SOC OPERATOR

LEVEL-1

FOR CISCO CYBER OPS

CISCO CERTIFIED CCNA CYBER OPS

EC-Council CIH Certified Incident Handler

CompTIA CySA+

להיות SOC OPERATOR.

להיות חלק ממוקד ניטור סייבר וצוות התגובה.

להבין את ארכיטקטורת אבטחת המידע הארגונית בשגרה, אך בד בבד - עם קרות אירוע, לזהות פעילות אנומלית ו/או זדונית במערך התקשוב הארגוני באמצעות כלי הניטור והבקרה; לנתח בקווים כלליים וראשוניים את מהות הפעילות והשלכותיה האפשריות; להכיל את האירוע תוך תחזימתו; לספק תשתית בסיסית להתאוששות אחר סילוק המפגע.

וְלֹא פָּחוֹת חָשׁוּב: נִלְמָד כְּפִי שֶׁרַק שִׂיא סֶקְיוּריטִי יוֹדַעַת לְלַמֵּד, עִם הַלֵּב.

המסלול להסמכת בקר SOC על-בסיס Cisco Cyber Ops

אודות המכללה

מכללת See Security הנה מכללה **בינלאומית** התמחותית **למקצועות הסייבר**, 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 הקבוצה שבה משולבת המכללה, מר אבי ויסמן, הינו ממובילי ענף הסייבר, יועץ לממשלת ישראל בנושא "אסדרת מקצועות הגנת הסייבר בישראל", פרשן בערוצי השידור בארץ ובחו"ל, מקימו של הפורום הלאומי לאבטחת מידע IFIS (לצד האלוף במיל' וראש המל"ל לשעבר, יעקב עמידרור), מנכ"ל משותף בחברה להשמת כוח אדם בענף הסייבר *SeeHR*, בחברה לייעוץ הגנת *סייבר See Secure Consulting*, בחברה לפתרונות Managed SEIM/SOC בשם See *Events* ובמכללה הבינלאומית לסייבר *See Security College International*.

אודות אסדרת מקצועות הסייבר בישראל: מערך הסייבר הלאומי

המערך אשר פועל במסגרת משרד ראש הממשלה כיחידה עצמאית, החליט להפעיל אסדרה (רגולציה) מחייבת בנושא הגדרתם של המקצועות השונים בעולם הסייבר, ומפעיל המלצות ברורות בנוגע לתכני הידע לכל מקצוע. חלק ממקצועות הסייבר דורשים הבנת סביבת ה- SOC.

אודות התכנית ללימודי בקר SOC

התחומים בהם עוסק הקורס הם נושאי הליבה הקריטיים בתחום הפעלת מוקדי ניטור סייבר וצוותי תגובה ראשוניים. בוגרי הקורס נדרשים ללמוד את רזי פעילות הליבה של סביבת ה- SOC. בתוך כך, הם נדרשים להכיר את האספקטים התיאורטיים העומדים מאחורי תחום האחריות שלהם ואת הפעולות האקטיביות אשר נדרש מהם לבצע עם היווצרות חשד לאירוע סייבר. באחריות איש הניטור להבין את ארכיטקטורת אבטחת המידע הארגונית שלו בשגרה. אך עם קרות אירוע, באחריותו: לזהות פעילות אנומלית ו/או זדונית במערך התקשוב הארגוני באמצעות כלי הניטור והבקרה; לנתח בקווים כלליים וראשוניים את מהות הפעילות והשלכותיה האפשריות; להכיל את האירוע תוך תחימתו; לספק תשתית בסיסית להתאוששות אחר סילוק המפגע.

במידת הצורך, יבצע הסלמה לאנליסט בכיר יותר Tier-2 או לאנשי Tier-3: מומחי פורנזיקה או Malware Analysis.

קהל יעד

בעלי ידע מתחום תשתיות התקשוב: תקשורת המחשבים והיכרות בסיסית עם עולם מערכות ההפעלה, בעלי עניין להתפתח בתחום Cyber Security Operation Center & Incident Response.

מטרת התכנית

התוכנית נבנתה לצרכי ידע מעשי: הכשרת אנשי מקצוע המתעתדים לאייש מוקדי ניטור ובקרה (SIEM/SOC) ו/או לשמש כצוותי תגובה ראשוניים לאירועי אבטחת מידע (Incident Response).

היכולת תירכש מתוך היכרות עם הטכנולוגיות, הטכניקות והוראות העבודה הנהוגות (Best Practice) בתחומים אלו, יכולת זו תוקנה לתלמיד בתוכנית הלימודים בין השאר, באמצעות הרצאות, התנסויות ותרגול.

תנאי קבלה

- רקע בעולם רשתות התקשורת ומערכות ההפעלה.
- נכונות לעבודה עצמית מונחית.
- ראיון אישי.

סגל מרצים

את התכנית מובילים עמי צרפתי ואלעזר בירו מחברת Cyber Control, ויקי בן-ניסן, מנהל תחום במכללה. המרצים ממובילי הענף, מומחים מקצועיים מובילים בתחומם, המתמחים בסביבות SOC ו- Incident Response, בעלי שם עולמי.

המסלול להסמכת בקר SOC
על בסיס CISCO CYBER OPS

עלות

סך 9,000 שח + 400 שח דמי רישום (כולל מע"מ).

מתכונת הלימודים

משך התכנית 80 שעות, במתכונת של מפגשי ערב (כ- 3 חודשים). הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח פעמיים בשנה.

חובות אקדמיות

- קיימת חובת נוכחות ב-90% מהמפגשים.
- קיימת חובת עמידה בדרישות סיום (עבודה או מבחן).
- בנושאים הטכניים: תרגול (Hands-on) בכיתה (מעבדה).

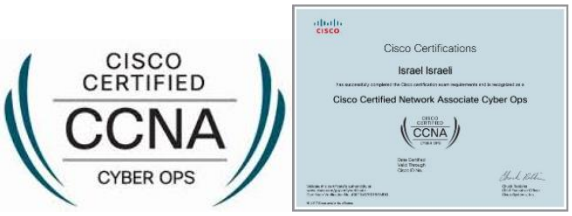
זכאות לתעודה והסמכות בינלאומיות

לעומדים בדרישות, תוענק תעודה מטעם See-Security:

"Certified SOC Analyst - בקר SOC".

מי שאינם עומדים בדרישות, יהיו זכאים לתעודת השתתפות, ולהשלמת מחויבויותיהם (השתתפות חוזרת / עבודות ומשימות) ללא תשלום, לצורך קבלת ההסמכה.

התכנית מכינה את הבוגרים להסמכה הבינלאומית של **Cisco**



הבוגרים מסוגלים לגשת למבחני ההסמכה בינלאומיים נוספים: CySA+ של CompTIA, ECiH של EC-Council.

כישורים מבוקשים לבקר SOC

סקרנות, ירידה לפרטים קטנים, עבודה מתודולוגית, עבודת צוות, שירותיות, יצירתיות, יכולת למידה עצמית, יכולת חיפוש (לוגיקה בחיפוש).

הערות

- פתיחת התכנית מותנית בכמות של 10 נרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכללה.
- המכללה מביאה לידיעת הנרשמים והסטודנטים כי ייתכנו שינויים במערך התכנית, במועדי הלימוד והבחינות או בכל נושא אחר. הודעה על שינוי תימסר למשתתפים.
- תוכנית הלימודים מחייבת בהכנת שיעורי בית להשגת יעדי הלימוד.
- משימות קריאה מהווים חובה לימודית, ובכללם, ספרי הקורס וחומרי הלימוד האחרים.

למידע נוסף / פגישת יעוץ

מידע מינהלי: אלוירה אליסייב, 03-6122831, 052-8787889,
elvira@see-security.com

יעוץ אקדמי: אבי ויסמן, 03-5799555, 054-5222305,
avi@see-security.com

הצהרת תלמיד בלימודי בקר SOC

הריני מאשר בזאת כי קיבלתי דף מידע זה, הבנתי את תכנו והסכמתי לתנאים המפורטים בו.

שם הנרשם: _____ תאריך: _____ חתימה _____

תכנית לימודים

נושא	שעות
Chapter 0: Course Introduction	2
Chapter 1: Cybersecurity and the Security Operations Center	2
Chapter 2 – Windows Operating System	2
Chapter 3: Linux Operating System	2
Chapter 4: Network Protocols and Services	2
Chapter 5: Network Infrastructure	2
Chapter 6: Principles of Network Security	8
Chapter 7: Network Attacks: A Deeper Look	4
Chapter 8: Protecting the Network	12
Chapter 9: Cryptography and the Public Key Infrastructure	1
Chapter 10: Endpoint Security and Analysis	3
Chapter 11: Security Monitoring	4
Chapter 12: Intrusion Data Analysis	20
Chapter 13: Incident Response and Handling	16
סך הכל	**80**

Chapter 0: Course Introduction

0.0 Welcome to CCNA: Cybersecurity Operations

0.0.1 Message to the Student
0.0.1.1 Welcome
0.0.1.2 A Global Community
0.0.1.3 More than Just Information
0.0.1.4 How We Teach
0.0.1.5 Ethical Hacking Statement
0.0.1.6 Course Overview

Chapter 1: Cybersecurity and the Security Operations Center

1.0.1.2 Activity – Top Hacker Shows Us How It is Done

1.1 The Danger

1.1.1 War Stories
1.1.2 Threat Actors
1.1.3 Threat Impact

1.2 Fighters in the War Against Cybercrime

1.2.1 The Modern Security Operations Center
1.2.2 Becoming a Defender
1.2.2.1 Certifications
1.2.2.4 Getting Experience

Chapter 2: Windows Operating System

2.1.2 Windows Architecture and Operations
2.2 Windows Administration
2.2.1 Windows Configuration and Monitoring
2.2.2 Windows Security

Chapter 3: Linux Operating System

3.1.1.3 Linux in the SOC
3.1.1.4 Linux Tools
3.1.2 Working in the Linux Shell
3.1.2.1 The Linux Shell
3.1.2.3 File and Directory Commands
3.1.3 Linux Servers and Clients
3.2 Linux Administration
3.2.1 Basic Server Administration
3.2.1.1 Service Configuration Files
3.2.1.2 Hardening Devices
3.2.1.3 Monitoring Service Logs
3.2.2 The Linux File System
3.3 Linux Hosts
3.3.1 Working with the Linux GUI
3.3.2 Working on a Linux Host

Chapter 4: Network Protocols and Services

4.1 Network Protocols
4.1.1 Network Communications Process
4.1.2 Communications Protocols
4.2 Ethernet and Internet Protocol (IP)
4.2.1 Ethernet
4.2.2 IPv4
4.2.3 IPv4 Addressing Basics
4.2.4 Types of IPv4 Addresses
4.2.5 The Default Gateway
4.2.6 IPv6
4.3 Connectivity Verification
4.3.1 ICMP
4.3.2 Ping and Traceroute Utilities
4.4 Address Resolution Protocol
4.4.1 MAC and IP
4.4.2 ARP
4.4.3 ARP Issues
4.5 The Transport Layer
4.5.1 Transport Layer Characteristics
4.5.2 Transport Layer Operation
4.6 Network Services
4.6.1 DHCP
4.6.2 DNS
4.6.3 NAT
4.6.4 File Transfer and Sharing Services
4.6.5 Email
4.6.6 HTTP

Chapter 5: Network Infrastructure

5.1 Network Communication Devices
5.1.1 Network Devices
5.1.2 Wireless Communications
5.2 Network Security Infrastructure
5.2.1 Security Devices
5.2.2 Security Services
5.3 Network Representations
5.3.1 Network Topologies

Chapter 6: Principles of Network Security

6.1 Attackers and Their Tools

6.1.1 Who is Attacking Our Network?
6.1.1.1 Threat, Vulnerability, and Risk
6.1.1.2 Hacker vs. Threat Actor
6.1.1.3 Evolution of Threat Actors
6.1.1.4 Cybercriminals
6.1.1.5 Cybersecurity Tasks
6.1.1.6 Cyber Threat Indicators
6.1.1.7 Activity – What Color is my Hat?
6.1.2 Threat Actor Tools
6.1.2.1 Introduction of Attack Tools
6.1.2.2 Evolution of Security Tools
6.1.2.3 Categories of Attacks
6.1.2.4 Activity: Classify Hacking Tools

6.2 Common Threats and Attacks

6.2.1 Malware
6.2.1.1 Types of Malware
6.2.1.2 Viruses
6.2.1.3 Trojan Horses
6.2.1.4 Trojan Horse Classification
6.2.1.5 Worms
6.2.1.6 Worm Components
6.2.1.7 Ransomware
6.2.1.8 Other Malware
6.2.1.9 Common Malware Behaviors
6.2.1.10 Activity: Identify the Malware Type
6.2.1.11 Lab: Anatomy of Malware
6.2.2 Common Network Attacks
6.2.2.1 Types of Network Attacks
6.2.2.2 Reconnaissance Attacks
6.2.2.3 Sample Reconnaissance Attacks
6.2.2.4 Access Attacks
6.2.2.5 Types of Access Attacks
6.2.2.6 Social Engineering Attacks
6.2.2.7 Phishing Social Engineering Attacks
6.2.2.8 Strengthening the Weakest Link
6.2.2.9 Lab – Social Engineering
6.2.2.10 Denial of Service Attacks
6.2.2.11 DDoS Attacks
6.2.2.12 Example DDoS Attack
6.2.2.13 Buffer Overflow Attack
6.2.2.14 Evasion Methods
6.2.2.15 Activity: Identify the Types of Network Attack
6.2.2.16 Activity: Components of a DDoS Attack

Chapter 7: Network Attacks: A Deeper Look

7.1 Network Monitoring and Tools

7.1.1 Introduction to Network Monitoring
7.1.1.1 Network Security Topology
7.1.1.2 Network Monitoring Methods
7.1.1.3 Network Taps
7.1.1.4 Traffic Mirroring and SPAN
7.1.2 Introduction to Network Monitoring Tools
7.1.2.1 Network Security Monitoring Tools
7.1.2.2 Network Protocol Analyzers
7.1.2.3 NetFlow
7.1.2.4 SIEM
7.1.2.5 SIEM Systems
7.1.2.6 Activity: Identify the Network Monitoring Tool
7.1.2.7 Packet Tracer: Logging Network Activity

7.2 Attacking the Foundation

7.2.1 IP Vulnerabilities and Threats
7.2.1.1 IPv4 and IPv6
7.2.1.2 The IPv4 Packet Header
7.2.1.3 The IPv6 Packet Header
7.2.1.4 IP Vulnerabilities
7.2.1.5 ICMP Attacks
7.2.1.6 DoS Attacks
7.2.1.7 Amplification and Reflection Attacks
7.2.1.8 DDoS Attacks

10.1.1.1 Endpoint Threats
10.1.1.2 Endpoint Security
10.1.1.3 Host-Based Malware Protection
10.1.1.4 Network-Based Malware Protection
10.1.1.5 Cisco Advanced Malware Protection (AMP)
10.1.1.6 Activity: Identify Antimalware Terms and Concepts

10.1.2 Host-Based Intrusion Protection
10.1.2.1 Host-Based Firewalls
10.1.2.2 Host-Based Intrusion Detection
10.1.2.3 HIDS Operation
10.1.2.4 HIDS Products
10.1.2.5 Activity: Identify the Host-Based Intrusion Protection Terminology

10.1.3 Application Security
10.1.3.1 Attack Surface
10.1.3.2 Application Blacklisting and Whitelisting
10.1.3.3 System-Based Sandboxing
10.1.3.4 Video Demonstration: Using a Sandbox to Launch Malware

10.2 Endpoint Vulnerability Assessment

10.2.1 Network and Server Profiling
10.2.1.1 Network Profiling
10.2.1.2 Server Profiling
10.2.1.3 Network Anomaly Detection
10.2.1.4 Network Vulnerability Testing
10.2.1.5 Activity: Identify the Elements of Network Profiling

10.2.2 Common Vulnerability Scoring System (CVSS)
10.2.2.1 CVSS Overview
10.2.2.2 CVSS Metric Groups
10.2.2.3 CVSS Base Metric Group
10.2.2.4 The CVSS Process
10.2.2.5 CVSS Reports
10.2.2.6 Other Vulnerability Information Sources
10.2.2.7 Activity: Identify CVSS Metrics

10.2.3 Compliance Frameworks
10.2.3.1 Compliance Regulations
10.2.3.2 Overview of Regulatory Standards
10.2.3.3 Activity: Identify Regulatory Standards

10.2.4 Secure Device Management
10.2.4.1 Risk Management
10.2.4.2 Activity: Identify the Risk Response
10.2.4.3 Vulnerability Management
10.2.4.4 Asset Management
10.2.4.5 Mobile Device Management
10.2.4.6 Configuration Management
10.2.4.7 Enterprise Patch Management
10.2.4.8 Patch Management Techniques
10.2.4.9 Activity: Identify Device Management Activities

10.2.5 Information Security Management Systems
10.2.5.1 Security Management Systems
10.2.5.2 ISO-27001
10.2.5.3 NIST Cybersecurity Framework
10.2.5.4 Activity: Identify the ISO 27001 Activity Cycle
10.2.5.5 Activity: Identify the Stages in the NIST Cybersecurity Framework

Chapter 11: Security Monitoring

11.1 Technologies and Protocols

11.1.1 Monitoring Common Protocols
11.1.1.1 Syslog and NTP
11.1.1.2 NTP
11.1.1.3 DNS
11.1.1.4 HTTP and HTTPS
11.1.1.5 Email Protocols
11.1.1.6 ICMP
11.1.1.7 Activity: Identify the Monitored Protocol

11.1.2 Security Technologies
11.1.2.1 ACLs
11.1.2.2 NAT and PAT
11.1.2.3 Encryption, Encapsulation, and Tunneling
11.1.2.4 Peer-to-Peer Networking and Tor
11.1.2.5 Load Balancing
11.1.2.6 Activity: Identify the Impact of the Technology on Security and Monitoring

11.2 Log Files

11.2.1 Types of Security Data
11.2.1.1 Alert Data
11.2.1.2 Session and Transaction Data
11.2.1.3 Full Packet Captures
11.2.1.4 Statistical Data
11.2.1.5 Activity: Identify Types of Network Monitoring Data

11.2.2 End Device Logs
11.2.2.1 Host Logs
11.2.2.2 Syslog
11.2.2.3 Server Logs
11.2.2.4 Apache Webserver Access Logs
11.2.2.5 IIS Access Logs
11.2.2.6 SIEM and Log Collection
11.2.2.7 Activity: Identify Information in Logged Events
11.2.3 Network Logs
11.2.3.1 Tcpdump
11.2.3.2 NetFlow
11.2.3.3 Application Visibility and Control
11.2.3.4 Content Filter Logs
11.2.3.5 Logging from Cisco Devices
11.2.3.6 Proxy Logs
11.2.3.7 NextGen IPS
11.2.3.8 Activity: Identify the Security Technology from the Data Description
11.2.3.9 Activity: Identify the NextGen IPS Event Type
11.2.3.10 Packet Tracer: Explore a NetFlow Implementation
11.2.3.11 Packet Tracer: Logging from Multiple Sources

Chapter 12: Intrusion Data Analysis

12.1 Evaluating Alerts

12.1.1 Sources of Alerts
12.1.1.1 Security Onion
12.1.1.2 Detection Tools for Collecting Alert Data
12.1.1.3 Analysis Tools
12.1.1.4 Alert Generation
12.1.1.5 Rules and Alerts
12.1.1.6 Snort Rule Structure
12.1.1.7 Lab: Snort and Firewall Rules
12.1.2 Overview of Alert Evaluation
12.1.2.1 The Need for Alert Evaluation
12.1.2.2 Evaluating Alerts
12.1.2.3 Deterministic Analysis and Probabilistic Analysis
12.1.2.4 Activity: Identify Deterministic and Probabilistic Scenarios
12.1.2.5 Activity: Identify the Alert Classification

12.2 Working with Network Security Data

12.2.1 A Common Data Platform
12.2.1.1 ELSA
12.2.1.2 Data Reduction
12.2.1.3 Data Normalization
12.2.1.4 Data Archiving
12.2.1.5 Lab – Convert Data into a Universal Format
12.2.2 Investigating Network Data
12.2.2.1 Working in Sguil
12.2.2.2 Sguil Queries
12.2.2.3 Pivoting from Sguil
12.2.2.4 Event Handling in Sguil
12.2.2.5 Working in ELSA
12.2.2.6 Queries in ELSA
12.2.2.7 Investigating Process or API Calls
12.2.2.8 Investigating File Details
12.2.2.9 Lab – Regular Expression Tutorial
12.2.2.10 Lab: Extract an Executable from a PCAP
12.2.3 Enhancing the Work of the Cybersecurity Analyst
12.2.3.1 Dashboards and Visualizations
12.2.3.2 Workflow Management

12.3 Digital Forensics

12.3.1 Evidence Handling and Attack Attribution
12.3.1.1 Digital Forensics
12.3.1.2 The Digital Forensics Process
12.3.1.3 Types of Evidence
12.3.1.4 Evidence Collection Order
12.3.1.5 Chain of Custody
12.3.1.6 Data Integrity and Preservation
12.3.1.7 Attack Attribution
12.3.1.8 Activity: Identify the Type of Evidence
12.3.1.9 Activity: Identify the Forensic Technique Terminology
12.4.1.1 Lab: Interpret HTTP and DNS Data to Isolate Threat Actor
12.4.1.2 Lab: Isolate Compromised Host using 5-Tuple

Chapter 13: Incident Response & Handling

13.1 Incident Response Models

13.1.1 The Cyber Kill Chain
13.1.1.1 Steps of the Cyber Kill Chain
13.1.1.2 Reconnaissance

13.1.1.3 Weaponization
13.1.1.4 Delivery
13.1.1.5 Exploitation
13.1.1.6 Installation
13.1.1.7 Command and Control
13.1.1.8 Actions on Objectives
13.1.1.9 Activity: Identify the Kill Chain Step
13.1.2 The Diamond Model of Intrusion
13.1.2.1 Diamond Model Overview
13.1.2.2 Pivoting Across the Diamond Model
13.1.2.3 The Diamond Model and the Cyber Kill Chain
13.1.2.4 Activity – Identify the Diamond Model Features
13.1.3 The VERIS Schema
13.1.3.1 What is the VERIS Schema?
13.1.3.2 Create a VERIS Record
13.1.3.3 Top-Level and Second-Level Elements
13.1.3.4 The VERIS Community Database
13.1.3.5 Activity – Apply the VERIS Schema to an Incident

13.2 Incident Handling

13.2.1 CSIRTs
13.2.1.1 CSIRT Overview
13.2.1.2 Types of CSIRTs
13.2.1.3 CERT
13.2.1.4 Activity – Match the CSIRT with the CSIRT Goal
13.2.2 NIST 800-61r2
13.2.2.1 Establishing an Incident Response Capability
13.2.2.2 Incident Response Stakeholders
13.2.2.3 NIST Incident Response Life Cycle
13.2.2.4 Preparation
13.2.2.5 Detection and Analysis
13.2.2.6 Containment, Eradication, and Recovery
13.2.2.7 Post-Incident Activities
13.2.2.8 Incident Data Collection and Retention
13.2.2.9 Reporting Requirements and Information Sharing
13.2.2.10 Activity: Identify the Incident Response Plan Elements
13.2.2.11 Activity: Identify the Incident Handling Term
13.2.2.12 Activity: Identify the Incident Handling Step
13.2.2.13 Lab: Incident Handling