



לימודי תעודה להכשרת מנהלי אבטחת מידע וסייבר CISO וקציני הגנת נתונים DPO

בהתאם לתוכנית ההכשרה הבינלאומית
של EC-COUNCIL | ACADEMIA

בית הספר
להייטק וסייבר
המערך לתוכניות ייעודיות
אוניברסיטת בר-אילן



אוניברסיטת בר-אילן, המערך לתוכניות ייעודיות
המדור לתוכניות מובנות ולימודי תעודה
03-7384481 | טלפון: Desigprog.biu.ac.il

* לימודים לא אקדמיים



מנהל אבטחת מידע וסייבר CISO וקצין הגנת הנתונים DPO

התוכנית להכשרת בכירים בניהול אבטחת מידע, סייבר ופרטיות הכוללת הכנה
מלאה להסמכות הבינלאומיות:

CISSP, CISM, CSXF, CIPP/E, C|CISO

מנהל אקדמי: מר ערן שחם, מנהל בית הספר להייטק וסייבר באוניברסיטת בר-אילן
יועצים אקדמיים: מר הילל קוברובסקי, מר אורן יגר ועו"ד אפרת גרינבוים

עם נסיון רב בהדרכות מקצועות אבטחת מידע טכניים וניהוליים, מאות קורסים שהועברו בהצלחה ואלפי סטודנטים המאיישים משרות בשוק הישראלי והעולמי, אוניברסיטת בר אילן גאה להציג את התוכנית המתקדמת בישראל להכשרת מנהלי אבטחת מידע וסייבר וקציני הגנת הנתונים. התוכנית היחידה בישראל המעניקה שתי תעודות אוניברסיטאיות של CISO ושל DPO, מכינה לקראת שבע הסמכות בינלאומיות ומועברת בהדרכתם של בולטי המרצים בתחום. עם סיומה, הסטודנט מוכשר כמנהל אבטחת מידע וסייבר וכקצין הגנת הנתונים בחברות.

ה-CISO הינו ה Security Enabler בארגון. מצד אחד מכיר את הרבדים השונים של אבטחת המידע, מנהל תקציב וצוותים טכנולוגיים ומצד שני הינו בעל ראייה עסקית חדה, בקיא בניהול סיכונים ומבין שנמצא בעסק שצריך למקסם את רווחיו. הוא מבין שצריך לרתום את אבטחת המידע לטובת החברה. בשנים האחרונות תפקידו של ה-CISO גדל עקב דרישות רגולטוריות וצרכים עסקיים והוא נדרש להבנה בנושאים משפטיים בעלי זיקה לתחום המיחשוב ותהליכים טכנולוגיים מורכבים.

ה-DPO – קצין הגנת הפרטיות, מפקח על אסטרטגיית הגנת הפרטיות ויישומה על מנת להבטיח עמידה בדרישות ה-GDPR. בישראל אחראי במקביל הן על העמידה בתנאי חוקי הגנת הפרטיות ותקנות אבטחת מידע שנכנסו לתוקף במאי 2018 והן על ההתאמה לתנאים הנדרשים לכל חברה שיש לה קשרי מסחר עם אירופה.

המסלול מכין למספר הבחינות הבינלאומיות הגדול בישראל, הכולל הכנה לבחינות CSX ו CISM של ארגון ISACA, בחינת CIPP/E של ארגון הפרטיות הגדול בעולם IAPP ובחינת CISSP מטעם ארגון ISC2. בנוסף, מאחר ואוניברסיטת בר-אילן הפכה לשותף אקדמי של EC-Council, יוכל הסטודנט לגשת גם למבחן ה C|CISO. המסלול כולל מכינה טכנולוגית ייחודית בתחומי ההגנה והתקיפה ושמבוצעת על חוות שרתים ייעודית המחוברת לאוניברסיטה. המכינה מאפשרת למשתתפים יישור קו עם הטכנולוגיות העדכניות בתחום. מערכת בחינות יעודית מבוססת ענן נוספה לקורס כדי להכין את המשתתפים לבחינות הבינלאומיות.

תכנית מנהלי אבטחת מידע CISO נבנתה לפי מסמך מדיניות מקצועות הגנת הסייבר במדינת ישראל, כפי שהופץ ע"י מטה הסייבר הלאומי במשרד ראש הממשלה ביום 31 בדצמבר 2015 ("ט בטבת התשע"ו). התכנית ותכניה מכוונים למקצועות אשר הוגדרו במסמך זה ובנויים לפיו. מעבר הבחינות הבינלאומיות בצרף תעודת CISO ותעודת DPO מטעם האוניברסיטה מהווה נקודת כניסה מעולה לתחום שנמצא בהתפתחות מתמדת.



תיאור התכנית

התכנית מכשירה לקראת 5 הסמכות בינלאומיות יוקרתיות:

- ISACA - Certified Cybersecurity Fundamentals (CSXF) של ארגון ISACA
- ISACA - Certified Information Security Manager (CISM) של ארגון ISACA
- IAPP - Certified Information Privacy Professional (CIPP/E) של ארגון IAPP
- ISC2 - Certified Information Systems Security Professional (CISSP) של ארגון ISC2
- EC-Council - Certified CISO (C|CISO) של ארגון EC-Council

יתרונותיה הבולטים של התכנית

לעומדים בדרישות התוכנית תעודות יוקרתיות של אוניברסיטת בר אילן, המערך לתוכניות ייעודיות:

- Certified Information Security Officer (CISO)
- Certified Data Protection Officer (DPO)

מפיקים את המקסימום:

- מסלול דו-חוגי המשלב תחומים מובילים ומקנה כלים וידע נוסף.
- לימוד תפקיד כפול של CISO ושל DPO בקורס אינטנסיבי אחד.

מתמקדים בהסמכות המוכרות בעולם:

- המסלול היחיד בישראל המכין אתכם לשש הסמכות בינלאומיות יוקרתיות של מיטב הארגונים
- CSXF, CISM, CIPP/E, CISSP, C|CISO

לומדים עם המרצים הטובים ביותר בתחום:

- צוות הקורס מורכב ממנהלי אבטחת מידע בעלי ניסיון בינלאומי ותארים בכירים מהתחום, המאשרים ע"י אוניברסיטת בר-אילן.
- מרצים אורחים בכירים מהתעשייה שישולבו במגוון הרצאות ושליבים שונים בלמידה.

מעמידים לרשותכם את כל הכלים להצלחה:

- עבודה מול חוות שרתים ייעודית לצורך הכרות עם כלי הגנה ותקיפה מתקדמים.
- אפשרות לחיזוק והשלמת חוסרי ידע בתחומים טכנולוגיים.
- תרגול בחינות בינלאומיות באמצעות מערכת בחינות יחודית שפותחה עבור הקורס

מעורבות אישית של צוות הקורס:

- ערוצי תקשורת דיגיטליים ישירים המקשרים בין המרצים, הסטודנטים והיועץ האקדמי.
- הרצאות מוקלטות של ההרצאות מאפשרות חזרה על חומר הלימוד, גם לאחר ההרצאה.
- ליווי אישי של התלמיד לאורך המסלול וגם לאחריו.

אודות המנהל האקדמי, מר ערן שחם

- בעל ניסיון עשיר כמרצה ומנהל הדרכות בתחום התקשורת ואבטחת המידע.
- מנהל בית הספר להייטק וסייבר באוניברסיטת בר-אילן.
- מנהל מרכזי הדרכה מורשים של החברות המובילות בעולם בתחום הווירטואליזציה, תקשורת ואבטחת המידע: Forcepoint, Check Point, EC-Council, VMware, Amazon AWS ומכשיר אינטגרטורים בקורסים מתקדמים. מכשיר לקוחות ושותפים של Check Point בטכנולוגיות מתקדמות כ 20 שנה.
- יזם, הקים וניהל את קורסי התעודה במחשבים ביחידה ללימודי המשך של מוסד הטכניון במשך 8 שנים.
- הקים וניהל את "מלם-תים הדרכה", מקבוצת מלם-תים, האחראית להכשרת 4000 עובדי הקבוצה.
- ניהל את קהילת אבטחת המידע במיקרוסופט ישראל.

אודות היועץ האקדמי, מר הילל קוברובסקי

- יועץ אסטרטגי ומנטור טכנולוגי בתחומים: הגנת סייבר, טרנדים ותחזיות טכנולוגיות, חדשנות ארגונית, עתידנות טכנולוגית, שיווק דיגיטלי, הכשרה טכנולוגית מקצועית.
- מדריך טכנולוגי בכיר בתחומים של סייבר, אבטחת מידע ותקשורת נתונים, קורסי הסמכה ליצרנים שונים, קורסים להכשרת מנהלי מכירות בתחום הסייבר, הרצאות בנושא טכנולוגיות עתידיות עבור מנהלים בכירים \ דירקטורים \ מנהלי מכירות, טרנדים ומגמות טכנולוגיות בתחום המחשוב והסייבר. רקורד מוכח וניסיון של 19 שנה בתחום ההדרכה, אלפי תלמידים ומאות קורסים.
- מדריך מוסמך של חברת Check Point מאז 1999, מדריך בכיר של חברת Fortinet מאז 2007, מדריך בכיר ב Cisco ישראל מאז 2018.
- 22 שנות ניסיון כארכיטקט פתרונות אבטחה בתחומי הסייבר, אבטחת המידע והתקשורת, רקורד של תכנון וביצוע ותחזוקה שוטפת של מאות פרויקטים בארץ ובעולם.
- ניסיון של 13 שנה כמייסד ומנכ"ל של חברת Professional Services מובילה בפתרונות סייבר.
- סיוע וליווי חברות טכנולוגיות בפיתוח עסקי ושיווקי: פיתוח מוצרים \ שירותים חדשים, ערוצי שיווק והפצה חדשים, הכנת תוכניות עסקיות ואסטרטגיות, הקמת מרכזי הדרכה והכשרה מקצועית.

אודות היועץ האקדמי, מר אורן יגר

- ארכיטקט דאטה וענן ומומחה הגנת סייבר.
- לאורן ניסיון עשיר בהדרכות טכנולוגיות בצה"ל ובמסגרות אקדמיה. הוא מוביל מקצועי ומרצה בכיר בקורס המשולב CISO&DPO באוניברסיטת בר-אילן ובעל הסמכות בינ"ל CISSP, CISM.
- יוצא יחידה 8200, בעל ותק של 25 שנה בחברות Enterprise בינ"ל כגון IBM ו Oracle ובתפקידי ליבה בתחומי ה IT, Middleware והענן.
- במסגרת פועלו, קיבל הכרה כ AWS Accredited Educator ו AWS Community Builder ועוזר לתכנן פתרונות אבטחת ענן בסביבות טכנולוגיות מאתגרות.
- בשנים האחרונות ממלא תפקיד מנהל אבטחת מידע CISO, קצין הגנת הנתונים DPO ויועץ בכיר בתחום הסייבר ואבטחת המידע.

אודות היועצת האקדמית, עו"ד אפרת גרינבוים

- מובילה מקצועית של תכני ה- DPO בקורס.
- בעלת ותק של כ-12 שנים בתחומי המשפט והפרטיות.
- מנהלת את כל תחום הפרטיות בישראל של החברה הבינלאומית Johnson&Johnson.
- שותפה להקמת חברת MyEDPO, המלווה חברות וארגונים בישראל ובעולם לעמידה ברגולציות הפרטיות השונות ונותנת שירותי DPO של עשרות חברות מתחומי תעשייה שונים ומגוונים.
- בעלת תואר ראשון במשפטים מאוניברסיטת בר-אילן ותואר שני במנהל עסקים.
- מרצה בכנסים בינלאומיים ומעבירה קורסים וסדנאות בתחומי הפרטיות.
- הכרות רבה עם רגולציית ה- GDPR ורגולציות פרטיות נוספות, מאפיון ועד להטמעה מתודולוגית בארגונים. כמו כן ליווי ארגונים לעמידה בתקנות הגנת הפרטיות בישראל.

קהל היעד

- בעלי רקע הולם באבטחת רשתות Windows או Linux, תקשורת, מנהלי מערכות מידע, יועצי אבטחת מידע ומבקרי מערכות מידע או בעלי רקע בפתוח תוכנה.
- מנהלי אבטחת מידע המעוניינים לקבל הסמכה בינלאומית.
- קציני ביטחון ויוצאי מערכות בטחוניות ומודיעיניות.
- נאמני אבטחת מידע במשרדים ממשלתיים.
- בוגרי קורס Certified Network Defender – CND של אוניברסיטת בר-אילן.

תנאי קדם

- הבנת מושגים טכניים וניהוליים באנגלית
- מעבר ראיון קבלה עם היועץ האקדמי

מתכונת לימודים

- פתיחת הלימודים: 13.9.2023
- משך הלימודים: כ- 7 חודשים ויתקיימו בימים ראשון ורביעי בין השעות 17:30-21:30
- תכנית הלימודים כוללת 270 שעות אקדמיות.

שכר לימוד

- דמי רישום: 480 ₪.
- שכר לימוד: 15,000 ₪.
- חניה: עבור תשלום של 200 ₪ ניתן להחנות את הרכב באוניברסיטה בשעות הלימוד עד סוף ספטמבר.
- בחינות ההסמכה הבינלאומיות חיצוניות ובתשלום נפרד

מקום הלימוד

- הלימודים נערכים בבית הספר להייטק וסייבר, קמפוס אוניברסיטת בר-אילן, רמת גן
- בהתאם להוראות משרד הבריאות והוראות האוניברסיטה ייתכן שחלק מהשיעורים יועברו באמצעות זום.

זכאות לתעודה

- חובת נוכחות ב-80% מהמפגשים, ועמידה במטלות התכנית.
- לעומדים בדרישות התכנית תוענק תעודה מטעם אוניברסיטת בר אילן, המערך לתוכניות ייעודיות.

הערות

- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם כלולים בשכר הלימוד ואינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי היחידה, בכפוף לתקנון לימודים של לימודי התעודה באוניברסיטת בר אילן.
- היחידה מביאה לידיעת הנרשמים כי ייתכנו שינויים במערך התכנית, במועדי הלימודים והבחינות או בכל נושא אחר. הודעה על כל שינוי תימסר למשתתפים, בכפוף לתקנון לימודי התעודה באוניברסיטת בר אילן.

נהלי רישום

ההרשמה תתבצע באמצעות חברת ערן שחם בע"מ, עבור אוניברסיטת בר אילן.

לפרטים והרשמה נא לפנות אלי:

אסתר אסולין

052-5886002

esther.asulin@biu.ac.il





תכנית הלימודים

התוכנית מורכבת מארבעה עשר תחומי התמחות, המכילים לבחינות הבינ"ל וביחד עוזרים להכרות מעמיקה עם עולמו ותפקידיו של ה CISO.

Domain 1: Preparation

- Understanding the three different lab topologies
- Hands on using defense technologies in a complex firewall lab
- Hands on using attack technologies in a complex attack lab
- Hands on using secure coding methodologies and techniques in a Dev lab
- Evaluation of defense and attack tools and methods

Domain 2: Security and Risk Management

- Understand and apply concepts of confidentiality, integrity and availability.
- Evaluate and apply security governance principles.
- Determine compliance requirements.
- Understand legal and regulatory issues that pertain to information security in a global context.
- Understand, adhere to, and promote professional ethics.
- Develop, document, and implement security policy, standards, procedures, and guidelines.
- Identify, analyze, and prioritize Business Continuity (BC) requirements.
- Contribute to and enforce personnel security policies and procedures.
- Understand and apply risk management concepts.
- Understand and apply threat modeling concepts and methodologies.
- Apply risk-based management concepts to the supply chain.
- Establish and maintain a security awareness, education, and training program.
- Integrate risk, threat and vulnerability identification and management into life cycle processes (e.g., project management, development, and procurement and employment life cycles).
- Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.

Domain 3: Asset Security

- Identify and classify information and assets.
- Determine and maintain information and asset ownership.
- Ensure appropriate asset retention.



- Determine data security controls.
- Establish information and asset handling requirements.

Domain 4: Privacy

- Data protection laws
- Personal data
- Controllers and processors
- Processing personal data
- Information provision
- Data subjects' rights
- Security of processing
- Accountability
- Cross-border data transfers
- Supervision and enforcement
- Compliance
- Privacy governance
- Applicable laws and regulations
- Data assessments
- Policies
- Training and awareness
- Protecting personal information
- Data breach incident plans

Domain 5: Information Security Governance, Program Development and Management

- Develop an information security strategy aligned with business goals and objectives.
- Align information security strategy with corporate governance.
- Develop business cases justifying investment in information security.
- Identify current and potential legal and regulatory requirements affecting information security.
- Identify drivers affecting the organization and their impact on information security.
- Obtain senior management commitment to information security.
- Define roles and responsibilities for information security throughout the organization.
- Establish internal and external reporting and communication that support information security.
- Develop and maintain plans to implement the information security strategy.



- Specify the activities to be performed within the information security program.
- Ensure alignment between the information security program and other assurance functions (e.g., physical, human resources, quality, IT).
- Identify internal and external resources (e.g., finances, people, equipment, Systems) required to execute the information security program.
- Ensure the development of information security architectures (e.g., people, processes, technology).
- Establish, communicate and maintain information security policies that support the security strategy.
- Design and develop a program for information security awareness, training and education.
- Ensure the development, communication, and maintenance of standards, procedures and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
- Integrate information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).
- Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).
- Establish metrics to evaluate the effectiveness of the information security program.
- Ensure that noncompliance issues and other variances are resolved in a timely manner.

Domain 6: Security Architecture and Engineering

- Implement and manage engineering processes using secure design principles.
- Understand the fundamental concepts of security models.
- Select controls based upon systems security requirements.
- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption).
- Assess and mitigate the vulnerabilities of security architectures and solution elements.
- Assess and mitigate vulnerabilities in web-based systems.
- Assess and mitigate vulnerabilities in mobile systems.
- Assess and mitigate vulnerabilities in embedded devices.
- Apply cryptography.
- Apply security principles to site and facility design.
- Implement site and facility security controls.

- The security implications of the adoption of emerging technologies.

Domain 7: Communication and Network Security

- Communication and network security fundamentals.
- Implement secure design principles in network architectures.
- Implement secure communication channels according to design.
- Security of networks, systems, applications and data.
- Security Architecture Principles.

Domain 8: Identity and Access Management (IAM)

- Control physical and logical access to assets.
- Manage identification and authentication of people, devices, and services.
- Integrate identity as a third-party service.
- Implement and manage authorization mechanisms.
- Manage the identity and access provisioning lifecycle.

Domain 9: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies.
- Conduct security control testing.
- Collect security process data (e.g., technical and administrative).
- Analyze test output and generate report.
- Conduct or facilitate security audits.

Domain 10: Security Operations

- Understand and support investigations.
- Understand requirements for investigation types.
- Conduct logging and monitoring activities.
- Securely provisioning resources.
- Understand and apply foundational security operations concepts.
- Apply resource protection techniques.
- Operate and maintain detective and preventative measures.
- Implement and support patch and vulnerability management.
- Understand and participate in change management processes.
- Implement recovery strategies.
- Implement Disaster Recovery (DR) processes.



- Test Disaster Recovery Plans (DRP).
- Participate in Business Continuity (BC) planning and exercises.
- Implement and manage physical security.
- Address personnel safety and security concerns.

Domain 11: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC).
- Identify and apply security controls in development environments.
- Assess the effectiveness of software security.
- Assess security impact of acquired software.
- Define and apply secure coding guidelines and standards.

Domain 12: Cloud Security

- Cloud Architecture
- Cloud Governance and Enterprise Risk Management
- Cloud Legal Issues: Contracts and Electronic Discovery
- Cloud Compliance and Audit Management
- Cloud Identity, Entitlement, and Access Management
- Security as a Service
- ENISA: Benefits, Risks and Recommendations for Information Security

Domain 13: Incident Management and Response

- Develop and implement processes for detecting, identifying, analyzing and responding to information security incidents.
- Establish escalation and communication processes and lines of authority.
- Develop plans to respond to, and document, information security incidents.
- Establish the capability to investigate information security incidents (e.g. forensics, evidence collection and preservation, log analysis, interviewing).
- Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers).
- Integrate information security incident response plans with the organization's disaster recovery (DR) and business continuity plan.
- Organize, train, and equip teams to respond to information security incidents.
- Periodically test and refine information security incident response plans.
- Manage the response to information security incidents.



- Conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk.

Domain 14: Final Steps for becoming a CISO

- Strategic Planning.
- Designing, Developing, and Maintaining an Enterprise Information Security Program.
- Understanding the Enterprise Architecture (EA).
- Understanding the Organization's Procurement Program.
- Vendor Management.
- CISO presentation in front of the Board & Senior Management.
- Information Security Best Practices.
- Final project presentation in Class in front of REAL EXTERNAL CISOs & Board members.
- How to become the CISO you want to be.

**** המערך לתוכניות ייעודיות שומר לעצמו את הזכות לערוך שינויים בתכנית הלימודים.**