המסלול להסמכת CIH|E מפעילי מרכז SOC ותומכי Incident Response

יועץ אקדמי: מר אבי ויסמן, מרצה ראשי: אורן אלימלך

תוכנית ממוקדת לאוכלוסיות טכנולוגיות, לבעלי רקע במחשבים להבנה והכרת כלים בעולם הניטור ה-SOC והתגובה לאירועים.

(תאריכים בעמוד הראשי של המכללה)

מבוא

תוכנית הלימודים להכשרת אנשי SOC ותומכים בסביבת Incident Response הינה תוכנית מקורית ראשונה מסוגה אשר נבנתה בישראל. 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 תחום זה. בתוך כך, הם נדרשים להכיר את האספקטים התיאורטיים העומדים מאחורי תחום האחריות שלהם ואף את הפעולות האקטיביות אשר נידרש מהם לבצע עם היווצרות חשד לאירוע סייבר. באחריות איש הניטור להבין את ארכיטקטורת אבטחת המידע הארגונית שלו בשגרה. 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.

מאפייני תוכנית הלימודים	
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית / **טכנית** / **יישום**
שלב:	מתחילים / **מתקדמים**
רוחב:	**ממוקד** / רחב
עומק:	סוקר / **עמוק למחצה**
הסמכות:	SOC/IR Practitioner
שעות:	**48 שעות**
פתיחה:	**ראה בעמוד הראשי של המכללה**
מתכונת:	**12 מפגשים ערב**
תרגול בית:	לא קיים / **קיים בהיקף 120 שעות**

מטרת התוכנית

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.

קהל יעד

בעלי ידע מתחום תשתיות התקשוב: תקשורת המחשבים והיכרות בסיסית עם עולם מערכות ההפעלה.

הסמכה

לעומדים בדרישות התוכנית, תוענק תעודה מטעם See-Security:

"מיישם מרכז בקרת סייבר מוסמך - Certified SOC Analyst".

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

הכרה

תוכנית הלימודים להכשרת אנשי SOC ותומכים בסביבת Incident Response, הינה הראשונה מסוגה בישראל, ונבנתה על-בסיס ההחלטות הרשמיות של המטה הקיברנטי הלאומי מינואר 2015 בנוגע לרשימת מקצועות הליבה באבטחת מידע וסייבר, ולצורך אספקת הביקוש לאנשי המקצוע המאיישים עמדות בקבוצת IR.

המסלול להכשרת מפעילי מרכז SOC ותומכי Incident Response

תנאי קבלה

- רקע בסיסי בעולם רשתות התקשורת ומערכות ההפעלה. התלמיד נדרש להכיר סוגיות בסיסיות במערכות ההפעלה המקובלות היום, פרוטוקולי תקשורת ומודל TCP/IP.
- נכונות לעבודה עצמית מונחית (כ- 120 שעות לימוד ביתי).
- ראיון אישי.

מטלות תוכנית הלימודים

- קיימת חובת נוכחות בכל המפגשים.
- קיימת חובת עמידה בדרישות סיום (עבודה או מבחן).
- בנושאים הטכניים - תרגול (Hands-on) בכיתת מעבדת מחשבים.

מתכונת הלימודים

משך התכנית כ- 48 שעות, במתכונת של 12 מפגשי ערב (כ- 1.5 חודשים). הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח פעמיים בשנה.

עלות הלימודים

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

המרצים בתוכנית

על המרצים נמנים מובילי הענף, בהם מומחים מקצועיים המובילים בתחומם, ולרבות רפי רוסו, מומחה Incident Response.

מידע נוסף

- **מידע מינהלי:** אלוירה אליסייב, 03-6122831, 052-8787889, elvira@see-security.com
- **יועץ אקדמי:** אבי ויסמן, 054-5222305, avi@see-security.com

תוכנית הלימודים

ECHI – Incident Response Expert	40

Module 01: Introduction to Incident Response and Handling

- Cyber Incident Statistics
- Computer Security Incident
- Information as Business Asset
- Data Classification
- Common Terminologies
- Information Warfare
- Key Concepts of Information Security
- Vulnerability, Threat, and Attack
- Types of Computer Security Incidents
- Examples of Computer Security Incidents
- Verizon Data Breach Investigations Report – 2008
- Incidents That Required the Execution of Disaster Recovery Plans
- Signs of an Incident
- Incident Categories
  - Incident Categories: Low Level
  - Incident Categories: Middle Level
  - Incident Categories: High Level
- Incident Prioritization
- Incident Response
- Incident Handling
- Use of Disaster Recovery Technologies
- Impact of Virtualization on Incident Response and Handling
  Estimating Cost of an Incident
  Key Findings of DBIR – 2017
- Incident Reporting
- Incident Reporting Organizations

- Vulnerability Resources

Module 02: Risk Assessment

- Risk
- Risk Policy
- Risk Assessment
- NIST's Risk Assessment Methodology
  - Step 1: System Characterization
  - Step 2: Threats Identification
  - Step 3: Identify Vulnerabilities
  - Step 4: Control Analysis
  - Step 5: Likelihood Determination
  - Step 6: Impact Analysis
  - Step 7: Risk Determination
  - Step 8: Control Recommendations
  - Step 9: Results Documentation
- Steps to Assess Risks at Work Place
  - Step 1: Identify Hazard
  - Step 2: Determine Who Will be Harmed and How
  - Step 3: Analyze Risks and Check for Precautions
  - Step 4: Implement Results of Risk Assessment
  - Step 5: Review Risk Assessment
- Business Impact Analysis (BIA)
  - Need for Business Approach to Important Services
- Risk Analysis
  - Need for Risk Analysis
  - Risk Analysis: Approach
- Risk Mitigation
  - Risk Mitigation Strategies
- Cost/Benefit Analysis (CBA)
- NIST Approach for Control Implementation & Cyber Security Framework (CSF)
- Residual Risk
- Risk Management Tools
  - CRAMM
  - Acuity STREAM
  - ISO/IEC:27001:2013 + 27002
  - EAR / Pilar
  - MSAT

Module 03: Incident Response and Handling Steps

- How to Identify an Incident
- Handling Incidents
- Need for Incident Response
- Goals of Incident Response
- Incident Response Plan
  - Purpose of Incident Response Plan
  - Requirements of Incident Response Plan
  - Preparation
- Incident Response and Handling Steps
  - Step 1: Identification
  - Step 2: Incident Recording
  - Step 3: Initial Response
  - Step 4: Communicating the Incident
  - Step 5: Containment
  - Step 6: Formulating a Response Strategy
  - Step 7: Incident Classification
  - Step 8: Incident Investigation
  - Step 9: Data Collection
  - Step 10: Forensic Analysis
  - Step 11: Evidence Protection
  - Step 12: Notify External Agencies
  - Step 13: Eradication
  - Step 14: Systems Recovery
  - Step 15: Incident Documentation
  - Step 16: Incident Damage and Cost Assessment
  - Step 17: Review and Update the Response Policies
- Training and Awareness
- Security Awareness and Training Checklist
- Incident Management
  - Purpose of Incident Management
  - Incident Management Process
  - Incident Management Team
- Incident Response Team
  - Incident Response Team Members
  - Incident Response Team Members Roles and Responsibilities
  - Developing Skills in Incident Response Personnel
  - Incident Response Team Structure
  - Incident Response Team Dependencies
  - Incident Response Team Services
- Defining the Relationship between Incident Response, Incident Handling, and Incident Management
- Incident Response Best Practices
- Incident Response Policy
- Incident Response Plan Checklist
- Incident Handling System: RTIR
- RPIER (Regimented Potential Incident Examination Report) 1st Responder Framework
- FastIR

Module 04: CSIRT

- What is CSIRT?
- What is the Need of an Incident Response Team (IRT)
- CSIRT Goals and Strategy
- CSIRT Vision
- Common Names of CSIRT
- CSIRT Mission Statement
- CSIRT Constituency
- CSIRT Place in the Organization

- CSIRT Relationship with Peers
- Types of CSIRT Environments
- Best Practices for creating a CSIRT
  - Step 1: Obtain Management Support and Buy-in
  - Step 2: Determine the CSIRT Development Strategic Plan
  - Step 3: Gather Relevant Information
  - Step 4: Design your CSIRT Vision
  - Step 5: Communicate the CSIRT Vision
  - Step 6: Begin CSIRT Implementation
  - Step 7: Announce the CSIRT
  - Step 8: Evaluate CSIRT Effectiveness
- Role of CSIRTs
- Roles in an Incident Response Team
- CSIRT Services
  - Reactive Services
  - Proactive Services
  - Security Quality Management Services
- CSIRT Policies and Procedures
  - Attributes
  - Content
  - Validity
  - Implementation, Maintenance, and Enforcement
- How CSIRT Handles a Case
- CSIRT Incident Report Form
- Incident Tracking and Reporting Systems – What is needed?
  - Application for Incident Response Teams (AIRT)
  - BMC Remedy Action Request System
  - The GNU Privacy Guard (GnuPG / PGP)
- CERT-CC
- CERT(R) Coordination Center: Incident Reporting Form
- CERT:OCTAVE
  - OCTAVE Method
  - OCTAVE-S
  - OCTAVE Allegro
- World CERTs
- IRTs Around the World

Module 05: Handling Network Security Incidents

- Denial-of-Service Incidents
- Distributed Denial-of-Service Attack
- Detecting DoS Attack
- Incident Handling Preparation for DoS
  - DoS Response Strategies
  - Preventing a DoS Incident
  - Following the Containment Strategy to Stop DoS
- Unauthorized Access Incident
  - Detecting Unauthorized Access Incident
  - Incident Handling Preparation
  - Incident Prevention
  - Following the Containment Strategy to Stop Unauthorized Access
  - Eradication and Recovery
  - Recommendations
- Inappropriate Usage Incidents
  - Detecting the Inappropriate Usage Incidents
  - Incident Handling Preparation
  - Incident Prevention
  - Recommendations
- Multiple Component Incidents
  - Preparation for Multiple Component Incidents
  - Following the Containment Strategy to Stop Multiple Component Incidents
  - Recommendations
- Network Traffic Monitoring Tools
  - Ntop
  - EtherApe
  - Ngrep
  - SolarWinds: Orion NetFlow Traffic Analyzer
  - Nagios: op5 Monitor
- Network Auditing Tools
  - Tenable: Nessus
  - OpenVAS
  - Rapid7: Nexpose
  - Nmap
  - Netcat
  - Wireshark
  - Argus - Audit Record Generation and Utilization System
  - Snort
- Network Protection Tools
  - Iptables
  - ModSecurity
  - NetDetector
  - TigerGuard
  - Web Application Firewalls

Module 06: Handling Malicious Code Incidents

- Count of Malware Samples
- Virus
- Worms
- Trojans and Spywares
- Incident Handling Preparation
- Incident Prevention
- Detection of Malicious Code
- Containment Strategy
- Evidence Gathering and Handling
- Eradication and Recovery
- Recommendations
- Antivirus Systems
- Integrity Systems
  - Tripwire Enterprise
  - OSSEC

Module 07: Handling Insider Threats

- Insider Threats
- Anatomy of an Insider Attack
- Insider Risk Matrix
- Insider Threats Detection
- Insider Threats Response
- Insider's Incident Response Plan
- Guidelines for Detecting and Preventing Insider Threats
  - Human Resources
  - Network Security
  - Access Controls
  - Security Awareness Program
  - Administrators and Privileged Users
  - Backups
  - Audit Trails and Log Monitoring
  - Employee Monitoring Tools

Module 08: Forensic Analysis and Incident Response

- Computer Forensics
- Objectives of Forensics Analysis
- Role of Forensics Analysis in Incident Response
- Forensic Readiness
- Forensic Readiness and Business Continuity
- Types of Computer Forensics
- Computer Forensic Investigator
- People Involved in Computer Forensics
- Computer Forensics Process
- Digital Evidence
- Characteristics of Digital Evidence
- Collecting Electronic Evidence
- Challenging Aspects of Digital Evidence
- Forensic Policy
- Forensics in the Information System Life Cycle
- Forensic Analysis Guidelines
- Forensics Analysis Tools
  - Helix
  - DEFT
  - CAINE
  - KALI
  - Windows Forensic Toolchest
  - Knoppix Linux
  - The Coroner's Toolkit (TCT)
  - EnCase Forensics
  - FTK
  - NirSoft Suite
  - DumpReg
  - DumpSec
  - DumpEvt
  - Foundstone Forensic ToolKit
  - Sysinternals Suite
  - NSLOOKUP
  - dig – DNS Lookup Utility
  - Whois
  - VisualRoute
  - Netstat Command
  - Autopsy
  - Linux: DD, Find, Arp, Top, Grep, Strings Commands and Windows equivalents
  - Linux: ps, ls, lsof Commands

Module 09: Incident Reporting

- Incident Reporting
- Why to Report an Incident
- Why Organizations do not Report Computer Crimes
- Whom to Report an Incident
- How to Report an Incident
- Details to be Reported
- Preliminary Information Security Incident Reporting Form
- CERT Incident Reference Numbers
- Contact Information
  - Sample Report Showing Contact Information
- Summary of Hosts Involved
  - Sample Report Showing Summary of Hosts Involved
- Description of the Activity
  - Sample Report Showing Description of the Activity
- Log Extracts Showing the Activity
  - Example Showing the Log Extracts of an Activity
- Time Zone
- Federal Agency Incident Categories
- Organizations to Report Computer Incident
  - United State Internet Crime Task Force
  - Internet Crime Complaint Center (IC3)
  - Computer Crime & Intellectual Property Section
  - Internet Watch Foundation (IWF)
- Incident Reporting Guidelines
- Sample Incident Reporting Form
- Sample Post Incident Report

Module 10: Incident Recovery

- Incident Recovery
- Principles of Incident Recovery
- Incident Recovery Steps
- Contingency/Continuity of Operations Planning

- Business Continuity Planning
- Incident Recovery Plan
- Incident Recovery Planning Process
  - Incident Recovery Planning Team
  - Business Impact Analysis
  - Incident Recovery Plan Implementation
  - Incident Recovery Training
  - Incident Recovery Testing

Module 11: Security Policies and Laws

- Security Policy
- Key Elements of Security Policy
- Goals of a Security Policy
- Characteristics of a Security Policy
- Design of Security Policy
- Implementing Security Policies
- Acceptable Use Policy (AUP)
- Access Control Policy
  - Sample Access Control Policy
  - Importance of Access Control Policies
- Asset Control Policy
- Audit Trail Policy
  - Sample Audit Trail Policy 1
  - Importance of Audit Trail Policy
- Logging Policy
  - Importance of Logging Policies
- Documentation Policy
- Evidence Collection Policy
- Evidence Preservation Policy
- Information Security Policy
  - Information Security Policy: University of California
  - Information Security Policy: SANS
  - Importance of Information Security Policy
- National Information Assurance Certification & Accreditation Process (NIACAP) Policy
  - Importance of NIACAP Policy
- Physical Security Policy
  - Sample Physical Security Policy 1
  - Sample Physical Security Policy 2
  - Importance of Physical Security Policies
- Physical Security Guidelines
- Personnel Security Policies & Guidance
- Law and Incident Handling
  - Role of Law in Incident Handling
  - Legal Issues When Dealing with an Incident
  - Law Enforcement Agencies
- Laws and Acts
  - Searching and Seizing Computers without a Warrant
    - Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers: General Principles
    - Private Searches
  - The Privacy Protection Act
  - Federal Information Security Management Act (FISMA)
  - Cybercrime Act 2001
  - Information Technology Act
  - Sarbanes-Oxley Act (SOX)
  - Social Security Act
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - GDPR
  - Singapore Laws
  - Mexico
  - Brazilian Laws
  - Canadian Laws
  - United Kingdom's Laws
  - Belgium Laws
  - German Laws
  - Italian Laws
- Intellectual Property Laws

הערות לתוכנית הלימודים

א. תוכנית הלימודים מחייבת בהכנת שיעורי בית להשגת יעדי הלימוד.
ב. משימות קריאה מהווים חובה לימודית, ובכללם, ספרי הקורס וחומרי הלימוד האחרים.
ג. נושאי טכנאות/יישום אבטחת מידע (התקנות ותחזוקה) לא כלולים בתוכנית הלימודים (ראה תוכנית מתחילים)

הערות מינהל

- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי ביה"ס.
- דמי ההרשמה ומבחנים חיצוניים כלשהם אינם כלולים בשכר הלימוד.
- ייתכנו שינויים במערך התכנית, במועדי הלימודים והבחינות או בכל נושא אחר. הודעה על כל שינוי תימסר למשתתפים.