التدريبية: الأمن السيبراني للقيادات العليا

وصناع القرار الدورة

يوليو ٢٠٢٦ ٣١ - ٢٧

لشبونة

(للشخص الواحد) € ٤٤٠٠

Ref: #CYB2914_273583

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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.
- الرقمية. جميع القطاعات التي تعتمد على البنية التحتية

الأقسام المؤسسية المستهدفة:

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

أهداف الدورة التدريبية:

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

- فهم المخاطر السيبرانية من منظور استراتيجي.
- الأعمال. القدرة على دمج الأمن السيبراني في استراتيجية
- (KPIs) تقييم الأداء الأمني وتحديد مؤشرات الأداء الرئيسية
- 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:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: الأمن السيبراني من منظور القيادة

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

الاستراتيجية الوحدة الثانية: إدارة المخاطر السيبرانية

- 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:

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

لا توجد شروط مسبقة.

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

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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