الذكاء الاصطناعي في أمن المعلومات: الكشف المتنبئ عن التهديدات في السيبرانية

المدة: 5 يوم

اللغة: ar

كود الكورس: PI2 - 118

هدف الكورس

مع نهاية هذه الدورة، سيكون المشاركون قادرين على:

- استيعاب كيفية توظيف الذكاء الاصطناعي وتعلم الآلة في مجال الأمن السيبراني.
- تحديد الأنماط والشذوذ التي تشير إلى التهديدات السيبرانية باستخدام أدوات الذكاء الاصطناعي.
- تنفيذ عمليات الكشف عن التسلل وتحليل السلوك المدعومة بالذكاء الاصطناعي.
- استكشاف آليات الدفاع الذاتي والاستجابة التلقائية للحوادث.
- تقييم حلول الذكاء الاصطناعي للتنبؤ بالتهديدات وتوفير الحماية في الوقت الفعلي.
- معالجة قضايا الخصوصية والتحيز والمساءلة في أنظمة الأمان المدعومة بالذكاء الاصطناعي.
- تصميم خارطة طريق لدمج الذكاء الاصطناعي في أطر الأمن السيبراني.

الجمهور

تُعد هذه الدورة مثالية لـ:

- محللي الأمن السيبراني ومتخصصي أمن تقنية المعلومات.
- أعضاء فرق مركز عمليات الأمن (SOC).
- مهندسي الشبكات والبنية التحتية.
- مهندسي الذكاء الاصطناعي وتعلم الآلة في مجال الأمن.
- مديري أمن المعلومات (CISOs)، ومديري التكنولوجيا (CTOs)، وقادة إدارة المخاطر التقنية.
- الهاكرز الأخلاقيين ومختبري الاختراق.
- وحدات الأمن السيبراني في القطاع الحكومي والعسكري.

منهجية التدريب

يجمع هذا المقرر بين الأطر النظرية والعروض التقنية والتمارين المستندة إلى السيناريوهات واستعراض الأدوات. سيقوم المشاركون باستكشاف منصات الأمان الحالية للذكاء الاصطناعي، وتحليل محاكاة الهجمات، وتصميم بروتوكولات دفاع معززة بالذكاء الاصطناعي. تركز الأنشطة الجماعية على تقييم المخاطر والتنفيذ الأخلاقي.

الملخص

مع تزايد تعقيد وتكرار التهديدات السيبرانية، لم تعد الأدوات الأمنية التقليدية كافية بمفردها. يلعب الذكاء الاصطناعي الآن دورًا حيويًا في تحويل الأمن السيبراني من حماية تفاعلية إلى دفاع استباقي. من خلال استخدام التعلم الآلي والأتمتة، تستطيع أنظمة الذكاء الاصطناعي اكتشاف الشذوذ، والتنبؤ بالهجمات، وحتى الاستجابة للتهديدات بشكل ذاتي في الوقت الفعلي.

تقدم هذه الدورة استكشافًا عمليًا لكيفية دمج الذكاء الاصطناعي في عمليات الأمن السيبراني الحديثة. سيتعلم المشاركون عن اكتشاف التهديدات المدعوم بالذكاء الاصطناعي، وتحليلات السلوك، وأنظمة الاستجابة الذاتية، والاعتبارات الأخلاقية لتفويض القرارات للآلات الذكية. من خلال أمثلة واقعية ومحاكاة عملية، سيكتسب المتعلمون المهارات اللازمة لتعزيز الدفاعات الرقمية باستخدام تقنيات الذكاء الاصطناعي.

محتوى الكورس والمخطط الزمني

Section 1: The Role of AI in Modern Cybersecurity

- Cybersecurity challenges in a hyperconnected world.
- Limitations of traditional threat detection systems.
- Introduction to AI and machine learning in security.
- Key technologies: supervised vs. unsupervised learning, anomaly detection.
- Cyber threat landscape: phishing, ransomware, zero-day exploits.
- Case study: How AI stopped a real-world cyberattack.

Section 2: Predictive Threat Detection with AI

- Behavioral analysis and user activity modeling.
- Machine learning for threat hunting and anomaly spotting.
- AI in email security, fraud detection, and phishing prevention.
- Natural Language Processing (NLP) in analyzing malicious communication.
- Building datasets and training security models.
- Hands-on demo: AI-based threat prediction in SIEM systems.

Section 3: Autonomous Response and Real-Time Defense

- What is autonomous defense? From alert to action.

- .SOAR (Security Orchestration, Automation, and Response) platforms
- .Automated patching, isolation, and mitigation techniques
- .AI-powered endpoint protection and network firewalls
- .Incident response bots and playbooks
- .Simulation: Responding to a breach using AI automation

Section 4: Challenges, Risks, and Ethical Considerations

- .Risks of false positives/negatives and automation errors
- .Bias in security models and fairness in AI responses
- .Balancing speed with human oversight
- .Privacy and legal implications in AI-driven surveillance
- .Transparency and explainability in AI decisions
- .Governance models for responsible AI in cybersecurity

Section 5: Implementing AI in Cyber Defense Strategy

- .Integrating AI tools into existing cybersecurity infrastructure
- .Choosing the right platforms and vendors
- .Skills and team requirements for AI-enhanced operations
- .Building cross-functional collaboration between AI and security teams
- .Metrics for success: detection rate, response time, incident reduction
- .Roadmap: Designing your AI-in-cybersecurity action plan

تفاصيل الشهادة

عند إتمام هذه الدورة التدريبية بنجاح، سيحصل المشاركون على شهادة إتمام التدريب من Holistique Training. وبالنسبة للذين يحضرون ويكملون الدورة التدريبية عبر الإنترنت، سيتم تزويدهم بشهادة إلكترونية (e-Certificate) من Holistique Training.

شهادات Holistique Training وخدمة اعتماد التطوير المهني (BAC) معتمدة من المجلس البريطاني للتقييم المستمر (CPD)، كما أنها معتمدة وفق معايير ISO 9001 وISO 21001 وISO 29993.

لهذه الدورة من خلال شهاداتنا، وستظهر هذه النقاط على شهادة إتمام (CPD) يتم منح نقاط التطوير المهني المستمر واحدة عن كل ساعة CPD يتم منح نقطة، CPD ووفقًا لمعايير خدمة اعتماد Holistique Training. التدريب من لأي دورة واحدة نقدمها حاليًا CPD حضور في الدورة. ويمكن المطالبة بحد أقصى قدره 50 نقطة.

التصنيفات

الذكاء الاصطناعي وإدارة البيانات, التكنولوجيا

مقالات ذات صلة

The Importance of Cyber Security Training in Today's World

Discover why cybersecurity training is critical in today's digital world. Learn about threats, training benefits, legal compliance, and risk reduction for organisations.