

القيادة المتقدمة في الأمن السيبراني وحوكمة الذكاء الاصطناعي وتحليل البيانات

15 – 19 مارس 2027

القاهرة

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

القيادة المتقدمة في الأمن السيبراني وحوكمة الذكاء الاصطناعي وتحليل البيانات

المرجع: 81790_103600588 **التاريخ:** 15 – 19 مارس 2027 **المكان:** القاهرة **الرسوم:** 4100 Euro

نظرة عامة على الدورة:

القيادة المتقدمة في الأمن السيبراني وحوكمة الذكاء الاصطناعي وتحليل البيانات لمديري البنية التحتية لتكنولوجيا المعلومات هو برنامج تدريبي تنفيذي شامل في الأمن السيبراني لمدة أسبوع مصمم لكبار المتخصصين في التكنولوجيا الذين يسعون للحصول على تدريب قيادة الأمن السيبراني بمستوى يضاهي دورة إعداد CCISO. يجمع البرنامج بين مبادئ تدريب كبير مسؤولي أمن المعلومات والقيادة التكنولوجية المتقدمة، مما يمكّن المشاركين من مواءمة مبادرات الأمن السيبراني مع أهداف الأعمال، وإدارة مخاطر المؤسسة، وقيادة التحول الرقمي الآمن.

تغطي الدورة استراتيجية الأمن السيبراني وحوكمته، وإدارة الأمن السيبراني للمؤسسات، وأطر حوكمة الأمن السيبراني، وإدارة برامج الأمن، وقيادة عمليات الأمن، واتخاذ القرارات في الأمن السيبراني للقادة. سيستكشف المشاركون إدارة أمن البنية التحتية لتكنولوجيا المعلومات، وتدريب هندسة البنية التحتية الآمنة، وتدريب أمن البنية التحتية السحابية، وأمن البنية التحتية الهجينة، وحوكمة البنية التحتية والامتثال، ومرونة البنية التحتية واستمرارية الأعمال.

بالإضافة إلى ذلك، يدمج البرنامج تدريب الذكاء الاصطناعي المتقدم، ومفاهيم برنامج القيادة التنفيذية للذكاء الاصطناعي، وحوكمة الذكاء الاصطناعي وإدارة المخاطر، والقيادة المسؤولة للذكاء الاصطناعي، والذكاء الاصطناعي التوليدي للمديرين التنفيذيين في التكنولوجيا. تقدم وحدات تدريب علوم البيانات المتقدمة تدريب تحليل البيانات الاستراتيجي، وحوكمة البيانات وتحليلها، وتدريب التحليلات التنبؤية، واستراتيجية وإدارة البيانات الضخمة، واتخاذ القرارات المدفوعة بالبيانات.

بالاعتماد على أطر قيادة الأمن السيبراني، ونماذج الحوكمة، ومفاهيم استراتيجية الذكاء الاصطناعي، ومنهجيات التحليلات المتقدمة، سيطور المشاركون قدرات على المستوى التنفيذي لقيادة منظمات تكنولوجية آمنة، مدفوعة بالبيانات، ومرنة.

AGILE LEADERS
Training Center

الجمهور المستهدف:

- مديري البنية التحتية لتكنولوجيا المعلومات
- مديري البنية التحتية والعمليات
- مديري أمن المعلومات
- مديري الأمن السيبراني
- مديري الشبكات ومراكز البيانات
- مديري البنية التحتية السحابية
- مديري تكنولوجيا المعلومات
- مديري التكنولوجيا
- مهندسي المؤسسات
- مهندسي الأمن
- مديري التحول الرقمي
- الطامحين لشغل مناصب كبار مسؤولي أمن المعلومات وقادة الأمن

الأقسام المستهدفة:

- قسم أمن المعلومات
- مركز عمليات الأمن السيبراني SOC
- قسم البنية التحتية لتكنولوجيا المعلومات
- عمليات السحابة ومراكز البيانات
- قسم هندسة المؤسسات
- مكتب التحول الرقمي
- قسم إدارة المخاطر
- الحوكمة والمخاطر والامتثال GRC
- فرق تحليل البيانات وذكاء الأعمال
- فرق الذكاء الاصطناعي والابتكار

تستفيد هذه الأقسام من استراتيجية الأمن السيبراني وحوكمته، وإدارة الأمن السيبراني للمؤسسات، واستراتيجية أمن البنية التحتية، وحوكمة الذكاء الاصطناعي وإدارة المخاطر، ومبادرات برنامج التحليلات التنفيذية للبيانات، وقدرات الأمن السيبراني للبنية التحتية الحيوية.

AGILE LEADERS
Training Center

القطاعات المستهدفة:

- الاتصالات
- الخدمات المصرفية والمالية
- القطاع الحكومي والعام
- الطاقة والمرافق
- النفط والغاز
- الرعاية الصحية
- التأمين
- الطيران والنقل
- التصنيع
- التكنولوجيا والبرمجيات
- مراكز البيانات ومقدمي الخدمات السحابية
- منظمات البنية التحتية الوطنية الحيوية

أهداف الدورة:

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطوير برامج استراتيجية وحوكمة الأمن السيبراني على مستوى المؤسسة.
- تطبيق أطر حوكمة الأمن السيبراني وممارسات قيادة الأمن التنفيذية.
- قيادة مبادرات إدارة الأمن السيبراني للمؤسسات بما يتماشى مع أهداف الأعمال.
- إجراء تمارين تدريبية في إدارة مخاطر الأمن السيبراني وتحديد أولويات المخاطر.
- تصميم استراتيجية أمن البنية التحتية للبيئات السحابية والهجينة والمحلية.
- تعزيز إدارة أمن البنية التحتية لتكنولوجيا المعلومات وهندسة البنية التحتية الآمنة.
- تحسين برامج حوكمة البنية التحتية والامتثال.
- قيادة مبادرات الأمن السيبراني للبنية التحتية الحيوية وتخطيط المرونة.
- تنفيذ استراتيجية الذكاء الاصطناعي لقادة التكنولوجيا وخرائط طريق تحول الذكاء الاصطناعي للمؤسسات.
- إنشاء ضوابط حوكمة الذكاء الاصطناعي وإدارة المخاطر لتبني الذكاء الاصطناعي المسؤول.
- تقييم الذكاء الاصطناعي التوليدي للمديرين التنفيذيين في التكنولوجيا وقدرات الأمن المدفوعة بالذكاء الاصطناعي.
- تطبيق تقنيات تدريب علوم البيانات المتقدمة على اتخاذ القرارات في الأمن السيبراني.
- الاستفادة من اتخاذ القرارات المدفوعة بالبيانات ومناهج تدريب تحليل البيانات الاستراتيجي.
- الاستفادة من تدريب التحليلات التنبؤية وتطبيقات التعلم الآلي المتقدمة للتنبؤ بالمخاطر.
- إنشاء لوحات معلومات تنفيذية للأمن السيبراني والتحليلات لتقارير مجلس الإدارة.

منهجية التدريب:

يجمع هذا البرنامج التعليمي التنفيذي التفاعلي للغاية في الأمن السيبراني بين مناقشات على المستوى التنفيذي، ومحاكاة القيادة، وورش عمل الحوكمة، وتمارين التخطيط الاستراتيجي، ودراسات حالة واقعية. سيفحص المشاركون تحديات قيادة الأمن السيبراني، وهياكل الحوكمة، وقيادة الاستجابة للحوادث، وممارسات إدارة المخاطر الرقمية المستوحاة من مسؤوليات كبير مسؤولي أمن المعلومات الحديثة.

تؤكد المنهجية على التطبيق العملي من خلال سيناريوهات حوكمة الأمن السيبراني، وتقييمات مخاطر المؤسسة، وتمارين التواصل على مستوى مجلس الإدارة، وورش عمل تطوير استراتيجية الأمن، ومحاكاة اتخاذ القرارات التنفيذية. سيقوم المشاركون بتقييم الاستثمارات الأمنية، ومبادرات إدارة برامج الأمن، واستراتيجيات مرونة البنية التحتية باستخدام حالات أعمال واقعية.

تتضمن وحدات الذكاء الاصطناعي المتقدمة مناقشات تنفيذية حول تبني الذكاء الاصطناعي، والقيادة المسؤولة للذكاء الاصطناعي، وحوكمة الذكاء الاصطناعي وإدارة المخاطر، وتحول الذكاء الاصطناعي للمؤسسات. تركز جلسات علوم البيانات على دورات حياة تحليل البيانات، ومفاهيم التحليلات التنبؤية، وحوكمة البيانات، وتفسير ذكاء الأعمال، وممارسات القيادة المدفوعة بالبيانات.

سيشارك المشاركون في تمارين جماعية، وورش عمل ميسرة، ومراجعات الأقران، وأنشطة التخطيط الاستراتيجي، ومحاكاة الأزمات السيبرانية، وجلسات تأمل موجهة. تعطي الدورة الأولوية للتفكير التنفيذي، ومواءمة الأعمال، وفعالية القيادة، والمرونة التنظيمية بدلاً من تفاصيل التنفيذ التقني.

أدوات الدورة:

ملاحظة: لا يتم توفير الأدوات. سيتلقى المشاركون رؤى وأمثلة وأطر عمل وعروض توضيحية للأدوات ذات الصلة عند الاقتضاء.

- قوالب أطر حوكمة الأمن السيبراني التنفيذية
- نماذج تطوير استراتيجية الأمن السيبراني
- قوالب تقييم مخاطر الأمن السيبراني
- أطر إدارة برامج الأمن
- نماذج تقييم نضج الأمن السيبراني
- قوائم مراجعة استراتيجية أمن البنية التحتية
- أمثلة حوكمة أمن السحابة
- أطر حوكمة الذكاء الاصطناعي وإدارة المخاطر
- قوالب تقييم الذكاء الاصطناعي المسؤول
- خرائط طريق تبني الذكاء الاصطناعي للمؤسسات
- أطر حوكمة البيانات والتحليلات
- نماذج لوحات المعلومات التنفيذية
- قوالب مؤشرات الأداء الرئيسية ومقاييس الأمن السيبراني
- قوالب تقارير مجلس الإدارة
- أدلة قيادة الاستجابة للحوادث
- قوائم مراجعة تقييم مرونة البنية التحتية
- نماذج إدارة المخاطر الرقمية
- دراسات حالة اتخاذ القرارات التنفيذية

AGILE LEADERS
Training Center

محتوى الدورة

اليوم الأول: حوكمة الأمن السيبراني واستراتيجيته والقيادة التنفيذية

- **الموضوع 1:** كبير مسؤولي أمن المعلومات الحديث ودور قيادة الأمن السيبراني
- **الموضوع 2:** أطر وسياسات حوكمة الأمن السيبراني
- **الموضوع 3:** تطوير استراتيجية الأمن للمؤسسات
- **الموضوع 4:** إعداد تقارير الأمن السيبراني والتواصل على مستوى مجلس الإدارة
- **الموضوع 5:** مهارات قيادة الأمن السيبراني واتخاذ القرارات
- **الموضوع 6:** بناء ثقافة تنظيمية تركز على الأمن أولاً
- **تأمل ومراجعة:** تحديات القيادة والأولويات الاستراتيجية

اليوم الثاني: إدارة المخاطر السيبرانية والامتثال وحوكمة برامج الأمن

- **الموضوع 1:** أطر إدارة المخاطر السيبرانية للمؤسسات
- **الموضوع 2:** تحمل المخاطر، وتحديد كمية المخاطر وتحديد أولوياتها
- **الموضوع 3:** إدارة برامج الأمن وحوكمتها
- **الموضوع 4:** الامتثال التنظيمي وقيادة التدقيق
- **الموضوع 5:** إدارة مخاطر الأمن السيبراني للجهات الخارجية وسلسلة التوريد
- **الموضوع 6:** مقاييس الأمن السيبراني، ومؤشرات الأداء الرئيسية، ولوحات المعلومات التنفيذية
- **تأمل ومراجعة:** إدارة المخاطر على مستوى المؤسسة

AGILE LEADERS
Training Center

اليوم الثالث: أمن البنية التحتية، أمن السحابة، والمرونة السيبرانية

- **الموضوع 1:** هندسة أمن البنية التحتية للمؤسسات
- **الموضوع 2:** أمن البنية التحتية السحابية والهجينة
- **الموضوع 3:** إدارة الهوية والوصول والحسابات ذات الامتيازات
- **الموضوع 4:** مراكز عمليات الأمن وذكاء التهديدات
- **الموضوع 5:** قيادة الاستجابة للحوادث وإدارة الأزمات
- **الموضوع 6:** استمرارية الأعمال، التعافي من الكوارث، والمرونة
- **تأمل ومراجعة:** القيادة خلال حوادث الأمن السيبراني

اليوم الرابع: حوكمة الذكاء الاصطناعي المتقدمة والأمن السيبراني المدعوم بالذكاء الاصطناعي

- **الموضوع 1:** أساسيات الذكاء الاصطناعي للمديرين التنفيذيين
- **الموضوع 2:** الذكاء الاصطناعي التوليدي وتقنيات الذكاء الاصطناعي الناشئة
- **الموضوع 3:** حوكمة الذكاء الاصطناعي، الأخلاقيات، والذكاء الاصطناعي المسؤول
- **الموضوع 4:** إدارة مخاطر الذكاء الاصطناعي وضوابط الأمن
- **الموضوع 5:** تطبيقات الذكاء الاصطناعي في الكشف عن التهديدات السيبرانية والاستجابة لها
- **الموضوع 6:** تأمين أنظمة الذكاء الاصطناعي والبنية التحتية المدفوعة بالذكاء الاصطناعي
- **تأمل ومراجعة:** تحديات قيادة وحوكمة الذكاء الاصطناعي

AGILE LEADERS
Training Center

اليوم الخامس: تحليل البيانات، استخبارات الأمن، واتخاذ القرارات التنفيذية

- **الموضوع 1:** تحليل البيانات الاستراتيجي لقادة تكنولوجيا المعلومات
- **الموضوع 2:** إدارة بيانات الأمن السيبراني وحوكمتها
- **الموضوع 3:** التحليلات التنبؤية للتنبؤ بالمخاطر والتهديدات
- **الموضوع 4:** استخبارات الأمن والتقارير التنفيذية
- **الموضوع 5:** إعداد ميزانية الأمن السيبراني، والاستثمار، وإدارة عائد الاستثمار
- **الموضوع 6:** التوجهات المستقبلية في الذكاء الاصطناعي، الأمن السيبراني، وقيادة البنية التحتية
- **تأمل ومراجعة:** تخطيط الإجراءات التنفيذية وخارطة طريق القيادة

الأسئلة الشائعة

ما هي المؤهلات أو المتطلبات المسبقة المحددة المطلوبة للمشاركين قبل التسجيل في الدورة؟

يجب أن يكون لدى المشاركين خبرة في البنية التحتية لتكنولوجيا المعلومات، أو الأمن السيبراني، أو عمليات السحابة، أو إدارة تكنولوجيا المؤسسات، أو الأدوار القيادية ذات الصلة. بينما تعتبر الخبرة التقنية العميقة مفيدة، تركز الدورة على القيادة التنفيذية، والحوكمة، وإدارة المخاطر، واستراتيجية الذكاء الاصطناعي، واتخاذ القرارات المدفوعة بالبيانات.

ما هي مدة كل جلسة يومية، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

تُصمم جلسة كل يوم بشكل عام لتستمر حوالي 4-5 ساعات، مع فترات راحة وأنشطة تفاعلية متضمنة. تمتد مدة الدورة الإجمالية لخمسة أيام، أي ما يقرب من 20-25 ساعة من التدريس.

كيف تختلف هذه الدورة عن دورة شهادة الأمن السيبراني التقنية؟

بخلاف دورات الأمن التقنية التي تركز على الأدوات والتكوين العملي، يركز هذا البرنامج على تدريب قيادة الأمن السيبراني، والحوكمة التنفيذية، واستراتيجية الأمن، وإدارة المخاطر، وقيادة الذكاء الاصطناعي، والإشراف على أمن البنية التحتية، ومسؤوليات اتخاذ القرارات الاستراتيجية المتوقعة من كبار قادة التكنولوجيا والطامحين لشغل مناصب كبار مسؤولي أمن المعلومات.

AGILE LEADERS
Training Center

كيف تختلف هذه الدورة عن دورات تدريب قيادة الأمن السيبراني الأخرى:

تركز معظم دورات الأمن السيبراني بشكل أساسي على الضوابط التقنية، أو عمليات الأمن، أو التحضير لامتحانات الشهادات. يتخذ هذا البرنامج منظورًا تنفيذيًا أوسع من خلال دمج تدريب قيادة الأمن السيبراني، وإدارة الأمن السيبراني للمؤسسات، وتدريب الذكاء الاصطناعي المتقدم، وتدريب علوم البيانات المتقدمة في إطار قيادي موحد.

تم تصميم الدورة خصيصًا لمديري البنية التحتية لتكنولوجيا المعلومات وكبار قادة التكنولوجيا الذين يجب عليهم الموازنة بين الأمن، والابتكار، والمرونة التشغيلية، وتبني الذكاء الاصطناعي، واتخاذ القرارات المدفوعة بالبيانات. يتعلم المشاركون كيفية مواءمة الأمن السيبراني مع استراتيجية الأعمال، والتواصل بفعالية مع المديرين التنفيذيين ومجالس الإدارة، وإدارة المخاطر على مستوى المؤسسة، وقيادة التحول الرقمي بأمان.

بخلاف دورات إعداد CCISO التقليدية التي تركز فقط على مجالات قيادة الأمن، يتوسع هذا البرنامج ليشمل استراتيجية الذكاء الاصطناعي لقادة التكنولوجيا، وقيادة الذكاء الاصطناعي المسؤولة، وتحول الذكاء الاصطناعي للمؤسسات، وتدريب تحليل البيانات الاستراتيجي، وقيادة ذكاء البيانات. يكتسب المشاركون فهمًا شاملاً لكيفية تقاطع الأمن السيبراني، والذكاء الاصطناعي، والتحليلات، وحوكمة البنية التحتية داخل المؤسسات الحديثة.

والنتيجة هي تجربة تطوير تنفيذي عملية تُعد القادة للإشراف على بيئات تكنولوجية آمنة، ومرنة، وذكية، ومدفوعة بالبيانات مع دعم النمو التنظيمي والابتكار.