, Hacking Essentials)

מדינת ישראל, באמצעות האגף להכשרה מקצועית במשרד העבודה, מפקחת
על התכנית ומאשרת אותה כתכנית רשתות ומבוא ללימודי סייבר.
לימודי ניהול רשתות ומבואות סייבר, מוסדרים ברגולציה של מדינת ישראל.

וודא קיום אישור משרד העבודה לכל תכנית לימודים, כי זה העתיד והכסף שלך!
אישור מס' 02436303 לחוק קליטת חיילים משוחררים התשנ"ד

See
cyber security college

Let's be a cyber Expert.

Let's Start. Let's start with Cyber preparation studies program.

Step by step, we will start with Microsoft server studies including preparation for MCSA certification, continue by learning Networking for Cisco-CCNA certification, and then, information security by Check Point for CCSA certification. Finally, we will continue with Linux for beginners to LPI certification, and finishing with the Python programming language.

Why? Because there is no other way...

תוכנית משולבת ללימודי ניהול רשתות ומבואות הגנת סייבר:
Cyber Security Preparation

התוכנית מהווה מכינה ללימודי מקצועות הסייבר על-בסיס הוראת אסדרת מקצועות הסייבר של מטה הסייבר הלאומי

ומוכרת לצורך שימוש בפקדון חיילים משוחררים

מנהל הקורס: מר יקי בן-ניסן

אודות המכללה

מכללת See Security הנה מכללה **בינלאומית** התמחותית **למקצועות ניהול רשתות וסייבר**, אחת מ- 7 מכללות מסוגה בעולם ועוסקת בלעדית בתחום זה בכל זמנה, תוך שימוש במתודולוגית הדרכה שנבנתה עבור גורמים ממלכתיים.

המכללה מייצאת את תכניות הלימודים לכל רחבי העולם, באמצעות המותג *See Security International*, ובאמצעות גופי סייבר ישראליים ידועי-שם העוסקים ביצוא בטחוני.

מנהל המכללה, מר אבי ויסמן, הינו ממובילי ענף הסייבר בישראל, פרשן ויועץ מבוקש בערוצי השידור בישראל, יו"ר הפורום הלאומי לאבטחת מידע IFIS, וכן מנכ"ל משותף בחברה להשמת כוח אדם - *SeeHR*, בחברה לייעוץ *Cyber – See Consulting*, בחברה לפתרונות Managed SEIM/SOC – *See Events*, ובמכללה הבינלאומית *See Security College International*.

מבוא לתכנית

תכנית ייחודית זו כוללת הסמכות לסביבות של Microsoft, Cisco, Check point, Linux ו- Python. מדוע? כי מסלול זה מיועד הן למתעניינים במקצוע ניהול רשתות המבקשים להתבלט, ובמיוחד - למעוניינים להתפתח בענף הסייבר.

המכללה הייעודית לסייבר See Security בנתה מסלול המיועד למעוניינים להתמחות באחד ממקצועות הליבה בסייבר, ונדרשים להכשרת מנהלי רשתות, הוסיפה רכיבים ייחודיים של סביבת סייבר כלימודי חובה, לצורך עמידה בדרישת הסף, לקראת המשך לימודיהם.

קהל יעד

קורס ניהול רשתות מתקדם מיועד לחסרי רקע קודם במחשבים המעוניינים לרכוש מקצוע הייטק מבוקש, תוך התמחות מקצועית וידע מעמיק בעולם הרשתות, ה- System והגנת סייבר, לשם התמחות כמנהל רשתות בסביבות Windows והתמחות מיישם הגנת סייבר או Linux.

סגל המרצים

המרצים של תכנית זו – גאוות המכללה. כולם בוגרים, בגילאים 32 עד 40, כולם מנוסים מאוד, כולם מחויבים לציון ממוצע 9 במשובי התלמידים: יקי בן-ניסן – מנהל תחום מתחילים בניהול רשתות, פיתוח ואבטחת מידע ומרצה.

שי שורצולד, מנהל תשתיות בערוץ 2' ומרצה בכיר. גם את/ה תתאהב ותשבח.

יקי בן-ניסן

שי שורצולד

הסמכות בינלאומיות

- See-Security: "System & Network Administrator"
- Microsoft MCSA
- Cisco CCNA
- Check Point CCSA
- LPI Linux
- Python code.
- Hacking Essentials

עלות

290 שעות, 400 ₪ דמי רישום וכן 16,900 ₪ כולל מע"מ.

* ממחזור נובמבר 2018 – המחיר 400 ₪ דמי רישום וכן 18,000 ₪ כולל מע"מ.

תנאי קבלה

- קריאה באנגלית, שימוש בסיסי במחשב, בוגר 12 שנות לימוד* (או באישור ועדת חריגים), ראיון אישי עם אבי ויסמן.

אחרי סיום הלימודים – הצעד הבא

לאחר סיום תכנית זו תוכל לבחור את המשך דרכך:

1. להתחיל לעבוד כמנהל רשתות (כנראה שבתחילת הדרך תתחיל כתומך טכני, ולאחר מכן – תומך טכני עסקי בכיר, ולאחר מכן – עוזר למנהל רשת...)
2. להתחיל את "***הצעד הבא***", מבין האפשרויות הבאות:
   א. קורס **מיישמי הגנת סייבר: CSP**.
   ב. קורס **מומחי ניטור במרכז SOC**: SOC-IR
   ג. קורס **ארכיטקט הגנת סייבר**: **CSTP** (**ארכיטקט**).
   ד. קורס **בודקי חדירות: CSPT** (מבוסס על קורס Hacking Defined Experts הבינלאומי).

למידע נוסף / פגישת יעוץ:
מידע מינהלי: אלוירה אליסייב, 03-6122831, 052-8787889, elvira@see-security.com
יועץ אקדמי: אבי ויסמן, 03-5799555, 054-5222305, avi@see-security.com

שעות כיתה ומשימות אישיות

290 שעות כיתה ומעבדה, וכן 320 שעות משימות אישיות.

מתכונת לימודים

הלימודים בקמפוס המכללה ברמת גן (צמוד לתחנת רכבת מרכז), מתקיימים פעמיים בשבוע בערב, 17:30 עד 21:30 במשך כ- 8 חודשים, 5 שעות אקדמיות למפגש.

זכאות לתעודה

קיימת חובת נוכחות ב-80% מהמפגשים. קבלת תעודת המכללה מותנית בעמידה במבחני מעבר, בציון 70 לפחות (מבחן חוזר ללא תשלום). לעומדים בדרישות התכנית תוענק תעודת הסמכה יוקרתית מטעם המכללה. זאת, בנוסף להסמכות הבינלאומיות המומלצות לגישה: Microsoft, Cisco, LPI Linux Essentials.

אחוזי ההצלחה במבחנים החיצוניים של בוגרי מסלול זה הם מהגבוהים בעולם.

שלד תכנית לימודים

1. Microsoft 20410: Installing and Configuring Windows Server 2012
2. Microsoft 20411: Administering Windows Server 2012
3. Microsoft 20412: Configuring Advanced Windows Server 2012 Services
4. Cisco CCNA: Interconnecting Cisco Network Devices 100-105 ICND1 (Part 1)
5. Cisco CCNA: Interconnecting Cisco Network Devices 100-105 ICND2 (Part 2)
6. Check Point CCSA: Check Point Certified Security Administrator 156-215.77
7. LPI Linux Essentials
8. Python for Beginners
9. Hacking Essentials

לתשומת לבך!

תהליך הייעוץ והסינון של היועץ האקדמי משמעותי לבחינת סיכוייך להצליח במסלול זה ו/או במסלולים אחרים, ובעתידך התעסוקתי בכלל.

עובד משרד הבטחון / צה"ל / משרד ראש הממשלה / מטה הסייבר / רשות הסייבר

בדוק עם הנהלת המכללה דרכי ההרשמה תחת פטור ספק יחיד, לגבי מסלול זה ולגבי לימודי ההמשך.

מדוע התכנית שונה כל-כך מלימודי רשתות רגילים?

מנקודת המבט של הנהלת המכללה, תלמיד מצליח אך ורק אם הצליח להשתלב אצל מעסיק בתפקיד רלוונטי. לכן הגדרת תכני הקורס נבנתה בהתאם לדרישת המעסיקים.

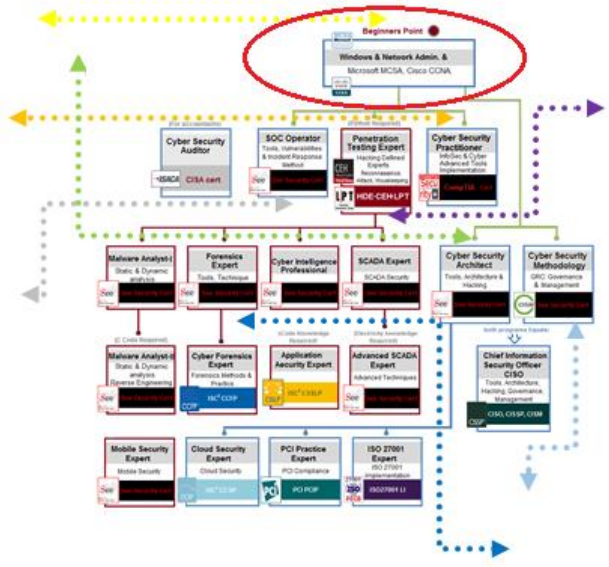
המעסיק דורש ומצפה כי בוגר של מכללה ייעודית לסייבר כמו See Security יגיע בוגר יותר, עשיר יותר ובעל ידע רב תחומי. לכן תוכנית זו מחייבת לימודים מולטי דיסיפלינאריים בסיסטם, Windows & Linux, בתקשורת על כל גווניה לפי Cisco, ובשפת פיתוח בסיסית ומשמעותית לעולם הסייבר: Python.

"המתחרה" של המועמד איננו המעסיק. להיפך: הוא מבקש את הטוב ביותר לעצמו. כאשר הוא מבקש לקלוט מועמד מתחיל, הוא מצפה לפחות שיהיה בעל ידע רב יותר ממועמדים המגיעים מחברות הדרכה המשווקות קורסים כלליים.

כך נבנה המוניטין של המכללה לאורך השנים!

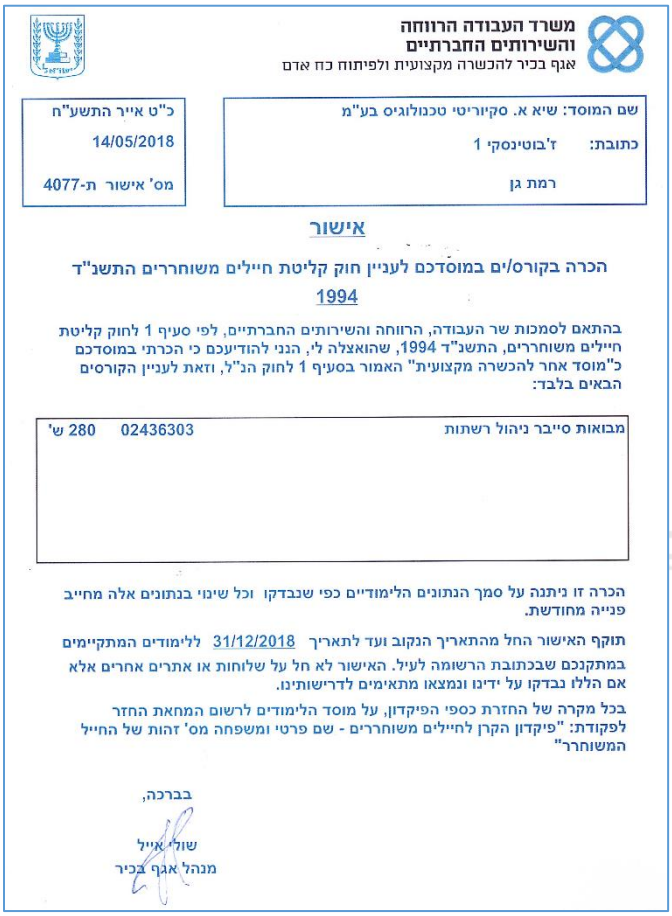
מה אנחנו מצפים מבוגר התכנית?

1. בתקופת הלימודים תשקיע את כל הזמן כדי לקיים את הנחיות המרצה, אינך הראשון ולא תהיה האחרון שימצא עצמו איש הייטק בלב התעשייה.
2. בסיום לימודיך היעזר בהנהלת המוסד לבניית טופס קורות חיים ההולם את מאמצייך.
3. הסתפק בתחילת דרכך במשרת רשתות מכל סוג שהוא כדי לצבור ניסיון (עשה זאת כבר בתקופת הלימודים ובכל מחיר ושכר).
4. בדוק עם היועץ האקדמי את איכות עמידתך בריאיון אישי לקראת ראיונות העבודה האמיתיים, במקרים מסויימים אפילו תלמיד מצטיין זקוק לתיקונים פשוטים יחסית שמשביחים מאוד את יכולתו למצוא משרה איכותית.
5. צא לדרכך, אל תשכח להמשיך ללמוד, דאג תמיד להיות מבחינת ידע רמה אחת יותר מהאחרים, כי ככל שתגביה כך יהיו לך פחות מתחרים, שכר גבוה יותר, וסיפוק רב יותר.



הערות

- ההרשמה לכל מבחן חיצוני, הנה בתשלום ותבוצע באחריות הסטודנט בלבד.
- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכללה.
- המכללה מביאה לידיעת הנרשמים כי ייתכנו שינויים במערך התכנית, במועדי הלימודים והבחינות או בכל נושא אחר. הודעה על כל שינוי תימסר למשתתפים.



משרד העבודה הרווחה והשירותים החברתיים
אגף בכיר להכשרה מקצועית ולפיתוח כח אדם

כ"ט אייר התשע"ח
14/05/2018
מס' אישור ת-4077

שם המוסד: שיא א. סקיוריטי טכנולוגיס בע"מ
כתובת: ז'בוטינסקי 1
רמת גן

אישור

הכרה בקורס/ים במוסדכם לעניין חוק קליטת חיילים משוחררים התשנ"ד 1994

בהתאם לסמכות שר העבודה, הרווחה והשירותים החברתיים, לפי סעיף 1 לחוק קליטת חיילים משוחררים, התשנ"ד 1994, שהואצלה לי, הנני להודיעכם כי הכרתי במוסדכם כ"מוסד אחר להכשרה מקצועית" האמור בסעיף 1 לחוק הנ"ל, וזאת לעניין הקורסים הבאים בלבד:

מבואות סייבר וניהול רשתות	02436303	280 ש'

הכרה זו ניתנה על סמך הנתונים הלימודיים כפי שנבדקו וכל שינוי בנתונים אלה מחייב פנייה מחודשת.

תוקף האישור החל מהתאריך הנקוב ועד לתאריך 31/12/2018 ללימודים המתקיימים במתקנכם שבכתובת הרשומה לעיל. האישור לא חל על שלוחות או אתרים אחרים אלא אם הללו נבדקו על ידינו ונמצאו מתאימים לדרישותינו.

בכל מקרה של החזרת כספי הפיקדון, על מוסד הלימודים לרשום המחאת החזר לפקודת: "פיקדון הקרן לחיילים משוחררים - שם פרטי ומשפחה מס' זהות של החייל המשוחרר"

בברכה,
שולי אייל
מנהל אגף בכיר

Curriculum:

Introduction to Networking — 20

This module gives an overview of elementary components of hardware, Windows Server operating system and Active Directory.

Lessons:

- Hardware Overview
- Networks Topology Overview
- 7 layers' model Overview
- TCP/IP model Overview
- Domain Services Overview

70-410 — 30

Installing and Configuring Windows Server 2012

Module 1: Introduction to Active Directory Domain Services

This module covers the structure of Active Directory Domain Services (AD DS) and its various components, such as forest, domain, and organizational units (OUs). It is also gives an overview of domain controllers, in addition to choices that are available with Windows Server 2012 for installing AD DS on a server.

Lessons:

- Windows Server 2012 Overview
- Installing Windows Server 2012
- Post-Installation Configuration of Windows Server 2012
- Overview of Windows Server 2012 Management
- Introduction to Windows PowerShell

Module 2: Managing Active Directory Domain Services Objects

This module describes how to manage user accounts and computer accounts, including how to manage various consumer devices that employees use. The module also covers how to manage an enterprise network by managing groups, and how to delegate administrative tasks to designated users or groups.

Lessons:

- Overview of AD DS
- Overview of Domain Controllers
- Installing a Domain Controller

Module 3: Managing Active Directory Domain Services Objects

This module describes how to manage user accounts and computer accounts, including how to manage various consumer devices that employees use. The module also covers how to manage an enterprise network by managing groups, and how to delegate administrative tasks to designated users or groups.

Lessons:

- Managing User Accounts
- Managing Groups
- Managing Computer Accounts
- Delegating Administration

Module 4: Automating Active Directory Domain Services Administration

This module describes how to use command line tools and Windows PowerShell to automate AD DS administration. It discusses various command-line tools and Windows PowerShell commands, and then describes how to use these tools and commands to modify objects individually and in bulk operations.

Lessons:

- Using Command-line Tools for AD DS Administration
- Using Windows PowerShell for AD DS Administration
- Performing Bulk Operations with Windows PowerShell

Module 5: Implementing IPv4

This module discusses using IPv4, which is the network protocol used on the Internet and on local area networks. In this module, students learn how to implement an IPv4 addressing scheme and how to troubleshoot network communication. This module also covers how to determine and troubleshoot network-related problems.

Lessons:

- Overview of TCP/IP
- Understanding IPv4 Addressing
- Subnetting and Supernetting
- Configuring and Troubleshooting IPv4

Module 6: Implementing Dynamic Host Configuration Protocol

This module covers supporting and troubleshooting a Windows Server–based network infrastructure by

deploying, configuring, and troubleshooting the Dynamic Host Configuration Protocol (DHCP) server role.

Lessons:

- Overview of the DHCP Server Role
- Configuring DHCP Scopes
- Managing a DHCP Database
- Securing and Monitoring DHCP

70-411 | 25

Administering Windows Server 2012

Module 1: Configuring and Troubleshooting Domain Name System

This module explains how to configure and troubleshoot DNS, including DNS replication and caching.

Lessons:

- Configuring the DNS Server Role
- Configuring DNS Zones
- Configuring DNS Zone Transfers
- Managing and Troubleshooting DNS

Module 2: Maintaining Active Directory Domain Services

This module explains how to implement virtualized domain controllers and read-only domain controller (RODCs). It is also explaining how to perform common AD DS administrative tasks and manage the AD DS Database.

Lessons:

- Implementing Virtualized Domain Controllers
- Implementing RODCs
- Administering AD DS
- Managing the AD DS Database

Module 3: Managing User and Service Accounts

This module explains how to create, configure and automate the creation of user accounts. It also explains how to configure account-related properties of user objects. It is further explaining how to create and administer Managed Service Accounts.

Lessons:

- Configuring Password Policy and User Account Lockout Settings
- Configuring Managed Service Accounts

Module 4: Implementing a Group Policy Infrastructure

This module explains how to implement a GPO infrastructure. This also teaches how to perform common GPO management tasks, and manage GPOs by using Windows PowerShell. It is also focuses on troubleshooting the application of GPOs.

Lessons:

- Introducing Group Policy
- Implementing and Administering GPOs
- Group Policy Scope and Group Policy Processing
- Troubleshooting the Application of GPOs.

Module 5: Managing User Desktops with Group Policy

This module explains how you can use Group Policy Objects (GPOs) to implement desktop environments across your organization by using Administrative Templates, Folder Redirection, Group Policy preferences, and where applicable, use software deployment to install and update application programs. It is important to know how to use these various GPO features so that you can configure your users' computer settings properly.

Lessons:

- Implementing Administrative Templates
- Configuring Folder Redirection and Scripts
- Configuring Group Policy Preferences
- Managing Software with Group Policy

Module 6: Installing, Configuring, and Troubleshooting the Network Policy Server Role

This module explains how to install and configure NPS, RADIUS Clients and servers. It is also describing NPS authentication methods. It describes NPS authentication methods and how to monitor and troubleshoot NPS.

Lessons:

- Installing and Configuring a Network Policy Server
- Configuring RADIUS Clients and Servers
- NPS Authentication Methods
- Monitoring and Troubleshooting a Network Policy Server

Module 7: Implementing DNS

This module describes name resolution for Windows operating system clients and Windows Server servers. It

is also covers installing and configuring a DNS Server service and its components

Lessons:

- Name Resolution for Windows Clients and Servers
- Installing a DNS Server
- Managing DNS Zones.

Module 8: Implementing IPv6

This module discusses the features and benefits of IPv6, how IPv6 affects IPv4 networks, and how to integrate IPv6 into IPv4 networks by using various transition technologies.

Lessons:

- Overview of IPv6
- IPv6 Addressing
- Coexistence with IPv4
- IPv6 Transition Technologies

Module 9: Implementing Local Storage

This module introduces several different storage technologies. It discusses how to implement the storage solutions in Windows Server 2012, and how to use the new Storage Spaces feature, which enables you to combine disks into pools that you can configure for automatic management.

Lessons:

- Overview of Storage
- Managing Disks and Volumes
- Implementing Storage Spaces

Module 10: Implementing File and Print Services

This module discusses how to provide le and print resources with Windows Server 2012. It describes how to secure les and folders, how to protect previous versions of les and folders by using shadow copies, and how to give workers remote access to corporate les by implementing the new Work Folders role service. It is also describing new network printing features that help manage the network printing environment.

Lessons:

- Securing Files and Folders
- Protecting Shared Files and Folders by Using Shadow Copies
- Configuring Work Folders
- Configuring Network Printing.

Module 11: Implementing Group Policy

This module provides an overview of Group Policy and provides details about how to implement Group Policy.

Lessons:

- Overview of Group Policy
- Group Policy Processing
- Implementing a Central Store for Administrative Templates

Module 12: Securing Windows Servers Using Group Policy Objects

This module describes Windows Server 2012 operating system security. It covers how to identify security threats, plan your strategy to mitigate security threats, and secure your Windows Server 2012 infrastructure.

Lessons:

- Security Overview for Windows Operating Systems
- Configuring Security Settings
- Restricting Software
- Configuring Windows Firewall with Advanced Security

Module 13: Implementing Server Virtualization with Hyper-V

This module describes virtualization technologies available on Windows, specially focusing on the Hyper-V role in Windows Server 2012 and Windows Server 2012 R2. It covers the components of the Hyper-V role, configuring and deploying the role, in addition to and how to configure and manage key components of a Hyper-V implementation, such as Storage and Networking.

Lessons:

- Overview of Virtualization Technologies
- Implementing Hyper-V
- Managing Virtual Machine Storage
- Managing Virtual Networks.

70-412 | 25

Configuring Advanced Windows Server 2012 Services

Module 1: Implementing Advanced Network Services

In this module students will be able to configure advanced features for Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS), and configure IP Address Management (IPAM).

Lessons:

- Configuring Advanced DHCP Features
- Configuring Advanced DNS Settings
- Implementing IPAM
- Managing IP Address Spaces with IPAM

Module 2: Implementing Advanced File Services

In this module students will be able to configure file services to meet advanced business requirements.

Lessons:

- Configuring iSCSI Storage
- Configuring BranchCache
- Optimizing Storage Usage

Module 3: Implementing Dynamic Access Control

In this module students will be able to plan and implement an Active Directory Domain Services (AD DS) deployment that includes multiple domains and forests.

Lessons:

- Overview of DAC
- Implementing DAC Components
- Implementing DAC for Access Control
- Implementing Access Denied Assistance
- Implementing and Managing Work Folders

Module 4: Implementing Distributed Active Directory Domain Services Deployments

In this module students will be able to configure advanced features for Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS), and configure IP Address Management (IPAM).

Lessons:

- Overview of Distributed AD DS Deployments
- Deploying a Distributed AD DS Environment
- Configuring AD DS Trusts

Module 5: Implementing Active Directory Domain Services Sites and Replication

In this module students will be able to plan and implement an AD DS deployment that includes multiple locations.

Lessons:

- AD DS Replication Overview
- Configuring AD DS Sites
- Configuring and Monitoring AD DS Replication

Module 6: Implementing AD CS

In this module students will be able to implement an Active Directory Certificate Services (AD CS) deployment.

Lessons:

- Using Certificates in a Business Environment
- PKI Overview
- Deploying CAs
- Deploying and Managing Certificate Templates
- Implementing Certificate Distribution and Revocation
- Managing Certificate Recovery

Module 7: Implementing Active Directory Rights Management Services

In this module students will be able to implement an AD RMS deployment.

Lessons:

- AD RMS Overview
- Deploying and Managing an AD RMS Infrastructure
- Configuring AD RMS Content Protection
- Configuring External Access to AD RMS

Module 8: Implementing and Administering AD FS

In this module students will be able to implement an Active Directory Federation Services (AD FS) deployment.

Lessons:

- Overview of AD FS
- Deploying AD FS
- Implementing AD FS for a Single Organization
- Deploying AD FS in a Business-to-Business Federation Scenario
- Extending AD FS to External Clients

Module 9: Implementing Network Load Balancing

In this module students will be able to provide high availability and load balancing for web-based applications by implementing Network Load Balancing (NLB).

Lessons:

- Overview of NLB
- Configuring an NLB Cluster
- Planning an NLB Implementation

Module 10: Implementing Failover Clustering

In this module students will be able to provide high availability for network services and applications by implementing failover clustering.

Lessons:

- Overview of Failover Clustering
- Implementing a Failover Cluster
- Configuring Highly Available Applications and Services on a Failover Cluster
- Maintaining a Failover Cluster
- Implementing a Multi-Site Failover Cluster

Module 11: Implementing Failover Clustering with Hyper-V

In this module students will be able to deploy and manage Hyper-V virtual machines in a failover cluster.

Lessons:

- Overview of Integrating Hyper-V with Failover Clustering
- Implementing Hyper-V Virtual Machines on Failover Clusters
- Implementing Hyper-V Virtual Machine Movement
- Lab : Implementing Failover Clustering with Hyper-V

Module 12: Implementing Business Continuity and Disaster Recovery

In this module students will be able to implement a backup and disaster recovery solution based on business and technical requirements.

Lessons:

- Data Protection Overview
- Implementing Windows Server Backup
- Implementing Server and Data Recovery

CISCO 100-105 ICND1 | 40

Interconnecting Cisco Network Devices Part 1

This course will enable students to understand QoS, virtualization and cloud services, and network programmability related to WAN, access and core segments. It will provide the foundational understanding of network layers 1-3 that are applicable to core routing and switching plus other advanced technologies. Several topics have been added including; understanding the interactions and network functions of firewalls, wireless controllers and access points, along with additional focus on IPv6 and basic network security. The configuration commands are introduced through examples and supported with lab exercises. A full suite of labs have been developed using the virtual IOS environment with flexible topologies that reinforce concepts with hands-on, guided discovery and challenge labs that align to each lesson module.

Module 1: Building a Simple Network

- Exploring the Functions of Networking
- Understanding the Host-to-Host Communication Model
- Introducing LANs
- Operating Cisco IOS Software
- Starting a Switch
- Understanding Ethernet and Switch Operation
- Troubleshooting Common Switch Media Issues

Module 2: Establishing Internet Connectivity

- Understanding the TCP/IP Internet Layer
- Understanding IP Addressing and Subnets
- Exploring the Functions of Routing
- Configuring a Cisco Router
- Exploring the Packet Delivery Process
- Enabling Static Routing
- Learning the Basics of ACL
- Enabling Internet Connectivity

Module 3: Summary Challenge

- Establish Internet Connectivity
- Troubleshoot Internet Connectivity

Module 4: Building a Medium-Sized Network

- Implementing VLANs and Trunks
- Routing Between VLANs
- Using a Cisco IOS Network Device as a DHCP Server
- Implementing RIPv2

Module 5: Network Device Management and Security

- Securing Administrative Access
- Implementing Device Hardening
- Configuring System Message Logging
- Managing Cisco Devices
- Licensing

Module 6: Summary Challenge

- Implementing a Medium-Sized Network
- Troubleshooting a Medium-Sized Network

Module 7: Introducing IPv6

- Introducing Basic IPv6
- Understanding IPv6 Operation
- Configuring IPv6 Static Routes

CISCO CCNA 100-105 ICND2 — 30

Interconnecting Cisco Network Devices Part 2

This course will students with the knowledge and skills needed to install, configure, operate, and troubleshoot a small enterprise network. It will ensure that students understand and are ready to deploy the latest shifts in technologies and solutions as follows:

- Understanding of Quality of Service (QoS) elements and their applicability
- How virtualized and cloud services will interact and impact enterprise networks
- An overview of network programmability and the related controller types and tools that are available to support software defined network architectures.

Module 1: Implement Scalable Medium-Sized Networks

- Troubleshooting VLAN Connectivity
- Building Redundant Switched Topologies
- Improving Redundant Switched Topologies with EtherChannel
- Understanding Layer 3 Redundancy

Module 2: Troubleshooting Basic Connectivity

- Troubleshooting IPv4 Network Connectivity
- Troubleshooting IPv6 Network Connectivity

Module 3: Implementing an EIGRP-Based Solution

- Understanding OSPF
- Implementing Multiarea OSPF IPv4
- Implementing OSPFv3 for IPv6
- Troubleshooting Multiarea OSPF

Module 4: Summary Challenge

- Implementing and Troubleshooting Scalable Medium-Sized Network
- Implementing and Troubleshooting Scalable Medium-Sized Network 2

Module 5: Implement a Scalable OSPF-Based Solution

- Understanding OSPF
- Implementing Multiarea OSPF IPv4
- Implementing OSPFv3 for IPv6
- Troubleshooting Multiarea OSPF

Module 6: Wide-Area Networks

- Understanding WAN Technologies
- Understanding Point-to-Point Protocols
- Configuring GRE Tunnels
- Configuring Single-Homed EBGP

Module 7: Network Device Management

- Implementing Basic Network Device Management and Security
- Evolution of Intelligent Networks
- Introducing QoS

Module 8: Summary Challenge

- Implementing and Troubleshooting Scalable Multiarea Network 1
- Implementing and Troubleshooting Scalable Multiarea Network 2

CCSA - Check Point Security Administration — 35

Check Point Security Administration (R77 GAiA) provides you with an understanding of the basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades. During this course, you will configure a Security Policy and learn about managing and monitoring a secure network, upgrading and configuring a Security Gateway, and implementing a virtual private network. This course prepares learners for CCSA exam #156-215.77.

Module 1: Check Point Security Management

- Check Point Security Management
- Architecture (SMART)
- SmartConsole
- Security Management Server
- Security Gateway

Module 2: The Check Point Firewall

- OSI Model
- Mechanism for controlling
- Network traffic.
- Packet Filtering
- Stateful Inspection
- Application Intelligence

Module 3: Security Gateway Inspection Architecture

- INSPECT Engine Packet Flow

Module 4: Deployment Considerations

- Standalone Deployment
- Distributed Deployment
- Standalone Full HA
- Bridge Mode

Module 5: Check Point SmartConsole Clients

- SmartDashboard
- Smartview Tracker
- SmartLog
- SmartEvent
- SmartView Monitor
- SmartReporter
- SmartUpdate
- SmartProvisioning
- SmartEndpoint

Module 6: Security Management Server

- Managing Users in SmartDashboard
- Users Database

Module 7: Securing Channels of Communication

- Secure Internal Communication
- Testing the SIC Status
- Resetting the Trust State

LPI – Linux Essentials | 35

This course teaches the basic concepts of processes, programs and the components of the Linux operating system. You learn the basic knowledge of computer hardware, gain an understanding of open source applications in the workplace, and learn to navigate systems on a Linux desktop rudimentary commands to navigate the Linux command line.

This course is a prep course for the Linux Essentials exam from Linux Professional Institute and is meant to help those without Linux experience to pass their first Linux certification. This course covers objectives for both the LPI Essentials exam version 1.0 and 1.5.

Module 1: The Linux Community and a Career in Open Source

- Linux Evolution and Popular Operating Systems
- Major Open Source Applications
- Understanding Open Source Software and Licensing
- ICT Skills and Working in Linux

Module 2: Finding Your Way on a Linux System

- Command Line Basics
- Using the Command Line to Get Help
- Using Directories and Listing Files
- Creating, Moving and Deleting Files

Module 3: The Power of the Command Line

- Archiving Files on the Command Line
- Searching and Extracting Data from Files
- Turning Commands into a Script

Module 4: The Linux Operating System

- Choosing an Operating System
- Understanding Computer Hardware
- Where Data is Stored
- Your Computer on the Network

Module 5: Security and File Permissions

- Basic Security and Identifying User Types
- Creating Users and Groups
- Managing File Permissions and Ownership
- Special Directories and Files

Python | 30

This course is a great introduction to both fundamental programming concepts and the Python programming language. By the end, you'll be familiar with Python syntax and you'll be able to put into practice what you'll have learned in a final project you'll develop locally.

The course aims to teach everyone the basics of programming computers using Python. The course covers the basics of how one constructs a program from a series of simple instructions in Python. The course has no pre-requisites. Anyone with moderate computer experience should be able to master the materials in this course.

Python is a general-purpose, versatile and popular programming language. It's great as a first language because it is concise and easy to read, and it is also a good language to have in any programmer's stack as it can be used for everything from web development to software development and scientific applications.

Module 1: Introduction

- Installing Python
- Writing Your First Program

Module 2: Python Basic Data Types and Variables

- Expressions, Statements, Variables

Module 3: Python Input / Output

- Using The Print Function
- Getting Input from The User

Module 4: Making Decisions - if Statements

- The Relational Operators
- The Logical Operators
- Simple if Statement
- if-else Statement
- if-elif Statement

Module 5: while Loops

- Introduction to while Loops
- Using continue
- Using break

Module 6: Graphs

- Creating graphs with Matplotlib
- Title, Xaxis, Yaxis, Legend
- Subplot
- Synchronous graphs

Module 7: for Loops and Iterators

- Introduction to for Loops
- Understanding Iterators
- Iterators And Dictionaries

Module 8: List Comprehensions

- Introduction to List Comprehensions
- Using List Comprehensions with Files

Module 9: Functions

- Defining Functions
- Calling Functions
- Functions with Multiple Arguments
- Recursive Functions

Module 10: Exception Handling

- Try-Except Statements
- Try-Except-Finally Statements

Module 11: Using Data Structures

- Lists
- Tuples
- Dictionaries

Module 12: Python Network Programming

- Networking – Socket
- Client Socket
- Server Socket
- Live Server
- Reteriving web page using urllib
- BeautifulSoap for Parsing HTML

Hacking Essentials — 20

This short module aims to give students a preliminary understanding of principle in hacking. Students will learn the following objectives:

- Cybersecurity threats, vulnerabilities and attacks
- Reconnaissance
- Denial-of-Service Attacks (DoS)
- Final Challenge: Hacking Essentials Lab

מה אני עושה לאחר סיום הלימודים? הצעד הבא

בסיום הקורס תוכל לבחור מהו הצעד הבא שלך:

1. **להתחיל לעבוד כמנהל סיסטם או כמנהל רשתות.**

2. **להמשיך בצעד הבא - תכנית הלימודים CSP – מיישם הגנת סייבר.**

The Cyber Security Practitioner is responsible for implementing the organization's cyber protection, and has the specific perspective of the following aspects:

1. The installation, operation and maintenance of cyber protection products.
2. The implementation of routine security procedures.
3. First level identification and treatment in cyber events based on types of threats and attacks.
4. May includes International Certification such as CompTIA Security+, or (ISC)^2 SSCP.
5. This is in recognition of understanding of the activities, needs and corporate objectives.

3. **להמשיך בצעד הבא - תכנית הלימודים SOC-IR – מומחה ניטור במרכז ניטור ותגובה לאירועי סייבר.**

A SOC-IR specialist is responsible for critical core subjects in operating cyber monitoring centers and primary response teams. The SOC operator performs the prelaminar necessary actions when a cyber event is identified.

4. **להמשיך בצעד הבא - תכנית הלימודים CSTP – ארכיטקט הגנת סייבר.**

A person with an academic background, wide-ranging and profound theoretical knowledge, who is in charge of:

1. Designing technological solutions for cyber protection in the organization combining technologies and security methods.
2. Adjusting cyber protection products and integrating them in the IT infrastructure, including storage and backup.
3. Accompanying the process of handling security events with a technology standpoint, acknowledging the organization activities, needs and objectives.
4. May includes International Certification such as CompTIA Security+, or (ISC)^2 SSCP.
5. This is in recognition of understanding of the activities, needs and corporate objectives.

5. **להמשיך בצעד הבא - תכנית הלימודים CSPT – מומחה בדיקות חדירות** (האקר, מבוסס על תכנית הלימודים הבינלאומית Hacking Defined Experts).

Before this course, the candidate should complete his knowledge in Linux Essentials and Python code. An Expert with wide and up dated knowledge as well as practical abilities in vulnerabilities detection and penetration testing in cyber systems.

הצהרת מועמד ללימודים:

הריני מאשר/ת בזאת כי קראתי את דף מידע זה והבנתי את תכנו. ידוע לי כי עלי לעמוד בדרישות הלימוד כתנאי לקבלת תעודה.

שם:_____ **תאריך:**_____

See Security International Cyber College