

الهيئة الوطنية للأمن السيبراني

National Cybersecurity Authority

الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم)

THE SAUDI CYBERSECURITY HIGHER EDUCATION FRAMEWORK

(SCyber-Edu – 2: 2026)

إشارة المشاركة: شفاف
تصنيف الوثيقة: عام

تنويه: لمواكبة المتغيرات بشأن تحديثات الوثائق الصادرة عن الهيئة الوطنية للأمن السيبراني، تود الهيئة الوطنية للأمن السيبراني التنويه على أهمية الاعتماد الدائم على نسخ الوثائق المنشورة في الموقع الإلكتروني للهيئة https://nca.gov.sa

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية)

أحمر (شخصي وسري للمستلم فقط)

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد، سواء أكان ذلك من داخل الجهة أم خارجها؛ خارج النطاق المحدد للاستلام.

برتقالي + مشدد (مشاركة في نفس الجهة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب.

برتقالي (مشاركة محدودة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب. ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر (مشاركة في نفس المجتمع)

المستلم يمكنه مشاركة المعلومات مع آخرين في الجهة نفسها، أو جهة أخرى على علاقة معهم أو في القطاع نفسه؛ ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض (غير محدود)

التحديثات على الوثيقة

النسخة	التاريخ	التغييرات
1.0	أكتوبر ٢٠٢٠م	النسخة الأولى
2.0	نوفمبر ٢٠٢٦م	مراجعة شاملة للوحدات المعرفية، وإضافة مسارات وبرامج متخصصة في الأمن السيبراني، والمواءمة مع الأطر الوطنية والدولية المُحدَّثة. يُرجى الرجوع إلى الملحق (ب) للاطلاع على تفاصيل التحديثات.

قائمة المحتويات

١ المقدمة..... ١٠
١-١ نطاق الإطار السعودي للتعليم العالي في الأمن السيبراني..... ١٠
١-٢ المنهجية..... ١١
١-٣ المتطلبات السابقة ومتطلبات الرياضيات..... ١٣
١-٤ هيكل الوثيقة..... ١٣
٢ البرامج..... ١٤
٢-١ الدبلوم المتوسط..... ١٤
٢-٢ البكالوريوس (مسار في الأمن السيبراني)..... ١٦
٢-٣ البكالوريوس (برنامج في الأمن السيبراني)..... ١٨
٢-٤ الدبلوم العالي (للمختصين في تقنية المعلومات)..... ٢٠
٢-٥ الدبلوم العالي (لغير المختصين في تقنية المعلومات)..... ٢٢
٢-٦ الماجستير (مسار في الأمن السيبراني..... ٢٤
٢-٧ الماجستير (برنامج في الأمن السيبراني ٢٦
٢-٨ الدكتوراه..... ٢٨
٣ الوحدات المعرفية..... ٣١
أساسيات الأمن السيبراني(CSF) Cybersecurity Fundamentals ٣١
مبادئ التصميم في الأمن السيبراني(CDP) Cybersecurity Design Principles ٣٢
مكونات أنظمة تقنية المعلومات (ISC) IT Systems Components..... ٣٣
أساسيات التشفير (BCY) Basic Cryptography..... ٣٤
أساسيات الشبكات(BNW) Basic Networking ٣٥
أساسيات البرمجة (BSP) Basic Scripting and Programming ٣٦
الدفاع عن الشبكات(NDF) Network Defense ٣٧
مفاهيم نظم التشغيل(OSC) Operating Systems Concepts ٣٨
التهديدات السيبرانية (CTH) Cyber Threats..... ٣٩
إدارة وتخطيط الأمن السيبراني (CPM) Cybersecurity Planning and Management..... ٤٠
السياسات والتشريعات والأخلاقيات والالتزام بها(PLE) Policy, Legal, Ethics and Compliance ٤١
إدارة البرامج الأمنية(SPM) Security Program Management ٤٢
تحليل المخاطر السيبرانية(SRA) Security Risk Analysis ٤٣
الخوارزميات المتقدمة(AAL) Advanced Algorithms ٤٤
ضبط الوصول(ACC) Access Control ٤٥
التشفير المتقدم(ACR) Advanced Cryptography ٤٦
الخوارزميات(ALG) Algorithms..... ٤٧
تقنية وبروتوكولات الشبكات المتقدمة
(ANT) Advanced Network Technology and Protocols..... ٤٨
الاتصالات التناظرية(ATC) Analog Telecommunications ٤٩
الأدوات التحليلية (ATT) Analytical Tools ٥٠

الوعي والفهم(AUU) Awareness and Understanding ٥١
استمرارية الأعمال، والتعافي من الكوارث، وإدارة الحوادث السيبرانية
Business Continuity, Disaster Recovery and Incident Management (BDR) ٥٢
الحوسبة السحابية(CCO) Cloud Computing ٥٣
التشفير(CRY) Cryptography ٥٤
هندسة التشفير(CRE) Cryptography Engineering ٥٥
الجريمة السيبرانية (CCR) Cyber Crime ٥٦
أخلاقيات الأمن السيبراني(CSE) Cybersecurity Ethics ٥٧
الأنظمة السيبرانية الفيزيائية(CPS) CyberPhysical System ٥٨
قواعد البيانات(DAT) Databases ٥٩
إدارة البيانات(DBA) Data Administration ٦٠
الاتصالات الرقمية(DCO) Digital Communications ٦١
التحليل الجنائي الرقمي(DFS) Digital Forensics ٦٢
سلامة البيانات وتوثيقها(DIA) Data Integrity and Authentication ٦٣
التعّلم العميق(DLL) Deep Learning ٦٤
إدارة أنظمة قواعد البيانات(DMS) Database Management Systems ٦٥
بنية الأنظمة الموزعة(DSA) Distributed Systems Architecture ٦٦
تراكيب البيانات(DST) Data Structures ٦٧
التحليل الجنائي الرقمي في الأجهزة(DVF) Device Forensics ٦٨
الأنظمة المدمجة (ESY) Embedded Systems ٦٩
المحاسبة الجنائية الرقمية (FAC) Forensic Accounting ٧٠
الأساليب المنهجية(FMD) Formal Methods ٧١
الأُسس الرياضية للتشفير (FCY) Mathematical Foundation of Cryptography ٧٢
إدارة منع الاحتيال والحد منه (FPM) Fraud Prevention and Management ٧٣
بنية الأجهزة والعتاد(HAA) Hardware Architecture ٧٤
أمن الأجهزة والعتاد والبرمجيات الثابتة (HFS) Hardware/Firmware Security ٧٥
التحليل الجنائي الرقمي للمضيف (HOF) Host Forensics ٧٦
الهندسة العكسية للأجهزة والعتاد (HRE) Hardware Reverse Engineering ٧٧
بنى توكيد المعلومات (IAA) Information Assurance Architectures ٧٨
الالتزام بتوكيد المعلومات(IAC) Information Assurance Compliance ٧٩
معايير توكيد المعلومات(IAS) Information Assurance Standards ٨٠
أنظمة التحكم الصناعية(ICS) Industrial Control Systems ٨١
بحث موجه /دراسة مستقلة(IDR) Independent/Directed Study/Research ٨٢
أنظمة منع/كشف التسلل(IDS) Intrusion Detection/Prevention Systems ٨٣
إدارة الهوية(IMM) Identity Management ٨٤
إنترنت الأشياء(IoT) Internet of Things ٨٥
أمن تخزين المعلومات (ISS) Information Storage Security ٨٦
مقدمة في الحوسبة النظرية (ITC) Introduction to the Theory of Computation ٨٧
أمن دورة حياة الأنظمة والمنتجات (LCS) Security Life.Cycle ٨٨
البرمجة منخفضة المستوى (LLP) Low Level Programming ٨٩

التحليل الجنائي الرقمي في الوسائط Forensics Media (MEF)..... ٩٠
تعلم الآلة Machine Learning (MLL)..... ٩١
تقنيات الهاتف الجوال Mobile Technologies (MOT)..... ٩٢
أمن إدارة الشبكات Network Security Administration (NSA)..... ٩٣
تقنية الشبكات والبروتوكولات Network Technology and Protocols (NTP)..... ٩٤
التحليل الجنائي الرقمي في الشبكات Network Forensics (NWF)..... ٩٥
إدارة نظم التشغيل Operating Systems Administration (OSA)..... ٩٦
تأمين نظم التشغيل Operating Systems Hardening (OSH)..... ٩٧
نظرية نظم التشغيل Operating Systems Theory (OST)..... ٩٨
اختبار الاختراق Penetration Testing (PTT)..... ٩٩
ضمان الجودة / فحص الوظيفة QA/Functional Testing (QAT)..... ١٠٠
مبادئ الترددات الراديوية Radio Frequency Principles (RFP)..... ١٠١
توكيد البرمجيات Software Assurance (SAS)..... ١٠٢
التحكم بالأنظمة System Control (SCC)..... ١٠٣
بروتوكولات الاتصالات الآمنة Secure Communication Protocols (SCP)..... ١٠٤
أمن سلاسل الإمداد Supply Chain Security (SCS)..... ١٠٥
برمجة النظم Systems Programming (SPG)..... ١٠٦
ممارسات البرمجة الآمنة Secure Programming Practices (SPP)..... ١٠٧
الهندسة العكسية للبرمجيات Software Reverse Engineering (SRE)..... ١٠٨
التحليل الأمني للبرمجيات Software Security Analysis (SSA)..... ١٠٩
هندسة أمن الأنظمة Systems Security Engineering (SSE)..... ١١٠
تحليل الثغرات الأمنية Vulnerability Analysis (VLA)..... ١١١
تقنيات البيئة الافتراضية Virtualization Technologies (VTT)..... ١١٢
أمن تطبيقات الويب Web Application Security (WAS)..... ١١٣
شبكات الاستشعار اللاسلكية Wireless Sensor Networks (WSN)..... ١١٤
٤ الملحق (أ): أمثلة على برامج الأمن السيبراني التخصصية..... ١١٥
٤-١ بكالوريوس الذكاء الاصطناعي في الأمن السيبراني..... ١١٥
٤-٢ ماجستير التشفير..... ١١٦
٤-٣ ماجستير الأمن السيبراني لأنظمة التحكم الصناعية/التقنيات التشغيلية..... ١١٧
٤-٤ ماجستير إدارة الأمن السيبراني..... ١١٨
٥ الملحق (ب): ملخص تحديثات الإصدار..... ١١٩
٦ المصادر..... ١٢٠

١ المقدمة

استناداً إلى تنظيم الهيئة الوطنية للأمن السيبراني الصادر بموجب الأمر الملكي الكريم رقم ٦٨٠١ وتاريخ ١٤٣٩/٠٢/١١هـ، والذي تضمن اختصاصات ومهمات الهيئة ومنها: "بناء القدرات الوطنية المتخصصة في مجالات الأمن السيبراني، والمشاركة في إعداد البرامج التعليمية والتدريبية الخاصة بها، وإعداد المعايير المهنية والأطر، وبناء وتنفيذ المقاييس والاختبارات القياسية المهنية ذات العلاقة"، وانطلاقا من حرص الهيئة على بناء وتطوير برامج أكاديمية وطنية عالية الجودة في مجال الأمن السيبراني ، فقد عملت الهيئة على إعداد "الإطار السعودي للتعليم العالي في الأمن السيبراني" ليكون دليلاً إرشادياً يمكن الاستفادة منه في تطوير وتقييم واعتماد برامج التعليم العالي في الأمن السيبراني. وقد تم تطوير هذا الإطار من قبل الهيئة بالتنسيق والتعاون مع وزارة التعليم وهيئة تقويم التعليم والتدريب.

يهدف هذا الإطار إلى المساهمة في وضع الحد الأدنى من متطلبات الخطط الدراسية لبرامج التعليم العالي في الأمن السيبراني، وذلك لضمان الجودة الأكاديمية لتلك البرامج، وضمان قدرتها على تخريج كوادر مؤهلة تأهيلًا عالياً في مجال الأمن السيبراني بحيث ينضمون إلى الكوادر الوطنية العاملة في مجال الأمن السيبراني، ويثرونها بمعرفتهم وخبراتهم، ويسهمون في الجهود الوطنية الرامية للوصول إلى "فضاء سيبراني سعودي آمن وموثوق يُمكن النمو والازدهار".

وقد تم إعداد الإطار السعودي للتعليم العالي في الأمن السيبراني ليكون متوافقًا مع التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات، وإرشادات المركز الوطني للتقويم والاعتماد الأكاديمي.

١-١ نطاق الإطار السعودي للتعليم العالي في الأمن السيبراني

يغطي هذا الإطار برامج التعليم العالي بعد المرحلة الثانوية في تخصصات الأمن السيبراني، ويشمل الدرجات العلمية التالية:

١. الدبلوم المتوسط
٢. البكالوريوس
٣. الدبلوم العالي
٤. الماجستير
٥. الدكتوراه

ويمكن الاستفادة من هذا الإطار وتطبيقه على البرامج التعليمية والدرجات العلمية في تخصصات الأمن السيبراني التي يتم تدريسها في المؤسسات التعليمية العامة والخاصة للتعليم بعد المرحلة الثانوية في المملكة العربية السعودية.

ولضمان امتلاك الخريجين الكفاءة والمعرفة الفنية اللازمة لتأمين الفضاء السيبراني الوطني بفعالية فقد تم استثناء برامج الدبلوم المشارك من هذا الإطار استناداً إلى أن الدبلوم المتوسط يُمثل الحد الأدنى من المتطلبات التعليمية لأي وظيفة في مجال الأمن السيبراني بحسب الإطار السعودي للكوادر السيبرانية (سيوف) - ملحق التقدم الوظيفي. وستتم مراجعة متطلبات الخطط الدراسية الواردة في هذا الإطار وتحديثها بصورة دورية لتواكب التطورات السريعة التي يشهدها مجال الأمن السيبراني.

٢-١ المنهجية

رغم أن مجال الأمن السيبراني يعد من المجالات الحديثة نسبياً مقارنة بالمجالات الأخرى ذات العلاقة التي مر وقت طويل على ظهورها مثل علوم وهندسة الحاسب، إلا أن العديد من الدول والمنظمات الأكاديمية الدولية بادرت بوضع أطر خاصة بالتعليم العالي في مجال الأمن السيبراني بهدف ضمان جودة مخرجات برامج التعليم في هذا المجال.

ومن الأمثلة على تلك الأطر: إطار برنامج المراكز الوطنية للتميّز الأكاديمي في الدفاع السيبراني (CAE-CD)[١] في الولايات المتحدة الأمريكية؛ ومعايير مجلس الاعتماد الأكاديمي للهندسة والتكنولوجيا (ABET) لبرامج الأمن السيبراني؛ وإرشادات مناهج الأمن السيبراني من معهد مهندسي الكهرباء والإلكترونيات (IEEE) وجمعية آلات الحوسبة (ACM)؛ بالإضافة إلى إطار برامج التعليم العالي المعتمدة من المركز الوطني للأمن السيبراني (NCSC) في المملكة المتحدة[٢]. وتتشارك هذه الأطر في عدد من السمات المشتركة. وقد تمت الاستفادة من تلك الأطر الدولية في تحديد منهجية إعداد الإطار السعودي للتعليم العالي في الأمن السيبراني وذلك بوضع الحد الأدنى من متطلبات الخطط الدراسية في الأمن السيبراني لكل برنامج من برامج الدرجات العلمية بتحديد توصيفات البرنامج Program Descriptors (PD) التي يتم من خلالها تحديد نواتج التعلم، والوحدات المعرفية Knowledge Units (KUs) التي يدرسها الطلبة في البرنامج. وكما ذكر سابقاً، فقد تم تصميم هذا الإطار بالتوافق مع التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات، وإرشادات المركز الوطني للتقويم والاعتماد الأكاديمي.

تتوافق توصيفات البرنامج في هذا الإطار مع توصيفات مستويات الإطار الوطني للمؤهلات التي تساعد المؤسسات التعليمية في تصميم نواتج التعلم للبرنامج Program Learning Outcomes (PLOs)، وهي مجموعة من المعارف والمهارات والقيم التي من المتوقع أن يكتسبها الخريجون عند استكمال دراسة البرنامج. ويهدف هذا الإطار إلى المساهمة في وضع الحد الأدنى من توصيفات البرنامج التي تُراعَى عند صياغة نواتج التعلم لكل برنامج من برامج الدرجات العلمية في الأمن السيبراني. وتستطيع كل مؤسسة تعليمية إضافة نواتج تعلم أخرى إلى برامجها التعليمية في الأمن السيبراني وفق ما تراه مناسباً.

ويصف هذا الإطار الوحدات المعرفية في الأمن السيبراني حيث أن الوحدة المعرفية هي مجموعة من المواضيع ذات الصلة التي تشكّل محتوى المنهج الذي يتم تدريسه، ومجموعة من نواتج التعلم التي يكتسبها الطلبة بعد إكمال دراسة هذه الوحدة. وتحدد نواتج التعلم الخاصة بكل وحدة معرفية الحد الأدنى لما يُتوقع أن يتعلمه الطالب ويقدر على فعله بعد إتمام دراسة تلك الوحدة المعرفية بنجاح، ومن المهم أن تُراعى المؤسسات التعليمية العمق والتوسع والتدرج في تلك النواتج بما يناسب مستوى البرنامج، وأن تُضمّن نواتج التعلم الخاصة بمهارات التواصل والقيم في المقررات الدراسية.

ويحدد الإطار الحد الأدنى من الوحدات المعرفية الأساسية التي يجب أن يغطيها البرنامج بالإضافة إلى قائمة بالوحدات المعرفية الاختيارية. وتستطيع المؤسسات التعليمية طرح الوحدات المعرفية الاختيارية ذات العلاقة ببرامجها والتي يستطيع الطلبة الاختيار من بينها لاستكمال متطلبات تخرجهم. ومن المهم ملاحظة أن الوحدة المعرفية ليست

[١] برامج مراكز التميز الأكاديمي في الدفاع السيبراني (CAE-CD) هو مبادرة برعاية وكالة الأمن القومي ووزارة الأمن الداخلي في الولايات المتحدة الأمريكية

[٢] برامج التعليم العالي المعتمدة في الأمن السيبراني هي مبادرة من المركز الوطني للأمن السيبراني في المملكة المتحدة

بالضرورة مقرراً دراسياً؛ فبالإمكان تغطية وحدة معرفية بمقرر دراسي واحد أو أكثر، كما يجوز أن يغطي المقرر الدراسي وحدة معرفية واحدة أو أكثر بشكل كامل أو بشكل جزئي.

بالنسبة لبرامج درجة البكالوريوس ودرجة الماجستير، فيميز هذا الإطار بين برنامج متخصص في الأمن السيبراني وبرنامج متخصص بأحد تخصصات تقنية المعلومات مع مسار الأمن السيبراني في ذلك البرنامج.

وقد تم استخلاص الوحدات المعرفية في هذا الإطار من المصادر التالية:

- البرنامج الإرشادي والوحدات المعرفية للمراكز الوطنية للتميز الأكاديمي في الدفاع السيبراني (CAE-CD)، عام ٢٠٢٤.
- الهيكل المعرفي للأمن السيبراني (CyBOK) (الإصدار ١,١,٠)، عام ٢٠٢١.
- مناهج الأمن السيبراني من معهد مهندسي الكهرباء والإلكترونيات وجمعية آلات الحوسبة (IEEE/ACM)، عام ٢٠١٧.
- مناهج علوم الحاسب من معهد مهندسي الكهرباء والإلكترونيات وجمعية آلات الحوسبة (IEEE/ACM)، عام ٢٠٢٣.

كما تم إجراء الإضافات والتعديلات اللازمة لتلبية الاحتياجات الوطنية في هذا المجال، والتوافق مع الأطر ذات الصلة في المملكة العربية السعودية.

وهناك ثلاثة أنواع من المتطلبات في هذا الإطار لكل برنامج من برامج التعليم العالي وهي:

١. متطلبات القبول Admission Requirements: قائمة بالمتطلبات التي يجب على الطالب أن يستوفيها قبل قبوله في البرنامج.
٢. الوحدات المعرفية الأساسية Core KUs: وحدات معرفية إلزامية يجب على الطالب استكمالها بشكل كامل كمتطلب أساسي للتخرج. وتم تصنيف هذه الوحدات الى الفئات التالية:

- **الوحدات المعرفية الأساسية في الأمن السيبراني**: تمثل الحد الأدنى من المشترك من المعارف والمهارات الأساسية في الأمن السيبراني وهي مطلوبة في جميع البرامج المشمولة في الإطار.
- **الوحدات المعرفية الأساسية الفنية**: تركز بصوره رئيسية على الأسس والمفاهيم والمهارات الفنية المرتبطة بالأنظمة والشبكات والبرمجيات والتشفير.
- **الوحدات المعرفية الأساسية غير الفنية**: تركز بصوره رئيسية على الجوانب التنظيمية والإدارية والتشريعية وإدارة المخاطر والتهديدات.

ويعتمد تصنف الوحدات المعرفية الأساسية على مجال تركيزها الغالب ولا يعني تصنيفها ضمن الوحدات غير الفنية خلوها من الموضوعات الفنية.

٣. الوحدات المعرفية الاختيارية Elective KUs: قائمة بالوحدات المعرفية الاختيارية التي تستطيع المؤسسة التعليمية و/أو الطالب الاختيار من بينها لاستكمال عدد الوحدات المعرفية المطلوبة للتخرج. وفي البرامج التخصصية في الأمن السيبراني يجب أن تكون هذه الوحدات الاختيارية ذات صلة بمسمى البرنامج.

١-٣ المتطلبات السابقة ومتطلبات الرياضيات

تعد بعض الوحدات المعرفية متطلبات سابقة لوحدات معرفية أخرى، ومن المهم أن يُراعَى ذلك في الخطط الدراسية للطلبة وترتيبها الزمني بشكل مناسب.

وبالإضافة إلى ذلك، فإن هناك ارتباطا أساسياً بين علم الرياضيات والعديد من مجالات الأمن السيبراني، وتتطلب معظم برامج الأمن السيبراني بعض الوحدات المعرفية الأساسية في الرياضيات. ولكن الوحدات المعرفية في الرياضيات المطلوبة لبرنامج معيّن تعتمد بشكل كبير على طبيعة هذا البرنامج وتركيزه؛ ولذلك فإنه من المهم أن تراعى المؤسسات التعليمية التي تقدم برامج البكالوريوس أو الدبلوم المتوسط في مجال الأمن السيبراني تضمين الوحدات المعرفية في الرياضيات ذات الصلة ببرامجها التي تلبي المتطلبات الأساسية للوحدات المعرفية في الأمن السيبراني في برامجها بشكل صحيح.

١-٤ هيكل الوثيقة

تم تنظيم الجزء المتبقي من هذه الوثيقة كما يلي:

القسم الثاني يستعرض برامج الأمن السيبراني المغطاة بالإضافة إلى توصيفات البرامج المستهدفة ومتطلبات الوحدات المعرفية لكل منها. القسم الثالث يصف بشكل تفصيلي جميع الوحدات المعرفية. كما يقدم الملحق (أ) أمثلة على برامج متخصصة في الأمن السيبراني، ويلخص الملحق (ب) التحديثات على هذه النسخة من الإطار.

٢ البرامج[٣]

٢-١ الدبلوم المتوسط[٤]

٢-١-١ توصيفات البرنامج		
المعرفة	المهارات	القيم
• معرفة عامة ومترابطة وفهم للأسس والنظريات والمبادئ والمفاهيم التقنية في مجال الأمن السيبراني. • معرفة وفهم المنهجيات التحليلية التي تستخدم في مواضيع الأمن السيبراني وتفسير المعلومات المتعلقة بها.	• توظيف مجموعة من المعارف النظرية والتقنية في العلوم ذات الصلة وتكييفها لتعكس الفهم النظري في سياقات محددة وغير مألوفة في مجال الأمن السيبراني. • توظيف التفكير الناقد والإبداعي، وتقديم الحلول العملية المبتكرة في سياقات متوسطة التعقيد وغير مألوفة، مرتبطة بمجال الأمن السيبراني. • استخدام منهجيات الدراسة والتقصي للاستفادة من نتائجها لحل مشكلات متوسطة التعقيد في الأمن السيبراني. التواصل بطرق مناسبة؛ وإظهار الفهم والمعرفة ونقلها للمستفيدين في مجال الأمن السيبراني. • إدارة فرق العمل التخصصية في مجال الأمن السيبراني، والمبادرة لبناء علاقات إيجابية، والمساهمة في تطوير الآخرين، والعمل على تحقيق الأهداف المشتركة بقدر من الاستقلالية. • اختيار واستخدام مجموعة متنوعة من الممارسات والأدوات التقنية وتكييفها للقيام بأنشطة عملية متوسطة التعقيد في مجال الأمن السيبراني. • تحليل احتياجات المهمة لاختيار أدوات وتطبيقات الذكاء الاصطناعي الأنسب في مجال الأمن السيبراني، واستخدامها بمسؤولية مهنية، والتحقق المتقدم من مخرجاتها من حيث الدقة والتحيز والموثوقية، وتوثيق استخدامها، وتحسين النتائج من خلال تطوير الأوامر والتعليمات.	• الالتزام بأخلاقيات المهنة للأمن السيبراني، والقيم والأخلاق المهنية والإنسانية المرتبطة بممارساته. • الالتزام بالمواطنة المسؤولة، والمشاركة الفاعلة في المبادرات الوطنية ذات العلاقة بالأمن السيبراني في سياقات متوسطة التعقيد، وغير مألوفة، والالتزام بالأنظمة الوطنية، وتشريعات وضوابط الأمن السيبراني تحت إشراف غير مباشر. • إدارة التعلم والعمل ذاتيًا، وتحديد الأهداف والعمل على تحقيقها، واتخاذ القرارات المتعلقة بالتعلم بقدر متوسط من الاستقلالية. • إدارة المهام والأنشطة المتعلّقة بالأمن السيبراني والعمل تحت إشراف غير مباشر. • تعزيز الجوانب الصحية والنفسية والاجتماعية ذات العلاقة بمجال الأمن السيبراني.

[٣] تمت الاستفادة من المصادر التالية لإعداد محتوى متطلبات البرامج: [١]، [٢].

[٤] يتوافق هذا البرنامج مع برنامج الدبلوم المتوسط في المستوى الخامس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات.

٢-١-٢ متطلبات القبول

- شهادة ثانوية عامة أو ما يعادلها.

٢-١-٣ الوحدات المعرفية الأساسية

يجب على الطلبة إكمال ما يلي:

- ثلاث وحدات معرفية أساسية في الأمن السيبراني:
  - أساسيات الأمن السيبراني Cybersecurity Fundamentals (CSF)
  - مبادئ التصميم في الأمن السيبرانيCybersecurity Design Principles (CDP)
  - مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)
- خمس وحدات معرفية أساسية فنية:
  - أساسيات التشفير Basic Cryptography (BCY)
  - أساسيات الشبكات Basic Networking (BNW)
  - أساسيات البرمجة Basic Scripting and Programming (BSP)
  - الدفاع عن الشبكات Network Defense (NDF)
  - مفاهيم نظم التشغيل Operating Systems Concepts (OSC)

٢-١-٤ الوحدات المعرفية الاختيارية

- هي جميع الوحدات المعرفية المتبقية، ويجب على الطلبة أن يستكملوا (٥) وحدات معرفية اختيارية على الأقل قبل التخرج.

٢-٢ البكالوريوس (مسار في الأمن السيبراني)[٥]

٢-٢-١ توصيفات البرنامج

المعرفة	المهارات	القيم
• معرفة بنطاق واسع ومتعمق من الأسس والنظريات والمبادئ والمفاهيم الأساسية في مجال الأمن السيبراني. • المعرفة والفهم المتعمق للعمليات والأدوات والتقنيات، والسياسات والممارسات المستخدمة في الأمن السيبراني. • مجموعة من المعارف المتخصصة والمتعلقة بالتطورات الحالية والمستجدة في مجال الأمن السيبراني.	• تطبيق النظريات والمبادئ والمفاهيم المتكاملة في سياقات مختلفة للأمن السيبراني. • تحليل وتقييم المعلومات المعقدة والمتنوعة في مجال الأمن السيبراني. • التقييم النقدي واختيار واستخدام أساليب ومنهجيات وأدوات الأمن السيبراني لحل المشكلات وتنفيذ الأعمال في مجال الأمن السيبراني. • استخدام منهجيات الدراسة والتقصي والأبحاث في مشاريع وأنشطة الأمن السيبراني. • أداء مجموعة واسعة من المهام والإجراءات باستخدام أدوات الأمن السيبراني في العمليات المعقّدة والمتنوّعة. • التواصل بالطرق المناسبة ونقل المعرفة والمهارات المتخصصة والمفاهيم المتقدمة. • تنفيذ مشاريع تعاونية تخصصية ومهنية في مجال الأمن السيبراني، والانفتاح على وجهات نظر مختلفة وتقدير التنوع، وتحليل وجهات نظر أصحاب المصلحة وحل النزاعات بأسلوب مرن، والقدرة على القيادة وريادة الأعمال وأداء المهام بمسؤولية. • اختيار أدوات وتطبيقات الذكاء الاصطناعي المرتبطة بالأمن السيبراني بمسؤولية وتكييفها، وتقويم نتائجها وتوثيقها وتحسينها من خلال تصميم الأوامر والتعليمات، والالتزام بمعايير وممارسات الحوكمة الأخلاقية للذكاء الاصطناعي ومتطلبات الحماية المتقدمة.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، والقيم والمعايير والأخلاق المهنية والإنسانية المرتبطة بممارساته. • تمثُّل واعٍ للمواطنة المسؤولة، والمشاركة الفاعلة في المبادرات الوطنية، ولا سيما ذات العلاقة بالأمن السيبراني، في سياقات متنوعة وغير مألوفة، والالتزام بالأنظمة الوطنية، ومنها التشريعات والضوابط الوطنية للأمن السيبراني. • اتخاذ قرارات بنّاءة في الحالات التي تتطلب الاعتماد على النفس للعمل والتعلم والابتكار باستقلالية. • إدارة المهام المتعلقة بالأمن السيبراني باستقلالية. • المشاركة الفعّالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

[٥] يتوافق هذا البرنامج مع برامج البكالوريوس في المستوى السادس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات

٢-٢-٢ متطلبات القبول

- شهادة ثانوية عامة أو ما يعادلها.

٢-٢-٣ الوحدات المعرفية الأساسية

يجب على الطلبة إكمال ما يلي:

- أولاً: ثلاث وحدات معرفية أساسية في الأمن السيبراني:
  - أساسيات الأمن السيبراني Cybersecurity Fundamentals (CSF)
  - مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)
  - مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)
- ثانياً: خمس وحدات معرفية أساسية فنية أو غير فنية بحسب طبيعة البرنامج:
  - وحدات معرفية أساسية فنية:
    - أساسيات التشفير Basic Cryptography (BCY)
    - أساسيات الشبكات Basic Networking (BNW)
    - أساسيات البرمجة Basic Scripting and Programming (BSP)
    - الدفاع عن الشبكات Network Defense (NDF)
    - مفاهيم نظم التشغيل Operating Systems Concepts (OSC)
  - وحدات معرفية أساسية غير فنية:
    - التهديدات السيبرانية Cyber Threats (CTH)
    - السياسات والتشريعات والأخلاقيات والالتزام بها Policy, Legal, Ethics, Compliance (PLE)
    - تحليل المخاطر السيبرانية Security Risk Analysis (SRA)
    - تخطيط وإدارة الأمن السيبراني Cybersecurity Planning and Management (CPM)
    - إدارة البرامج الأمنية Security Program Management (SPM)

٢-٢-٤ الوحدات المعرفية الاختيارية

- هي جميع الوحدات المعرفية المتبقية، ويجب على الطلبة أن يستكملوا (٤) وحدات معرفية اختيارية على الأقل قبل التخرج.

٢-٣ البكالوريوس (برنامج في الأمن السيبراني)[٦]

١-٣-٢ توصيفات البرنامج		
المعرفة	المهارات	القيم
• معرفة بنطاق واسع ومتعمق من الأسس والنظريات والمبادئ والمفاهيم الأساسية في مجال الأمن السيبراني. • المعرفة والفهم المتعمق للعمليات والأدوات والتقنيات، والسياسات والممارسات المستخدمة في الأمن السيبراني. • مجموعة من المعارف المتخصصة والمتعلقة بالتطورات الحالية والمستجدة في مجال الأمن السيبراني.	• تطبيق النظريات والمبادئ والمفاهيم المتكاملة في سياقات مختلفة للأمن السيبراني. • تحليل وتقييم المعلومات المعقدة والمتنوعة في مجال الأمن السيبراني. • التقييم النقدي واختيار واستخدام أساليب ومنهجيات وأدوات الأمن السيبراني لحل المشكلات وتنفيذ الأعمال في مجال الأمن السيبراني. • استخدام منهجيات الدراسة والتقصي والأبحاث في مشاريع وأنشطة الأمن السيبراني. • أداء مجموعة واسعة من المهام والإجراءات باستخدام أدوات الأمن السيبراني في العمليات المعقّدة والمتنوّعة. • التواصل بالطرق المناسبة ونقل المعرفة والمهارات المتخصصة والمفاهيم المتقدمة. • تنفيذ مشاريع تعاونية تخصصية ومهنية في مجال الأمن السيبراني، والانفتاح على وجهات نظر مختلفة وتقدير التنوع، وتحليل وجهات نظر أصحاب المصلحة وحل النزاعات بأسلوب مرن، والقدرة على القيادة وريادة الأعمال وأداء المهام بمسؤولية. • اختيار أدوات وتطبيقات الذكاء الاصطناعي المرتبطة بالأمن السيبراني بمسؤولية وتكييفها، وتقويم نتائجها وتوثيقها وتحسينها من خلال تصميم الأوامر والتعليمات، والالتزام بمعايير وممارسات الحوكمة الأخلاقية للذكاء الاصطناعي ومتطلبات الحماية المتقدمة.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، والقيم والمعايير والأخلاق المهنية والإنسانية المرتبطة بممارساته. • تمثُّل واعٍ للمواطنة المسؤولة، والمشاركة الفاعلة في المبادرات الوطنية، ولا سيما ذات العلاقة بالأمن السيبراني، في سياقات متنوعة وغير مألوفة، والالتزام بالأنظمة الوطنية، ومنها التشريعات والضوابط الوطنية للأمن السيبراني. • اتخاذ قرارات بنّاءة في الحالات التي تتطلب الاعتماد على النفس للعمل والتعلم والابتكار باستقلالية. • إدارة المهام المتعلقة بالأمن السيبراني باستقلالية. • المشاركة الفعّالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

[٦] يتوافق هذا البرنامج مع برامج البكالوريوس في المستوى السادس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات

٢-٣-٢ متطلبات القبول

- شهادة ثانوية عامة أو ما يعادلها.

٢-٣-٣ الوحدات المعرفية الأساسية

يجب على الطلبة إكمال ما يلي:

- ثلاث وحدات معرفية أساسية في الأمن السيبراني:
  - أساسيات الأمن السيبراني Cybersecurity Fundamentals (CSF)
  - مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)
  - مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)
- سبع وحدات معرفية أساسية فنية:
  - أساسيات التشفير Basic Cryptography (BCY)
  - أساسيات الشبكات Basic Networking (BNW)
  - أساسيات البرمجة Basic Scripting and Programming (BSP)
  - الدفاع عن الشبكات Network Defense (NDF)
  - مفاهيم نظم التشغيل Operating Systems Concepts (OSC)
  - تراكيب البيانات Data Structures (DST)
  - قواعد البيانات Databases (DAT)
- خمس وحدات معرفية أساسية غير فنية:
  - التهديدات السيبرانية Cyber Threats (CTH)
  - السياسات والتشريعات والأخلاقيات والالتزام بها Policy, Legal, Ethics, Compliance (PLE)
  - تحليل المخاطر السيبرانية Security Risk Analysis (SRA)
  - تخطيط وإدارة الأمن السيبراني Cybersecurity Planning and Management (CPM)
  - إدارة البرامج الأمنية Security Program Management (SPM)

٢-٣-٤ الوحدات المعرفية الاختيارية

- هي جميع الوحدات المعرفية المتبقية، ويجب على الطلبة أن يستكملوا (١٠) وحدات معرفية اختيارية على الأقل قبل التخرج.

٢-٤ الدبلوم العالي (للمختصين في تقنية المعلومات)[٧]

٢-٤-١ توصيفات البرنامج

المعرفة	المهارات	القيم
• نطاق متعمق ومتخصص من المعارف النظرية والتقنية والفهم للمواضيع الأساسية في الأمن السيبراني. • المعرفة والفهم المتعمق للعمليات والأدوات والتقنيات، والسياسات والممارسات المستخدمة في الأمن السيبراني. • فهم عميق للتطورات الجديدة والمواضيع المتقدمة في الأمن السيبراني.	• اختيار المفاهيم النظرية والمنهجيات والتقنيات والأدوات الخاصة بإجراء أعمال الأمن السيبراني وتقييمها واستخدامها في سياقات معقدة ومتقدمة. • تقييم المفاهيم والمبادئ والنظريات الرئيسية في الأمن السيبراني، ومراجعتها بشكل نقدي، وإبداء الرأي فيها. • تقديم وتصميم حلول إبداعية في سياقات معقدة ومتقدّمة لمشكلات في الأمن السيبراني. • التواصل بطرق مختلفة ونقل المعرفة والمهارات المتخصصة مع فئات مختلفة من المستفيدين. • تنفيذ مشاريع تعاونية تخصصية ومهنية في مجال الأمن السيبراني، وتحليل وجهات نظر أصحاب المصلحة وحل النزاعات بأسلوب مرن، وتولي دور القيادة، وتحمّل مسؤولية عالية. • اختيار أدوات وتطبيقات الذكاء الاصطناعي المرتبطة بالأمن السيبراني بمسؤولية وتكييفها، وتقويم نتائجها وتوثيقها وتحسينها من خلال تصميم الأوامر والتعليمات، والالتزام بمعايير وممارسات الحوكمة الأخلاقية للذكاء الاصطناعي ومتطلبات الحماية المتقدمة.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، وإظهار النزاهة والقيم المهنية والإنسانية في ممارساته. • تمثُّل واعٍ للمواطنة المسؤولة، والمشاركة الفاعلة في المبادرات الوطنية، ولا سيما ذات العلاقة بالأمن السيبراني، في سياقات متنوعة وغير مألوفة، والالتزام بالأنظمة الوطنية، ومنها التشريعات والضوابط الوطنية للأمن السيبراني. • التخطيط الاحترافي للتعلم والعمل والتطوير المهني، والمشاركة في اتخاذ القرارات الاستراتيجية المهنية باستقلالية عالية. • إدارة المهام بشكل فعّال واستقلالية عالية في مجال الأمن السيبراني. • المشاركة الفعّالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

[٧] يتوافق هذا البرنامج مع برنامج الدبلوم العالي في المستوى السادس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات

٢-٤-٢ متطلبات القبول

- شهادة بكالوريوس في الأمن السيبراني أو في علوم الحاسوب أو في أي مجال ذي صلة.
- كفاءة اللغة الإنجليزية.

٢-٤-٣ الوحدات المعرفية الأساسية

- إذا لم يكمل الطالب واحدةً أو أكثر من الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني المدرجة في القسم (٢,٢,٣) قبل القبول، فيجب إكمالها في برنامج الدراسة لهذه الدرجة العلمية.

٢-٤-٤ الوحدات المعرفية الاختيارية

هي جميع الوحدات المعرفية المتبقية، ويجب على الطلبة أن يستكملوا (٨) وحدات معرفية اختيارية على الأقل قبل التخرج.

٢-٥ الدبلوم العالي (لغير المختصين في تقنية المعلومات)[٨]

٢-٥-١ توصيفات البرنامج

المعرفة	المهارات	القيم
• نطاق من المعارف النظرية المتخصصة والفهم للمواضيع الأساسية في الأمن السيبراني. • المعرفة والفهم الدقيق للنواحي التنظيمية والأخلاقية، والسياسات، والممارسات، والحوكمة، وإدارة المخاطر، ومتابعة الالتزام بالضوابط والمعايير في مجال الأمن السيبراني. • فهم عميق للتطورات الجديدة في الأمن السيبراني.	• تطبيق المبادئ والمنهجيات والمفاهيم والأدوات الخاصة في سياقات متقدمة في الأمن السيبراني. • تحليل وبناء وتحديث السياسات، والنواحي التنظيمية والأخلاقية، ومتابعة الالتزام بها، وإدارة المخاطر، والحوكمة في مجال الأمن السيبراني. • تقييم المفاهيم والمبادئ والمنهجيات الرئيسية ومراجعتها بشكل نقدي، وإبداء الرأي فيها، وتقديم حلول إبداعية في سياقات معقدة ومتقدّمة لمشكلات في الأمن السيبراني. • أداء مجموعة من المهام والإجراءات باستخدام أدوات لتقييم المخاطر السيبرانية. • التواصل بطرق مختلفة ونقل المعرفة والمهارات المتخصصة مع فئات مختلفة من المستفيدين. • تنفيذ مشاريع تعاونية مهنية في مجال الأمن السيبراني، وتحليل وجهات نظر أصحاب المصلحة وحل النزاعات بأسلوب مرن، وتولي دور القيادة، وتحمّل مسؤولية عالية. • استخدام أدوات وتطبيقات الذكاء الاصطناعي ذات الصلة بأعمال الأمن السيبراني بمسؤولية، وتقويم نتائجها والتحقق منها وتحسينها من خلال تصميم الأوامر والتعليمات، والالتزام بمعايير وممارسات الحوكمة الأخلاقية للذكاء الاصطناعي.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، وإظهار النزاهة والقيم المهنية والإنسانية في ممارساته. • تمثُّل واعٍ للمواطنة المسؤولة، والمشاركة الفاعلة في المبادرات الوطنية، ولا سيما ذات العلاقة بالأمن السيبراني، في سياقات متنوعة وغير مألوفة، والالتزام بالأنظمة الوطنية، ومنها التشريعات والضوابط الوطنية للأمن السيبراني. • التخطيط الاحترافي للتعلم والعمل والتطوير المهني، والمشاركة في اتخاذ القرارات الاستراتيجية المهنية باستقلالية عالية. • إدارة المهام بشكل فعّال واستقلالية عالية في مجال الأمن السيبراني. • المشاركة الفعّالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

٢-٥-٢ متطلبات القبول

- شهادة بكالوريوس.
- كفاءة اللغة الإنجليزية.

[٨] يتوافق هذا البرنامج مع برنامج الدبلوم العالي في المستوى السادس في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات

٢-٥-٣ الوحدات المعرفية الأساسية

يجب على الطلبة إكمال ما يلي:

- ثلاث وحدات معرفية أساسية في الأمن السيبراني:
  - أساسيات الأمن السيبراني Cybersecurity Fundamentals (CSF)
  - مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)
  - مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)
- ثلاث وحدات معرفية أساسية غير فنية:
  - التهديدات السيبرانية Cyber Threats (CTH)
  - السياسات والتشريعات والأخلاقيات والالتزام بها Policy, Legal, Ethics, Compliance (PLE)
  - تحليل المخاطر السيبرانية Security Risk Analysis (SRA)

٢-٥-٤ الوحدات المعرفية الاختيارية

- هي جميع الوحدات المعرفية المتبقية، ويجب على الطلبة أن يستكملوا وحدتين معرفيتين اختياريتين على الأقل قبل التخرج.

٢-٦ الماجستير (مسار في الأمن السيبراني)[٩]

٢-٦-١ توصيفات البرنامج

المعرفة	المهارات	القيم
• معرفة بنطاق واسع ومتعمق من الموضوعات النظرية والتقنية في مجال الأمن السيبراني. • فهم عميق للعمليات والممارسات في الأمن السيبراني. • فهم عميق للتطورات والنظريات الحديثة والمتقدمة في الأمن السيبراني. • معرفة مجموعة من الأساليب المتخصصة في البحث والاستقصاء في مجال الأمن السيبراني.	• استخدام مجال واسع من الأدوات والأساليب والممارسات المتخصصة المستندة إلى معرفة بأحدث التطورات في مجال الأمن السيبراني. • تخطيط وتنفيذ الأبحاث السيبرانية المتقدمة والمشاريع الابتكارية لتطوير منتجات وخدمات الأمن السيبراني. • تطبيق النظريات والمبادئ والمفاهيم المتخصصة، واستخدام مجال كبير من المنهجيات والأساليب والممارسات في سياقات معقدة ومتقدمة في مجال الأمن السيبراني، وتقويمها وإجراء مراجعة نقدية لها، وتقديم حلول إبداعية لقضاياه ومشكلاته. • استخدام عمليات وتقنيات وأدوات متقدمة ومتخصصة؛ للقيام بالأعمال المعقدة في الأمن السيبراني. • توظيف أدوات الذكاء الاصطناعي بفاعلية لإنجاز مهام متقدمة التعقيد والتعامل مع قضايا مركّبة في مجال الأمن السيبراني، وتقويم فعاليتها ومخرجاتها وتحسينها وتوثيقها، باعتماد أساليب متقدمة في التوجيه وهندسة الأوامر، والالتزام بمعايير وممارسات الحوكمة الأخلاقية للذكاء الاصطناعي ومتطلبات الحماية المتقدمة. • التواصل بطرق مختلفة ونقل المعرفة والمهارات المتخصصة مع فئات مختلفة من المستفيدين. • تنفيذ مشاريع ومبادرات تعاونية متقدمة في مجال الأمن السيبراني، والتفاعل مع زملاء من ثقافات متعددة، وتبادل الأفكار والمصادر لتطوير عمل الفريق، وتولي دور القيادة، وتحمّل مسؤوليات متعددة.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، وإظهار النزاهة والقيم المهنية والإنسانية عند التعامل مع القضايا والمشكلات المختلفة في مجال الأمن السيبراني. • تمثُّل واعٍ للمواطنة المسؤولة، والمشاركة الفاعلة في المبادرات الوطنية، ولا سيما ذات العلاقة بالأمن السيبراني، في سياقات معقدة ومتقدمة، والالتزام بالأنظمة الوطنية، ومنها التشريعات والضوابط الوطنية للأمن السيبراني. • التخطيط الاحترافي للتعلم والعمل والتطوير المهني، والمشاركة في اتخاذ القرارات الاستراتيجية المهنية باستقلالية عالية. • إدارة المهام بشكل فعّال وإنجازها بانضباط وباستقلالية عالية في مجال الأمن السيبراني. • المشاركة الفعّالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

[٩] يتوافق هذا البرنامج مع برنامج الماجستير في المستوى السابع في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات.

٢-٦-٢ متطلبات القبول

- شهادة بكالوريوس في الأمن السيبراني أو في علوم الحاسب أو في أي مجال ذي صلة.
- كفاءة اللغة الإنجليزية.

٢-٦-٣ الوحدات المعرفية الأساسية

- إذا لم يكمل الطالب واحدةً أو أكثر من الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني المدرجة في القسم (٢,٢,٣) قبل القبول، فيجب إكمالها في برنامج الدراسة لهذه الدرجة العلمية.
- إتمام رسالة أو مشروع حول موضوع في الأمن السيبراني.

٢-٦-٤ الوحدات المعرفية الاختيارية

- يجب على الطلبة إكمال (٤) وحدات معرفية اختيارية على الأقل قبل التخرج، وتشمل الوحدات المعرفية الاختيارية المتاحة لهذا البرنامج جميع الوحدات المعرفية باستثناء الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني المدرجة في القسم (٢,٢,٣).

٢-٧ الماجستير (برنامج في الأمن السيبراني)[١٠]

٢-٧-١ توصيفات البرنامج

المعرفة	المهارات	القيم
• معرفة بنطاق واسع ومتعمق من الموضوعات النظرية والتقنية في مجال الأمن السيبراني. • فهم عميق للعمليات والممارسات في الأمن السيبراني. • فهم عميق للتطورات والنظريات الحديثة والمتقدمة في الأمن السيبراني. • معرفة مجموعة من الأساليب المتخصصة في البحث والاستقصاء في مجال الأمن السيبراني.	• استخدام مجال واسع من الأدوات والأساليب والممارسات المتخصصة المستندة إلى معرفة بأحدث التطورات في مجال الأمن السيبراني. • تخطيط وتنفيذ الأبحاث السيبرانية المتقدمة والمشاريع الابتكارية لتطوير منتجات وخدمات الأمن السيبراني. • تطبيق النظريات والمبادئ والمفاهيم المتخصصة، واستخدام مجال كبير من المنهجيات والأساليب والممارسات في سياقات معقدة ومتقدمة في مجال الأمن السيبراني، وتقويمها وإجراء مراجعة نقدية لها، وتقديم حلول إبداعية لقضاياه ومشكلاته. • استخدام عمليات وتقنيات وأدوات متقدمة ومتخصصة؛ للقيام بالأعمال المعقدة في الأمن السيبراني. • توظيف أدوات الذكاء الاصطناعي بفاعلية لإنجاز مهام متقدمة التعقيد والتعامل مع قضايا مركّبة في مجال الأمن السيبراني، وتقويم فعاليتها ومخرجاتها وتحسينها وتوثيقها، باعتماد أساليب متقدمة في التوجيه وهندسة الأوامر، والالتزام بمعايير وممارسات الحوكمة الأخلاقية للذكاء الاصطناعي ومتطلبات الحماية المتقدمة. • التواصل بطرق مختلفة ونقل المعرفة والمهارات المتخصصة مع فئات مختلفة من المستفيدين. • تنفيذ مشاريع ومبادرات تعاونية متقدمة في مجال الأمن السيبراني، والتفاعل مع زملاء من ثقافات متعددة، وتبادل الأفكار والمصادر لتطوير عمل الفريق، وتولي دور القيادة، وتحمّل مسؤوليات متعددة.	• الالتزام بأخلاقيات ومعايير المهنة للأمن السيبراني، وإظهار النزاهة والقيم المهنية والإنسانية عند التعامل مع القضايا والمشكلات المختلفة في مجال الأمن السيبراني. • تمثُّل واعٍ للمواطنة المسؤولة، والمشاركة الفاعلة في المبادرات الوطنية، ولا سيما ذات العلاقة بالأمن السيبراني، في سياقات معقدة ومتقدمة، والالتزام بالأنظمة الوطنية، ومنها التشريعات والضوابط الوطنية للأمن السيبراني. • التخطيط الاحترافي للتعلم والعمل والتطوير المهني، والمشاركة في اتخاذ القرارات الاستراتيجية المهنية باستقلالية عالية. • إدارة المهام بشكل فعّال وإنجازها بانضباط وباستقلالية عالية في مجال الأمن السيبراني. • المشاركة الفعّالة في تطوير تخصص الأمن السيبراني وخدمة المجتمع.

[١٠] يتوافق هذا البرنامج مع برنامج الماجستير في المستوى السابع في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات.

٢-٧-٢ متطلبات القبول

- شهادة بكالوريوس في الأمن السيبراني أو في علوم الحاسب أو في أي مجال ذي صلة.
- كفاءة اللغة الإنجليزية.

٢-٧-٣ الوحدات المعرفية الأساسية

- إذا لم يكمل الطالب واحدةً أو أكثر من الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني المدرجة في القسم (٢,٢,٣) قبل القبول، فيجب إكمالها في برنامج الدراسة لهذه الدرجة العلمية.
- إتمام رسالة أو مشروع حول موضوع في الأمن السيبراني.

٢-٧-٤ الوحدات المعرفية الاختيارية

- يجب على الطلبة إكمال (٧) وحدات معرفية اختيارية على الأقل قبل التخرج، وتشمل الوحدات المعرفية الاختيارية المتاحة لهذا البرنامج جميع الوحدات المعرفية باستثناء الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني المدرجة في القسم (٢,٢,٣).

٢-٨ الدكتوراه[١١]

٢-٨-١ توصيفات البرنامج

المعرفة	المهارات	القيم
• معرفة وفهم عميق لنطاق واسع من الموضوعات في مجال الأمن السيبراني، تتكامل فيها الموضوعات المتقدمة والنظريات المتخصصة، والمبادئ والمفاهيم الرائدة اللازمة لإيجاد معرفة جديدة وأصيلة، وتتضمّن تكامل المجالات فيما بينها.	• تقويم المفاهيم والمبادئ والنظريات الحديثة، والجمع بينها، والمراجعة النقدية لها، وتطوير حلول إبداعية ومبتكرة ورائدة لقضايا ومشكلات ومنتجات وخدمات عالية التعقيد وحديثة في مجال الأمن السيبراني. • تطبيق نظريات ومبادئ ومفاهيم رائدة، واستخدام نطاق واسع من المنهجيات والأساليب والسياسات والممارسات في سياقات عالية التعقيد في مجال الأمن السيبراني.	• إظهار مستوى عال من النزاهة والقيم الأكاديمية في مجال الأمن السيبراني عند التعامل مع القضايا الأخلاقية والمهنية الناشئة والبحث والمعرفة، ودعمها. • تمثُّل واعٍ للمواطنة المسؤولة، والمشاركة الفاعلة في المبادرات الوطنية في مجال الأمن السيبراني، في سياقات جديدة عالية التعقيد، والالتزام بالأنظمة الوطنية ومنها التشريعات والضوابط الوطنية للأمن السيبراني.
• المعرفة والفهم التفصيلي الدقيق بعمليات، وتقنيات، وسياسات، وممارسات الأمن السيبراني لحماية البيانات والأنظمة والشبكات.	• تطوير مناهج البحث والاستقصاء المتقدّمة وتكييفها وتطبيقها؛ لإيجاد معرفة أصيلة تُسهم بشكل كبير في الأمن السيبراني. • استخدام عمليات وتقنيات وأدوات وأجهزة متقدمة وحديثة، في مجال الأمن السيبراني، للقيام بأنشطة عملية مستجدة وصعبة وعالية التعقيد.	• تطوير الخبرات المهنية بصورة مستمرة، واتخاذ قرارات استراتيجية أكاديمية ومهنية باستقلالية عالية؛ وصياغة أو استحداث حلول مبتكرة للمهمات المعقدة، وإدارة المهام والأنشطة البحثية والمتخصصة في مجال الأمن السيبراني وإنجازها بإتقان وانضباط
• معرفة وفهم شامل للتطورات الحديثة والقضايا والتحديات الناشئة في الأمن السيبراني.	• التواصل بطرق متعددة؛ لنشر المعرفة الأصيلة والرؤى الجديدة وتعزيزها، وإجراء حوار علمي ومهني مع الأقران والمجموعات المتخصصة والمجتمع ككل.	
• معرفة متقدمة بمنهجيات إجراء البحوث الأصيلة والأنشطة العلمية التي تُسهم في تطوير مجال الأمن السيبراني.	• بناء فرق بحثية ومهنية متعددة التخصصات في مجال الأمن السيبراني، والتفاعل على المستويات المؤسسية والمجتمعية، وتولي زمام المبادرة والقيادة فيها، وتحمّل مسؤولية أنشطته العلمية باستقلالية عالية. • معالجة البيانات الكمية والكيفية وتفسيرها، واستخدامها في البحوث والمشاريع أو الابتكارات الحديثة وعالية التعقيد، المرتبطة بمجال الأمن السيبراني، مع الالتزام بمتطلبات حماية البيانات والخصوصية في البحث العلمي والممارسات المهنية. • توظيف أدوات الذكاء الاصطناعي وتطبيقاته وتكييفها بفاعلية لدعم البحث والابتكار وتطوير حلول مبتكرة في الأمن السيبراني، مع تحسين جودة النتائج ودقتها من خلال التوجيه المتقدم وهندسة الأوامر القائمة على التجريب والتحسين المستمر، والالتزام بمعايير وممارسات الحوكمة الأخلاقية للذكاء الاصطناعي.	• تعزيز العلاقات المهنية وخدمة المجتمع في مجال الأمن السيبراني.

[١١] يتوافق هذا البرنامج مع برنامج الدكتوراه في المستوى الثامن في التصنيف السعودي الموحد للمستويات والتخصصات التعليمية، والإطار الوطني للمؤهلات.

٢-٨-٢ متطلبات القبول

- شهادة الماجستير في الأمن السيبراني أو في علوم الحاسوب أو في أي مجال ذي صلة.[١٢]
- كفاءة اللغة الإنجليزية.

٢-٨-٣ الوحدات المعرفية الأساسية

- إذا لم يكمل الطالب واحدةً أو أكثر من الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني المدرجة في القسم (٢,٢,٣) قبل القبول، فيجب إكمالها في برنامج الدراسة لهذه الدرجة العلمية.
- إتمام رسالة علمية حول موضوع في الأمن السيبراني.

٢-٨-٤ الوحدات المعرفية الاختيارية

- يجب على الطلبة إكمال (٣) وحدات معرفية اختيارية على الأقل قبل التخرج، وتشمل الوحدات المعرفية الاختيارية المتاحة لهذا البرنامج جميع الوحدات المعرفية باستثناء الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني المدرجة في القسم (٢,٢,٣).

[١٢] يجوز قبول الحاصل على شهادة البكالوريوس في الأمن السيبراني أو في علوم الحاسب أو في أي مجال ذي صلة في برامج الدكتوراة بعد البكالوريوس مباشرة بحسب الإطار الوطني للمؤهلات

	الدبلوم المتوسط	البكالوريوس (مسار في الأمن السيبراني)	البكالوريوس (برنامج في الأمن السيبراني)	الدبلوم العالي (لغير المختصين في تقنية المعلومات)	الدبلوم العالي (للمختصين في تقنية المعلومات)	الماجستير (مسار في الأمن السيبراني)	الماجستير (برنامج في الأمن السيبراني)	الدكتوراه
متطلبات القبول	شهادة الثانوية العامة أو ما يعادلها			شهادة بكالوريوس	شهادة بكالوريوس في الأمن السيبراني أو في علوم الحاسب أو في أي مجال ذي صلة			شهادة الماجستير في الأمن السيبراني أو في علوم الحاسب أو في أي مجال ذي صلة
الوحدات المعرفية الأساسية	CSF, CDP, ISC, BCY, BNW, BSP, NDF, OSC	CSF, CDP, ISC, and either: • BCY, BNW, BSP, NDF, OSC • CTH, PLE, SRA, CPM, SPM	CSF, CDP, ISC, BCY, BNW, BSP, NDF, OSC, DST, DAT, CTH, PLE, SRA, CPM, SPM	CSF, CDP, ISC, CTH, PLE, SRA	إذا لم يكمل الطالب واحدة أو أكثر من الوحدات المعرفية الأساسية لدرجة البكالوريوس كمسار في الأمن السيبراني قبل القبول، فيجب إكمالها في برنامج الدراسة لهذه الرجة العلمية.		إتمام رسالة أو مشروع حول موضوع في الأمن السيبراني	إتمام رسالة علمية حول موضوع في الأمن السيبراني
الوحدات المعرفية الاختيارية	٣ وحدات معرفية اختيارية على الأقل	٤ وحدات معرفية اختيارية على الأقل	٤ وحدات معرفية اختيارية على الأقل	٨ وحدات معرفية اختيارية على الأقل	وحدتين معرفية اختيارية على الأقل	وحدات معرفية اختيارية على الأقل	٧ وحدات معرفية اختيارية على الأقل	٣ وحدات معرفية اختيارية على الأقل

الشكل:١ ملخص متطلبات القبول، والوحدات المعرفية الأساسية، والوحدات المعرفية الاختيارية لجميع البرامج.

٣ الوحدات المعرفية

أساسيات الأمن السيبراني Cybersecurity Fundamentals (CSF)

الوصف	تقدم هذه الوحدة المعرفية معارف عامة حول المفاهيم الأساسية في مجال الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أهمية الأمن السيبراني ٢. مفاهيم الأمن السيبراني ٣. المخاطر والتهديدات والثغرات السيبرانية ٤. مثلث السرية والسلامة والتوافر ٥. ضبط الوصول والتوثيق والتصريح وعدم الإنكار ٦. التشفير واستخداماته ٧. الحوكمة وإدارة المخاطر السيبرانية ٨. حماية البيانات والأنظمة والشبكات ٩. اكتشاف الحوادث السيبرانية والاستجابة لها ١٠. التقنيات والحلول المستخدمة في الأمن السيبراني ١١. الهندسة الاجتماعية ودور العنصر البشري في الأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تعريف المبادئ والأهداف الأساسية للأمن السيبراني. ٢. تحديد المخاطر والتهديدات والثغرات السيبرانية الشائعة. ٣. وصف الهجمات السيبرانية الشائعة، بما في ذلك هجمات الهندسة الاجتماعية. ٤. شرح المنهجيات والطرق المستخدمة لحماية البيانات والأنظمة والشبكات. ٥. تحديد التدابير الأساسية التي ينبغي اتخاذها عند تعرض النظام للاختراق. ٦. توضيح دور الحوكمة وإدارة المخاطر السيبرانية في دعم ممارسات الأمن السيبراني.

مبادئ التصميم في الأمن السيبراني Cybersecurity Design Principles (CDP)

الوصف	تقدم هذه الوحدة المعرفية المعارف الخاصة بأساسيات التصميم الآمن لتصميم أنظمة سيبرانية آمنة وموثوقة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مبادئ تصميم البرامج والأنظمة ٢. فصل المهمات والمجالات ٣. الأمن الكافي ٤. العزل ٥. دمج العناصر مع بعضها في مكون واحد ٦. تصميم الوحدات ٧. مرونة الأنظمة والمنظمات ٨. التصميم الآمن ٩. المساءلة ١٠. البساطة في التصميم ١١. تقليص التنفيذ ١٢. التصميم المفتوح ١٣. التسوية الكاملة ١٤. تصميم الدفاع الأمني متعدد الطبقات ١٥. الحد الأدنى من الصلاحيات ١٦. الاستفادة من المكونات الموجودة ١٧. نماذج مستويات أمن النظم وصلاحيات الوصول ١٨. وضع السلامة والأمان في حالة الأعطال ١٩. تقليل المفاجآت في أداء الأجهزة ٢٠. تقليص سطح الثقة ٢١. التصميم الآمن وسهولة الاستخدام ٢٢. علاقات الثقة ٢٣. أنماط البرمجة الآمنة ٢٤. أخلاقيات الأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التعبير عن مبادئ التصميم الآمن. ٢. شرح أهمية مبادئ تصميم الأمن السيبراني وأثر كل مبدأ على تصميم الأنظمة الموثوقة. ٣. تمييز مبدأ التصميم الذي تمت مخالفته لكل نقطة من نقاط الضعف الأمنية الشائعة في الأنظمة. ٤. تحليل مبادئ تصميم الأمن السيبراني المطلوبة في إعدادات معينة ٥. تطبيق مبادئ تصميم الأمن السيبراني على برامج و/أو أنظمة معقدة.

مكونات أنظمة تقنية المعلومات IT Systems Components (ISC)

الوصف	تقدم هذه الوحدة المعرفية مقدمة عامة حول مكونات أنظمة تقنية المعلومات الشائعة والآثار العامة للأمن السيبراني المرتبطة بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. حماية الأجهزة الطرفية في الشبكات (مثل: محطات العمل، الحواسيب المحمولة، الأجهزة اللوحية، الخوادم، الأجهزة الملحقة، الأجهزة المحمولة، الأجهزة الطرفية مثل الطابعات والماسحات ووحدات التخزين الخارجية، والأجهزة القابلة للارتداء) ٢. أجهزة التخزين (مثل: وحدات التخزين الخارجية، أنظمة الملفات، خوادم الملفات المشتركة، قواعد البيانات) ٣. بنى الأنظمة (مثل: المؤسسية، السحابية، SaaS/PaaS/IaaS، وغيرها) والتقنيات الممكنة (مثل: الحاويات، الافتراضية) ٤. البيئات البديلة للخدمات المدارة (مثل: بيئات التحكم الإشرافي وجمع البيانات (SCADA)، الأنظمة ذات الاستجابة اللحظية، والبنى التحتية الحساسة) ٥. إدارة الإعدادات ٦. الشبكات (الإنترنت، الشبكات المحلية، الشبكات اللاسلكية، الشبكات الواسعة، شبكات التحكم الداخلية.، إنترنت الأشياء، أنظمة السيارات، والمدن الذكية) ٧. معدات الشبكات (مثل: الموجهات، المحولات، الجدران النارية، وكابلات الشبكة) ٨. تعيينات الشبكة (تحديد وحصر مكونات الشبكة) ٩. مكونات أمن الشبكات (منع فقدان البيانات، الشبكات الخاصة الافتراضية، الجدران النارية، أنظمة المراقبة، وأنظمة كشف التسلل) ١٠. أنظمة رصد ومنع التسلل، والاستجابة للحوادث السيبرانية ١١. الخدمات المدارة ١٢. إدارة ومراقبة تقنية المعلومات (مثل: أدوات مراقبة النظام، أدوات إدارة الإعدادات، وأدوات النسخ الاحتياطي والاستعادة) ١٣. البرمجيات: (مثل: أنظمة التشغيل، التطبيقات، وبرامج البيئات الافتراضية) ١٤. أمن البرمجيات: (مبادئ البرمجة الآمنة، ومشكلات البرمجيات حسب النوع) ١٥. إدارة الإعدادات ١٦. التحديثات والإصلاحات البرمجية للأنظمة والتطبيقات (مثل: إدارة التصحيحات) ١٧. فحص الثغرات الأمنية (مثل: نافذة الثغرة، وتوفر التصحيح لثغرات اليوم الصفري) ١٨. الأمن المادي والبيئي ١٩. إنترنت الأشياء ٢٠. الهيكل التنظيمي لتقنية المعلومات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحديد مكونات أنظمة تقنية المعلومات من أجهزة وبرمجيات، وتوضيح وظائفها الأساسية. ٢. شرح التأثيرات الرئيسية للأمن السيبراني في بيئات تقنية المعلومات الحالية والمستقبلية. ٣. التعبير عن أنظمة الأمن السيبراني الشائعة ومكوناتها وأنشطتها وقيمها بالنسبة للأمن السيبراني. ٤. وصف بنى الأنظمة والبرمجيات ومكوناتها الرئيسية. ٥. وصف كيفية إدارة البرمجيات داخل المنظمة.

أساسيات التشفير Basic Cryptography (BCY)

الوصف	تقدم هذه الوحدة المعرفية مقدمة في خوارزميات وتطبيقات التشفير الأساسية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الوظائف الأمنية للتشفير ٢. تاريخ التشفير والتشفير الكلاسيكي ٣. خوارزميات التشفير المتماثلة ٤. البيانات الكتلية والبيانات الانسيابية ٥. طرق عمليات التشفير الكتلية ٦. خوارزميات التشفير غير المتماثلة ٧. إنشاء وإدارة وتبادل وتوزيع المفاتيح ٨. الشهادات الرقمية والبنية التحتية للمفاتيح العامة ٩. دوال الاختزال ١٠. خصائص دوال الاختزال للتشفير ١١. التواقيع الرقمية ١٢. بروتوكولات ومعايير التشفير الشائعة ١٣. أنواع الهجمات في التشفير
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف وظائف الأمن الرئيسية التي يمكن تحقيقها باستخدام التشفير. ٢. شرح المكونات الرئيسية لأي نظام تشفير. ٣. التمييز بين خوارزميات التشفير المتماثلة وغير المتماثلة. ٤. شرح استخدام دوال الاختزال في التشفير لضمان أصالة البيانات والتحقق من سلامة الرسائل. ٥. توضيح استخدام البنية التحتية للمفاتيح العامة في إجراء التواقيع الرقمية وتشفير البيانات.

أساسيات الشبكات Basic Networking (BNW)

الوصف	تقدم هذه الوحدة المعرفية مقدمة حول الشبكات وتشمل: العمليات، المكونات، الطبقات، البروتوكولات، الخدمات، التطبيقات، الأدوات، أمن الشبكات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. نموذج ISO/OSI ونموذج TCP/IP في الشبكات ٢. وسائط الشبكات السلكية والبصرية واللاسلكية ٣. هيكلية الشبكة: الناقل (Bus)، النجمي (Star)، الشبكة الجزئية والكاملة (Partial and Full Mesh) ٤. بنى الشبكات وهيكليتها: PAN, LAN, WAN, DMZ, VLAN, NAT، التقسيمات والتجميعات الشبكية ٥. نماذج خدمات الشبكات: النظير إلى النظير، والعميل والخادم ٦. أجهزة الشبكات الشائعة: الموجهات، المبدلات، العملاء والخوادم، نقاط الوصول اللاسلكية، وجدران الحماية ٧. بروتوكولات طبقة الشبكة وطبقة النقل: IP, TCP, UDP, ICMP ٨. بروتوكولات خدمات الشبكات: DNS, NTP, DHCP وغيرها ٩. بروتوكولات تطبيقات الشبكات: SMTP, HTTP, VoIP, SSH وغيرها ١٠. الأدوات الأساسية لإدارة الشبكات: PING و Traceroute ١١. لمحة شاملة عن مفاهيم أمن الشبكات: الثقة المعدومة (Zero Trust)، والدفاع متعدد الطبقات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المفاهيم الأساسية لشبكات البيانات بما فيها المكونات والطبقات والبروتوكولات والخدمات والتطبيقات والأدوات. ٢. تصميم هيكلية شبكة أساسية بناءً على سيناريو إعدادات معين. ٣. تحديد مسار حزم البيانات بالنسبة لروابط بسيطة. ٤. تطبيق أدوات الشبكة للتعرف على سير حزم البيانات المترابطة. ٥. توضيح الثغرات الأمنية والتهديدات الشائعة في الشبكات.

أساسيات البرمجة Basic Scripting and Programming (BSP)

الوصف	تركز هذه الوحدة المعرفية على تمكين كتابة نصوص برمجية/برامج بسيطة لأتمتة وتنفيذ عمليات بسيطة، وتوفير المهارات اللازمة لتنفيذ النصوص البرمجية واستخدام لغات البرمجة لحل المسائل. كما تشمل هذه المعرفة الممارسات الأساسية للأمن السيبراني عند تطوير النصوص البرمجية/البرامج.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المفاهيم الأساسية والتطبيقات الأولية للتعابير النمطية ٢. أساسيات تراكيب البيانات والخوارزميات ٣. العمليات المنطقية (Boolean) ٤. كتابة النصوص البرمجية في أنظمة ويندوز ولينكس. ٥. بيئات التطوير المتكاملة (IDE)، والمترجمات/المفسرات ٦. مفاهيم وبنى البرمجة الأساسية: المتغيرات وأنواع البيانات، السلاسل النصية والمصفوفات والسجلات، التنفيذ المتسلسل والمتوازي، الجمل والتعابير البرمجية، القرارات والتفرعات، الحلقات في البرمجة وأنواعها، الوظائف والإجراءات والاستدعاءات، طرق اكتشاف الأخطاء، الإدخال/الإخراج عبر الشاشة والملفات، والمكتبات ٧. المفاهيم الأساسية للبرمجة الآمنة: الصلاحيات، فحص الحدود، التحقق من صحة المدخلات، فحص نوع البيانات، التحقق من معاملات الدوال، ومعالجة الأخطاء البرمجية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطوير وتنفيذ برامج باستخدام لغة عالية المستوى بالاعتماد على مفاهيم وبنى البرمجة الأساسية. ٢. كتابة نصوص برمجية بسيطة لأتمتة مهام إدارة الأنظمة. ٣. تطوير وتنفيذ برامج آمنة وموثوقة مع مراعاة خصائص أنظمة التشغيل والبيئات المختلفة. ٤. تطبيق ممارسات الأمن السيبراني الأساسية في كتابة النصوص البرمجية، بما في ذلك فحص الحدود والتحقق من صحة المدخلات.

الدفاع عن الشبكات Network Defense (NDF)

الوصف	تقدم هذه الوحدة المعرفية المفاهيم والمهارات والمعرفة والأدوات اللازمة للدفاع عن الشبكات وحمايتها ضد التهديدات السيبرانية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مفاهيم الدفاع عن الشبكات: الدفاع بعمق، الهجمات على الشبكات واستغلالها، تأمين الشبكات، تقليص الانكشاف (مثل: سطح الهجوم ومتجهاته) ٢. أدوات الدفاع/المراقبة في الشبكات: جدران الحماية، المناطق الوسيطة المعزولة (DMZ) / الخوادم الوسيطة، الشبكات الخاصة الافتراضية (VPN)، المصائد (مثل: مصائد الهجمات وشبكات مصائد الهجمات)، تركيب وتشغيل أنظمة رصد ومنع التسلل، تحليل تواقيع المرور، وكشف الأنشطة غير الطبيعية في الشبكة ٣. عمليات الشبكات: مراقبة أمن الشبكات (مثل: مراكز عمليات الشبكة NOCs، ومراكز عمليات الأمن السيبراني SOCs)، تحليل مرور البيانات في الشبكات ٤. سياسات أمن الشبكات المتعلقة بالدفاع/الأمن: ضبط الوصول في الشبكات (الداخلي والخارجي)، تطوير وتطبيق سياسات الشبكات ٥. نظام إدارة سجل الاحداث ومراقبة الأمن السيبراني (SIEM): تحليل السجلات، وتصور الأنشطة غير الطبيعية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح المفاهيم الرئيسية في الدفاع عن الشبكات. ٢. استخدام أدوات الدفاع عن الشبكات للدفاع ضد الهجمات والتقليل من الثغرات الأمنية. ٣. تحليل تنفيذ السياسات الأمنية لحماية الشبكات. ٤. فحص العمليات المتعلقة بالدفاع عن الشبكات.

مفاهيم نظم التشغيل Operating Systems Concepts (OSC)

الوصف	تقدم هذه الوحدة المعرفية مقدمة عامة عن الأدوار والوظائف والخدمات الأساسية لنظم التشغيل.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. حالات الصلاحيات الممنوحة وغير الممنوحة ٢. العمليات وإدارة العمليات ٣. حزم التعليمات والتزامن ٤. الجدولة ٥. إدارة الذاكرة ٦. إدارة المدخلات والمخرجات ٧. أنظمة الملفات ٨. البيئات الافتراضية ومشغلات الأجهزة الافتراضية (Hypervisors) ٩. التصميم الآمن في نظم التشغيل ١٠. ضبط الوصول: النماذج، والآليات ١١. فصل النطاقات، عزل العمليات، تغليف الموارد، منح أدنى الصلاحيات الممكنة ١٢. إدارة الحوادث
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح الأدوار والوظائف والخدمات الأساسية لنظم التشغيل. ٢. شرح كيفية تعامل نظم التشغيل مع مكونات الأجهزة والتطبيقات البرمجية الأخرى. ٣. شرح مسائل الأمن السيبراني الرئيسية المتعلقة بنظم التشغيل. ٤. تأمين نظم التشغيل في بيئة افتراضية.

التهديدات السيبرانية Cyber Threats (CTH)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات الخاصة بالتهديدات والهجمات السيبرانية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. نماذج وأنواع التهديدات السيبرانية ٢. نموذج المهاجم السيبراني: الموارد، القدرات، الدوافع، كراهية المجازفة، الوصول ٣. أساليب الهجمات: الأبواب الخلفية، أحصنة طروادة، الفيروسات، برمجيات الفدية، الهجمات اللاسلكية، الهندسة الاجتماعية، القنوات السرية ٤. تخمين وكسر كلمة المرور ٥. اعتراض البيانات، التنصت، الانتحال، اختطاف الجلسة، وهجوم الرجل في المنتصف ٦. تهديدات كشف وتغيير وتخريب البيانات ٧. تهديدات الإنكار للعمليات ٨. هجوم تعطيل الخدمة، والهجوم الموزع لتعطيل الخدمة، والبرمجيات الآلية وشبكاتها (Bots) ٩. هجمات تطبيقات الويب، وهجمات الحوسبة السحابية ١٠. تجاوز سعة الذاكرة (Buffer Overflow) ١١. الاستمرارية (Persistence) ١٢. الهجمات غير المعروفة مسبقاً (Zero-Day Exploits) ١٣. مؤشرات الاختراق ١٤. الوقائع الدالة على حدوث الهجمات السيبرانية وتوقيتها ١٥. الجهات المهاجمة: التهديدات الداخلية، المهاجمون المبتدئون (Script Kiddies)، التهديدات المستمرة المتقدمة (APT) ١٦. أسطح الهجمات ومتجهات الهجمات وأشجار الهجمات ١٧. مصادر معلومات التهديدات السيبرانية ١٨. تهديدات أنظمة التشفير ١٩. الهندسة الاجتماعية ٢٠. التكتيكات والتقنيات والإجراءات (TTPs)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصنيف موارد وقدرات وأساليب ودوافع المهاجمين. ٢. وصف أنواع الهجمات السيبرانية المختلفة وخصائصها. ٣. تمييز وتحديد الوقائع الدالة على حدوث الهجمات السيبرانية. ٤. تحديد ما إذا كان هجوم معين يمثل تهديداً لمنظمة معينة.

إدارة وتخطيط الأمن Cybersecurity Planning and Management (CPM) السيبراني

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات الضرورية على المستوى الاستراتيجي لتطوير وتنفيذ والتواصل الفعال والإشراف على سياسات وإجراءات وعمليات وخطط الأمن السيبراني للمنظمات، مع مواءمة مبادرات الأمن السيبراني مع أهداف المنظمة والمتطلبات التنظيمية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المعارف العامة والشائعة المتعلقة بالتخطيط والإدارة في مجال الأمن السيبراني ٢. التخطيط والإدارة على المستويات العملية والتكتيكية والاستراتيجية ٣. الوظائف التنفيذية العليا ذات العلاقة بالأمن السيبراني ٤. الأمن السيبراني كعنصر أساسي في الاستراتيجيات التنظيمية ٥. تقييم وإدارة المخاطر ٦. سياسات وإجراءات الأمن السيبراني ٧. أفضل ممارسات وأطر الأمن السيبراني ٨. الامتثال والمتطلبات التنظيمية ٩. لمحة عامة عن هندسة وتصميم الأمن السيبراني ١٠. إدارة مخاطر الموردين والأطراف الثالثة ١١. لمحة عامة عن المعلومات الاستباقية للتهديدات وتحليلها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحليل وظائف أمن الأنظمة ونقاط القوة والضعف فيها. ٢. تحديد وتوضيح الأدوار والمسؤوليات في تخطيط الأمن السيبراني والإدارة الأمنية. ٣. تطوير السياسات والعمليات والإجراءات بما يتوافق مع الأنظمة والمعايير الدولية ومتطلبات الأعمال.

السياسات والتشريعات والأخلاقيات والالتزام بها Policy, Legal, Ethics and Compliance (PLE)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بتشريعات ومعايير ولوائح وإرشادات وسياسات وأخلاقيات الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أفضل الممارسات لأخلاقيات العمل في مجال الأمن السيبراني للمنظمات والأفراد ٢. القضايا المتعلقة بأخلاقيات وممارسات استخدام منصات التواصل الاجتماعي ٣. التشريعات الوطنية والدولية لمكافحة الجرائم السيبرانية ٤. السلطات القضائية والاتفاقات والمعاهدات والمنظمات الدولية ذات العلاقة بالأمن السيبراني ٥. معايير وضوابط الأمن السيبراني الوطنية والدولية (مثلاً: الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني، ISO 27001, PCI DSS) ٦. تشريعات ولوائح الخصوصية وحماية البيانات ٧. تشريعات ولوائح حماية الملكية الفكرية ٨. الإرشادات وأفضل الممارسات في التوجهات الحديثة مثلاً: سياسة استخدام الأجهزة الشخصية في العمل (BYOD)، إرشادات الأمن السيبراني لإنترنت الأشياء ٩. أفضل الممارسات للمواءمة مع تشريعات وضوابط ومعايير الأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مناقشة القضايا المتعلقة بأخلاقيات وممارسات استخدام التقنية والأمن السيبراني. ٢. مناقشة التشريعات واللوائح والإرشادات والسياسات الرئيسية في مجال الأمن السيبراني. ٣. تحديد المسائل التشريعية والأخلاقية المهمة عند التعامل مع البيانات. ٤. شرح الممارسات الصحيحة للموائمة مع تشريعات وضوابط ومعايير الأمن السيبراني. ٥. شرح التحديات والمعضلات التي يواجهها مختص الأمن السيبراني في الجوانب القانونية والأخلاقية.

إدارة البرامج الأمنية Security Program Management (SPM)

الوصف	تقدم هذه الوحدة المعرفية المعارف الضرورية لتنفيذ وتشغيل وإدارة برامج الأمن السيبراني لحماية المنظمات والدفاع عنها في الفضاء السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أهداف وغايات برامج الأمن السيبراني ٢. الأدوار والمسؤوليات ٣. وضع خط الأساس للأمن السيبراني ٤. مراقبة وضبط برامج الأمن السيبراني ٥. التوعية والتدريب والتعليم في مجال الأمن السيبراني ٦. قياس الفاعلية ٧. مؤشرات وقياس أداء الأمن السيبراني وإعداد التقارير ٨. الأتمتة ٩. يشمل برنامج الأمن السيبراني: الأمن المادي، أمن الموظفين، التعرف على الأنظمة والبيانات، خطط أمن الأنظمة، إدارة الإعدادات والتحديثات والإصلاحات، توثيق الأنظمة، إدارة برامج الاستجابة للحوادث السيبرانية، إدارة برامج التعافي من الكوارث، التصديق والاعتماد، استمرارية الأعمال وإدارة الأزمات ١٠. التعليم والتدريب والتوعية في مجال الأمن السيبراني ١١. خطة حماية الملكية الفكرية ١٢. متطلبات ضوابط الوصول وإدارة تنفيذها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم وتحضير وإدارة برنامج الأمن السيبراني مع وضع الأهداف والغايات والمقاييس لمنظمة معينة. ٢. قياس الفاعلية لبرنامج معين في الأمن السيبراني. ٣. تصميم وتحضير خطط طوارئ تتضمن استمرارية الأعمال، والتعافي من الكوارث والاستجابة للحوادث السيبرانية. ٤. تصميم خطة إدارة التحديثات والإصلاحات والتغيير، وخطة حماية الملكية الفكرية، وخطة تنفيذ ضوابط الوصول.

تحليل المخاطر السيبرانية Security Risk Analysis (SRA)

الوصف	تتضمن هذه الوحدة المعرفية المعارف والمهارات الخاصة بالنماذج والمنهجيات والعمليات لتقييم المخاطر السيبرانية وإدارتها والتعامل معها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مبادئ ومفاهيم تقييم وتحليل وإدارة مخاطر الأمن السيبراني ٢. دورة وخطوات إدارة المخاطر ٣. نماذج المخاطر السيبرانية ٤. منهجيات قياس وتقييم المخاطر السيبرانية ٥. ضوابط الأمن السيبراني ٦. اقتصاديات تخفيف وتقليل المخاطر السيبرانية ٧. نقل وقبول وإنهاء والتعامل مع المخاطر السيبرانية ٨. التواصل والتوثيق وتسجيل المخاطر السيبرانية ٩. معايير وأطر إدارة المخاطر السيبرانية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. ربط المخاطر بسياسات الأمن السيبراني. ٢. شرح المنهجيات الرئيسية لإدارة المخاطر السيبرانية. ٣. تقييم وتصنيف المخاطر السيبرانية بالنسبة للتقنيات والأفراد والكيانات. ٤. اختيار المنهجية المناسبة للتعامل مع المخاطر السيبرانية مع الأخذ بعين الاعتبار المزايا والعيوب. ٥. تطبيق المعايير والأطر والمتطلبات القانونية والتنظيمية والسياسات المؤسسية عند إجراء تقييم المخاطر.

الخوارزميات المتقدمة Advanced Algorithms (AAL)

الوصف	تركز هذه الوحدة المعرفية على القدرة على اختيار وتطبيق الخوارزميات المتقدمة لحل مشكلات محددة، وتحليل فعالية هذه الخوارزميات في سياقها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. فلاتر بلوم ٢. مصنفات بايز ٣. التطبيق والتبسيط (Map-Reduce) ٤. خوارزميات البرمجة الخطية ٥. خوارزميات البرمجة الديناميكية ٦. سلسلة ماركوف مونتي كارلو ٧. الترميز وضغط البيانات ٨. خوارزميات الرسوم البيانية ٩. المطابقة المستقرة ١٠. صعوبة المسائل ومجموعة NP ١١. الخوارزميات التقريبية ١٢. الخوارزميات العشوائية ١٣. خوارزميات الذكاء الاصطناعي
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم خوارزميات متقدمة لحل مسائل حقيقية بكفاءة وجودة عالية. ٢. تطبيق الخوارزميات المتقدمة لحل المشكلات ذات الصلة بطريقة فعالة وكفؤة. ٣. تحليل الخوارزميات المتقدمة وتقييم مدى تعقيدها.

ضبط الوصول Access Control (ACC)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول أساليب ضبط الوصول إلى البيانات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الأمن المادي للبيانات: أمن مركز البيانات، الوصول بمفتاح، بطاقات المفاتيح، كاميرات المراقبة، الأمن على مستوى كبائن الخوادم، إتلاف البيانات ٢. ضبط الوصول الإلكتروني للبيانات: قوائم ضبط الوصول، سياسات المجموعات، كلمات المرور، ضبط الوصول الاحترازي، ضبط الوصول الإجباري، ضبط الوصول بناء على الدور الوظيفي، ضبط الوصول بناء على الخصائص، ضبط الوصول بناء على القواعد، ضبط الوصول بناء على السجلات التاريخية، ضبط الوصول بناء على الهوية، ضبط الوصول بناء على المنظمة، الهويات المتحدة وضبط الوصول ٣. تصميم البنية الآمنة: مبادئ بنية الأمن وحماية المعلومات في أنظمة الحاسب ٤. طرق منع تسرب البيانات: التحكم بالحدود والقنوات والوجهات المصرح بها، ومنهجيات مشاركة البيانات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مناقشة الضوابط الرئيسية للأمن المادي لضمان سلامة البيانات. ٢. شرح مفاهيم ضبط الوصول الإلكتروني. ٣. التمييز بين أنواع الهويات المختلفة مثل الهويات الموحدة. ٤. تحليل نماذج ضبط الوصول مثل: المعتمد على الأدوار، والمعتمد على القواعد، والمعتمد على الخصائص.

التشفير المتقدم Advanced Cryptography (ACR)

الوصف	تقدم هذه الوحدة المعرفية معارف متقدمة حول خوارزميات التشفير الحديثة والناشئة، والبروتوكولات، ومنهجيات التنفيذ الآمن.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التشفير المتماثل الحديث: التشفير الموثق (AEAD)، التشفير خفيف الوزن، تراكيب الإسفنج والتراكيب المزدوجة ٢. التشفير ما بعد الحوسبة الكمية ٣. منهجيات تقييم وحدات التشفير ما بعد الكمي ٤. تحليل التشفير ما بعد الكمي ٥. نماذج الهجمات الكمية وتأثيرات خوارزميات Grover و Shor ٦. الانتقال إلى التشفير ما بعد الكمي والتنفيذ الهجين ٧. التشفير الكمي ٨. توزيع المفاتيح الكمية ٩. بروتوكولات توزيع المفاتيح الكمية (مثلاً: BB84، E91، BBM92، B92، KMB09، AWEM.QKD) ١٠. قيود التنفيذ والتنفيذ الهجين ١١. التشفير المعتمد على الاقتران ١٢. التشفير المعتمد على الهوية والتشفير المعتمد على الخصائص ١٣. التشفير الوظيفي ١٤. الأمان الأمامي والتشفير متغير المفاتيح ١٥. التشفير الحدّي وتوليد المفاتيح الموزع ١٦. التشفير باستخدام براهين المعرفة الصفرية ١٧. تشفير الحساب الآمن متعدد الأطراف ١٨. التشفير المتماثل/الهومومورفي (جزئياً وكلياً) ١٩. المراسلة الآمنة (مثلاً Double Ratchet) ٢٠. أنظمة الاعتماد المجهولة وبروتوكولات التصويت ٢١. سلاسل الكتل والسجلات في التشفير: مجمّعات التشفير، أشجار ميركل، الالتزامات المتجهية، تشفير الإجماع، والتشفير للشبكات اللامركزية ٢٢. نماذج هجمات التشفير ٢٣. تحليل القنوات الجانبية المتقدم ووسائل الحماية ٢٤. هجمات الأعطال ووسائل الحماية ٢٥. التحقق المنهجي لتنفيذ التشفير ٢٦. التنفيذ الآمن على مستوى العتاد ٢٧. إدارة المفاتيح في الأنظمة المتقدمة ٢٨. حوكمة التشفير والمعايير والتقييم ٢٩. متطلبات وحدات التشفير FIPS 140.3 واختبارات الاعتماد (ISO/IEC 19790، ISO/IEC 24759) ٣٠. متطلبات المعايير المشتركة (ISO/IEC 15408) ٣١. برامج وأنظمة التحقق من التشفير (CMVP، CAVP، ACVTS، ACMVP، ACVT)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحليل تراكيب التشفير المتماثل الحديثة. ٢. تقييم وتطبيق التشفير ما بعد الكمي والتنفيذ الهجين للتعامل مع نماذج الهجمات الكمية. ٣. تصميم أنظمة باستخدام التشفير المتماثل/الهومومورفي والتشفير متعدد الأطراف الآمن لمعالجة البيانات الحساسة دون فك تشفيرها. ٤. تطبيق براهين المعرفة الصفرية والتشفير الحدّي لإنشاء أنظمة اعتماد مجهولة وبيئات ثقة موزعة. ٥. تقييم آليات التشفير المستخدمة في الأنظمة اللامركزية. ٦. تقييم حوكمة التشفير وأطر التحقق والاعتماد.

الخوارزميات Algorithms (ALG)

الوصف	تركز هذه الوحدة المعرفية على القدرة على اختيار وتطبيق الخوارزميات لحل مشكلات محددة، وتحليل فعالية هذه الخوارزميات في سياقها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تحليل الخوارزميات ٢. التعقيد الحوسبي ٣. أفضل وأسوأ ومتوسط الحالات ٤. التحسين ٥. خوارزميات البحث والترتيب ٦. خوارزميات مطابقة السلاسل النصية ٧. الخوارزميات التكرارية ٨. الاستدعاء الذاتي ٩. الخوارزميات المعتمدة على الطمع ١٠. خوارزمية تسلق التل
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحليل الخوارزميات وتقييم فعاليتها. ٢. تصميم الخوارزميات لحل المشكلات بطريقة صحيحة وفعالة.

تقنية وبروتوكولات الشبكات المتقدمة
Advanced Network Technology and Protocols (ANT)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول مفاهيم بناء الشبكات المتقدمة والمسائل المعقدة في أمن الشبكات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. خوارزميات وبروتوكولات التوجيه المتقدمة: BGP، OSPF، MPLS، التوجيه الاستاتيكي "الثابت" والديناميكي، بروتوكولات متجهات المسافة (Distance vector) وبروتوكولات حالة الوصلة (Link state) ٢. تبديل الإيثرنت: بروتوكول الشجرة الممتدة، الشبكات المحلية الافتراضية VLANs، الوصلات Trunks، تجميع الروابط، التغذية عبر الإيثرنت POE، انعكاس المنافذ ٣. الشبكات اللاسلكية (مثل: هيكلية WLAN، الهوائيات، الترددات، القنوات، المعايير، المسائل ذات العلاقة بالأمن السيبراني) ٤. الوصول عن بُعد: الشبكات الخاصة الافتراضية VPN، الربط موقع إلى موقع مقابل عميل إلى موقع، المعايير والبروتوكولات، وبروتوكول سطح المكتب البعيد RDP ٥. مبادئ وبروتوكولات وآثار الشبكات المعرفة بالبرمجيات SDN ٦. حزمة شبكات IPv6 بما في ذلك مسائل الأمن السيبراني لشبكات IPv6 ٧. جودة الخدمة ٨. خدمات الشبكات ٩. تنفيذ الشبكات الاجتماعية ومسائل الأمن السيبراني المتعلقة بها ١٠. الهواتف الشبكية ١١. الإرسال متعدد الوجهات ١٢. موضوعات متقدمة في أمن الشبكات: تأمين أنظمة أسماء النطاقات DNS، ترجمة عناوين الشبكة NAT، الفحص العميق لحزم البيانات، وأمن طبقة النقل ١٣. استكشاف الأخطاء وإصلاحها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح عمل بروتوكولات الشبكات المتقدمة الشائعة. ٢. تحليل أمن بروتوكولات الشبكات المتقدمة. ٣. تشغيل أدوات الشبكة لفحص أداء بروتوكولات الشبكات المتقدمة.

الاتصالات التناظرية Analog Telecommunications (ATC)

الوصف	تقدم هذه الوحدة المعرفية مقدمة عامة حول أنظمة الاتصالات التناظرية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مكونات أنظمة الاتصالات التناظرية. ٢. منهجيات إرسال الإشارات ٣. بنى الاتصالات التناظرية ٤. القنوات والمبدلات ٥. درجة الخدمة ٦. الحجب ٧. نماذج وصول المكالمات ٨. مسائل التداخل
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المكونات والبنية الرئيسية لأنظمة الاتصالات التناظرية. ٢. التمييز بين أنواع التضمين من حيث المميزات والتطبيقات.

الأدوات التحليلية Analytical Tools (ATT)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة للتعرف على الهجمات السيبرانية ومراقبتها وحجبها وتحويلها والاستجابة لها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مقاييس الأداء ٢. تحليل البيانات ٣. المعلومات الاستباقية للتهديدات السيبرانية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم وتنفيذ وإدارة استخدام المقاييس لتحديد الفاعلية للبرنامج الأمني بشكل كامل. ٢. استخدام الطرق والتقنيات لتحديد وتقييم المنفعة من مقاييس الأداء. ٣. استخدام التقنيات للتعامل مع كميات كبيرة من البيانات للتعرف على الهجمات السيبرانية وحجبها وتحويلها والاستجابة لها. ٤. جمع وتحليل ونشر المعلومات الاستباقية للتهديدات السيبرانية التي تشمل معلومات التهديدات وقدرات المهاجمين.

الوعي والفهم Awareness and Understanding (AUU)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المخاطر السيبرانية والممارسات السيبرانية الصحية وتثقيف المستخدمين والتوعية بالثغرات الأمنية والتهديدات السيبرانية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. إدراك المخاطر السيبرانية والتواصل بشأنها ٢. الممارسات السيبرانية الصحية ٣. تثقيف المستخدمين في الأمن السيبراني ٤. التوعية بالثغرات الأمنية والتهديدات السيبرانية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح الممارسات السيبرانية الصحية وتثقيف المستخدمين في الأمن السيبراني والتوعية بالثغرات الأمنية والتهديدات السيبرانية. ٢. عرض برامج التثقيف والتدريب والتوعية في الأمن السيبراني. ٣. شرح المخاطر السيبرانية وإدراكها والتواصل بشأنها في مجال الأمن السيبراني.

استمرارية الأعمال، والتعافي من الكوارث، وإدارة الحوادث السيبرانية
Business Continuity, Disaster Recovery and Incident Management (BDR)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول استمرارية الأعمال والتعافي من الكوارث وطرق إدارة الحوادث السيبرانية التي تدعم صمود المنظمات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مقدمة في استمرارية الأعمال والتعافي من الكوارث: التعريف والأهمية، المفاهيم الأساسية، الفرق بين استمرارية الأعمال والتعافي من الكوارث ٢. تقييم المخاطر وتحليل أثر الأعمال (BIA): تحديد المخاطر المحتملة، تقييم أثرها على الأعمال، تحديد أولويات الوظائف الحرجة ٣. التخطيط لاستمرارية الأعمال: إعداد خطة استمرارية الأعمال، استراتيجيات الحفاظ على استمرارية العمليات، خطط الاتصال وأدوار أصحاب المصلحة ٤. التخطيط للتعافي من الكوارث: إعداد خطة التعافي من الكوارث، استعادة الأنظمة والبيانات، زمن الاستعادة المستهدف (RTO) ونقطة الاستعادة المستهدفة (RPO)، خطط الاتصال وأدوار أصحاب المصلحة ٥. التنفيذ والاختبار: تنفيذ الخطط، الاختبارات الدورية والتمارين السيبرانية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح معنى الصمود، وتحديد البيئات التي تظهر فيها أهميته. ٢. مناقشة أساسيات خطط استمرارية الأعمال وخطط التعافي من الكوارث والفرق بينهما. ٣. تحليل المخاطر والثغرات المحتملة في خطط استمرارية الأعمال والتعافي من الكوارث الحالية، واقتراح تحسينات لتعزيز فعاليتها. ٤. إعداد خطط واقعية أو مبنية على حالة معينة للتعافي من الكوارث واستمرارية الأعمال. ٥. تقييم فعالية خطط استمرارية الأعمال والتعافي من الكوارث من خلال الاختبارات وتمارين المحاكاة، وتقديم توصيات للتحسين.

الحوسبة السحابية Cloud Computing (CCO)

الوصف	تقدم هذه الوحدة المعرفية مقدمة عامة حول تقنيات الحوسبة السحابية وخدامتها ونماذجها وأمنها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منصات البيئات الافتراضية ٢. الخدمات السحابية: SaaS، PaaS، DaaS، IaaS، FaaS ٣. القابلية للتوسع ٤. مشغلات الأجهزة الافتراضية (Hypervisors) وتنفيذ الحوسبة السحابية ٥. البنى الموجهة نحو الخدمة ٦. اتفاقيات مستوى الخدمة (SLAs) ٧. نماذج تنصيب الخدمة: خاص، عام، مجتمعي، هجين ٨. أمن الحوسبة السحابية ٩. أدوات وخدمات أمن السحابة الشائعة ١٠. أفضل الممارسات في الأمن السيبراني للحوسبة السحابية ١١. التخزين ١٢. إدارة الهوية والوصول (IAM) في الأنظمة السحابية ١٣. الصمود والتعافي من الكوارث ١٤. التحليل الجنائي الرقمي والاستجابة للحوادث في البيئات السحابية ١٥. المسائل التشريعية ومتطلبات الامتثال
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح خدمات الحوسبة السحابية. ٢. مناقشة مزايا وعيوب البيئات الافتراضية. ٣. تنصيب تطبيقات سحابية. ٤. تخصيص موارد للمستخدمين والتطبيقات بكفاءة. ٥. مناقشة أهمية إدارة الموارد في الحوسبة السحابية. ٦. شرح المتطلبات للبيئات السحابية الآمنة.

التشفير Cryptography (CRY)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات المتعلقة بخوارزميات وبروتوكولات التشفير القياسية، مع التركيز على التصميم الوظيفي وخصائص الأمان وتحليل التشفير المتماثل وغير المتماثل، ودوال الاختزال، والتواقيع الرقمية، باعتبارها الأساس التقني لحماية المعلومات والاتصالات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التشفير الانسيابي: مبادئ التصميم، المعتمد على الجداول مثل RC4، والمعتمد على سجلات الإزاحة ذات التغذية الراجعة الخطية LFSR مثل Salsa، ChaCha، Trivium، Grain، ZUC وSnow ٢. التشفير الكتلي: شفرة Feistel، AES، Camellia، Serpent، وبنية الخوارزميات ٣. المعايير وأنماط التشغيل الحديثة ٤. رموز توثيق الرسائل (HMAC، CMAC، KMAC) ٥. التشفير الموثق (GCM وCCM) ٦. تحليل التشفير المتماثل :الهجمات المعروفة على التشفير الكتلي والانسيابي ٧. RSA: التشفير، DSA، وافتراضات الأمان ٨. تبادل المفاتيح Diffie.Hellman ٩. تشفير ElGamal وخوارزمية DSA ١٠. التشفير بالمنحنيات الإهليلجية (ECDH، ECDSA) ١١. مخططات التواقيع الرقمية ١٢. مقدمة في التشفير الكمي (PQC، QKD، QRNG) ١٣. تحليل التشفير غير المتماثل ١٤. دوال الاختزال SHA.2 وSHA.3 (Keccak) ١٥. توثيق الرسائل باستخدام دوال الاختزال ١٦. أشجار ميركل ومخططات الالتزام ١٧. تحليل دوال الاختزال ١٨. الشهادات وسلطات إصدار الشهادات: الجذرية، الوسيطة، الفرعية، وشهادات المستخدم ١٩. بنية شهادات X.509 ٢٠. التحقق من الشهادات وبروتوكولات الإلغاء ٢١. التشفير باستخدام مفاتيح عامة بدون شهادات رقمية ٢٢. نماذج الثقة: الهرمية، شبكة الثقة ٢٣. وحدات الأمان العتادية (HSM)، وحدات المنصة الموثوقة (TPM)، والبطاقات الذكية ٢٤. إنشاء المفاتيح: مولدات الأرقام العشوائية (PRNG، TRNG، QRNG)، ومولدات الأرقام العشوائية الهجينة، والاختبارات الإحصائية لمولدات الأعداد العشوائية ٢٥. دوال حماية المفاتيح ٢٦. دوال اشتقاق المفاتيح ٢٧. هجمات القنوات الجانبية: التوقيت، تحليل استهلاك الطاقة، حقن الأعطال ٢٨. الثغرات الواقعية ومشكلات التنفيذ مثل Padding Oracle
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحليل آلية عمل التشفير الكتلي والانسيابي لتحديد التنفيذ الأكثر أمانًا في سيناريو معين. ٢. تطبيق تقنيات تشفير المفتاح العام لتحقيق تبادل مفاتيح آمن والتواقيع الرقمية. ٣. تقييم خصائص الأمان لدوال الاختزال لضمان موثوقية البيانات والتحقق من سلامة الرسائل. ٤. تصميم وتقييم عمليات توليد المفاتيح وإدارتها بشكل آمن. ٥. تطبيق تقنيات تحليل التشفير لكسر البيانات المشفرة.

هندسة التشفير Cryptography Engineering (CRE)

الوصف	تقدم هذه الوحدة المعرفية مقدمة في مبادئ وممارسات هندسة التشفير، مع التركيز على التصميم الآمن، والتنفيذ، والتقييم، وحوكمة أنظمة التشفير.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مبادئ هندسة التشفير: التنفيذ الآمن للتشفير، التصميم الآمن للتشفير، التخزين الآمن للمفاتيح والمصادقة، الإقلاع الآمن، والتصميم المقاوم لهجمات القنوات الجانبية ٢. حوكمة التشفير والمعايير والجوانب التنظيمية: الوثائق التنظيمية من الهيئة الوطنية للأمن السيبراني (مثل: NCS، ECC، CSCC، DCC، CCC)، سلسلة معايير NIST SP 800، الامتثال لأنظمة التشفير الوطنية، متطلبات إيداع المفاتيح، التشفير وحقوق الملكية الرقمية، الاستخدام الأخلاقي لأدوات التشفير ٣. بروتوكولات التشفير: بروتوكولات تبادل المفاتيح والمصادقة الآمنة، المراسلة الآمنة، بروتوكولات التصويت والآليات متعددة الأطراف الآمنة، بروتوكولات براهين المعرفة الصفرية ٤. التشفير التطبيقي: تشفير الأقراص، تشفير الشبكات، البريد الإلكتروني الآمن، التشفير من طرف إلى طرف، أمن كلمات المرور وأنظمة المصادقة ٥. هندسة التشفير وأمن التنفيذ: هجمات الأعطال ووسائل الحماية، التحقق المنهجي من تنفيذ التشفير، العتاد الآمن، البرمجة بزمن ثابت والبرمجة المقاومة للتسرب، إدارة المفاتيح في الأنظمة المتقدمة، تنفيذ التشفير على مستوى العتاد (FPGA، ARM، RISC.V، ASIC) ٦. تقييم التشفير وتقويمه والتحقق من صحة التنفيذ: اختبارKAT ، التقييم التدخّلي وغير التدخّلي، التحقق من بنية Red-Black، تقييم الانبعاثات.
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم ودمج وحدات التشفير داخل الأنظمة. ٢. مواءمة تنفيذ التشفير مع المعايير والسياسات الوطنية والدولية. ٣. تحليل أمان وكفاءة بروتوكول تشفير معين. ٤. تطبيق بروتوكولات التشفير لتأمين أنظمة البرمجيات والعتاد.

الجريمة السيبرانية Cyber Crime (CCR)

الوصف	تقدم هذه الوحدة المعرفية مقدمة عامة عن الجرائم السيبرانية والانتهاكات في الفضاء السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أنواع الجرائم السيبرانية: الهندسة الاجتماعية، الاختراق، التسلل، البرمجيات الضارة، التجسس، انتهاك الملكية الفكرية، الاحتيال، الابتزاز، تعطيل الخدمات، تسريب البيانات أو إتلافها أو تعديلها ٢. المطاردة والتصيّد في الفضاء السيبراني ٣. التنمر السيبراني ٤. انتحال الهوية ٥. ارتكاب الجرائم من خلال الفضاء السيبراني ٦. الإرهاب السيبراني ٧. تشريعات مكافحة الجرائم السيبرانية: التشريعات الوطنية، التشريعات الدولية، الاتفاقيات الدولية ٨. القواعد الأخلاقية والمعايير المجتمعية: حقوق الآخرين، الاحترام ومبادئ المجتمع، استخدام الموارد وتخصيصها وإساءة استخدامها، الأمن السيبراني والمسؤولية الاجتماعية ٩. الأساليب الشائعة المستخدمة في الجرائم السيبرانية ١٠. أثر الجرائم السيبرانية (مثل: الخسائر المالية، الضرر بالسمعة، العواقب القانونية، تعطيل العمليات)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح الجرائم السيبرانية المحتملة والمطاردة السيبرانية والتنمر السيبراني وغيرها من السلوكيات المسيئة في الفضاء السيبراني. ٢. استخدام تطبيقات الأمن السيبراني للدفاع ضد الجرائم والانتهاكات. ٣. تحليل دراسات حالة لأساليب الجرائم السيبرانية عبر الإنترنت ووسائل الحماية المحتملة.

أخلاقيات الأمن السيبراني Cybersecurity Ethics (CSE)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بالمسائل الأخلاقية في مجال الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المحافظة على الخصوصية وسرية المعلومات عند تأدية أعمال الأمن السيبراني ٢. حماية حقوق المستخدمين عند تأدية أعمال الأمن السيبراني ٣. المواثيق والأطر ذات العلاقة بأخلاقيات الأمن السيبراني ٤. الجوانب الأخلاقية في حماية الأنظمة والشبكات الحساسة ذات الأثر والأهمية على المجتمع والأفراد ٥. التوازن بين حماية الأنظمة والشبكات وتمكين الاستفادة منها ٦. المسؤولية الوطنية والاجتماعية في أعمال الأمن السيبراني ٧. الأسس الأخلاقية في الأمن السيبراني ٨. المعضلات الأخلاقية الشائعة في الأمن السيبراني ٩. أدوات اتخاذ القرار الأخلاقي ١٠. دور الأمن السيبراني في تعزيز القيم الأخلاقية ١١. أثر ممارسات الأمن السيبراني على المجتمع
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المواضيع الأساسية في أخلاقيات الأمن السيبراني. ٢. ممارسة أعمال الأمن السيبراني مع الالتزام بالجوانب الأخلاقية المتعلقة به.

الأنظمة السيبرانية الفيزيائية Cyber-Physical System (CPS)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بالمفاهيم والمبادئ والممارسات المتبعة في تصميم وتطوير ونشر الأنظمة السيبرانية الفيزيائية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. البنية والتصميم: تصميم الأنظمة، النمذجة، والمحاكاة ٢. الأمن السيبراني للأنظمة السيبرانية الفيزيائية بما في ذلك التهديدات والثغرات وتقييم المخاطر واستراتيجيات التخفيف منها ٣. الأنظمة اللحظية: الجدولة، التزامن، وتحليل التوقيت ٤. الأنظمة الشبكية: بروتوكولات الاتصال، بنية الشبكات، والأنظمة الموزعة ٥. الأنظمة المدمجة: المتحكمات الدقيقة، البرمجيات المدمجة، وتكامل العتاد والبرمجيات ٦. أنظمة الحساسات والمشغلات: دمج الحساسات، التحكم في المشغلات، وآليات التغذية الراجعة ٧. أنظمة التحكم: نظرية التحكم، تحليل الاستقرار، وطرق التحسين ٨. واجهة التفاعل بين الإنسان والآلة (HMI): تصميم واجهات المستخدم، العوامل البشرية، وسهولة الاستخدام ٩. السلامة والموثوقية: تحليل المخاطر، تحمل الأعطال، وموثوقية الأنظمة ١٠. المعايير واللوائح: المعايير الصناعية، المتطلبات التنظيمية، والامتثال ١١. أنظمة إدارة معلومات الأمن الفيزيائي (PSIM) ١٢. أمن الطائرات بدون طيار (UAV/الدرون): أمن المنصات، الاتصالات، الأدلة الرقمية، وسلسلة التوريد في التصميم والبناء
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف تكامل العمليات الحاسوبية والفيزيائية، بما في ذلك دور الحساسات والمشغلات وأنظمة التحكم في الأنظمة السيبرانية الفيزيائية. ٢. تطبيق استراتيجيات لضمان السلامة والأمن والموثوقية في الأنظمة السيبرانية الفيزيائية، خاصة في التطبيقات الحرجة مثل الرعاية الصحية والنقل والأتمتة الصناعية. ٣. تحليل وتقييم تطبيقات الأنظمة السيبرانية الفيزيائية في مجالات مختلفة مثل الشبكات الذكية والمركبات ذاتية القيادة والمدن الذكية.

قواعد البيانات Databases (DAT)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة لإدارة أنظمة قواعد البيانات واستخدامها وحمايتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أنواع أنظمة إدارة قواعد البيانات: علاقاتية، هرمية، غير علاقاتية (NoSQL)، قائمة على الكائنات (Object.Based)، موجهة للكائنات (Object.Oriented)، موزعة ٢. نماذج أمن قواعد البيانات: الاستدلال، التجميع، الحقن، الاختزال، التشفير، تلف البيانات، الوصول غير المصّرح به، ضوابط الوصول إلى قواعد البيانات (DAC, MAC, RBAC, Clark.Wilson)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التمييز بين أنواع أنظمة إدارة قواعد البيانات المختلفة من حيث البنية والتطبيقات. ٢. توضيح الجوانب الأمنية المتعلقة بقواعد البيانات وأنظمة إدارة قواعد البيانات.

إدارة البيانات Data Administration (DBA)

الوصف	تقدم هذه الوحدة المعرفية معارف عامة عن دورة حياة البيانات وجودتها وأمنها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. دورة حياة البيانات: الحصول على البيانات وصونها وتحويلها واستخدامها وتوزيعها وأرشفتها وتنقيتها ٢. جودة البيانات: الدقة والاكتمال والصلة والاتساق والسلامة والتنقية والتحقق والتأكد من الصحة ٣. سهولة الوصول إلى البيانات ٤. منفعة البيانات ٥. تخزين وأرشفة البيانات: تخزين البيانات، الأرشفة طويلة الأمد والبيانات الضخمة ٦. أنظمة إدارة البيانات مثل (HBASE، MongoDB، Hadoop) ٧. ضوابط البيانات: الملكية، الإشراف، الإدارة، الحيازة، الحوكمة ٨. سياسات البيانات: السياسات الداخلية والخارجية ٩. أمن البيانات: ضبط الوصول وتصنيف البيانات والتشفير
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح مراحل دورة حياة البيانات ومناقشة مسائل الأمن السيبراني ذات العلاقة ٢. تحليل جودة البيانات وسهولة الوصول إليها ومنفعتها. ٣. إدارة إنشاء البيانات وتغييرها وتوزيعها وتخزينها وحذفها بطريقة آمنة. ٤. مناقشة وشرح ملكية البيانات والإشراف عليها وإدارتها وحيازتها وحوكمتها. ٥. توضيح أهمية تصنيف البيانات في الأمن السيبراني.

الاتصالات الرقمية Digital Communications (DCO)

الوصف	تقدم هـذه الوحدة المعرفية المعارف بأنظمة الاتـصـالات الرقمية والبروتوكولات ذات العلاقة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مكونات نظام الاتصالات الرقمية ٢. طرق الترميز ٣. إرسال الإشارات الرقمية والتضمين ٤. إشارات الانتشار الطيفي ٥. الوصول إلى قنوات الاتصال متعددة المستخدمين (مثل: CDMA، TDMA، FDMA، SDMA، PDMA)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف أنظمة الاتصالات الرقمية من حيث الأنظمة الفرعية وطرق التضمين المستخدمة. ٢. شرح مبادئ ومزايا إشارات الانتشار الطيفي فيما يتعلق بمقاومة التداخل والتشويش. ٣. التمييز بين طرق الوصول متعددة المستخدمين في الاتصالات.

التحليل الجنائي الرقمي Digital Forensics (DFS)

الوصف	تقدم هذه الوحدة المعرفية المعارف بطرق التحليل الجنائي الرقمي والمهارات؛ لتطبيقها في أعمال البحث والتحقيق بطريقة تراعي المتطلبات التشريعية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مصطلحات التحليل الجنائي الرقمي ٢. الامتثال للتشريعات: التشريعات المعمول بها، الإقرارات، الشهادات، السوابق القضائية، وسلسلة حفظ الأدلة ٣. التحقيق الرقمي: الاكتشاف الإلكتروني، توثيق الأدلة، إجراءات سلسلة حفظ الأدلة، وتحليل السبب الجذري ٤. الحصول على الأدلة وحفظها: حظر الكتابة، إجراءات التصوير، التحليل الجنائي الرقمي الحي، تحليل الأدلة وتوثيقها باستخدام الاختزال ٥. تحليل الأدلة: تحليل السبب الجذري، البيانات الوصفية واسترجاع الملفات المحذوفة ٦. استخدام الأدوات والتقنيات في التحقيق الجنائي الرقمي ٧. تسجيل النتائج وتقديمها: الجدول الزمني للأحداث ونسبة الهجوم إلى مصدره
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. إجراء تحقيق جنائي رقمي متكامل عبر كامل دورة حياة التحقيق الرقمي. ٢. توضيح المسائل التشريعية والتنظيمية المتعلقة بالتحليل الجنائي الرقمي وفق الأنظمة واللوائح والتعليمات والقرارات المرعية في المملكة العربية السعودية.

سلامة البيانات وتوثيقها Data Integrity and Authentication (DIA)

الوصف	توفر هذه الوحدة المعرفية المعارف حول طرق سلامة البيانات وتوثيقها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. قوة التوثيق: التوثيق بعوامل متعددة، التوثيق باستخدام الأداة المشفرة، الأجهزة المشفرة، التوثيق بالقياسات الحيوية، كلمات المرور لمرة واحدة، والتوثيق القائم على المعرفة ٢. أساليب هجمات كلمات المرور: الهجوم بالقاموس، الهجوم بجميع الاحتمالات، الهجوم بجداول قوس المطر، التصيد الإلكتروني، الهندسة الاجتماعية، الهجوم باستخدام البرمجيات الضارة، التجسس، التحليل بدون اتصال، أدوات كسر كلمة المرور ٣. طرق تخزين كلمات المـرور: دوال الاختزال في التشفير، مقاومة التعارض، إضافة بيانات عشوائية، عداد التكرار، اشتقاق المفتاح القائم على كلمة المرور ٤. سلامة البيانات: رموز توثيق الرسائل (HMAC ،CBC.MAC)، التواقيع الرقمية، التشفير والتوثيق، وأشجار الاختزال
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المفاهيم الأساسية في التوثيق والتصريح وضبط الوصول وسلامة البيانات. ٢. توضيح نقاط القوة والضعف في طرق التوثيق. ٣. عرض الهجمات الشائعة على كلمات المرور.

التعلّم العميق Deep Learning (DLL)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات اللازمة لتطوير وتطبيق الشبكات العصبية الاصطناعية الحديثة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الشبكات العصبية الاصطناعية: التصنيف الثنائي، الانحدار اللوجستي، دالة تكلفة الانحدار اللوجستي، النزول المتدرج، المشتقات، حوسبة الرسومات، حوسبة المتجهات ٢. الشبكات العصبية الاصطناعية الضحلة: تمثيل الشبكات العصبية الاصطناعية، دوال التنشيط، دوال التنشيط غير الخطية، مشتقات دوال التنشيط، النزول المتدرج، الانتشار الأمامي، الانتشار العكسي وحوسبة الرسومات ٣. الشبكات العصبية الاصطناعية الالتفافية: الشبكات الكلاسيكية والشبكات العصبية المتكررة ودوال الخسارة والتحسين ٤. التعلّم العميق بدون إشراف ٥. التعلّم المعزز العميق ٦. التدريب العدائي وشبكات الأعداء التوليدية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح أساسيات التعلّم العميق وبنى الشبكات العميقة. ٢. استخدام شبكات التعلّم العميق لحل مشكلات مرتبطة بالأمن السيبراني. ٣. تطبيق أساليب التدريب العدائي لتعزيز أمن نماذج التعلّم العميق.

أنظمة إدارة قواعد البيانات Database Management Systems (DMS)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المفاهيم الأساسية لأنظمة إدارة قواعد البيانات بالإضافة إلى المهارات والقدرات اللازمة لاستخدام أنظمة إدارة قواعد البيانات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أنواع قواعد البيانات: المسطحة، العلاقاتية، الشبكية، الهرمية، القائمة على الكائنات (Object.Based)، الموجهة للكائنات (Object.Oriented)، المبنية على قيم المفاتيح، الموزعة ٢. التعامل مع البيانات من خلال لغة الاستعلام الهيكلية(SQL): SELECT, INSERT, DELETE, UPDATE ٣. تعريف البيانات في لغة SQL ٤. إدارة قواعد البيانات بلغة SQL: إنشاء وحذف المستخدمين والصلاحيات وضبط الوصول ٥. مفاهيم قواعد البيانات: الفهرسة والاستدلال والتجميع والتمثيل المتعدد ٦. أمن قواعد البينات وحمايتها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح المفاهيم الأساسية لقواعد البيانات. ٢. التمييز بين دور قاعدة البيانات، ونظام إدارة قواعد البيانات (DBMS)، وخادم قواعد البيانات ضمن نظام معقد يدعم عدة تطبيقات. ٣. تطبيق لغة SQL لإنشاء قواعد البيانات وإدارتها وتشغيلها. ٤. إدارة ضوابط الوصول ومستويات الصلاحيات في أنظمة إدارة قواعد البيانات. ٥. رسم الهياكل لتخزين البيانات في أنظمة إدارة قواعد البيانات. ٦. تصميم قواعد البيانات وتنفيذها لتطبيق معين.

بنية الأنظمة الموزعة Distributed Systems Architecture (DSA)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول الأنظمة الموزعة وكيفية الاتصال فيما بينها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المفاهيم العامة للأنظمة الموزعة ٢. أمثلة على الأنظمة الموزعة ٣. البروتوكولات والطبقات ٤. حوسبة الأداء العالي ٥. مشغلات الأجهزة الافتراضية (Hypervisors) وتنفيذ الحوسبة السحابية ٦. الثغرات الأمنية وأمثلة على استغلالها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف مكونات وواجهات معيار شبكي معين. ٢. شرح عملية في أحد نظم التشغيل وتقديم بنى متعددة لتشغيل العمليات وتمكين الاتصال فيما بينها. ٣. وصف الحوسبة عالية الأداء وحالات الاستخدام التي تميّزها عن الإنترنت الاعتيادية. ٤. فحص أسطح الهجمات لنماذج الحوسبة الموزعة المتعددة مع التأكيد على أن كل واجهة تقدم مجموعة من الثغرات الأمنية المحتملة.

تراكيب البيانات Data Structures (DST)

الوصف	تركز هذه الوحدة المعرفية على فهم أنواع البيانات المجردة والعمليات المرتبطة بها، وتطبيقها لحل المسائل البرمجية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. البيانات العددية ٢. السلاسل النصية ٣. المصفوفات والمتجهات ٤. القوائم: قائمة متصلة، قائمة مزدوجة الاتصال ٥. الأكوام ٦. الصفوف والأكداس ٧. الكائنات، الخرائط، جداول الاختزال، القواميس ٨. المجموعات ٩. المخزنات المؤقتة ١٠. الأشجار ١١. الرسومات ١٢. تراكيب البيانات الأصلية الخاصة بلغات البرمجة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تنفيذ أنواع البيانات المجردة الشائعة. ٢. استخدام أنواع بيانات مجردة معينة وعملياتها لتنفيذ حلول لمسائل معينة. ٣. التفريق بين مختلف تراكيب البيانات واستخداماتها ومميزاتها وعيوبها ٤. تصميم مواصفات لتراكيب بيانات مطلوبة بناء على احتياجات معينة ٥. توضيح مفهوم التجريد وتحديد حالات الإخلال بالتجريد لمواصفات تراكيب بيانات معينة.

التحليل الجنائي الرقمي في الأجهزة Forensics Device (DVF)

الوصف	تقدم هذه الوحدة المعرفية المهارات والقدرات لتطبيق تقنيات التحليل الجنائي الرقمي في فحص الأجهزة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الحصول على الأجهزة واستخراج الأدلة منها: أجهزة الهاتف الجوال، والأنظمة المدمجة (نظام تحديد المواقع العالمي GPS ولوحات تشغيل الألعاب وأجهزة التلفاز الذكية)، وأجهزة إنترنت الأشياء ٢. تحليل الأجهزة ٣. الاعتبارات التشريعية المرتبطة بالتحليل الجنائي الرقمي في الأجهزة ٤. أدوات التحليل الجنائي الرقمي في الأجهزة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح أساليب الحصول على البيانات واستخراجها من الأنظمة المدمجة وأجهزة الهاتف الجوال وأجهزة إنترنت الأشياء. ٢. إجراء تحليل على الأنظمة المدمجة وأجهزة الهاتف الجوال وأجهزة إنترنت الأشياء. ٣. مناقشة الجوانب التشريعية المرتبطة بعمليات التحليل الجنائي الرقمي على الأنظمة المدمجة وأجهزة الهاتف الجوال وأجهزة إنترنت الأشياء.

الأنظمة المدمجة Embedded Systems (ESY)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول الأنظمة المدمجة ومسائل الأمن السيبراني المتعلقة بها، بالإضافة للمهارات والقدرات اللازمة لتصميم مكونات الأنظمة المدمجة وبرمجتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مقدمة في الأنظمة المدمجة: التعريف والخصائص، الأمثلة والتطبيقات، الفروقات بين الأنظمة المدمجة والحاسبات ذات الأغراض العامة ٢. مكونات الأنظمة المدمجة (مثل: العتاد المادي والبرمجيات) ٣. تصميم الأنظمة المدمجة وتطويرها ٤. بنى المتحكمات الدقيقة/المعالجات المدمجة ٥. وحدات التحكم المنطقية القابلة للبرمجة (PLCs)، ومصفوفات البوابات، وغيرها من الأجهزة المنطقية القابلة للبرمجة الشائعة ٦. المدخلات والمخرجات، والتحويل من التماثلي إلى الرقمي، والسجلات، والحساسات، والمشغلات، ومكونات العتاد المادي المدمجة. ٧. الذاكرة (مثل: RAM، ROM، Flash) ٨. اتصالات أجهزة الأنظمة المدمجة ٩. معالجة المقاطعات ومسائل التوقيت ١٠. إدارة الموارد في الأنظمة اللحظية ١١. نظم التشغيل للأنظمة المدمجة: الأجهزة التي لا تحتوي على نظم تشغيل، ونظم التشغيل اللحظية (RTOS) ١٢. الأمن في الأنظمة المدمجة: المسائل الأمنية الناتجة عن محدودية الموارد ١٣. لغات البرمجة وبيئاتها للأنظمة المدمجة: سلاسل الأدوات، نظم التشغيل والأجهزة المستهدفة، والمترجمات العابرة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف المكونات الأساسية وبنية الأنظمة المدمجة، بما في ذلك المتحكمات الدقيقة، والحساسات، والمشغلات. ٢. شرح القيود والتحديات المرتبطة بتطوير التطبيقات للأجهزة المدمجة. ٣. تصميم وتطوير وبناء نماذج أولية لحلول الأنظمة المدمجة التي تعالج مشكلات واقعية محددة، مع التكامل الفعال بين مكونات العتاد والبرمجيات.

المحاسبة الجنائية الرقمية Forensic Accounting (FAC)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول تقنيات التحليل الجنائي الرقمي للبحث والتحري المالي، والمهارات والقدرات اللازمة لتطبيقها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المحاسبة الاستقصائية ٢. الإبلاغ عن عمليات الاحتيال المالي ٣. اختلاس الأصول ٤. الأساليب غير المباشرة لإعادة بناء الدخل ٥. غسيل الأموال ٦. التدفقات المالية الدولية ٧. خدمات التقاضي ٨. إدارة الأدلة ٩. الأضرار الاقتصادية وتقييم الأعمال
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف التلاعبات الشائعة في القوائم المالية وطرق اكتشافها ٢. تقدير الإيرادات والدخل المخفي. ٣. توضيح طرق غسيل الأموال وطرق اكتشافها ومنعها. ٤. تقييم خسائر عمليات الاحتيال والسرقات والأضرار الناجمة عنها.

الأساليب المنهجية Formal Methods (FMD)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المنطق الرياضي والمهارات اللازمة لتطبيقها في تصميم الأنظمة الآمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مفهوم الأساليب المنهجية ٢. المنطق الرياضي ٣. تطبيق الأساليب المنهجية في تصميم الأنظمة وهندسة البرمجيات ٤. حدود إمكانيات الأساليب المنهجية ٥. ضوابط الوصول الإلزامية Bell-LaPadula ٦. أدوات الاستنتاج المؤتمتة ٧. نمذجة الأنظمة ومواصفاتها ٨. البراهين ٩. فحص النماذج والبحث عنها ١٠. المقارنة مع الأدوات والتقنيات الأخرى لاكتشاف العيوب (مثل: الاختبار، والاختبار العشوائي Fuzzing) ١١. الأساليب المنهجية لنمذجة البرمجيات وتحليلها: أدوات التحقق من النماذج، وأدوات إيجاد النماذج
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق الأساليب المنهجية في حالات واقعية. ٢. وصف استخدام المنطق الرياضي في تصميم الأنظمة الآمنة. ٣. توضيح قيمة الأساليب المنهجية طرق التحليل بالمقارنة مع الاختبارات في التحقق والتأكد من صحة البرمجيات. ٤. تطبيق الأساليب المنهجية على تصاميم البرمجيات ٥. شرح مزايا وعيوب لغات المواصفات المنهجية.

الأُسس الرياضية للتشفير Mathematical Foundations of Cryptography (FCY)

الوصف	تقدم هذه الوحدة المعرفية الأسس النظرية والرياضية للتشفير الحديث.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. نظرية الأرقام ٢. الحقول المنتهية ٣. اللوغاريتمات المتقطعة ٤. تحليل الأعداد إلى عوامل ٥. الاحتمالات ٦. نظرية المعلومات ٧. مولدات مصادر الإنتروبيا الحقيقية ٨. مولدات الأرقام العشوائية (PRNG، TRNG، QRNG) ٩. مولدات الأرقام العشوائية الهجينة ١٠. التوليد المتقدم للأرقام العشوائية ١١. المنحنيات الإهليلجية ١٢. الشبكات في التشفير ١٣. الأمن التام والتعقيد الحوسبي ١٤. نماذج الخصوم وافتراضات التهديد ١٥. مبدأ كيركهوف (Kerckhoffs' principle) في التشفير ونظرية المعلومات لكلود شانون (Shannon Claude) ١٦. تعريفات الأمن المبنية على نظرية التعقيد ١٧. الأمن المبني على المحاكاة (IND.CPA، IND.CCA1، IND.CCA2 ...) ١٨. إطار القابلية العامة للتركيب ١٩. افتراضات الصعوبة (LWE، RSA، CDH، DDH...)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح افتراضات الصعوبة الرياضية الأساسية التي يقوم عليها التشفير الحديث. ٢. التمييز بين الأمن التام والأمن الحوسبي. ٣. توضيح المتطلبات الرياضية اللازمة لتوليد أرقام عشوائية ذات قوة تشفيرية. ٤. التمييز بين افتراضات الصعوبة في التشفير، بما في ذلك الافتراضات المعتمدة على نظرية الأعداد، ونظرية الزمر، والشبكات.

إدارة منع الاحتيال والحد منه Fraud Prevention and Management (FPM)

الوصف	تقدم هذه الوحدة المعرفية المعارف والقدرات لتصميم الخطط والعمليات لمنع الاحتيال والتخفيف من أضراره.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مقدمة عن الاحتيال والمصطلحات المتعلقة به ٢. التدقيق ومنع الاحتيال: المنهج العلمي وقانون بينفورد ٣. التعامل مع البيانات: جمع البيانات وتنظيفها والتحقق منها وتطبيعها ٤. فهم البيانات: التحليل والرسم البياني والترتيب والفهرسة والتلخيص والتنظيم ٥. الاختبارات الرقمية للاحتيال: القيم المستخدمة بشكل متكرر، المقادير المتساوية، التقريب، تحليل النسبة/التباين، اختبار القيم المتطرفة، الاختبارات الإحصائية، اختبارات العشوائية ٦. نمذجة الاحتيال: طرق تعلم الآلة للكشف عن الاحتيال ٧. الكشف المتقدم للاحتيال ومنعه
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تقييم تكلفة وفاعلية منهجيات كشف الاحتيال ومنعه. ٢. شرح المسائل التشريعية والأخلاقية المتعلقة بالكشف عن الاحتيال ومنعه. ٣. تطبيق أدوات وطرق الكشف عن الاحتيال ومنعه.

بنية الأجهزة والعتاد Hardware Architecture (HAA)

الوصف	تتضمن هذه الوحدة المعرفية مقدمة عن مزايا معايير بنى الأجهزة والعتاد (Hardware) والثغرات الأمنية المحتملة فيها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. البنى المعيارية ٢. معايير واجهة الأجهزة والعتاد (مثل: ISA، PCI) ٣. البنى الشائعة (مثل: شرائح المعالج، اللوحة الأم للحاسب الشخصي، ومعايير الإيثرنت)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح فكرة البنى المعيارية ومزايا المعايير الموحدة. ٢. وصف المعايير المختلفة لواجهات الأجهزة والعتاد الخاصة بموصلات الشبكة.

أمن الأجهزة والعتاد والبرمجيات الثابتة Hardware/Firmware Security (HFS)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتصلة بمكونات الأجهزة والعتاد والبرمجيات الثابتة ومسائل الأمن السيبراني المتعلقة بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الثغرات المادية: قنوات اتصال غير مستخدمة وغير آمنة، منصات الاختبار، مسارات الاختبار، الأبواب الخلفية، أحصنة طروادة، الدارات الخفية، إضافة الشوائب إلى أشباه الموصلات، الأعطال المستحثة، الهندسة العكسية، الوصول غير المصرح به إلى الذاكرة ٢. هجمات القنوات الجانبية على الأجهزة والعتاد: التوقيت، تحليل الطاقة، الكهرومغناطيسية، تحليل الترددات اللاسلكية، إضافة عتاد، القنوات خارج النطاق ٣. هجمات المصدر: الأجزاء المزيفة والمقلدة والمقرصنة وتعطيل سلاسل التوريد ٤. هجمات تدمير الأجهزة ٥. مكونات أمن الأجهزة: هويات الأجهزة القابلة للتحقق، مولدات الأرقام العشوائية، التواقيع الرقمية لتشغيل ذاكرة القراءة فقط، وحدات التشفير المبنية على العتاد، أجهزة التحكم الأمنية/المعالجات المساعدة ومسرعات التشفير، وحدة المنصة الموثوقة (TPM)، التشغيل الآمن في UEFI ٦. سمات الأمن المادي: التأكد من صحة الجهاز، الخوارزميات الأمنية المقبولة/المفتوحة، توليد الأرقام العشوائية القوية، مصدر التوقيت الآمن، واجهة المطور المعيارية، التوثيق الواضح، النسخ الاحتياطية للمفاتيح وحمايتها، المقاومة ضد التلاعب، قابلية التوسع ٧. ثغرات محمّل التشغيل: هجمات قطاع التشغيل، وضع المستخدم المنفرد، التشغيل لنظم تشغيل غير آمنة، إعادة إعداد محمل التشغيل، تجاوزات التشغيل الآمن في UEFI ٨. الثغرات الأمنية في الرموز المصغرة ٩. ثغرات البرمجيات الثابتة: إعادة تحميل BIOS/PROMs ١٠. الدور الأمني للطبقات الوسيطة: طبقة تجريد الأجهزة والعتاد وطبقات البيئات الافتراضية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح الثغرات الأمنية الرئيسية في الأجهزة والعتاد والبرمجيات الثابتة. ٢. استخدام قدرات أمن الأجهزة والعتاد. ٣. شرح تهيئة الأنظمة وتحميل البرمجيات والتأكد من صحتها ٤. مناقشة الدور الأمني لطبقات تجريد الأجهزة والعتاد.

التحليل الجنائي الرقمي للمضيف Host Forensics (HOF)

الوصف	تقدم هذه الوحدة المعرفية القدرات والمهارات اللازمة للبحث والتحقيق في مضيف شبكة باستخدام طرق التحليل الجنائي الرقمي.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أنظمة الملفات والتحليل الجنائي الرقمي لأنظمة الملفات ٢. تحليل مشغلات الأجهزة الافتراضية (Hypervisors) ٣. تحليل التشفير ٤. جداول قوس المطر ٥. فلترة الملفات المعروفة ٦. إخفاء المعلومات ٧. إعادة تجميع الملفات ٨. تحقيقات النظام الحي ٩. تحليل الجدول الزمني ١٠. التحليل الجنائي الرقمي لتطبيقات المضيف
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحديد البيانات القابلة للاسترداد من بيئات أنظمة تشغيل متعددة. ٢. عرض منهجيات التحليل الجنائي الرقمي للمضيف. ٣. إجراء تحقيقات النظام الحي وإعداد تقرير التحليل الجنائي الرقمي.

الهندسة العكسية للأجهزة والعتاد Hardware Reverse Engineering (HRE)

الوصف	تقدم هذه الوحدة المعرفية المعارف والقدرات والمهارات لتحديد وظيفة مكونات عتاد معينة ومدخلاتها ومخرجاتها وبياناتها المخزنة باستخدام إجراءات وطرق الهندسة العكسية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أساسيات الهندسة العكسية ٢. المحفزات، جمع البيانات، تحليل البيانات ٣. تطوير المواصفات ٤. تحسين القدرات وأساليب التعديل ٥. اكتشاف التعديل ٦. منهجيات التحفيز وقياس الأجهزة ٧. معايير JTAG IEEE 1149.1 ٨. تعريف الواجهات وتعدادها ٩. التفكيك إلى مكونات بناء على الوظائف
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض طرق الهندسة العكسية للعتاد. ٢. تطبيق عملية التقاط البيانات وقياسها وجمعها من أجل تحديد وظيفة مكون عتاد معطى. ٣. وصف إحدى طرق الهندسة العكسية لفهم وظائف الدوائر المتكاملة.

توكيد بنى المعلومات Information Assurance Architectures (IAA)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة ببنى الأمن السيبراني المستخدمة لحماية أنظمة المعلومات والبيانات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الدفاع بعمق ٢. المناطق الوسيطة المعزولة (DMZs) ٣. الخوادم الوسيطة ٤. التكوين والأمن ٥. التوالي ٦. الخصائص الناشئة ٧. التبعيات ٨. مجموعات قاعدة الحوسبة الموثوقة الفرعية ٩. البنى المؤسسية وبنى الأمن السيبراني ١٠. تصميم الشبكة الآمنة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التمييز والربط بين مراحل ومكونات بنية توكيد المعلومات. ٢. شرح قدرات المنهجيات الحالية وحدودها في تقييم حلول بنى تأمين المعلومات وتخطيطها وتنفيذها والحفاظ عليها. ٣. فحص الثغرات الأمنية المحتملة لبنية معينة. ٤. تصميم بنى آمنة لتطبيقات معينة.

الالتزام بتوكيد المعلومات Information Assurance Compliance (IAC)

الوصف	توفر هذه الوحدة المعرفية المعارف بالقواعد واللوائح والمسائل المتعلقة بالتدقيق والالتزام بالتشريعات واللوائح المعمول بها في الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. العلاقة بين الالتزام والتدقيق ٢. أنواع التدقيق: داخلي وخارجي ٣. أغراض التدقيق: المتطلبات، المواصفات، السياسة، المعايير، التشريعات، الضوابط التنظيمية والداخلية ٤. عملية التدقيق: الميثاق، خط الأساس، الأنشطة، إعداد التقارير، النتائج، التوصيات، الاستجابة، استراتيجية تقليل جوانب القصور ٥. مراقبة الالتزام ٦. التدريب على الالتزام
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التمييز بين متطلبات الالتزام الإلزامية والاختيارية. ٢. تصميم وتخطيط وإجراء عمليات التدقيق لفحص الالتزام.

معايير توكيد المعلومات Information Assurance Standards (IAS)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بالمعايير الوطنية والدولية الشائعة الخاصة بتوكيد المعلومات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المعايير الوطنية ذات العلاقة بالأمن السيبراني ٢. اللوائح التنظيمية والمعايير الدولية ذات العلاقة بالأمن السيبراني مثل (NIST) ٣. المعايير التجارية مثل (PCI/DSS) ٤. المعايير المفتوحة مثل (OWSAP)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مقارنة أنواع مختلفة من التشريعات واللوائح التنظيمية والسياسات والأطر والمعايير الوطنية والدولية. ٢. شرح تأثير المعايير أو اللوائح التنظيمية على أنظمة معينة. ٣. توضيح تأثير المعايير على المقاولين الفرعين والعملاء. ٤. سرد أحكام المعايير الرئيسية وشرحها.

أنظمة التحكم الصناعية Industrial Control Systems (ICS)

الوصف	توفر هذه الوحدة المعرفية المعارف بأنظمة التحكم الصناعية إلى جانب الثغرات الأمنية التي ترتبط بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منظومة العمليات الصناعية: القطاعات الصناعية، الأدوار والمسؤوليات المهنية، أنواع العمليات، دورات الحياة الصناعية، السلامة في بيئة العمل ٢. أنظمة القياس والتحكم: أنظمة التحكم الإشرافي وتحصيل البيانات (SCADA)، أنواع أنظمة التحكم الصناعية (مثل: أنظمة توزيع الطاقة، والتصنيع)، نماذج أنظمة التحكم الصناعية (مثل: المستندة إلى الوقت مقابل المستندة إلى الأحداث)، الحساسات والمشغلات، وحدات التحكم (أجهزة التحكم المنطقي القابلة للبرمجة (PLC)، الوحدات الطرفية البعيدة (RTUs)، أنظمة التحكم الموزعة (DCS))، برمجة وحدات التحكم (مخطط السلم، الكتل الوظيفية، النص الهيكلي، مخطط الوظائف التسلسلي)، واجهات التفاعل بين الإنسان والآلة (HMIs) في أنظمة التحكم الصناعية وSCADA ٣. معدات العمليات: مكونات الأجهزة والعتاد لأنظمة التحكم الصناعية وأنظمة SCADA ٤. شبكات واتصالات التحكم الصناعي: بروتوكولات وشبكات أنظمة التحكم الصناعية وSCADA (مثل: Ethernet/IP، MODBUS، PROFINET، DNP3، OPC، ICCP، HART)، وطرق الاتصالات الأخرى في أنظمة التحكم الصناعية (مثل: الاتصال التسلسلي، RS232/485، ZIGBEE، MHz0900، Bluetooth، X.25) ٥. سلامة العمليات وموثوقيتها: أسباب مخاطر السلامة، تقييم المخاطر، تحليل الأثر ٦. الإرشادات واللوائح الخاصة بالأمن السيبراني الصناعي: المتطلبات التنظيمية ومتطلبات الامتثال والمعايير والإرشادات الصناعية الخاصة بأنظمة التحكم الصناعية وSCADA، وبنى أمن شبكات أنظمة التحكم الصناعية ٧. أوجه الضعف الشائعة في بيئات أنظمة التحكم الصناعية: تحديات أمن أنظمة التحكم الصناعية وSCADA، الثغرات الأمنية الشائعة في البنى التحتية الحساسة وأنظمة التحكم الصناعية وSCADA، والتهديدات ومتجهات الهجوم المؤثرة في بيئات أنظمة التحكم الصناعية ٨. الاستجابة للحوادث والتعافي منها في أنظمة التحكم الصناعية ٩. التقنيات الدفاعية في الأمن السيبراني لأنظمة التحكم الصناعية: تقسيم الشبكات، كشف الأنشطة غير الطبيعية، تقوية الأجهزة، والضوابط الهندسية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف مكونات نظام التحكم الصناعي الإشرافي وتحصيل البيانات (SCADA). ٢. وصف استخدامات وتطبيقات أجهزة التحكم المنطقي القابلة للبرمجة (PLCs) في الأتمتة. ٣. وصف الأساليب المستخدمة لمعالجة أوجه الضعف الشائعة مع مراعاة الخصائص والمتطلبات الفريدة لأنظمة التحكم الصناعية. ٤. تطبيق المعرفة بأنظمة التحكم الصناعية وSCADA لتحديد الثغرات والتهديدات المحتملة. ٥. شرح اختلاف بيئات أنظمة التحكم الصناعية عن بيئات أنظمة المعلومات التقليدية. ٦. شرح كيفية استخدام نماذج الأمن السيبراني لتوجيه أمن أنظمة التحكم الصناعية وSCADA.

بحث موجه/ دراسة مستقلة Independent/Directed Study/Research (IDR)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتصلة بالمواضيع الحديثة والناشئة في مجال الأمن السيبراني.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التقنيات الناشئة إلى جانب مسائل الأمن السيبراني ذات العلاقة ٢. الأدوات والأساليب والمنهجيات الناشئة المتعلقة بالأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مناقشة التقنيات المتقدمة الحديثة والناشئة إلى جانب مسائل الأمن السيبراني ذات العلاقة. ٢. تطبيق وعرض ومناقشة استخدام الأدوات والأساليب والمنهجيات المتقدمة الحديثة والناشئة في الأمن السيبراني.

أنظمة كشف/ منع التسلل Intrusion Detection/Prevention Systems (IDS)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المنهجيات والأساليب لاكتشاف وتحليل الثغرات الأمنية والتهديدات، بالإضافة للمهارات اللازمة لاستخدامها للتخفيف من أضرار المخاطر المصاحبة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الفحص العميق لحزَم البيانات ٢. تحليل ملفات السجلات ٣. بيانات القياس عن بعد ٤. دمج السجلات ٥. المقارنة والتحليل المتبادَل للسجلات ٦. كشف الأنشطة غير الطبيعية: إنشاء ملفات التعريف ٧. خوارزميات كشف الأنشطة غير الطبيعية: المنهجيات الإحصائية، وأساليب الارتباط، ومنهجيات المنطق الضبابي، والذكاء الاصطناعي، وخوارزميات الترشيح، والشبكات العصبية ٨. كشف إساءة الاستخدام: كشف التوقيع ٩. الكشف القائم على المواصفات ١٠. كشف ومنع التسلل القائم على الأنظمة المضيفة: الكشف السلوكي للملفات والعمليات ١١. كشف ومنع التسلل القائم على الشبكة: وضع التخفّي ١٢. كشف التسلل الموزَّع ١٣. أنظمة كشف التسلل الهرمية ١٤. مصائد الهجمات وشبكات مصائد الهجمات ١٥. الاستجابة للتسلل: إعادة تهيئة الجهاز، الإخطارات، تسجيل التتبع، فتح التطبيقات، مقاطعة الجلسة، وإعادة الاتصال
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. كشف حالات التسلل إلى المضيف والشبكة والاستجابة لها. ٢. تطبيق الأدوات لتحليل السجلات وكشف الأنشطة غير الطبيعية على الشبكة. ٣. تصميم الإجراءات التصحيحية للاستجابة لحالات التسلل المكتشفة. ٤. تهيئة أنظمة كشف/منع التسلل لتحسين أدائها ودقتها.

إدارة الهوية Identity Management (IMM)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول طرق إدارة الهوية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التعريف والتوثيق: الأشخاص والأجهزة، ضبط الوصول للشبكة، إدارة الهوية والوصول، الأدوار، الأنظمة متعددة المنهجيات للتعرف والتوثيق، أنظمة التوثيق المعتمدة على الخصائص الحيوية، الدقة / معدل قبول الخطأ / معدل رفض الخطأ، المقاومة، الخصوصية، سهولة الاستخدام وقابلية التساهل للمنهجيات ٢. ضوابط الأصول المادية والمنطقية: أجهزة الأنظمة، أصول الشبكات، أجهزة النسخ الاحتياطي/التخزين، ضوابط الوصول القائمة على القواعد، ضوابط الوصول القائمة على الدور الوظيفي، منهجيات تتبع المخزون، ومنهجيات إنشاء الهوية ٣. الهوية كخدمة ٤. خدمات هوية الأطراف الخارجية ٥. الهجمات ضد ضبط الوصول وطرق مواجهتها: هجمات كلمة المرور، هجمات تعتمد على القاموس، هجمات جميع الاحتمالات وهجمات انتحال الشخصية/ البريد الإلكتروني، التحقق من الهوية متعدد العوامل، سياسة كلمة المرور القوية، ملفات كلمة المرور الآمنة، والوصول المحدود إلى الأنظمة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. التمييز بين المفاهيم التالية: 'تحديد الهوية' و 'التوثيق' و 'تصريح الدخول'. ٢. مناقشة مسارات التدقيق وأهمية حفظ السجلات في تحديد الهوية والتوثيق. ٣. تطبيق مفاهيم أدنى الصلاحيات وفصل المهام والمسؤوليات ٤. شرح الهجمات ضد ضبط الوصول ومناقشة طرق مواجهتها.

إنترنت الأشياء Internet of Things (IoT)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بإنترنت الأشياء والثغرات الأمنية المحتملة المرتبطة بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. بنية إنترنت الأشياء (مثل: تصميم الأنظمة، النمذجة، والمحاكاة) ٢. تطبيقات إنترنت الأشياء ٣. بروتوكولات الاتصال في إنترنت الأشياء ٤. نظم التشغيل الخاصة بإنترنت الأشياء ٥. تهديدات وهجمات إنترنت الأشياء ٦. دورة حياة البرمجيات الآمنة لإنترنت الأشياء ٧. معايير تقييم الأمن السيبراني لمنصات إنترنت الأشياء ٨. وسوم تحديد الهوية بالترددات الراديوية (RFID) ٩. مواصفات وصف استخدام المُصنِّع (MUD) ١٠. عملية الترقية الآمنة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف بنية إنترنت الأشياء وتطبيقاتها. ٢. وصف أفضل تدابير الأمن السيبراني لتأمين أجهزة إنترنت الأشياء. ٣. تحديد معايير تقييم الأمن السيبراني الخاصة بمنصات إنترنت الأشياء.

أمن تخزين المعلومات Information Storage Security (ISS)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول طرق تأمين تخزين المعلومات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تشفير الأقراص والملفات: تشفير الأجهزة مقابل تشفير البرمجيات ٢. محو البيانات: الاستبدال، إزالة المغنطة، طرق الإتلاف المادي والبقايا العالقة في ذاكرة التخزين ٣. قناع البيانات: لأجل الاختبار والتعتيم والخصوصية ٤. أمن قاعدة البيانات: الوصول، التوثيق، التدقيق، نماذج تكامل التطبيقات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مناقشة تشفير أجهزة التخزين المطبق على مستوى العتاد والبرمجيات. ٢. المقارنة بين أساليب محو البيانات وقيود تنفيذها. ٣. شرح تطبيقات تقنيع البيانات. ٤. مناقشة الوصول إلى قاعدة البيانات والتوثيق والتدقيق وتكامل التطبيقات.

مقدمة في الحوسبة النظرية Introduction to the Theory of Computation (ITC)

الوصف	تقدم هذه الوحدة المعرفية المعارف بنماذج آلات الحالات المنتهية ودورها واستخداماتها في الحوسبة. وتقدم كذلك المهارات والقدرات لتحليل تعقيد مسائل الحوسبة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. نماذج الآلات ٢. نماذج آلات تيورنق ٣. نماذج آلات الحالات المنتهية المحددة وغير المحددة ٤. نظرية اللغات المنهجية ٥. القابلية للحوسبة وعدم القابلية للحوسبة ٦. القابلية للحوسبة في آلات تيورنق ٧. تحليل الخوارزميات ٨. قياسات التعقيد: الوقت والتخزين والاتصالات وأعداد وحدات المعالجة ٩. رمز O الكبير في تحليل تعقيد الخوارزميات ١٠. أفضل وأسوأ ومتوسط درجة التعقيد ١١. الحدود العليا والدنيا لدرجة التعقيد ١٢. فئات درجة تعقيد: NP، P، وصعوبة التعامل
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح نظرية الآلات المجردة ونماذج الآلات. ٢. التفريق بين الوظائف القابلة وغير القابلة للحوسبة. ٣. شرح التعقيد وتقييم المتطلبات من الموارد لحوسبة المسائل. ٤. تحليل مسائل معينة باستخدام آلات الحالات المنتهية المحددة وغير المحددة.

أمن دورة حياة الأنظمة والمنتجات Life-Cycle Security (LCS)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المفاهيم الأمنية، والمهارات لتطبيقها لتحسين الجوانب الأمنية خلال دورة حياة الأنظمة والمنتجات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مراحل ومسائل دورة حياة الأنظمة: التهيئة، المتطلبات، التصميم، التطوير، الاختبار، النشر، العمليات، الصيانة، والإنهاء ٢. تعيين الثغرات الأمنية وإدارتها وإمكانية تتبعها ٣. نمذجة التهديدات ٤. نموذج نضج توكيد البرمجيات ٥. دور إدارة المشاريع والبرامج ٦. دور إدارة العمليات ٧. أهمية الثقافة والتدريب ٨. عمليات ونماذج التطوير ٩. إدارة الإعدادات ١٠. تهديدات التطوير
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف أهمية البرمجيات الآمنة، وأفضل ممارسات البرمجة، وعمليات ومنهجيات التطوير التي تؤدي إلى برمجيات آمنة. ٢. شرح مراحل دورة حياة الأنظمة والمسائل الأمنية المتعلقة بها. ٣. تحديد عناصر نماذج النضج.

البرمجة منخفضة المستوى Low Level Programming (LLP)

الوصف	تقدم هذه الوحدة المعرفية المهارات لأداء العمليات منخفضة المستوى بأمان باستخدام لغات البرمجة منخفضة المستوى.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. لغات البرمجة عالية المستوى التي تسمح بالوصول منخفض المستوى، مثل لغة C ٢. البرمجة بلغة التجميع ٣. أمن دوال المكتبات ٤. المؤشرات والتعامل معها ٥. تكوين الوحدات البرمجية في البرامج منخفضة المستوى ٦. طرق البرمجة الدفاعية ٧. ترجمة وتجميع وربط ملفات الكائنات ٨. الاستدعاءات في لغة التجميع
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق البرمجة منخفضة المستوى لتنفيذ مكونات نظم التشغيل وبرامج تشغيل العتاد. ٢. مناقشة فوائد ومخاطر استخدام البرمجة منخفضة المستوى.

التحليل الجنائي الرقمي في الوسائط Forensics Media (MEF)

الوصف	تقدم هذه الوحدة المعرفية المهارات والقدرات اللازمة للبحث والتحقيق في الوسائط الرقمية باستخدام طرق التحليل الجنائي الرقمي.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الحصول على وسيط التخزين ٢. توثيق الأدلة: التحقق والتأكد من صحتها والاختزال ٣. البيانات الوصفية: أختام الوقت للتحديث والوصول والتغيير MAC Timestamps ٤. الاستحواذ الحي مقابل الاستحواذ الثابت ٥. التصوير المتناثر مقابل التصوير الكامل ٦. المساحات التخزينية المتبقية ٧. الملفات والمجموعات والتقسيمات المخفية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض أساليب التحليل الجنائي الرقمي وطرق الحصول على البيانات في وسائط معينة. ٢. تطبيق طرق التحقيق الجنائي الرقمي على وسائط محددة.

تعلم الآلة Machine Learning (MLL)

الوصف	تقدم هذه الوحدة المعرفية المعارف في خوارزميات تعلم الآلة والنماذج الرياضية والإحصائية، كما تقدم أيضا المهارات اللازمة لاستخدام هذه الخوارزميات والنماذج في تطبيقات تعلم الآلة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. الانحدار الخطي ٢. التصنيف الخطي ٣. الانحدار اللوجستي ٤. الجيران الأقرب ٥. مقاييس التقييم: AUC، الدقة، الاستدعاء، التحديد، MAPE، MSE، RMSE ٦. اختبار الفرضية ٧. النزول المتدرج ٨. أشجار القرارات ٩. الغابات العشوائية ١٠. آلات متجهات الدعم ١١. المصنِّفات الاحتمالية ١٢. الشبكات العصبية الاصطناعية ١٣. التقسيم إلى فئات ١٤. تحليل القيمة المنفردة (SVD)، وتحليل المكونات الرئيسية (PCA)، والمرمِّزات الآلية ١٥. التعلم المعزِّز ١٦. أخلاقيات تعلم الآلة ١٧. تطبيقات خوارزميات تعلم الآلة المرتبطة بالأمن السيبراني
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق خوارزميات ونماذج تعلمّ الآلة لحل مسائل التصنيف والانحدار والتجميع. ٢. تقييم وتفسير نتائج الخوارزميات. ٣. تحليل ومعالجة مجموعات البيانات الضخمة. ٤. المقارنة بين عدة أساليب للتعلّم وبيان أوجه الاختلاف بينها. ٥. وصف المسائل الأخلاقية المتعلقة باختيار البيانات، وخطوات المعالجة المسبقة، واختيار الخوارزمية، وتصوير النتائج وعرضها، وذلك في تطبيقات الأمن السيبراني المعتمدة على تعلم الآلة.

تقنيات الهاتف الجوال Mobile Technologies (MOT)

الوصف	تقدم هذه الوحدة المعرفية المعارف بتقنيات الهاتف الجوال بما في ذلك العتاد والاتصالات والإدارة وبيئات البرمجة الخاصة بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. لشبكات الخلوية (مثل:4G/LTE, 5G, 6G): المعايير والبنى الأساسية وتطورها الزمني ٢. خيارات التصميم ٣. التشفير ٤. إدارة التنقل ٥. إشارات التحكم في الموارد الراديوية (RRC) ٦. الفوترة/الاحتساب ٧. أمن الهاتف الجوال
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح طريقة عمل أنظمة الهاتف الجوال في تأمين المكالمات الصوتية والبيانات. ٢. شرح كيفية الحفاظ على الاتصال بالشبكة أثناء الحركة ٣. المقارنة بين معايير الشبكات الخلوية المختلفة من حيث البنية والأمن.

أمن إدارة الشبكات Network Security Administration (NSA)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بإدارة وصيانة أمن البنى التحتية للمنظمات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. ربط أهداف الأعمال بأهداف التقنيات ٢. حلول الأمن الرئيسية وفئات وميزات المنتجات ٣. تعارض الأمن السيبراني مع الحلول التقنية ٤. أفضل الممارسات في مجال الأمن السيبراني ٥. تطبيق سياسات أمن الشبكات ٦. وضع المخاطرة والقابلية للمخاطرة ٧. أدوات مراقبة الشبكات والأنظمة ٨. تقييم حالات الأمن السيبراني والاستجابة لها وإدارتها ٩. اكتشاف الحوادث السيبرانية ١٠. عمليات الاستجابة للحوادث السيبرانية وإدارتها ١١. عمليات النشر والترقية ١٢. اختبار قبول المستخدم ١٣. خطط الحجب ١٤. فترات الصيانة وإدارتها
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تحليل متطلبات الشبكة والتوصية بالحلول والمنتجات والتقنيات. ٢. تحديد أفضل ممارسات الأمن السيبراني لتلبية أهداف الأعمال وفقاً لافتراضات المخاطر. ٣. حماية أصول تقنية المعلومات والبنية التحتية من التهديدات المحتملة. ٤. تنفيذ مراقبة الأنظمة لكشف الأنماط الشاذة، وإجراء تحديثات وتعديلات دورية للأنظمة. ٥. تنفيذ أنشطة الاستجابة للحوادث السيبرانية مثل الانتهاكات والتسلل وسرقة المعلومات. ٦. تخطيط واختبار وتنفيذ وتقييم نشر البرمجيات والعتاد.

تقنية الشبكات والبروتوكولات Network Technology and Protocols (NTP)

الوصف	تقدم هذه الوحدة المعرفية المعارف الخاصة بروتوكولات الشبكات ومكوناتها، وتقدم كذلك المهارات اللازمة لاستخدام الأدوات لمراقبة وتحليل الشبكات.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مبدلات الشبكات: Ethernet، وARP، وRARP ٢. مسائل الأمن السيبراني في الطبقة الثانية من الشبكات ٣. بروتوكول الإنترنت الإصدار الرابع IPv4: عنونة IPv4 ٤. بروتوكول الإنترنت الإصدار السادس IPv6: عنونة IPv6 ٥. التوجيه في بروتوكولات الإنترنت الإصدار الرابع (IPv4) والإصدار السادس (IPv6): خوارزميات التوجيه، وجداول التوجيه، ومقاييس التوجيه ٦. مسائل الأمن السيبراني في الطبقة الثالثة من الشبكات ٧. التسمية في الشبكات: أدلة وخدمات أسماء النطاقات DNS، NetBIOS ٨. تحليل الشبكات واكتشاف الأخطاء وإصلاحها وبروتوكول تدفق الشبكة: NetFlow ٩. أدوات تحليل البروتوكولات وحزم البيانات: Wireshark
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح بناء الطبقة الثانية من الشبكات. ٢. توضيح تراكيب بروتوكولات الإنترنت الإصدار الرابع (IPv4) والإصدار السادس (IPv6). ٣. اكتشاف وتخفيف أضرار مسائل الأمن السيبراني للطبقتين الثانية والثالثة في الشبكات. ٤. تطبيق أدوات تحليل الشبكات وحزم البيانات لاستكشاف الأخطاء وإصلاحها.

التحليل الجنائي الرقمي في الشبكات Network Forensics (NWF)

الوصف	تقدم هذه الوحدة المعرفية المهارات والقدرات اللازمة للبحث والتحقيق في تدفق البيانات في الشبكات وتحليلها باستخدام طرق التحليل الجنائي الرقمي.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التقاط حزم البيانات وتحليلها ٢. التحقيق في حوادث أمن الشبكات ٣. كشف ومنع التسلل ٤. تداخل التحليل الجنائي الرقمي للأجهزة والشبكات ٥. تحليل ملفات السجلات ٦. قواعد الكشف Sigmag Yara ٧. أطر MITRE ATT&CK/ATLAS ٨. المعلومات الاستباقية للتهديدات السيبرانية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض منهجيات التحليل الجنائي الرقمي في الشبكات. ٢. تحليل تدفق البيانات في الشبكات. ٣. اكتشاف الأنشطة الضارة والأنماط غير الطبيعية وآثارها.

إدارة نظم التشغيل Operating Systems Administration (OSA)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات اللازمة لتنفيذ العمليات الأساسية في إدارة نظم التشغيل.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تثبيت نظام التشغيل ٢. إدارة حسابات المستخدمين: ضبط الوصول، سياسات كلمة المرور، طرق التوثيق، سياسات المجموعات ٣. واجهات سطر الأوامر ٤. إدارة الإعدادات ٥. التحديثات والتصحيحات ٦. تسجيل وتدقيق الأحداث ٧. إدارة خدمات النظام ٨. البيئات الافتراضية ٩. النسخ الاحتياطية واستعادة البيانات ١٠. أمن نظام الملفات ١١. إعدادات الشبكة ١٢. كشف التسلل إلى الجهاز المضيف ١٣. إعداد السياسات الأمنية ١٤. تهيئة الجدار الناري للمضيف وحماية الأجهزة الطرفية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. إعداد حسابات المستخدمين وإعداد وتطبيق سياسات التوثيق. ٢. تصميم وتنفيذ إعدادات التدقيق. ٣. تنفيذ عمليات النّسخ الاحتياطية والاستعادة. ٤. مراجعة سجلات الأمن والنظام. ٥. تثبيت التحديثات والتصحيحات. ٦. تهيئة إعدادات الأمن الأساسية في نظام التشغيل.

تأمين نظم التشغيل Operating Systems Hardening (OSH)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة لتحسين أمن نظم التشغيل ومتانتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. التثبيت الآمن ٢. إزالة المكونات غير الضرورية ٣. صيانة نظام الملفات: عزل البيانات الحساسة ٤. قيود المستخدم: الوصول والتفويضات ٥. إدارة المستخدمين والمجموعات والملفات ٦. معايير ومتطلبات كلمات المرور ٧. إيقاف الخدمات غير الضرورية التي ليس لها حاجة ٨. إغلاق المنافذ غير الضرورية التي ليس لها حاجة ٩. إدارة التصحيحات وتحديث البرمجيات ١٠. البيئات الافتراضية ١١. فحص الثغرات الأمنية ١٢. تهيئة الجدار الناري للمضيف ١٣. التشغيل الآمن ١٤. تشفير وحدات التخزين
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. عرض خطوات تأمين نظام تشغيل معين لتقليل مساحة سطح الهجوم. ٢. إجراء التثبيت الآمن لنظام تشغيل وتعطيل المكونات والخدمات والمنافذ التي ليس لها حاجة. ٣. إجراء تصحيحات وتحديثات دورية لأنظمة التشغيل. ٤. توظيف القدرات المدمجة في نظم التشغيل و/أو تطبيقات الطرف الثالث لتعزيز الوضع الدفاعي.

نظرية نظم التشغيل Operating Systems Theory (OST)

الوصف	تقدم هذه الوحدة المعرفية المعارف لمفاهيم نظم التشغيل ومكوناتها وواجهاتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. حالات الصلاحيات ٢. العمليات، وحزم التعليمات، وإدارة العمليات وحزم التعليمات ٣. إدارة الذاكرة والذاكرة الافتراضية ٤. الاتصالات ما بين العمليات ٥. التوازي والتزامن وحالات الوصول لطريق مسدود ٦. أنظمة الملفات ٧. المدخلات والمخرجات ٨. نظم تشغيل الاستجابة اللحظية ومسائل الأمن السيبراني ذات العلاقة ٩. بنى نظم التشغيل الموزعة ومسائل الأمن السيبراني ذات العلاقة ١٠. حالات السباق ١١. حالات تجاوز سعة المخزن المؤقت ١٢. البيئات الافتراضية ١٣. دلالات الواجهات الواضحة ١٤. بنية الثقة الصفرية ١٥. التقسيم الدقيق والبيئات المعزولة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. توضيح وعرض نظرية نظم التشغيل وتنفيذها. ٢. تصميم وتنفيذ التغييرات في بنى نظم التشغيل.

اختبار الاختراق Penetration Testing (PTT)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول طرق استغلال الثغرات الأمنية للوصول للأنظمة والتحكم بها، كما تقدم المهارات والقدرات اللازمة لاستخدام وتطبيق هذه الطرق.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منهجيات فرضيات العيوب ٢. منهجيات أخرى مثل (OSSTMM) ٣. تحديد العيوب من الوثائق ٤. تحديد العيوب من تحليل الرموز المصدرية ٥. فحص الثغرات الأمنية ٦. فئات الهجمات ٧. العيوب التي تؤدي إلى ثغرات ٨. التعداد والاستطلاع ٩. اكتشاف سطح الهجمات ١٠. متجهات الهجمات ١١. أطر الهجمات (مثل: MITRE ATT&CK/ATLAS) ١٢. طرق الاستغلال وما بعد الاستغلال ١٣. الاستخدام الأخلاقي لاختبار الاختراق ١٤. تقارير اختبار الاختراق الاحترافية ١٥. أدوات ونصوص برمجية لاختبار الاختراق (مثل: Metasploit، وKali Linux، وغيرها) ١٦. المعلومات الاستباقية للتهديدات ذات المصادر المفتوحة (OSINT) ١٧. الاستطلاع السلبي/الاستطلاع النشط
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تخطيط وإجراء اختبارات الاختراق على شبكة معينة أو نظام معين. ٢. مناقشة ومقارنة فئات وأنواع الهجمات. ٣. تحليل الثغرات الأمنية في الأنظمة والشبكات. ٤. مناقشة طرق ما بعد الاستغلال. ٥. تحديد أسطح الهجوم لاختبار الاختراق. ٦. إعداد تقرير احترافي لاختبار الاختراق يتضمن النتائج والمكتشفات. ٧. تقييم المتطلبات الأخلاقية والقانونية للتقييم الأمني واختبار الاختراق.

ضمان الجودة/ فحص الوظيفة QA/Functional Testing (QAT)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول المنهجيات المتبعة لتقييم مدى تلبية وحدة وظيفية للمتطلبات المطلوبة منها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منهجيات الاختبارات: اختبارات الصندوق الأبيض والرمادي والأسود ٢. أنواع ومستويات الاختبارات: اختبار الوحدة، اختبار التكامل، اختبار النظام، اختبار القبول، اختبار الأداء، واختبار الأمن السيبراني ٣. تحليل تغطية الاختبار ٤. الإنتاج الآلي واليدوي لمدخلات الاختبار ٥. تنفيذ الاختبار ٦. التأكد من صحة النتائج ٧. توثيق نتائج الاختبار
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم وتطوير اختبارات فعالة ومنسقة ومنظمة. ٢. إجراء اختبار وظيفي للأمن السيبراني لإظهار التنفيذ الكامل والصحيح للسياسات والآليات الأمنية.

مبادئ الترددات الراديوية Radio Frequency Principles (RFP)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول الاتصالات عبر الـترددات الراديوية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أساسيات الإشعاع الكهرومغناطيسي ٢. الهوائيات ٣. تضمن المعلومات ٤. التضمن الرقمي ٥. التمثيل الطيفي ٦. عرض المجال Bandwidth ٧. معدل الأخطاء BER ٨. نسب الطاقة والإشارة والتشويش والعلاقة بينها Eb/No ،S/N ٩. تقييد الوصول في الترددات الراديوية ١٠. مبادئ الانتشار
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح منهجيات عزل انبعاثات الترددات الراديوية ٢. تحديد طرق تعتيم إرسال الترددات الراديوية. ٣. شرح العلاقة بين نقل البيانات والتضمن والتعقيد ومعدل الخطأ المقبول وانتشار الإشارة.

توكيد البرمجيات Software Assurance (SAS)

الوصف	تقدم هذه الوحدة المعرفية المعارف بالطرق والأساليب التي تؤدي إلى برمجيات آمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. المبادئ الأمنية: الفصل، العزل، دمج العناصر في مكون واحد، منح أدنى الصلاحيات، البساطة، التقليل، وضع السلامة والأمان في حالة الأعطال، التشغيل الآمن في حالة الأعطال، تصميم الوحدات، تصميم الطبقات الأمنية المتعددة، تقليل المفاجآت، التصميم المفتوح، سهولة الاستخدام، تقليص سطح الهجمات ٢. أمن التصاميم البديلة ٣. أنماط التصميم الآمنة ٤. المتطلبات الأمنية لبيانات النظام ٥. مسار التدقيق ٦. طرق النمذجة الأمنية وتعيين الثغرات ٧. الصمود ٨. مراجعات التصميم
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق مبادئ التصميم الآمن. ٢. توضيح تأثيرات تصميم النظام وبنيته على الأمن. ٣. إنشاء تصميم لنظام محسّن لتلبية المتطلبات الأمنية المناسبة. ٤. بناء تصميم آمن باستخدام النمذجة وتقييم الثغرات الأمنية. ٥. مناقشة كيف يمكن أن تساعد مراجعة التصميم على تحسين الأمن بشكل كبير.

التحكم بالأنظمة System Control (SCC)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول طرق التحكم بالأنظمة بما فيها الكشف عن الهجمات، والتعويض عن أضرارها، ومواجهتها ومنعها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. ضبط الوصول إلى الموارد ٢. نماذج التصاريح ٣. اكتشاف التسلل: الأنماط غير الطبيعية، إساءة الاستخدام (القائم على القواعد، والقائم على التوقيع) والطرق القائمة على المواصفات ٤. نماذج الهجمات: أشجار الهجمات والرسومات ٥. الدفاعات: التوزيع العشوائي للعناوين ASLR، تغيير عناوين الإنترنت IP، تحمل التسلل ٦. التدقيق: حفظ السجلات، تحليل السجلات، العلاقة بالكشف عن حالات التسلل ٧. البرمجيات الضارة: الفيروسات، الديدان البرمجية، وبرمجيات الفدية ٨. نماذج الثغرات: نماذج RISOS، CWE، CVE، PA ٩. اختبار الاختراق: منهجية فرضية العيوب، OSSTMM ،ISSAF ،GISTA، PTES، ١٠. متطلبات الأنظمة للتحليل الجنائي الرقمي ١١. التعافي والصمود
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. المقارنة بين الطرق المختلفة المرتبطة بالأنظمة في التوثيق والتصريح وضبط الوصول. ٢. وصف كيفية اكتشاف الأنشطة الضارة، بما في ذلك استخدام أنظمة كشف التسلل. ٣. التمييز بين أنواع البرمجيات الضارة. ٤. مناقشة آليات التعافي والصمود التي تساعد على ضمان توافر الأنظمة.

بروتوكولات الاتصالات الآمنة Secure Communication Protocols (SCP)

الوصف	تقدم هذه الوحدة المعرفية المعارف حول بروتوكولات الاتصالات الآمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. بروتوكولات طبقة التطبيقات والنقل: SSL/TLS، SSH، HTTPS، HTTP ٢. الهجمات على بروتوكول أمن طبقة النقل TLS: هجمات تخفيض المستوى، تزوير الشهادات، آثار سرقة الشهادات الجذرية، شفافية الشهادة ٣. بروتوكولات أمن طبقة الإنترنت/الشبكة: حزمة البروتوكولات الأمنية IPsec، الشبكات الافتراضية الخاصة VPN ٤. بروتوكولات أمن الشبكات اللاسلكية: WEP، WPA، WPA2، WPA3 ٥. بروتوكولات أمن طبقة ربط البيانات: بروتوكولات RADIUS، PPP، L2TP
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح بروتوكولات الاتصالات الآمنة الرئيسية في طبقات الشبكة المختلفة. ٢. توضيح الهجمات ووسائل الحماية المضادة على بروتوكول أمن طبقة النقل.

أمن سلاسل الإمداد Supply Chain Security (SCS)

الوصف	تقدم هذه الوحدة المعرفية المعارف بالمخاطر ومسائل الأمن السيبراني المتعلقة بمكونات الطرف الثالث المستخدمة في بناء أنظمة معقدة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. مخاطر سلاسل الإمداد: مخاطر الأمن السيبراني المتعلقة بالطرف الثالث وأفضل الممارسات للتعامل معها ٢. توجهات التطوير على المستوى العالمي ٣. الإنتاج خارج الحدود ٤. نقل ولوجستيات مكونات تقنية المعلومات ٥. تقييم ممارسات التطوير لدى الطرف الثالث ٦. قدرات وحدود الهندسة العكسية للبرمجيات والعتاد ٧. عملية التوريد والمشتريات: الأمن المادي، تقسيم التصنيع، قابلية التتبع، فحص الشحنات، التأكد من صحتها، التحقق من الموردين
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. مناقشة المسائل والمخاطر السيبرانية المتعلقة بالاستعانة بمصادر خارجية لتوريد وتطوير ودمج العتاد والبرمجيات. ٢. وصف التهديدات والمخاطر الأمنية في العتاد والبرمجيات عند شراء المكونات. ٣. شرح طرق التعامل مع المخاطر السيبرانية المتعلقة بسلاسل الإمداد وطرق تخفيفها وشرح التحديات في هذه الطرق.

برمجة النظم Systems Programming (SPG)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة لتطوير برمجيات معقدة على المستوى المنخفض، والمصممة لتقديم خدمات إلى برمجيات أخرى.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. واجهات وتفاعلات العتاد والبرمجيات ٢. أنواع برامج النظم: بيئات التطوير، نظم التشغيل، الخدمات، وظائف الشبكات، برامج تشغيل الأجهزة، أطر التخزين، محركات الألعاب ٣. تصميم الخدمات في طبقات ٤. واجهات برمجة التطبيقات (API) ٥. برمجة الواجهات الداخلية لنظم التشغيل ٦. برمجة المستوى المنخفض: لغة التجميع، لغة C ٧. تحسين استخدام الموارد ٨. إدارة الموارد ٩. تقليص الوقت الزائد للتشغيل ١٠. التحكم المباشر بالوصول إلى الذاكرة والتحكم بالانسياب ١١. إدارة الذاكرة في برمجيات الأنظمة ١٢. المخاوف الأمنية في برمجيات الأنظمة ١٣. مراقبة وتسجيل برمجيات الأنظمة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطوير برامج بإمكانها العمل بشكل صحيح باستخدام موارد محدودة ٢. تطبيق نهج الطبقات للوصول إلى واجهات برمجة التطبيقات (API). ٣. تنفيذ وظائف جديدة يمكن تضمينها في لب نظام التشغيل. ٤. تنفيذ وظائف الأنظمة بدون استخدام مكتبات خارجية.

ممارسات البرمجة الآمنة Secure Programming Practices (SPP)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات والقدرات اللازمة لتطوير وتنفيذ برمجيات آمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تفسير المتطلبات الأمنية وتحقيقها ٢. مبادئ البرمجة الآمنة ٣. البرمجة المتينة ٤. البرمجة الدفاعية: التحقق من صحة المدخلات، وفحص نوع البيانات، وفحص الحدود، وتغطية جميع المسارات، ومعالجة الاستثناءات، وتجنب تراكيب البرمجة الخطرة، ومنع تسرب المعلومات ٥. الممارسات الأمنية في الفئات: منع تغيير بيانات الواجهات الخارجية بالمرجع، واستخدام السياق للوصول إلى البيانات، والتحقق من تحديث البيانات، والتوثيق ٦. العيوب البرمجية: تجاوز سعة المخزن المؤقت، وأخطاء الأعداد الصحيحة، والتحقق من صحة المدخلات، وإساءة استخدام واجهات برمجة التطبيقات، والخصائص الأمنية، والوقت والحالة، والأخطاء، وجودة الشفرة البرمجية، ودمج العناصر في مكون واحد، والبيئة ٧. التحليل الثابت والتحليل الديناميكي للبرامج ٨. تعتيم البيانات ٩. حماية البيانات ١٠. تهديدات تطبيقات الويب ١١. نماذج البرمجة الآمنة: البرمجة الثنائية، ومراجعة الشفرة البرمجية، والتطوير المعتمد على الاختبارات ١٢. استخدامات التشفير في البرمجة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تصميم وتطوير برمجيات آمنة تلبي متطلباتها الوظيفية. ٢. وصف خصائص البرمجة الآمنة. ٣. شرح الثغرات الأمنية المتأصلة في لغات البرمجة المختلفة. ٤. فحص الثغرات الأمنية الناتجة عن استخدام المكتبات وطرق التخفيف منها.

الهندسة العكسية للبرمجيات Software Reverse Engineering (SRE)

الوصف	تقدم هذه الوحدة المعرفية المهارات والقدرات اللازمة لإجراء الهندسة العكسية على برمجيات قابلة للتنفيذ لتحديد وظائفها وتأثيرها وتفاصيل تنفيذها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تحليل البرمجيات الضارة ٢. أدوات وتقنيات الهندسة العكسية ٣. التحليل الثابت والتحليل الديناميكي ٤. وضع الحماية والفحص Sandboxing ٥. تقنيات منع الهندسة العكسية ٦. أدوات ضغط البرمجيات التجارية ٧. تفكيك الشفرة البرمجية ٨. أدوات تحليل الذاكرة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق أدوات الهندسة العكسية للبرمجيات لاكتشاف وظائف وتفاصيل التنفيذ وطريقة عمل البرمجيات الضارة وتفاصيل تنفيذها. ٢. تحليل البرمجيات الضارة باستخدام تقنيات التحليل الثابت أو الديناميكي أو تحليل الشفرة البرمجية أو تحليل الذاكرة.

التحليل الأمني للبرمجيات Software Security Analysis (SSA)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات اللازمة لاستخدام الأدوات والمنهجيات لتحليل أمن البرمجيات بصيغتها الثنائية أو في صورة الشفرة المصدرية.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. منهجيات الاختبار ٢. تحليل الرموز البرمجية المصدرية والثنائية ٣. طرق التحليل الثابت والديناميكي ٤. وضع الحماية والفحص Sandboxing ٥. أدوات وطرق التحليل الشائعة
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. وصف الأدوات والطرق المستخدمة للتحليل الأمني للبرمجيات. ٢. تطبيق أدوات التحليل الأمني للبرمجيات لتحليل مكونات البرمجيات غير المعروفة.

هندسة أمن الأنظمة Systems Security Engineering (SSE)

الوصف	تقدم هذه الوحدة المعرفية المهارات اللازمة للمشاركة في تطوير أنظمة آمنة واسعة النطاق باستخدام التقنيات والطرق ذات العلاقة في كافة مراحل دورة حياة النظام.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تصميم الاختبار ٢. منهجيات الاختبار ٣. الخصائص الناشئة ٤. هندسة الأنظمة ٥. دمج الأنظمة ٦. تحليل قرار الصناعة أو الشراء ٧. تحليل أمن الأنظمة ٨. مكونات النظام المؤسسي
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطوير مكونات الأنظمة من خلال جمع وتحليل المتطلبات إلى جانب تصميم المكونات وتنفيذها وفحصها وصيانتها. ٢. تحليل المكونات في نظام مركبّ وكيفية تفاعلها. ٣. تحليل تصميم نظام معين، وتقييم مدى تلبيته لمتطلبات أمن النظام.

تحليل الثغرات الأمنية Vulnerability Analysis (VLA)

الوصف	تقدم هذه الوحدة المعرفية المعارف والمهارات المتعلقة باكتشاف ثغرات الأنظمة والشبكات، والتعرف عليها، وتحديد السبب الجذري لها، وتخفيف أضرارها ومعالجتها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تعريف الثغرات الأمنية ٢. طرق نمذجة الأنظمة ٣. تعيين الثغرات الأمنية ٤. خصائص وتصنيف الثغرات الأمنية ٥. التصنيف: تجاوز سعة المخزن المؤقت، تصعيد الصلاحيات، الجذور الخفية، أحصنة الطروادة، الأبواب الخلفية، الفيروسات، البرمجة الموجهة للعودة، ثغرات الهندسة الاجتماعية، وتأثير الصلاحيات الإدارية على الثغرات الأمنية ٦. الأسباب الجذرية للثغرات الأمنية ٧. استراتيجيات تخفيف الأضرار ٨. تحليل التدابير المضادة ٩. الإفصاح عن الثغرات الأمنية ١٠. أدوات وطرق اكتشاف الثغرات الأمنية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. تطبيق أدوات وطرق اكتشاف الثغرات الأمنية. ٢. بناء خريطة الثغرات الأمنية لنظام معين. ٣. تتبع الثغرات الأمنية لتحديد أسبابها الجذرية. ٤. تحليل التدابير المضادة لتخفيف أضرار الثغرات الأمنية. ٥. مناقشة السيناريوهات التي يجب فيها الإفصاح عن الثغرات الأمنية.

تقنيات البيئة الافتراضية Virtualization Technologies (VTT)

الوصف	تقدم هذه الوحدة المعرفية المعارف المتعلقة بالبيئات الافتراضية الحديثة للمضيف وتنفيذها ونشرها واستخدامها ومكونات أنظمتها وأمنها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. بنى البيئات الافتراضية ٢. طرق البيئات الافتراضية لتنفيذ الرموز البرمجية ٣. إدارة الذاكرة في البيئات الافتراضية ٤. الشبكات في البيئات الافتراضية ٥. التخزين في البيئات الافتراضية ٦. جدولة الآلات الافتراضية ٧. الترحيل واللقطات ٨. طبقات الإدارة الافتراضية ٩. التحليل الجنائي الرقمي في البيئات الافتراضية ١٠. المخاطر والاعتبارات الأمنية (مثل: انتشار الآلات الافتراضية، البرمجيات الضارة، الهروب من البيئة المعزولة للآلة الافتراضية)
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح مفاهيم البيئة الافتراضية. ٢. المقارنة بين بنى البيئات الافتراضية المختلفة وبيان أوجه الاختلاف بينها. ٣. تصميم البيئات الافتراضية وبنائها وتنفيذها وضبط إعداداتها. ٤. مناقشة المخاطر الأمنية المحتملة في البيئات الافتراضية واستراتيجيات التخفيف منها.

أمن تطبيقات الويب Web Application Security (WAS)

الوصف	تقدم هذه الوحدة المعرفية المعارف بالتقنية والأدوات والممارسات المتعلقة بتطبيقات الويب، كما تقدم المهارات اللازمة لتطبيق هذه الأدوات والممارسات لتطوير ونشر تطبيقات ويب آمنة.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. تقنيات تطبيقات الويب: بروتوكول HTTP، تصاميم الترميز، بنى تطبيقات الويب، وتقنيات/ لغات jSON، XML، AjAX ٢. الضوابط من طرف الخادم ٣. التوثيق ٤. إدارة الجلسات ٥. ضوابط الوصول ٦. الضوابط من طرف العميل ٧. الثغرات القائمة على المدخلات: حقن SQL، حقن SQL الأعمى، النصوص البرمجية عبر المواقع، تزوير الطلب عبر المواقع ٨. هجمات javaScript، هجمات معلومات التصفح المحفوظة Cookies ٩. ثغرات المدخلات الخاصة بالوظيفة ١٠. مهاجمة منطق التطبيقات ١١. الهجمات الحديثة الشائعة ١٢. ثغرات الاستضافة المشتركة ١٣. ثغرات خادم التطبيقات
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. شرح تقنيات تطبيقات الويب الشائعة ومسائل الأمن السيبراني ذات العلاقة. ٢. تطوير ونشر تطبيقات ويب آمنة. ٣. توضيح مبادئ أمن تطبيقات الويب.

شبكات الاستشعار اللاسلكية Wireless Sensor Networks (WSN)

الوصف	تتضمن هذه الوحدة المعرفية المعارف المتعلقة بمبادئ شبكات الاستشعار اللاسلكية، والتحديات والنواحي الأمنية المتعلقة بها.
المواضيع	يجب أن تتضمن هذه الوحدة المعرفية المواضيع التالية: ١. أجهزة الاستشعار اللاسلكية ٢. تطبيقات شبكات الحساسات اللاسلكية ٣. نشر شبكات الاستشعار اللاسكلية: منظم، عشوائي، البنية، التحكم بقوة الإشارة، التغطية، التنقل ٤. تحديد المواقع ٥. التزامن ٦. خصائص الإرسال اللاسلكي ٧. الوصول للقناة ٨. جدولة السبات ٩. استهلاك الطاقة بشكل فعال ١٠. الخدمات الشبكية المتمحورة حول البيانات ١١. التحكم بالازدحام، واعتمادية النقل ١٢. النواحي الأمنية المرتبطة بشبكات الاستشعار اللاسلكية
نواتج التعلم	بعد استكمال هذه الوحدة المعرفية، يجب أن يكون الطلبة قادرين على: ١. إجراء عمليات محاكاة لشبكات الاستشعار اللاسلكية لسيناريوهات معيّنة. ٢. تطبيق التدابير الأمنية المناسبة لشبكات الاستشعار اللاسلكية. ٣. وصف التحديات المرتبطة بشبكات الاستشعار اللاسلكية، بما في ذلك تحديد المواقع والتزامن واستهلاك الطاقة.

٤ الملحق (أ): أمثلة على برامج الأمن السيبراني التخصصية

٤-١ بكالوريوس الذكاء الاصطناعي في الأمن السيبراني

	وصف الوحدات المعرفية
الوحدات المعرفية المطلوبة	١. أساسيات الأمن السيبراني (CSF) ٢. مبادئ التصميم في الأمن السيبراني (CDP) ٣. مكونات أنظمة تقنية المعلومات (ISC) ٤. أساسيات التشفير (BCY) ٥. أساسيات الشبكات (BNW) ٦. أساسيات البرمجة (BSP) ٧. الدفاع عن الشبكات (NDF) ٨. مفاهيم نظم التشغيل (OSC) ٩. تراكيب البيانات (DST) ١٠. قواعد البيانات (DAT) ١١. التهديدات السيبرانية (CTH) ١٢. السياسات والتشريعات والأخلاقيات والالتزام بها (PLE) ١٣. تحليل المخاطر السيبرانية (SRA) ١٤. تخطيط وإدارة الأمن السيبراني (CPM) ١٥. إدارة البرامج الأمنية (SPM)
الوحدات المعرفية الاختيارية	١. التعلّم العميق (DLL) ٢. التعلّم الآلة (MLL) ٣. الأدوات التحليلية (ATT) ٤. إدارة البيانات (DBA) ٥. الخوارزميات (ALG) ٦. الخوارزميات المتقدمة (AAL) ٧. الحوسبة السحابية (CCO) ٨. ممارسات البرمجة الآمنة (SPP) ٩. أنظمة كشف/منع التسلل (IDS) ١٠. تحليل الثغرات الأمنية (VLA)

٢-٤ ماجستير التشفير

	وصف الوحدات المعرفية
الوحدات المعرفية المطلوبة	١. أساسيات الأمن السيبراني (CSF) ٢. مبادئ التصميم في الأمن السيبراني (CDP) ٣. مكونات أنظمة تقنية المعلومات (ISC) ٤. أساسيات التشفير (BCY) ٥. أساسيات الشبكات (BNW) ٦. أساسيات البرمجة (BSP) ٧. الدفاع عن الشبكات (NDF) ٨. مفاهيم نظم التشغيل (OSC)
الوحدات المعرفية الاختيارية	١. الأسس الرياضية للتشفير (FCY) ٢. مقدمة في نظرية الحوسبة (ITC) ٣. التشفير (CRY) ٤. سلامة البيانات وتوثيقها (DIA) ٥. الخوارزميات (ALG) ٦. هندسة التشفير (CRE) ٧. التشفير المتقدم(ACR)

٣-٤ ماجستير الأمن السيبراني لأنظمة التحكم الصناعية/التقنيات التشغيلية

	وصف الوحدات المعرفية
الوحدات المعرفية المطلوبة	١. أساسيات الأمن السيبراني (CSF) ٢. مبادئ التصميم في الأمن السيبراني (CDP) ٣. مكونات أنظمة تقنية المعلومات (ISC) ٤. أساسيات التشفير (BCY) ٥. أساسيات الشبكات (BNW) ٦. أساسيات البرمجة (BSP) ٧. الدفاع عن الشبكات (NDF) ٨. مفاهيم نظم التشغيل (OSC)
الوحدات المعرفية الاختيارية	١. أنظمة التحكم الصناعية (ICS) ٢. الأنظمة السيبرانية الفيزيائية (CPS) ٣. الأنظمة المدمجة (ESY) ٤. أمن الأجهزة والعتاد والبرمجيات الثابتة (HFS) ٥. إنترنت الأشياء (IoT) ٦. شبكات الاستشعار اللاسلكية (WSN) ٧. استمرارية الأعمال، والتعافي من الكوارث، وإدارة الحوادث السيبرانية (BDR)

٤-٤ ماجستير إدارة الأمن السيبراني

وصف الوحدات المعرفية	
الوحدات المعرفية المطلوبة	١. أساسيات الأمن السيبراني (CSF) ٢. مبادئ التصميم في الأمن السيبراني (CDP) ٣. مكونات أنظمة تقنية المعلومات (ISC) ٤. التهديدات السيبرانية (CTH) ٥. السياسات والتشريعات والأخلاقيات والالتزام بها (PLE) ٦. تحليل المخاطر السيبرانية (SRA) ٧. تخطيط وإدارة الأمن السيبراني (CPM) ٨. إدارة البرامج الأمنية (SPM)
الوحدات المعرفية الاختيارية	١. استمرارية الأعمال، والتعافي من الكوارث، وإدارة الحوادث السيبرانية (BDR) ٢. معايير توكيد المعلومات (IAS) ٣. الامتثال في توكيد المعلومات (IAC) ٤. أمن سلاسل الإمداد (SCS) ٥. بنى توكيد المعلومات (IAA) ٦. أمن دورة حياة الأنظمة والمنتجات (LCS) ٧. الجريمة السيبرانية (CCR)

٥ الملحق (ب): ملخص تحديثات الإصدار

يمثل هذا الإصدار (SCyber.Edu – 2: 2026) تحديثًا رئيسياً للإطار السعودي للتعليم العالي في الأمن السيبراني، وذلك لمواكبة الطبيعة المتسارعة والديناميكية لتخصص الأمن السيبراني. وتشمل أبرز التحديثات ما يلي:

١- **مراجعة شاملة للوحدات المعرفية:** تمت مراجعة جميع موضوعات ونواتج التعلم الخاصة بالوحدات المعرفية (KUs) ما يعكس الاتجاهات التقنية الحديثة ومشهد التهديدات السيبرانية الحالي.

٢- **توسعة الوحدات المعرفية:** تم تحديث وإضافة وحدات معرفية جديدة، بما يضمن المحافظة على ترابط الإطار وملاءمته.

٣- **تحديثات البرامج:** تم تحديث أوصاف البرامج التعليمية ومتطلبات الوحدات المعرفية الخاصة بها بما يحقق المواءمة مع أحدث المعايير والأطر المرجعية.

٤- **مسارات برامج جديدة:** تم استحداث درجة الماجستير (مسار الأمن السيبراني) لتغطية برامج الماجستير القائمة في التخصصات ذات العلاقة التي تتضمن مساراً في الأمن السيبراني في مؤسسات التعليم العالي.

٥- **ملحق التخصصات:** تمت إضافة ملحق جديد يقدم أمثلة على برامج الأمن السيبراني التخصصية ، بهدف تقديم إرشادات لمؤسسات التعليم العالي التي تتجه إلى طرح برامج تخصصية تتجاوز البرامج العامة في الأمن السيبراني.

٦ المصادر

[١] الإطار الوطني للمؤهلات من هيئة تقويم التعليم والتدريب، عام ٢٠٢٦

[٢] البرنامج الإرشادي والوحدات المعرفية للمراكز الوطنية للتميّز الأكاديمي في الدفاع السيبراني (CAE-CD)، عام ٢٠٢٤

[٣] مناهج الأمن السيبراني من معهد مهندسي الكهرباء والإلكترونيات وجمعية آلات الحوسبة (IEEE/ACM)، عام ٢٠١٧

[٤] مناهج علوم الحاسوب من معهد مهندسي الكهرباء والإلكترونيات وجمعية آلات الحوسبة ،(IEEE/ACM)، عام ٢٠٢٣

[٥] كتاب "أنماط الأمن في الممارسة: تصميم بنيات آمنة باستخدام أنماط البرمجيات "Security Patterns in Practice: Designing Secure Architectures Using Software Patterns"،
إدواردو فرنانديز.بوغليوني، الطبعة الأولى، عام 2013

[٦] كتاب "اكتمال البرمجة: دليل عملي لبناء البرامج A Practical Handbook of Software Construction Code Complete:"، ستيف ميكونل، الطبعة الثانية، عام 2014

[٧] كتاب "نمذجة التهديد: التصميم من أجل الأمن Modeling: Designing for Security Threat"، آدم شوستاك، عام 2014

[٨] كتاب "الأخلاقيات في تقنية المعلومات Ethics in Information Technology"، سينجاج ليرنينج، الطبعة الخامسة، عام 2014

[٩] كتاب "مجموعة أدوات تقييم مخاطر أمن المعلومات: تقييمات عملية من خلال جمع البيانات وتحليل البيانات Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis" جيسون مارتن، مارك تالبيس، عام ٢٠١٣

[١٠] كتاب "مقدمة للخوارزميات Introduction to Algorithms"، توماس كورمن، تشارلز ليزرسون، رونالد رايفست، كليفورد ستن الطبعة الثالثة، عام ٢٠٠٩

[١١] نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية.

[١٢] كتاب "ربط شبكات الحساسات اللاسلكية Networking Wireless Sensors"، باسكار كريشنامشاري، عام ٢٠٠٩

[١٣] الهيكل المعرفي للأمن السيبراني (CyBOK) (الإصدار ١,١,٠)، عام ٢٠٢١


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority