للمؤسسات الدورة التدريبية: خبير أمن المعلومات والحوكمة الرقمية المتقدمة

Ref: #IT4439

مقدمة الدورة التدريبية / لمحة عامة:

الأعمال وحماية الأصول مجرد تحدٍ تقني، بل أصبح ركيزة أساسية للحوكمة في العصر الرقمي المتسارع، لم يعد أمن المعلومات وتتطور باستمرار، مما يفرض على المؤسسات تبني الحيوية للمؤسسات. تتزايد التهديدات السيبرانية الرقمية وضمان استمرارية لتزويد المشاركين بالمعرفة التنظيمية والمعايير العالمية. هذه الدورة استراتيجيات شاملة لأمن المعلومات تتوافق مع الأطر أفضل المعلومات والحوكمة الرقمية، بدءاً من فهم المفاهيم والمهارات اللازمة ليصبحوا خبراء في مجال أمن التدريبية مصممة الهجمات السيبرانية، وتطوير الممارسات في إدارة المخاطر والامتثال. سيتعمق الأساسية للأمن السيبراني وصولاً إلى تطبيق الشفافية والمساءلة في البيئة الرقمية. إن مفهوم استراتيجيات الدفاع، وتطبيق أطر الحوكمة لضمان المشاركون في تحليل السيبراني للرئيس الأمريكي، البروفيسور هوارد شميدت (Howard Schmidt)، الأمن ليس غاية، بل عملية مستمرة" الذي طرحه" متكامل بتقديم تدريب BIG BEN Training Center يؤكد على الطبيعة الديناميكية لهذا المجال. يلتزم المستشار السابق للأمن رقمية فعالة، وحماية لتمكين قادة الأمن والمختصين من بناء أنظمة دفاعية يجمع بين النظريات المتقدمة والتطبيقات العملية، الثقة والامتثال المؤسسي في المشهد البيانات والمعلومات الحساسة من أي تهديدات محتملة، قوية، ووضع سياسات حوكمة الرقمي المعقد. مما يعزز

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مدراء أمن المعلومات.
- متخصصو الأمن السيبراني.
- مسؤولو الامتثال والمخاطر.
- مدققو نظم المعلومات.
- مدراء تقنية المعلومات.
- المستشارون في مجال الأمن والحوكمة الرقمية.
- المحامون والمشرعون في القانون الرقمي.
- المهندسون والمطورون المعنيون بأمن الأنظمة.
- المعلومات. قادة الأعمال الذين يرغبون في فهم أعمق لأمن

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- قطاع الاتصالات.
- القطاع الحكومي والعام.
- قطاع الرعاية الصحية.
- شركات التكنولوجيا والبرمجيات.
- شركات الطاقة والمرافق.
- قطاع التجزئة والتجارة الإلكترونية.
- شركات الاستشارات الأمنية.
- المؤسسات التعليمية والبحثية.

الأقسام المؤسسية المستهدفة:

- أقسام أمن المعلومات.
- أقسام تقنية المعلومات.
- أقسام إدارة المخاطر والامتثال.
- أقسام التدقيق الداخلي والخارجي.
- الأقسام القانونية.
- أقسام الحوكمة المؤسسية.
- أقسام تطوير الأعمال والمنتجات الرقمية.
- أقسام العمليات التشغيلية.

أهداف الدورة التدريبية:

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

- أهداف المؤسسة. وضع استراتيجيات شاملة لأمن المعلومات تتوافق مع
- الدولية. تطبيق أطر الحوكمة الرقمية ومعايير الامتثال
- تحديد وتقييم ومعالجة المخاطر الأمنية بشكل فعال.
- تطوير وتنفيذ سياسات وإجراءات الأمن السيبراني.
- إدارة حوادث الأمن والاستجابة لها بفعالية.
- فهم تحديات أمن الحوسبة السحابية والبيانات الضخمة.
- تطبيق مبادئ الخصوصية وحماية البيانات الشخصية.
- الأمن السيبراني. الاستفادة من تقنيات الذكاء الاصطناعي في تعزيز
- إعداد خطط التعافي من الكوارث واستمرارية الأعمال.

منهجية الدورة التدريبية:

العملي المكثف، التدريبية على منهجية تدريبية متطورة تجمع بين يعتمد BIG BEN Training Center في هذه الدورة تشمل المنهجية محاضرات تفاعلية يقدمها لضمان بناء خبراء في أمن المعلومات والحوكمة المعرفة النظرية العميقة والتطبيق بتطبيق المفاهيم بالإضافة إلى ورش عمل مكثفة تركز على السيناريوهات نخبة من الخبراء في مجال الأمن السيبراني، الرقمية. الفعلية التي تعرض لأحدث التهديدات المكتسبة لحل مشكلات أمنية معقدة. يتم التركيز على الواقعية، حيث يقوم المشاركون للهجمات المشاركين رؤى عملية حول كيفية بناء نظم دفاعية السيبرانية وأفضل أساليب الدفاع، مما يمنح دراسات الحالة الأزمات الأمنية بفعالية. الهدف هو السيبرانية والاستجابة للحوادث، لتدريب المشاركين مرنة. كما تتضمن الدورة جلسات محاكاة صياغة استراتيجيات أمنية متكاملة، وإدارة المخاطر، تزويد المشاركين بمهارات تحليلية ونقدية تمكنهم من على التعامل مع الأمنية المتزايدة. بفاعلية في حماية الأصول الرقمية لمؤسساتهم في ظل وضمان الامتثال للمعايير التنظيمية، والمساهمة التحديات

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الحوكمة الرقمية. الوحدة الأولى: أساسيات أمن المعلومات ومفاهيم

- مقدمة لأمن المعلومات والأمن السيبراني.
- مفاهيم ومبادئ الحوكمة الرقمية.
- أهمية أمن المعلومات والحوكمة في المؤسسات الحديثة.
- التهديدات والهجمات السيبرانية الشائعة.
- المخاطر الأمنية وتصنيفاتها.
- دور الإنسان في سلسلة الأمن السيبراني.
- أخلاقيات الأمن السيبراني.

الوحدة الثانية: استراتيجيات وتقنيات أمن المعلومات المتقدمة.

- أنظمة إدارة أمن المعلومات (ISMS) ومعيار ISO ٢٧٠٠١.
- أمن الشبكات والاتصالات.
- أمن التطبيقات وقواعد البيانات.
- التشفير وإدارة المفاتيح.
- أنظمة كشف ومنع التسلل (IDS/IPS).
- أمن الحوسبة السحابية.
- أمن إنترنت الأشياء (IoT) والأنظمة التشغيلية (OT).

الوحدة الثالثة: إدارة المخاطر الأمنية والاستجابة للحوادث.

- منهجيات تقييم المخاطر الأمنية.
- تحليل الثغرات وإدارة نقاط الضعف.
- خطط الاستجابة للحوادث الأمنية.
- التحقيق الجنائي الرقمي (Digital Forensics).
- التعافي من الكوارث واستمرارية الأعمال.
- إدارة الأزمات الأمنية.
- فرق الاستجابة للطوارئ الحاسوبية (CSIRT).

الوحدة الرابعة: أطر الحوكمة الرقمية والامتثال التنظيمي

- أطر الحوكمة الأمنية مثل NIST وCOBIT
- الامتثال للوائح حماية البيانات (GDPR، CCPA)
- أمن المعلومات والقوانين المحلية والدولية
- إدارة الهوية والوصول (IAM)
- التحكم في الوصول والأذونات
- تدقيق أمن المعلومات وتقييم الامتثال
- التقارير الأمنية والامتثال للجهات التنظيمية

الوحدة الخامسة: مستقبل أمن المعلومات والاتجاهات الحديثة

- السيبراني الذكاء الاصطناعي والتعلم الآلي في الأمن
- أمن البلوك تشين والعملات الرقمية
- التهديدات المتقدمة المستمرة (APTs)
- الأمن السلوكي (Behavioral Security)
- الخصوصية بال تصميم (Privacy by Design)
- العمليات الأمنية المدارة (Managed Security Services)
- التعاون الدولي في مكافحة الجريمة السيبرانية

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:

مستدامة تتجاوز مجرد وتتعقد أطر الحوكمة الرقمية، كيف يمكن للمؤسسات في عالم تتسارع فيه وتيرة التهديدات السيبرانية

الدفاع؟ الامتثال وتصل إلى التنبؤ بالمخاطر والابتكار في ضمان بناءٔ مرونة أمنية

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تركز على جانب واحد وعميقة لمفاهيم أمن المعلومات والحوكمة الرقمية، تتميز هذه الدورة التدريبية بتقديمها رؤية شاملة بل نركز على تمكين المشاركين من صياغة فقط. نحن لا نقدم مجرد معلومات حول الأدوات متجاوزةً بذلك الدورات التي وتحليل معمق تتلاءم مع التحديات الحالية والمستقبلية. ترتكز استراتيجيات أمنية متكاملة وبناء أطر حوكمة فعالة والتقنيات، تطبيق المفاهيم النظرية في بيئات لسيناريوهات أمنية معقدة، مما يمنح المتدربين فهماً الدورة على دراسات حالة واقعية الدولية. مثل الذكاء الاصطناعي في الأمن السيبراني، وإدارة العمل الحقيقية. كما نركز على دمج أحدث الاتجاهات عملياً لكيفية والتدريب العملي المكثف، بالإضافة إلى إن هذا المزيج الفريد من المعرفة الأكاديمية المخاطر المعقدة، وأهمية الامتثال للوائح وثقة. يضمن للمشاركين اكتساب مهارات قيادية تمكنهم من التركيز على التفكير الاستراتيجي في مجال الأمن، العميقة حماية الأصول الرقمية لمؤسساتهم بفاعلية