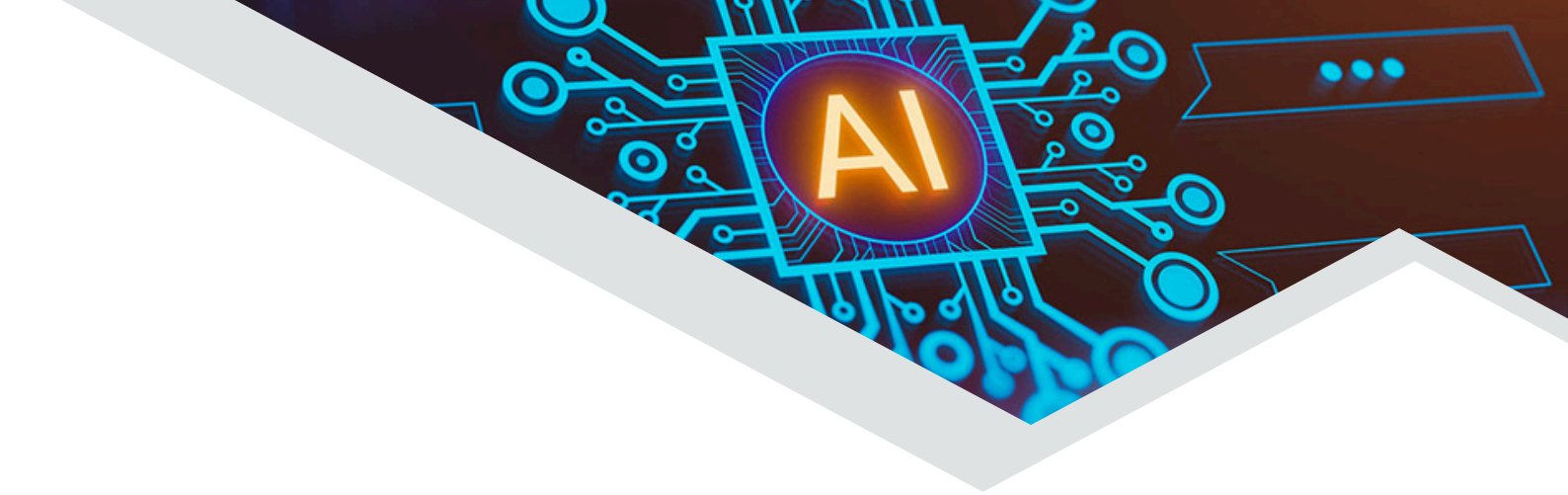
AI & Innovation

Selection and management of artificial intelligence security applications

Code: 254020

FUTURE CENTRE
مركز المستقبل

futurecentre.net



Course Introduction

The cybersecurity landscape is undergoing a seismic shift. As adversaries increasingly leverage Artificial Intelligence to launch sophisticated, automated attacks, traditional defense mechanisms are no longer sufficient. AI-powered security tools offer the promise of predictive threat detection, automated response, and unparalleled scalability. However, selecting the right AI security application is fraught with complexity, and managing it introduces unique challenges around explainability, integration, and adversarial manipulation.

This five-day intensive course is designed for cybersecurity leaders and practitioners. It provides a strategic framework for navigating the crowded marketplace of AI security solutions, from AI-powered SIEMs and EDRs to autonomous penetration testing tools. Participants will learn how to critically evaluate vendors, integrate AI tools into existing security architectures, and establish robust governance to ensure these powerful systems are effective, ethical, and resilient against attack.

Training Method

- Pre-assessment
- Live group instruction
- Use of real-world examples, case studies and exercises
- Interactive participation and discussion
- Power point presentation, LCD and flip chart
- Group activities and tests
- Each participant receives a binder containing a copy of the presentation
- slides and handouts
- Post-assessment

Course Objectives

Upon completion of this course, participants will be able to:

- **Evaluate AI Security Solutions:** Critically assess the capabilities, claims, and underlying technology of AI-powered security applications across various categories (e.g., threat detection, fraud prevention, vulnerability management).
- **Understand the AI Threat Landscape:** Identify how attackers use AI (e.g., AI-powered malware, deepfakes for social engineering, adversarial attacks) to justify and guide AI security investments.
- **Manage the AI Security Lifecycle:** Develop processes for the ongoing management, monitoring, and tuning of AI security tools to maintain efficacy and reduce false positives/negatives.
- **Integrate AI into Security Architecture:** Design a strategy for seamlessly integrating new AI tools with existing security infrastructure (SOAR, SIEM, etc.) for a cohesive defense posture.
- **Mitigate AI-Specific Risks:** Address unique risks such as model poisoning, data bias, algorithmic transparency, and supply chain vulnerabilities in AI security products.
- **Build a Business Case and ROI Model:** Calculate and articulate the value and return on investment of proposed AI security applications to executive leadership.

Who Should Attend?

This course is designed for professionals responsible for securing organizational assets and making technology investment decisions:

- **Chief Information Security Officers (CISOs) & Deputy CISOs**
- **Security Architects & Engineers**
- **SOC Managers & Analysts**
- **IT Risk and Compliance Managers**
- **Security Operations Center (SOC) Team Members**
- **Network Security Specialists**
- **IT Directors & Heads of Infrastructure**
- **Cybersecurity Consultants & Auditors**
- **Procurement Professionals specializing in security technology**

Course Outline

Day 1: Foundations of AI in Cybersecurity

AM: The New Arms Race: AI vs. AI in Cybersecurity

- How attackers are using AI: automated exploits, intelligent phishing, deepfakes, and evasion techniques.
- How defenders use AI: threat hunting, anomaly detection, automated response (SOAR), and behavioral analytics.
- Key AI Concepts for Security Pros: Supervised vs. Unsupervised Learning, NLP, and Graph Analysis in a security context.

PM: The AI Security Application Landscape

- Mapping the vendor ecosystem: AI in EDR, XDR, SIEM, NDR, Fraud Detection, and Cloud Security Posture Management (CSPM).
- Understanding the "AI" in the product: from marketing buzzwords to genuine machine learning capabilities.
- Workshop: Deconstructing vendor datasheets and whitepapers.

Day 2: The Selection Process: Evaluating and Procuring AI Tools

AM: Defining Requirements and Building a Shortlist

- Aligning AI tool selection with organizational risk profile and security strategy.
- Developing a weighted evaluation criteria framework: accuracy, performance, integration capabilities, cost, and vendor viability.
- Creating a proof-of-concept (PoC) test plan that rigorously evaluates AI claims.

PM: Technical Deep Dive and PoC Execution

- Key questions to ask vendors about data sources, model training, false positive rates, and update cycles.
- Hands-on PoC testing: simulating attack patterns and evaluating detection and response efficacy.
- Case Study: Evaluating two competing AI-powered intrusion detection systems.

Day 3: Implementation and Integration

AM: Architecting for AI

- Integration strategies: Connecting AI applications to existing SIEM, SOAR, and ticketing systems.
- Data pipeline requirements: Ensuring clean, relevant, and sufficient data feeds for AI tools.
- Managing the handoff: from AI-driven alerting to human investigation and response.

PM: Change Management and Tuning

- Upskilling the SOC: Training analysts to work with AI-generated insights and alerts.
- The continuous tuning cycle: Calibrating models to your environment and reducing noise.
- Workshop: Tuning an AI-based alert system to minimize false positives without missing true threats.

Course Outline

Day 4: Managing Risks and Ensuring Governance

AM: The Risks of Your AI Security Tools

- Adversarial AI: Understanding and defending against model poisoning, evasion attacks, and data manipulation aimed at your defenses.
- Ensuring Explainability: Moving from “black box” to “glass box” – why did the AI flag this event?
- Addressing Bias: Ensuring your AI security tools don’t create blind spots or target specific groups.

PM: Governance, Compliance, and Ethics

- Establishing AI governance frameworks for security: accountability, oversight, and review processes.
- Compliance considerations (GDPR, EU AI Act): How using AI for security monitoring intersects with privacy regulations.
- Group Discussion: Developing an acceptable use policy for AI security monitoring.

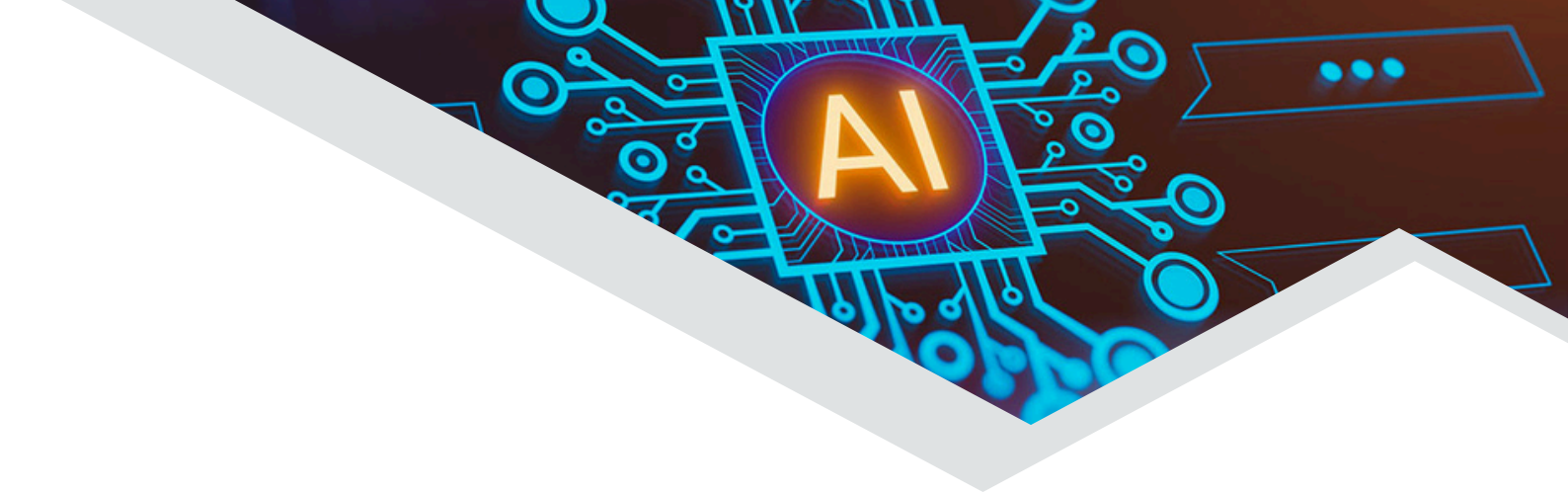
Day 5: Strategy, ROI, and the Future

AM: Measuring Success and Building the Business Case

- Defining KPIs for AI security tools: Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), alert fatigue reduction, and workload deflection.
- Calculating ROI: Quantifying efficiency gains, risk reduction, and cost savings.
- Communicating value to the board and other non-technical stakeholders.

PM: Capstone Project and Future Trends

- **Capstone Exercise:** Teams are given a scenario and budget to select an AI security portfolio, justifying their choices based on organizational need, integration, and risk.
- **Future Trends:** Generative AI in security, autonomous response, and the evolving AI threat landscape.
- Course Wrap-Up: Developing a personal strategic action plan for AI security adoption.



المقدمة

يشهد مشهد الأمن السيبراني تحولاً جذرياً. فمع تزايد استخدام الخصوم للذكاء الاصطناعي لشن هجمات آلية متطورة، لم تعد آليات الدفاع التقليدية كافية. توفر أدوات الأمن المدعومة بالذكاء الاصطناعي إمكانية الكشف التنبئي عن التهديدات، والاستجابة الآلية، وقابلية توسع لا مثيل لها. إلا أن اختيار تطبيق أمن الذكاء الاصطناعي المناسب محفوف بالتعقيد، وإدارته تُطرح تحديات فريدة تتعلق بسهولة التفسير والتكامل والتلاعب بالخصم.

صُممت هذه الدورة المكثفة، التي تمتد لخمسة أيام، لرواد وممارسي الأمن السيبراني. وتوفر إطارًا استراتيجيًا للتنقل في سوق حلول أمن الذكاء الاصطناعي المزدحم، بدءًا من أنظمة إدارة الأحداث الأمنية (SIEMs) وأنظمة الاستجابة للحوادث (EDRs) المدعومة بالذكاء الاصطناعي، وصولًا إلى أدوات اختبار الاختراق المستقلة. سيتعلم المشاركون كيفية تقييم الموردين بشكل نقدي، ودمج أدوات الذكاء الاصطناعي في هياكل الأمن الحالية، وإرساء حوكمة متينة لضمان فعالية هذه الأنظمة القوية وأخلاقيتها ومرونتها في مواجهة الهجمات.

طريقة التدريب

- التقييم المسبق
- تدريب جماعي مباشر
- استخدام أمثلة واقعية ودراسات حالة وتمارين
- مشاركة ونقاش تفاعلي
- عرض تقديمي باستخدام باور بوينت، وشاشة LCD، ولوح ورقي
- أنشطة واختبارات جماعية
- يحصل كل مشارك على ملف يحتوي على نسخة من العرض التقديمي
- شرائح ومطبوعات
- التقييم اللاحق

أهداف الدورة

عند الانتهاء من هذه الدورة، سيكون المشاركون قادرين على:

- **تقييم حلول أمان الذكاء الاصطناعي:** قم بتقييم القدرات والمطالبات والتكنولوجيا الأساسية لتطبيقات الأمان المدعومة بالذكاء الاصطناعي عبر فئات مختلفة (على سبيل المثال، اكتشاف التهديدات، ومنع الاحتيال، وإدارة الثغرات الأمنية).
- **فهم مشهد تهديدات الذكاء الاصطناعي:** تحديد كيفية استخدام المهاجمين للذكاء الاصطناعي (على سبيل المثال، البرامج الضارة المدعومة بالذكاء الاصطناعي، والتزييف العميق للهندسة الاجتماعية، والهجمات المعادية) لتبرير وتوجيه استثمارات أمن الذكاء الاصطناعي.
- **إدارة دورة حياة أمان الذكاء الاصطناعي:** تطوير العمليات اللازمة للإدارة المستمرة ومراقبة وضبط أدوات أمان الذكاء الاصطناعي للحفاظ على الفعالية وتقليل الإيجابيات/السلبيات الخاطئة.
- **دمج الذكاء الاصطناعي في بنية الأمن:** تصميم استراتيجية لدمج أدوات الذكاء الاصطناعي الجديدة بسلاسة مع البنية التحتية الأمنية الحالية (SOAR، SIEM، وما إلى ذلك) للحصول على وضع دفاعي متماسك.
- **تخفيف المخاطر الخاصة بالذكاء الاصطناعي:** معالجة المخاطر الفريدة مثل تسميم النماذج، وتحيز البيانات، والشفافية الخوارزمية، وثغرات سلسلة التوريد في منتجات أمان الذكاء الاصطناعي.
- **بناء دراسة حالة ونموذج عائد الاستثمار:** حساب وتوضيح قيمة وعائد الاستثمار لتطبيقات أمن الذكاء الاصطناعي المقترحة للقيادة التنفيذية.

من ينبغي أن يهتم؟

تم تصميم هذه الدورة للمحترفين المسؤولين عن تأمين أصول المنظمة واتخاذ قرارات الاستثمار في التكنولوجيا:

- **كبار مسؤولي أمن المعلومات (CISOs) ونائبيهم**
- **مهندسو ومهندسو الأمن**
- **مديرو ومحللو مركز العمليات الأمنية**
- **مديري مخاطر تكنولوجيا المعلومات والامتثال**
- **أعضاء فريق مركز عمليات الأمن (SOC)**
- **متخصصون في أمن الشبكات**
- **مديري تكنولوجيا المعلومات ورؤساء البنية التحتية**
- **مستشارو ومدققو الأمن السيبراني**
- **متخصصون في المشتريات متخصصون في تكنولوجيا الأمن**

محتويات الكورس

اليوم الأول أساسيات الذكاء الاصطناعي في الأمن السيبراني

الذكاء الاصطناعي في مواجهة الذكاء الاصطناعي في مجال الأمن السيبراني

- كيف يستخدم المهاجمون الذكاء الاصطناعي: الاستغلال الآلي، والتصيد الذكي، والتزييف العميق، وتقنيات التهرب.
- كيف يستخدم المدافعون الذكاء الاصطناعي: البحث عن التهديدات، واكتشاف الشذوذ، والاستجابة الآلية (SOAR)، والتحليلات السلوكية.
- مفاهيم الذكاء الاصطناعي الأساسية لمحترفي الأمن: التعلم الخاضع للإشراف مقابل التعلم غير الخاضع للإشراف، ومعالجة اللغة الطبيعية، وتحليل الرسوم البيانية في سياق الأمان.

مشهد تطبيقات أمن الذكاء الاصطناعي

- رسم خريطة للنظام البيئي للبائعين: الذكاء الاصطناعي في EDR وXDR وSIEM وNDR والكشف عن الاحتيال وإدارة وضع الأمان السحابي (CSPM).
- فهم "الذكاء الاصطناعي" في المنتج: من المصطلحات التسويقية إلى قدرات التعلم الآلي الحقيقية.
- ورشة عمل: تفكيك بيانات البائعين والأوراق البيضاء

اليوم الثاني عملية الاختيار: تقييم وشراء أدوات الذكاء الاصطناعي

تحديد المتطلبات وبناء القائمة المختصرة

- مواءمة اختيار أدوات الذكاء الاصطناعي مع ملف المخاطر التنظيمية واستراتيجية الأمن.
- تطوير إطار معايير التقييم المرجح: الدقة والأداء وقدرات التكامل والتكلفة وقابلية البائعين للتطبيق.
- إنشاء خطة اختبار إثبات المفهوم (PoC) التي تقوم بتقييم ادعاءات الذكاء الاصطناعي بشكل صارم.

الغوص العميق في المجال التقني وتنفيذ إثبات المفهوم

- الأسئلة الرئيسية التي يجب طرحها على البائعين حول مصادر البيانات، وتدريب النموذج، ومعدلات الإيجابيات الخاطئة، ودورات التحديث.
- اختبار PoC العملي: محاكاة أنماط الهجوم وتقييم فعالية الكشف والاستجابة.
- دراسة الحالة: تقييم نظامين متنافسين للكشف عن التطفل يعتمدان على الذكاء الاصطناعي

اليوم الثالث التنفيذ والتكامل

هندسة الذكاء الاصطناعي

- استراتيجيات التكامل: ربط تطبيقات الذكاء الاصطناعي بأنظمة SIEM وSOAR والتذاكر الحالية.
- متطلبات خط أنابيب البيانات: ضمان توفير بيانات نظيفة وذات صلة وكافية لأدوات الذكاء الاصطناعي.
- إدارة عملية التسليم: من التنبيهات التي تعتمد على الذكاء الاصطناعي إلى التحقيق والاستجابة البشرية.

إدارة التغيير والضبط

- تطوير مهارات مركز العمليات الأمنية: تدريب المحللين على العمل مع الرؤى والتنبيهات التي تولدها الذكاء الاصطناعي.
- دورة الضبط المستمر: معايرة النماذج لبيئتك وتقليل الضوضاء.
- ورشة عمل: ضبط نظام تنبيه قائم على الذكاء الاصطناعي لتقليل الإيجابيات الخاطئة دون تفويت التهديدات الحقيقية.

محتويات الكورس

اليوم الرابع إدارة المخاطر وضمان الحوكمة

مخاطر أدوات أمن الذكاء الاصطناعي الخاصة بك

- الذكاء الاصطناعي المعادي: فهم تسميم النماذج وهجمات التهرب والتلاعب بالبيانات التي تستهدف دفاعاتك والدفاع ضدها.
- ضمان إمكانية التفسير: الانتقال من "الصندوق الأسود" إلى "الصندوق الزجاجي" - لماذا قامت الذكاء الاصطناعي بتمييز هذا الحدث؟
- معالجة التحيز: التأكد من أن أدوات أمان الذكاء الاصطناعي الخاصة بك لا تخلق نقاطًا عمياء أو تستهدف مجموعات محددة.

الحوكمة والامتثال والأخلاقيات

- إنشاء أطر حوكمة الذكاء الاصطناعي للأمن: المساءلة والإشراف وعمليات المراجعة.
- اعتبارات الامتثال (اللائحة العامة لحماية البيانات، وقانون الذكاء الاصطناعي في الاتحاد الأوروبي): كيف يتقاطع استخدام الذكاء الاصطناعي لمراقبة الأمن مع لوائح الخصوصية.
- مناقشة جماعية: تطوير سياسة الاستخدام المقبولة لمراقبة أمن الذكاء الاصطناعي.

اليوم الخامس الاستراتيجية، والعائد على الاستثمار، والمستقبل

قياس النجاح وبناء دراسة الجدوى

- تحديد مؤشرات الأداء الرئيسية لأدوات أمان الذكاء الاصطناعي: متوسط الوقت للكشف (MTTD)، ومتوسط الوقت للاستجابة (MTTR)، وتقليل إجهاد التنبيه، وتحويل عبء العمل.
- حساب العائد على الاستثمار: قياس مكاسب الكفاءة، وخفض المخاطر، وتوفير التكاليف.
- توصيل القيمة إلى مجلس الإدارة وأصحاب المصلحة غير الفنيين الآخرين.

مشروع التخرج والاتجاهات المستقبلية

- **تمرين التخرج:** يتم منح الفرق سيناريو وميزانية لاختيار محفظة أمان الذكاء الاصطناعي، وتبرير اختياراتهم بناءً على احتياجات المنظمة والتكامل والمخاطر.
- **الاتجاهات المستقبلية:** الذكاء الاصطناعي التوليدي في مجال الأمن، والاستجابة المستقلة، ومشهد التهديدات المتطورة للذكاء الاصطناعي.
- اختتام الدورة: تطوير خطة عمل استراتيجية شخصية لتبني أمن الذكاء الاصطناعي

Terms & Conditions

Complete & Mail to future centre or email

Info@futurecentre.com

Cancellation and Refund Policy

Delegates have 14 days from the date of booking to cancel and receive a full refund or transfer to another date free of charge. If less than 14 days' notice is given, then we will be unable to refund or cancel the booking unless on medical grounds. For more details about the Cancellation and Refund policy, please visit
https://futurecentre.net/

Registration & Payment

Please complete the registration form on the course page & return it to us indicating your preferred mode of payment. For further information, please get in touch with us

Course Materials

The course material, prepared by the future centre, will be digital and delivered to candidates by email

Certificates

Accredited Certificate of Completion will be issued to those who attend & successfully complete the programme.

Travel and Transport

We are committed to picking up and dropping off the participants from the airport to the hotel and back.

Registration & Payment

Complete & Mail to future centre or email

Info@futurecentre.com

Registration Form

- Full Name (Mr / Ms / Dr / Eng) .....
- Position .....
- Telephone / Mobile .....
- Personal E-Mail .....
- Official E-Mail .....
- Company Name .....
- Address .....
- City / Country .....

Payment Options

- ☐ Please invoice me
- ☐ Please invoice my company

Course Calander:

18/05/2026 - 22/05/2026 Click Now

VENUES

- LONDON
- BARCELONA
- KUALA LUMPER
- AMSTERDAM
- DAMASCUS
- ISTANBUL
- SINGAPORE
- PARIS
- DUBAI

OUR PARTNERS

THANK YOU

CONTACT US

+963 112226969

+963 953865520

Info@futurecentre.com

Damascus - Victoria - behind Royal Semiramis hotel

FUTURE CENTRE
مركز المستقبل

futurecentre.net