תכנית הלימודים למקצוע בקר SOC Tier 1

מכללת שיא סקיוריטי בשיתוף חברת ה-SOC שיא סקיור קונסלטינג

תכנית ייחודית למתחילים בעלי רקע בתמיכה טכנית ו-IT המעוניינים להשתלב במקצוע סייבר ראשוני עם ביקוש רב לעובדים.

הסמכות CCNA-Cyber Ops, CompTIA-CySA+ ו-EC Council-ECIH.

SeeSecure

להיות SOC ANALYST.

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 תחימתו; לספק תשתית בסיסית להתאוששות אחר סילוק המפגע.

התחומים המכוסים בתוכנית הכשרה מקיפה זו מתייחסים למיומנויות הליבה ולידע שאתה צריך לדעת לעבודה ולתפעול של מרכזי SOC ו-IR. בוגרי ההכשרה יבינו את המרכיבים התיאורטיים והמעשיים הקשורים לתפקיד אנליסט SOC. סטודנטים יכולים גם לנסות את הסמכות CCNA-Cyber Ops ו/או CompTIA-CySA+ ו/או הסמכות של EC Council-ECIH.

וְלֹא פָּחוֹת חָשׁוּב: נִלְמָד כְּפִי שָׁרַק שִׂיא סָקְיוּרִיטִי יוֹדַעַת לְלַמֵּד, עִם הַלֵּב.

המסלול להסמכת בקר SOC

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

אנליסט SOC הוא איש מקצוע בתחום אבטחת סייבר שעובד כחלק מצוות כדי לנטר ולהילחם באיומים על תשתית ה-IT של הארגון, ולהעריך מערכות אבטחה ואמצעי אבטחה עבור חולשות ושיפורים אפשריים. ה-SOC מהווה "מרכז פעולות אבטחה", זוג של "חדר מלחמה לסייבר"; והצוות שבו מורכב מאנליסטים ומקצועני אבטחה אחרים, שבדרך כלל פועלים במיקום פיזי אחד. SOC עשוי להיות צוות פנימי המשרת ארגון יחיד או שירות במיקור חוץ המספק אבטחה ללקוח חיצוני אחד או יותר.

אנליסט SOC הוא מקצוע ומשרה שיכולה להיות אבן דרך נהדרת לקריירת אבטחת סייבר. ישנם שלושה שכבות עיקריות (או רמת מומחיות) בהתקדמות זו:

- אנליסט SOC Tier-1 הוא מומחה טריאז' שמנטר, מנהל ומגדיר כלי אבטחה, בודק תקריות כדי להעריך את דחיפותם, ומסלים תקריות במידת הצורך.
- אנליסט Tier 2 SOC מגיב לאירועים, מנהל התקפות חמורות שהוסלמו מ- Tier 1, מעריך את היקף ההתקפה והמערכות המושפעות מההתקפה, ואוסף נתונים לניתוח נוסף.
- אנליסט של Tier 3 SOC הוא צייד איומים, שפועל באופן יזום כדי לחפש חולשות ותוקפים חמקנים, עורך בדיקות חדירה ובדיקת הערכות פגיעות.

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).

קורס זה מספק את מרבית התשתית התיאורטית הנדרשת מגורמי הניטור ואף את הניסיון המעשי בכלים השונים אותם גורמי הניטור נדרשים להכיר ולהפעיל.

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

סגל מרצים

את התכנית מובילים אנשי מקצוע אמיתיים, מנהלי מרכזי SOC ו-Incident Response ותיקים מאוד ומקצוענים מהשורה הראשונה בישראל. בבעלותה של מכללת שיא סקיוריטי חברה נוספת שעוסקת במתן שירותי SOC מסוג זה, ואחראית על התוכנית.

עלות

סך 9,500 שח + 400 שח דמי רישום (כולל מע"מ).

מתכונת הלימודים

משך התכנית כ- 100 שעות, במתכונת של מפגשי בוקר (כ- 1.5 חודשים). הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח פעמיים בשנה.

חובות אקדמיות

- קיימת חובת נוכחות בכל המפגשים.
- 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:

"בקר SOC - Certified SOC Analyst".

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

התכנית מכינה את הבוגרים גם להסמכה הבינלאומית של CCNA-Cyber Ops ו/או +CompTIA-CySA, או ECIH.

הערות

- פתיחת התכנית מותנית במינימום 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.

מתווה התוכנית

Main Topics
Module 0: Course Introduction
Module 1: Information Security Basics
Module 2: Security Operations
Module 3: Monitoring & Analysis
Module 4: Threat & Vulnerability
Module 5: Monitoring & Intrusion
Module 6: Incident Response
Module 7: Windows Security Monitoring
Module 8: SIEM system

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

עיקרי תכנית הלימודים:

Module 0: Course Introduction

Welcome to SOC Analyst Course

- Message to the Student
- Welcome
- Today's Cybersecurity Analyst

Module 1: Information Security Basics

Information Security Terminology

- Information Security
- CIA
- Defense in depth
- Information Security Solutions

Module 2: Security Operations

SOC Operation

- Legacy vs Modern Security Operations
- Three Pillars
- People
- SOC Structure
- Tiered SOC Model
- Tireless SOC Model
- Processes
- SOC Charter
- Onboarding
- Security information and event management (SIEM) review

Module 3: Monitoring & Analysis of Common Protocols

SIEM & Monitoring Basics

- Technology - SIEM
- McAfee SIEM Foundation
- Log Collection
- Main Data Sources
- Network
- Network Traffic by Layer
- Network Traffic Collection
- Endpoint Traffic
- SIEM Terms & Definitions
- Event Examples
- Example of Security Solutions Alerts
- Type of SIEM Alerts
- High Severity Alert Flow
- Technology - Incident Management System
- Threat Intelligence Platform
- SOAR
- Automation

Module 4: Threat & Vulnerability Management

Incident response process.

Utilization of threat intelligence to support organizational security

- Threat Intelligence and its importance
- Definitions
- Intelligence sources
- Confidence levels
- Indicator management
- Threat classification
- Collection
- Commodity malware
- Attack frameworks
- Threat research
- Threat modeling methodologies

Module 5: Monitoring & Intrusion Data Analysis

1. **Analyze data as part of security monitoring activities**
   - Heuristics
   - Trend analysis
   - Endpoint
   - Network
   - Log review
   - Impact analysis
   - E-mail analysis
2. **Hardening controls to improve security**
   - Permissions
   - Allow list (previously known as whitelisting)
   - Blocklist (previously known as blacklisting)
   - Firewall
   - Intrusion prevention system (IPS) rules
   - Data loss prevention (DLP)
   - Endpoint detection and response (EDR)
   - Network access control (NAC)
   - Sinkholing
   - Malware signatures - Development/rule writing
   - Sandboxing
   - Port security

3. **Proactive threat hunting**
   - § Establishing a hypothesis
   - § Profiling threat actors and activities
   - § Threat hunting tactics - Executable process analysis
   - § Reducing the attack surface area
   - § Bundling critical assets
   - § Attack vectors
   - § Integrated intelligence
   - § Improving detection capabilities

Module 6: Incident Response

1. **Incident response process**
   - § Response coordination with relevant entities
   - § Factors contributing to data criticality
2. **Incident response procedure**
   - § Preparation
   - § Detection and analysis
   - § Containment
   - § Eradication and recovery
   - § Post-incident activities
3. **Potential indicators of compromise**

Incident Response in action

- § Network-related
- § Host-related
- § Application-related
- § Real life Incident Response cases

Module 7: Windows Security Monitoring

Introduction to Windows Security Monitoring

- § Windows Auditing Subsystem
- § Security Monitoring Scenarios
- § Local User Accounts
- § Local Security Groups
- § Microsoft Active Directory
- § Active Directory Objects
- § Authentication Protocols
- § Operating System Events
- § Logon Rights and User Privileges
- § Windows Applications
- § Filesystem and Removable Storage
- § Windows Registry
- § Network File Shares and Named Pipes

Module 8: SIEM system

1. **Getting to know the SIEM (Sentinel, QRadar, Splunk)**
   - § Introduction to **Azure Sentinel** SIEM interface, dashboard, logs, devices
   - § Introduction to **QRadar** SIEM interface, dashboard, logs, devices
   - § Introduction to **WatchDog-Splunk** SIEM interface, dashboard, logs, devices
   - § Architecture Overview
   - § Devices and Settings
   - § Data Sources
   - § Event Analysis
   - § Aggregation
   - § Watch Lists and Policy Editor
   - § Query Filters
   - § Rule Correlation
   - § Alarms
2. **Gaining Hands on experience**
   - § Working on the SIEM - queries, detection, analysis
   - § Domain User activity, Anti-Virus, Perimeter Defense, firewall, Correlation Engine…
3. **Detecting & Analyzing Attack scenarios**
   - § SIEM scenarios and analysis