التدريبية: إدارة الأمن السيبراني المتقدمة

للمؤسسات الدورة

Ref: #SM8832

مقدمة الدورة التدريبية / لمحة عامة:

الأعمال وسلامة تعد إدارة الأمن السيبراني مجرد مهمة تقنية، بل في ظل التطور المتسارع للتهديدات السيبرانية، لم رؤى عميقة واستراتيجيات متقدمة المعلومات في المؤسسات. تتجاوز هذه الدورة المفاهيم أصبحت ركيزة أساسية لاستمرارية استكشاف أحدث التحديات والحلول، سيتعلم المشاركون لإدارة الأمن السيبراني بشكل فعال وشامل. من خلال الأساسية لتقدم والتطبيقية، مستندة بكفاءة، وتطبيق أفضل الممارسات الدولية. تركز كيفية بناء دفاعات سيبرانية قوية، وإدارة المخاطر للمعايير والتقنية (NIST Cybersecurity إلى أطر عمل معترف بها عالميًا مثل إطار عمل المعهد الدورة على الجوانب العملية Schmidt هذا المجال، مثل الدكتور Howard Schmidt Howard، وتستلهم من أعمال خبراء بارزين في Framework الوطني لتزويد القادة والمتخصصين بالبيت الأبيض. يقدم BIG BEN Training Center هذه الذي كان مستشار الأمن السيبراني الخاص السيبراني بنجاح، وضمان حماية الأصول الرقمية بالمعرفة والمهارات اللازمة لقيادة مبادرات الأمن الدورة المصممة خصيصًا الاستجابة للحوادث، وإدارة المشاركون تحليل التهديدات السيبرانية الناشئة، للمؤسسات في بيئة متغيرة باستمرار. سيتناول تعزيز ثقافة الأمن السيبراني داخل مؤسساتهم. الامتثال للوائح الأمن السيبراني، بالإضافة إلى وتطوير استراتيجيات

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مديرو تقنية المعلومات.
- مديرو الأمن السيبراني.
- مسؤولو أمن المعلومات.
- متخصصو الامتثال والمخاطر.
- مستشارين الأمن السيبراني.
- مديرو المشاريع التقنية.
- القادة وصناع القرار في المؤسسات.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- قطاع الرعاية الصحية.
- شركات الطاقة والمرافق.
- قطاع الاتصالات.
- القطاعات الحكومية وما في حكمها.
- شركات التكنولوجيا والبرمجيات.
- المؤسسات التعليمية والبحثية.
- شركات الصناعات التحويلية.

الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- إدارة الأمن السيبراني.
- إدارة المخاطر والامتثال.
- القسم القانوني.
- الإدارة العليا.
- بالأمن السيبراني). قسم الموارد البشرية (فيما يتعلق بوعي الموظفين
- إدارة العمليات التشغيلية.

أهداف الدورة التدريبية:

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

- تطوير استراتيجيات شاملة لإدارة الأمن السيبراني.
- فعال. تقييم المخاطر السيبرانية وتحديد أولوياتها بشكل
- تصميم وتنفيذ سياسات وإجراءات أمن المعلومات.
- إدارة الاستجابة للحوادث الأمنية والتعافي منها.
- السيبراني. ضمان الامتثال للمعايير واللوائح الدولية للأمن
- بناء فرق عمل قوية في مجال الأمن السيبراني.
- تطبيق أحدث التقنيات والحلول الأمنية.
- المؤسسة. تعزيز الوعي بالأمن السيبراني في جميع مستويات

منهجية الدورة التدريبية:

إدارة الأمن السيبراني. وتطبيقية تهدف إلى تمكين المشاركين من اكتساب فهم تتبنى هذه الدورة التدريبية منهجية تفاعلية يقدمها خبراء متخصصون، يليها نقاشات جماعية تعتمد المنهجية على مزيج من المحاضرات التفاعلية عميق ومهارات عملية في تحليل التحديات المشاركين. تُقدم دراسات حالة واقعية من بيئات عمل مفتوحة لتشجيع تبادل الخبرات والمعارف بين التي التركيز بشكل كبير على التمارين العملية وورش الأمنية الفعلية وتطبيق الحلول المناسبة. يتم مختلفة، مما يتيح للمتدربين الاستجابة للحوادث، وإعداد النظرية على سيناريوهات محاكاة، مثل تقييم نقاط العمل، حيث يقوم المشاركون بتطبيق المفاهيم العمل الجماعي والتعاون بين المتدربين لتطوير حلول تقارير المخاطر. يشجع BIG BEN Training Center الضعف، وتطوير خطط قوية لدى المتدربين مستمرة وفردية لضمان تطور المهارات. تهدف هذه مبتكرة للمشكلات المعقدة. يتم توفير تغذية راجعة السيبراني، قادرين على مواجهة التحديات الأمنية ليصبحوا قادة فعالين في مجال إدارة الأمن المنهجية إلى بناء قدرات المعاصرة بثقة وكفاءة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

في المؤسسات الوحدة الأولى: أسس ومفاهيم إدارة الأمن السيبراني

- مقدمة إلى إدارة الأمن السيبراني وأهميتها.
- الهجمات: فهم التهديدات السيبرانية المتزايدة وأنواع
- التوافر: مبادئ الأمن السيبراني: السرية، التكاملية،
- ISO، NIST) نماذج وأطر عمل الأمن السيبراني (مثل ٢٧٠٠١).
- تطوير رؤية واستراتيجية الأمن السيبراني للمؤسسة.
- مؤشرات الأداء الرئيسية (KPIs) للأمن السيبراني.
- تكامل الأمن السيبراني مع استراتيجية الأعمال.

الوحدة الثانية: تقييم وإدارة المخاطر السيبرانية

- مفهوم المخاطر السيبرانية وعناصرها.
- منهجيات تقييم المخاطر (Qualitative and Quantitative).
- تحديد الأصول الحساسة وتقييم قيمتها.
- تحليل الثغرات ونقاط الضعف.
- تطوير استراتيجيات تخفيف المخاطر والتحكم فيها.
- إدارة مخاطر الجهات الخارجية وسلاسل التوريد.
- مراقبة المخاطر السيبرانية والإبلاغ عنها.

الوحدة الثالثة: حوكمة الأمن السيبراني والامتثال

- أهمية حوكمة الأمن السيبراني في المؤسسات.
- بناء هيكل حوكمة فعال للأمن السيبراني.
- دور اللجان التنفيذية ومجلس الإدارة في الأمن السيبراني.
- الامتثال للوائح والقوانين المحلية والدولية (مثل GDPR، CCPA).
- تطوير سياسات وإجراءات الأمن السيبراني.
- إدارة التدقيق والامتثال الداخلي والخارجي.
- المسؤولية القانونية والأخلاقية في الأمن السيبراني.

الكوارث الوحدة الرابعة: الاستجابة للحوادث والتعافي من

- مراحل دورة حياة الاستجابة للحوادث السيبرانية.
- تطوير خطة الاستجابة للحوادث (IRP).
- فرق الاستجابة للحوادث الأمنية (CSIRT/CERT).
- تقنيات التحقيق الجنائي الرقمي.
- إدارة الاتصالات أثناء الحوادث.
- خطط التعافي من الكوارث واستمرارية الأعمال.
- التدريبات والمحاكاة لاختبار خطط الاستجابة.

التشغيلي الوحدة الخامسة: تقنيات متقدمة وإدارة الأمن

- أمن الشبكات والخوادم المتقدم.
- أمن تطبيقات الويب وقواعد البيانات.
- إدارة الهوية والوصول (IAM).
- أمن الحوسبة السحابية (Cloud Security).
- الذكاء الاصطناعي وتعلم الآلة في الأمن السيبراني.
- أمن إنترنت الأشياء (IoT Security) وأنظمة التحكم الصناعي (ICS).
- التهديدات الداخلية وكيفية إدارتها.

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:

التهديدات المتطورة؟ التكنولوجي المتسارع والحفاظ على مستوى عالٍ من كيف يمكن للمؤسسات تحقيق التوازن بين الابتكار

الأمن السيبراني في بيئة

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

نقدم للمشاركين رؤى شاملة الإدارية والاستراتيجية للأمن السيبراني، متجاوزةً تتميز هذه الدورة بتركيزها العميق على الجوانب استراتيجية العمل الكلية، وليس كمجرد وظيفة دعم. حول كيفية دمج الأمن السيبراني كجزء لا يتجزأ من مجرد الجوانب التقنية. تحاكي سيناريوهات النظري بالخبرة العملية، من خلال تحليل دراسات حالة تعتمد الدورة على منهجية تطبيقية تعزز الفهم والبرامج المحددة، نركز على المفاهيم الجوهرية التهديدات الحقيقية. بدلاً من التركيز على الأدوات معقدة وورش عمل تفاعلية الأمن السيبراني، كما يضمن فريق المدربين، من ذوي الخبرة الأكاديمية والمنهجيات القابلة للتطبيق في أي بيئة تكنولوجية. خلال هذه الدورة Training Center تقديم محتوى عالي الجودة ومعاصر. يهدف BIG BEN والعملية الطويلة في مجال إدارة في عالم دائم المعقدة، وقيادة فرقهم بفعالية لحماية الأصول قادة قادرين على مواجهة التحديات السيبرانية إلى إعداد من التغير. الرقمية وضمان استمرارية الأعمال