الدورة التدريبية: الأمن السيبراني للقيادات العليا وصناع القرار



16 - 20 نوفمبر 2026
برشلونة
5900 € (للشخص الواحد)
Ref: #CYB2914_328166

مقدمة الدورة التدريبية / لمحة عامة:

في بيئة الأعمال الحديثة، لم يعد الأمن السيبراني مجرد مسؤولية تقنية، بل أصبح قضية استراتيجية على مستوى مجلس الإدارة. إن الفشل في فهم المخاطر السيبرانية ودمجها في استراتيجية الأعمال يمكن أن يؤدي إلى خسائر مالية هائلة، والإضرار بالسمعة، وفقدان ثقة العملاء. إن القيادات العليا وصناع القرار يحتاجون إلى فهم شامل للمشهد الأمني، ليس من منظور تقني بحت، بل من منظور إدارة المخاطر والحوكمة. تقدم هذه الدورة التدريبية المتخصصة للرؤساء التنفيذيين، أعضاء مجلس الإدارة، ومديري الأقسام، المعرفة والمهارات اللازمة لبناء ثقافة أمنية قوية من القمة. سنتناول في هذه الدورة مفاهيم الأمن السيبراني بلغة الأعمال، إدارة المخاطر الاستراتيجية، والاستجابة للحوادث الكبرى. سيكتسب المشاركون القدرة على تقييم الأداء الأمني، تحديد الأولويات الاستثمارية، واتخاذ قرارات مستنيرة بشأن الأمن السيبراني. تهدف الدورة إلى بناء قادة قادرين على تحويل الأمن إلى ميزة تنافسية. يستند المحتوى إلى أحدث المعايير وأفضل الممارسات الدولية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور هوارد شميت (Howard A. Schmidt)، المعروف بأعماله في حوكمة الأمن السيبراني. يقدم BIG BEN Training Center هذه الدورة لتمكين القيادات العليا من حماية المؤسسة بشكل فعال.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- الرؤساء التنفيذيون وأعضاء مجلس الإدارة.
- مديرو الأمن السيبراني (CISO).
- المديرون التنفيذيون في مختلف الأقسام.
- مديرو إدارة المخاطر والامتثال.
- المستشارون القانونيون للشركات.
- قادة الفرق وفرق الإدارة العليا.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- الجهات الحكومية وما في حكمها.
- قطاع الرعاية الصحية.
- شركات التكنولوجيا.
- شركات الطاقة.
- جميع القطاعات التي تعتمد على البنية التحتية الرقمية.

الأقسام المؤسسية المستهدفة:

- الإدارة التنفيذية.
- مجلس الإدارة.
- إدارة الأمن السيبراني.
- الإدارة القانونية.
- إدارة المخاطر.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم المخاطر السيبرانية من منظور استراتيجي.
- القدرة على دمج الأمن السيبراني في استراتيجية الأعمال.
- تقييم الأداء الأمني وتحديد مؤشرات الأداء الرئيسية (KPIs).
- إدارة المخاطر السيبرانية على مستوى المؤسسة.
- وضع خطط للاستجابة للأزمات الناتجة عن الهجمات.
- التواصل الفعال مع الأقسام الفنية حول الأمن.
- الاستثمار الأمثل في حلول الأمن السيبراني.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية تفاعلية ومحاكية للواقع، مصممة خصيصًا للقيادات العليا. سيتمكن المتدربون من خلال دراسات الحالة الواقعية لانتهاكات أمنية كبرى، وجلسات نقاش جماعية، من فهم تأثير القرارات الاستراتيجية على الأمن. تتضمن المنهجية ورش عمل عملية حول بناء إطار حوكمة أمنية، وتقييم الاستثمارات الأمنية، ووضع خطط للاستجابة للأزمات. سيتم التركيز على الجانب الاستراتيجي للأمن، وتشجيع المشاركين على التفكير في كيفية تحويل الأمن السيبراني من تكلفة إلى ميزة تنافسية. يقدم BIG BEN Training Center هذه الدورة لتمكين القادة من اتخاذ قرارات أمنية مستنيرة تدعم نمو واستمرارية المؤسسة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: الأمن السيبراني من منظور القيادة

- مقدمة في الأمن السيبراني بلغة الأعمال.
- التهديدات السيبرانية وأثرها على استراتيجية المؤسسة.
- المخاطر القانونية والسمعة المتعلقة بالأمن.
- دور القيادات العليا في الأمن السيبراني.
- حوكمة الأمن السيبراني.
- بناء ثقافة أمنية من القمة.
- التوازن بين الابتكار والأمن.

الوحدة الثانية: إدارة المخاطر السيبرانية الاستراتيجية

- تحديد المخاطر السيبرانية الرئيسية.
- تقييم تأثير المخاطر على الأعمال.
- إدارة المخاطر الأمنية بشكل استباقي.
- وضع استراتيجية شاملة للأمن السيبراني.
- تحديد أولويات الاستثمار في الأمن.
- التعامل مع المخاطر في سلسلة التوريد.
- التحليل المالي للمخاطر.

الوحدة الثالثة: اتخاذ القرار في الأزمات الأمنية

- بناء خطة للاستجابة للأزمات السيبرانية.
- القيادة أثناء الاختراق الأمني.
- التواصل الداخلي والخارجي خلال الأزمة.
- التعافي من الهجمات واستمرارية الأعمال.
- التعامل مع الجهات القانونية والجهات التنظيمية.
- تحليل الأزمات واتخاذ القرارات اللاحقة.
- الدروس المستفادة من حوادث الأمن الكبرى.

الوحدة الرابعة: الاستثمار في الأمن والقياس

- تحديد مؤشرات الأداء الرئيسية (KPIs).
- قياس فعالية برنامج الأمن السيبراني.
- إعداد ميزانية الأمن وتقديمها للإدارة.
- تحديد العائد على الاستثمار (ROI) للأمن.
- الاستثمار في التكنولوجيا والمواهب البشرية.
- تقييم حلول الأمن المختلفة.
- التقارير الأمنية للإدارة التنفيذية.

الوحدة الخامسة: مستقبل الأمن السيبراني

- التشريعات واللوائح المستقبلية.
- تأثير الذكاء الاصطناعي على الأمن.
- أمن إنترنت الأشياء (IoT) والمدن الذكية.
- استراتيجيات الأمن الاستباقي (Zero Trust).
- المرونة السيبرانية والتكيف مع التهديدات.
- التعاون مع القطاعين العام والخاص.
- تحويل الأمن إلى ميزة تنافسية.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

في ظل التطور المتسارع للتهديدات السيبرانية، كيف يمكن للقيادات العليا أن تبتكر إطار حوكمة لا يقتصر على مجرد الامتثال للوائح، بل يُنشئ ثقافة أمنية شاملة، ويُمكن المؤسسة من تحويل المخاطر إلى فرص، ويضمن أن يكون الأمن السيبراني جزءًا لا يتجزأ من الحمض النووي الاستراتيجي للشركة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الاستراتيجي على الأمن السيبراني من منظور القيادة، مما يوفر محتوى مصممًا خصيصًا لتلبية احتياجات صناع القرار. بدلاً من الغوص في التفاصيل التقنية، نغوص في التطبيق العملي لإدارة المخاطر، ووضع استراتيجيات الأمن، والتعامل مع الأزمات. تقدم الدورة دراسات حالة واقعية لأزمات أمنية كبرى، مع تحليل مفصل لكيفية استجابة القيادات العليا. نركز على الجانب المالي والاستراتيجي للأمن، مما يضمن أن المشاركين سيخرجون بمهارات تحليلية قوية وقدرة على اتخاذ قرارات مستنيرة. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء قادة قادرين على حماية المؤسسة بشكل فعال في العصر الرقمي.