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

בית הספר
להייטק וסייבר
המערך לתוכניות ייעודיות
אוניברסיטת בר־אילן

אקדמיה מורשית של הארגונים הבינלאומיים:
ISC2 ISACA EC-COUNCIL

ISACA

ISC2
ACADEMIC
PARTNER

אוניברסיטת בר-אילן, המערך לתוכניות ייעודיות
המדור לתוכניות מובנות ולימודי תעודה
hitech-school.biu.ac.il | טלפון: 052-5886002

* לימודים לא אקדמיים

מנהל אבטחת מידע וסייבר CISO
וקצין הגנת הנתונים DPO

התוכנית להכשרה של בכירים בניהול אבטחת מידע, סייבר ופרטיות
הכוללת הכנה מלאה להסמכות הבינלאומיות:
CISSP, CISM, CC, CIPP/E, C|CISO

מנהל התוכנית: **מר ערן שחם, מנהל ביה"ס להייטק וסייבר של אוניברסיטת בר-אילן**

יועצים מקצועיים: **מר אורן יגר, עו"ד אפרת גרינבוים, מר ניצן לוי ומר הילל קוברובסקי**

עם נסיון רב בהדרכה של מגוון מקצועות אבטחת מידע וסייבר, הן בתחומים הטכניים והן בתחומים הניהוליים, ועם אלפי סטודנטים המאיישים משרות בשוק הישראלי והעולמי, אוניברסיטת בר אילן גאה להציג את התוכנית המתקדמת בישראל להכשרת מנהלי אבטחת מידע וסייבר וקציני הגנת הנתונים.

התכנית שלנו היא היחידה בישראל המעניקה שתי תעודות אוניברסיטאיות, של CISO ושל DPO, ומכינה לקראת חמש הסמכות בינלאומיות. התכנית מועברת בהדרכתם של בולטי המרצים בתחום, ועם סיומה הסטודנט מוכשר כמנהל אבטחת מידע וסייבר וכקצין הגנת הנתונים בחברות. **השותפות האקדמית של האוניברסיטה עם הארגונים ISACA ו- ISC2, מהארגונים הידועים בתחום אבטחת המידע בעולם, מאפשרת לימוד באמצעות ערכות מקוריות ועל ידי מרצים בעלי הסמכה בינלאומית מטעמם.**

ה- CISO הינו ה-Security Enabler בארגון. מצד אחד הוא מכיר את הרבדים השונים של אבטחת המידע ומנהל צוותים טכנולוגיים, ומצד שני הינו בעל ראייה עסקית חדה, כך שהוא בקיא גם בניהול סיכונים וגם בניהול תקציב אבטחת המידע. בשנים האחרונות תפקידו של ה- CISO גדל עקב דרישות רגולטוריות הולכות ומחמירות בעולם, אל מול הצרכים העסקיים של הארגון בו הוא עובד. כיום נדרשת מה- CISO גם הבנה בנושאים משפטיים בעלי זיקה לתחום הטכנולוגי.
ה-DPO הינו מנהל אבטחת פרטיות המידע, והוא מפקח על אסטרטגיית הגנת נתונים ויישומה על מנת להבטיח עמידה בדרישות ה- GDPR והיכרות עם ה- CCPA. בישראל הוא אחראי במקביל הן על העמידה בתנאי תקנות הפרטיות, שנכנסו לתוקף במאי 2018 בישראל, והן על ההתאמה לתנאים הנדרשים מכל חברה שיש לה קשרי מסחר עם אירופה.

תיאור התכנית

קורס CISO מכשיר בכירים בניהול אבטחת מידע, סייבר ופרטיות. זהו המסלול היחיד בישראל שמציע שתי תעודות אוניברסיטאיות: אחת של CISO ואחת של DPO, ומועבר בהדרכתם של בולטי המרצים בתחום. הקורס מכין לקראת חמש הסמכות בינלאומיות יוקרתיות:

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

מעבר של הבחינות הבינלאומיות, בצירוף תעודת CISO וגם תעודת DPO מטעם אוניברסיטת בר-אילן, מהווים נקודת כניסה מעולה לתחום שנמצא בהתפתחות מתמדת, ומניחים את התשתית לקריירה מעניינת, מאתגרת ומתגמלת בתעשיה עתירת הידע.

יתרונותיה הבולטים של התכנית

לבוגרי קורס CISO ו- DPO מוענקות שתי תעודות יוקרתיות מטעם אוניברסיטת בר-אילן:

CISO: Certified Information Security Officer

DPO: Certified Data Protection Officer

בנוסף, מוענקות התעודות הבאות:

INCD Cyber Defense Doctrine 2.0

ISC2 CC - Course completion certificate

ISC2 CISSP - Course completion certificate

ISACA CISM - Course completion certificate

- הכנה לשני תפקידים: CISO וגם DPO בקורס אינטנסיבי אחד.
- המסלול היחיד בישראל המכין אתכם לחמש הסמכות בינלאומיות יוקרתיות של מיטב הארגונים: CC, CISM, CIPP/E, CISSP, C|CISO.
- צוות הקורס מונה מנהלי אבטחת מידע בעלי ניסיון בינלאומי והסמכות בכירות בתחום.
- במהלך קורס CISO ו- DPO נפגשים עם מרצים אורחים בכירים מהתעשייה המלמדים על תחומי הסייבר והפרטיות השונים.
- תרגול לבחינות בינלאומיות באמצעות מערכת בחינות ייחודית שפותחה עבור הקורס.
- ערוצי תקשורת דיגיטליים ישירים המקשרים בין המרצים, הסטודנטים והיועץ המקצועי.
- הקלטות של ההרצאות מאפשרות חזרה על חומר הלימוד, גם לאחר ההרצאה, בכל שעה ומכל מקום.
- ליווי אישי של התלמיד לאורך המסלול וגם לאחריו.

<u>הכירו את סגל המרצים בקורס CISO ו-DPO:</u>
אודות מנהל התוכנית ומנהל בית הספר להייטק וסייבר, מר ערן שחם:

- בעל ניסיון עשיר של למעלה מ-30 שנים כמרצה ומנהל הדרכות בתחום הסייבר ואבטחת המידע.
- מנהל בית הספר להייטק וסייבר של אוניברסיטת בר-אילן.
- מנהל מרכזי הדרכה מורשים של החברות המובילות בעולם בתחום הווירטואליזציה, תקשורת ואבטחת מידע ISC2, Forcepoint, Check Point, EC-Council, VMware, Amazon AWS ומכשיר אינטגרטורים בקורסים המתקדמים.
- 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, בת"א, חיפה וירושלים.
- הקים וניהל את "מלם-תים הדרכה", מקבוצת "מלם-תים", האחראית להכשרת 4,000 עובדי הקבוצה.
- ניהל את קהילת אבטחת המידע במיקרוסופט ישראל.

אודות היועץ המקצועי, מר אורן יגר:

- ארכיטקט דאטה וענן ומומחה הגנת סייבר.
- בעל ניסיון עשיר בהדרכות טכנולוגיות בצה"ל ובמסגרות אקדמיות. הוא מוביל מקצועי ומרצה בכיר בקורס המשולב CISO&DPO באוניברסיטת בר-אילן ובעל הסמכות בינ"ל CISM, CISSP.
- 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 שלל תפקידי מנהל אבטחת מידע CISO, קצין הגנת הנתונים DPO ויועץ בכיר בתחום הסייבר ואבטחת המידע.

אודות היועץ המקצועי, מר הלל קוברובסקי:

- יועץ אסטרטגי ומנטור טכנולוגי בתחומי: הגנת סייבר, טרנדים ותחזיות טכנולוגיות, חדשנות ארגונית, עתידנות טכנולוגית, שיווק דיגיטלי, הכשרה טכנולוגית מקצועית.
- סיוע וליווי חברות טכנולוגיות בפיתוח עסקי ושיווקי: פיתוח מוצרים ושירותים חדשים, ערוצי שיווק והפצה חדשים, הכנת תוכניות עסקיות ואסטרטגיות, הקמת מרכזי הדרכה והכשרה מקצועית.
- מרצה בכיר בתחומים של חדשנות טכנולוגית: יעילות, מזעור המחשוב, אנרגיה ירוקה, מהפכת הבינה המלאכותית, השפעת התפתחות הטכנולוגיה המואצת על האנושות.
- 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 ומנהלי מכירות, טרנדים ומגמות טכנולוגיות בתחום המחשוב והסייבר.
- רקורד מוכח וניסיון של 19 שנה בתחום ההדרכה, אלפי תלמידים ומאות קורסים והרצאות.
- משמש מדריך מוסמך של חברת Check Point משנת 1999, מדריך בכיר של חברת Fortinet משנת 2007 ומשנת 2018 משמש מדריך בכיר ב-Cisco ישראל.
- 22 שנות ניסיון כארכיטקט פתרונות אבטחה בתחומי הסייבר, אבטחת מידע ותקשורת, רקורד של תכנון וביצוע ותחזוקה שוטפת של מאות פרויקטים בארץ ובעולם.
- ניסיון של 13 שנה כמייסד ומנכ"ל של חברת אינטגרציה לפתרונות סייבר.
- מייסד ומנהל של מעל 14 קהילות ופורומים בתחומי סייבר, תקשורת, חדשנות ארגונית, עתידנות טכנולוגית, חדשנות ארגונית כאסטרטגיה עסקית, טרנדים ומגמות טכנולוגיות בתחום הסייבר.

אודות היועצת המקצועית, 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 פעילות שונים ומגוונים.
- בעלת תואר ראשון במשפטים מאוניברסיטת בר-אילן ותואר שני במנהל עסקים מהמכללה למנהל.
- מרצה בכנסים בינלאומיים ומעבירה קורסים וסדנאות בתחומי הפרטיות.
- בעלת היכרות רבה עם רגולציית ה- GDPR ורגולציות פרטיות נוספות, מאפיון ועד להטמעה מתודולוגית בארגונים. בנוסף, עוסקת בליווי ארגונים לעמידה בתקנות הגנת הפרטיות בישראל.

אודות היועץ המקצועי, מר ניצן לוי:

- בעל תואר ראשון B.Sc. בהנדסת תכנה, ובעל תואר שני תואר שני בממשל, עם התמחות בביטחון ולוחמה בטרור מאוניברסיטת רייכמן.
- מנתח מערכות מוסמך מטעם לשכת מנתחי מערכות מידע בישראל.
- מרצה מוסמך מטעם ISC2 ו ISACA.
- בעל ניסיון עשיר בהדרכות תוך התמקדות בקורסי אבטחת מידע, קורסים טכנולוגיים ובפיתוח מאובטח,
- מומחה הגנת סייבר, פיתוח מאובטח וביקורת IT.
- בעל 18 שנות ניסיון בתחומי פיתוח תכנה, ארכיטקטורה, אבטחת מידע וסייבר אשר נרכשו תוך ביצוע מגוון תפקידים בתעשיית התכנה והייטק בישראל.
- בשנים האחרונות ממלא תפקיד מנהל אבטחת מידע, ניהול פיתוח, הובלת פרוייקטים בילאומיים ויועץ בכיר בתחום הסייבר ואבטחת המידע.

קהל היעד

- מנהלי אבטחת מידע המעוניינים לקבל הסמכות בינלאומיות.
- בעלי רקע ב- System, תקשורת, מנהלי מערכות מידע, יועצי אבטחת מידע.
- מבקרי מערכות מידע או בעלי רקע בפיתוח תוכנה.
- קציני בטחון, מנהלי בטחון ויוצאי מערכות בטחוניות ומודיעיניות.
- נאמני אבטחת מידע במשרדים ממשלתיים.
- יועצי אבטחת מידע תשתיתיים ואפליקטיביים.
- בוגרי קורס DevOps /CND עם התמחות בסייבר של אוניברסיטת בר-אילן.

נדרשת הבנת במושגים טכניים וניהוליים בשפה האנגלית.

תנאי קדם

- הבנת מושגים טכניים וניהוליים באנגלית.
- מעבר ראיון קבלה עם יועץ הלימודים.

מתכונת לימודים

- **פתיחת הלימודים: 15.01.2024.**
- **משך הלימודים:** כשבעה חודשים, בימים ראשון ורביעי בין השעות 17:30 – 21:30 .
  * **שיעורי השלמה יתכנו בימים שאינם ימי הלימוד הרגילים.**
- תכנית הלימודים כוללת **270 שעות אקדמיות פרונטליות.**

שכר לימוד

- **דמי רישום:** 480 ₪.
- **שכר לימוד:** 16,500 ₪.
- **ביה"ס להייטק וסייבר הינו אקדמיה מורשית של ISC2, מחיר הקורס כולל ערכות לימוד בינ"ל מקוריות בשווי אלפי שקלים!**
- **בחינות ההסמכה הבינלאומיות חיצוניות והן בתשלום נפרד.**

מקום הלימוד

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

זכאות לתעודה

- חובת נוכחות ב-80% מהמפגשים, ועמידה במטלות התכנית.
- לעומדים בדרישות התכנית יוענקו שתי תעודות מטעם אוניברסיטת בר אילן, ביה"ס להייטק וסייבר.

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

- הרישום לקורס יתבצע באמצעות חברת ערן שחם בע"מ, עבור אוניברסיטת בר-אילן.

לפרטים והרשמה נא לפנות אל:
אסתר אסולין
052-5886002
esther.asulin@biu.ac.il

תעודות לדוגמא

תכנית הלימודים

התוכנית מורכבת מארבעה עשר תחומי התמחות, המכינים 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.

<u>Domain 6: Security Architecture and Engineering</u>

- 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.

<u>Domain 14: Final Steps for becoming a CISO</u>

- 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.**

בפיקוח אקדמי של אוניברסיטת בר-אילן