التدريبية: تحليل المخاطر وإدارة الأمن في مشاريع وبنى تحتية الاتصالات الدورة

مايو ٢٠٢٦ ١٥ - ١١

القاهرة - *

(للشخص الواحد) ٤١٠٠ €

Ref: #TEL6359_595252

مقدمة الدورة التدريبية / لمحة عامة:

وتشغيلية متزايدة تشكل العمود الفقري للاقتصادات الحديثة، ولكنها في يُعتبر قطاع الاتصالات من القطاعات الحيوية التي في مشاريع الاتصالات يمكن أن يؤدي إلى التعقيد. إن الفشل في تحليل المخاطر وإدارة الأمن الوقت نفسه تواجه مخاطر أمنية قدرات قوية الخدمات، والإضرار بالسمعة. لذلك، أصبح من الضروري خسائر فادحة، بما في ذلك تسرب البيانات، وتوقف بفعالية أمنية شاملة. تقدم هذه الدورة في تقييم المخاطر السيبرانية والمادية، وتطبيق للمؤسسات العاملة في هذا القطاع تطوير للمفاهيم الأساسية والمنهجيات المتقدمة في تحليل التدريبية من BIG BEN Training Center فهمًا شاملاً استراتيجيات الضعف، وتطوير خطط سنتناول في هذه الدورة إطار عمل إدارة المخاطر، المخاطر وإدارة الأمن ضمن سياق مشاريع الاتصالات. أمنية للاتصالات من الهجمات السيبرانية والتخريب المادي. الاستجابة للحوادث، وتأمين البنية التحتية وتقييم التهديدات ونقاط الأعمال. تستند محاور الدورة إلى أحدث فعالة، والامتثال للمعايير الدولية، وضمان سيتعرف المشاركون على كيفية بناء برامج في كتابه في إدارة أمن المعلومات والمخاطر، مستلهمة من رؤى المعايير الصناعية وأطر العمل المعترف بها عالميًا استمرارية الأمن السيبراني. هذه الدورة هي والذي يُعد ,Computer Security: Art and Science أكاديميين وخبراء مثل Matt Bishop قطاع الاتصالات، مما يمكنك من حماية الأصول الحيوية بوابتك نحو إتقان تحليل المخاطر وإدارة الأمن في مرجعًا في مفاهيم وضمان مرونة العمليات.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء أمن المعلومات.
- مهندسو الشبكات والاتصالات.
- مدراء المشاريع التقنية.
- أخصائيو الأمن السيبراني.
- مدراء المخاطر والامتثال.
- مهندسو البنية التحتية للاتصالات.
- المحللون الأمنيون.
- المدققون الفنيون.
- صناع القرار في قطاع الاتصالات.

القطاعات والصناعات المستهدفة:

- شركات الاتصالات ومزودو خدمات الإنترنت.
- المؤسسات الحكومية المعنية بالبنية التحتية.
- شركات الأمن السيبراني والاستشارات الأمنية.
- شركات تطوير ونشر شبكات الجيل الخامس (G.0).
- قطاع الطاقة والشبكات الذكية (Smart Grids.).
- الاتصالات). البنوك والمؤسسات المالية (بسبب اعتمادها على
- شركات النقل والخدمات اللوجستية (شبكاتها الخاصة).
- مراكز البيانات ومقدمو الخدمات السحابية.
- الجهات الأمنية والدفاعية.

الأقسام المؤسسية المستهدفة:

- قسم أمن المعلومات.
- إدارة المشاريع.
- قسم إدارة المخاطر.
- إدارة العمليات.
- قسم البنية التحتية للاتصالات.
- إدارة الامتثال.
- قسم الشبكات.
- إدارة الأمن المادي.
- قسم استمرارية الأعمال.

أهداف الدورة التدريبية:

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

- فهم إطار عمل شامل لتحليل وإدارة المخاطر.
- تحديد التهديدات ونقاط الضعف في أنظمة الاتصالات.
- تطبيق منهجيات تقييم المخاطر (كمية ونوعية).
- تطوير خطط أمنية متكاملة لمشاريع الاتصالات.
- تنفيذ ضوابط أمنية فعالة لحماية البنية التحتية.
- صياغة خطط الاستجابة للحوادث والتعافي.
- ضمان الامتثال للمعايير الأمنية الدولية.
- تحسين مرونة الأنظمة واستمرارية الأعمال.
- إدارة مخاطر أمن سلسلة التوريد.

منهجية الدورة التدريبية:

في مشاريع الاتصالات وعملية، مصممة لتزويد المشاركين بالمهارات اللازمة تعتمد هذه الدورة التدريبية على منهجية تطبيقية والأمن السيبراني، مدعومة بدراسات حالة بفعالية. ستبدأ الدورة بشرح نظري لمفاهيم إدارة لتحليل المخاطر وإدارة الأمن عملية، حيث الاتصالات وكيفية الاستفادة منها. سيشارك المتدربون واقعية لأمثلة على حوادث أمنية كبرى في قطاع المخاطر وتقييم التهديدات ونقاط الضعف، سيتعلمون كيفية إجراء تقييمات المخاطر، وتحديد في ورش عمل تطبيقية وجلسات تدريب التمارين العملية التي تحاكي سيناريوهات الهجمات وتطوير خطط المعالجة الأمنية. سيتم التركيز على الأصول الحيوية، BIG BEN ، اكتساب خبرة مباشرة في التعامل مع هذه التحديات. السيبرانية والأعطال التشغيلية، مما يتيح للمشاركين الاتصالات، تغذية راجعة الذين يمتلكون خبرة عملية واسعة في الأمن السيبراني يقدم المدربون الخبراء فيTraining Center على تحليل المخاطر بشكل استباقي، وتطبيق فورية ومخصصة. تهدف هذه المنهجية إلى بناء قدرات وإدارة المخاطر لمشاريع اتصالات معقدة ومتطورة. حلول أمنية قوية، وضمان استمرارية الأعمال في بيئة المتدربين

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات تحليل المخاطر وإدارة الأمن.

- مقدمة إلى إدارة المخاطر الأمنية.
- مفاهيم التهديد، الضعف، والمخاطرة.
- .Identify, Protect, Detect, Respond, Recover) إطار عمل إدارة المخاطر
- تشغيلية). أنواع المخاطر في قطاع الاتصالات (سيبرانية، مادية،
- مبادئ الأمن السيبراني الأساسية.
- الحوكمة، المخاطر، والامتثال (.GRC)
- أهمية تحليل المخاطر للمؤسسات.

الوحدة الثانية: تقييم المخاطر في مشاريع الاتصالات.

- منهجيات تقييم المخاطر (.ISO ٢٧٠٠٥, NIST SP ٨٠٠-٣٠)
- تحديد الأصول الحيوية في مشاريع الاتصالات.
- تقييم التهديدات ونقاط الضعف.
- تحليل تأثير المخاطر (.Impact Analysis)
- تقييم الاحتمالية (.Likelihood Assessment)
- سجل المخاطر (.Risk Register)
- إعداد تقارير المخاطر.

الأمنية. الوحدة الثالثة: إدارة الأمن وتطوير الضوابط

- تطوير استراتيجيات الأمن في الاتصالات.
- ضوابط الأمن الإدارية، التقنية، والمادية.
- .IDS/IPS) أمن البنية التحتية للشبكات (جدران الحماية،
- تأمين الأنظمة الصناعية (.ICS/SCADA)
- أمن الاتصالات اللاسلكية (.Wireless Security)
- إدارة الثغرات الأمنية (.Vulnerability Management)
- التشفير وإدارة المفاتيح.

الكوارث. الوحدة الرابعة: الاستجابة للحوادث والتعافي من

- تطوير خطة الاستجابة للحوادث (Incident Response Plan).
- مراحل الاستجابة للحوادث (الكشف، الاحتواء، الاستئصال، التعافي).
- فرق الاستجابة للطوارئ (CSIRT).
- تحليل الأدلة الجنائية الرقمية (Digital Forensics).
- تخطيط استمرارية الأعمال (BCP) والتعافي من الكوارث (DRP).
- اختبار خطط الاستجابة والتعافي.
- التواصل أثناء الأزمات الأمنية.

والمعايير. الوحدة الخامسة: أمن سلسلة التوريد والامتثال

- إدارة مخاطر أمن سلسلة التوريد (Supply Chain Security).
- أمن الأطراف الثالثة والموردين.
- الامتثال للمعايير الدولية (ISO ٢٧٠٠١, NIS٢ Directive).
- المتطلبات التنظيمية الخاصة بقطاع الاتصالات.
- التدقيق الأمني (Security Auditing).
- قياس وتقييم فعالية الضوابط الأمنية.
- التطورات المستقبلية في المخاطر والأمن.

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:

تجاوز النهج التقليدي لإدارة السيبرانية والتعقيد المتزايد لمشاريع الاتصالات، في ظل المشهد المتغير باستمرار للتهديدات أنظمة ومبتكرة لا تكتفي برد الفعل، بل تعمل على بناء المخاطر، وتطوير استراتيجيات أمنية استباقية كيف يمكن للمهنيين المستقبلية غير المتوقعة؟ الاتصالات لضمان بقائها آمنة وموثوقة في مواجهة مرونة متأصلة في تصميم وبناء وتشغيل التحديات

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

مختلفة بشكل جوهري عن عميقًا وعمليًا على تحليل المخاطر وإدارة الأمن في تتميز هذه الدورة التدريبية بتقديمها تركيزًا المشاريع. بخلاف الدورات التي تتناول الأمن بشكل الدورات العامة في الأمن السيبراني أو إدارة مشاريع الاتصالات، مما يجعلها BIG BEN هذه الدورة الفريدة لقطاع الاتصالات، وتُقدم حلولا تطبيقية عام، تُسلط هذه الدورة الضوء على التحديات والمخاطر الحالة الواقعية لحوادث أمنية كبرى، بمنهجية تدريبية تجمع بين المعرفة التقنية المتخصصة ومتقدمة. يقدم Training Center أمنية المخاطر. سيتم تزويد المشاركين بالمهارات اللازمة وتدريبات عملية مكثفة على أدوات ومنهجيات تقييم ودراسات في قطاع الاتصالات. قوية، والاستجابة الفعالة للحوادث، مما يمكنك من لتقييم المخاطر بفعالية، وتصميم استراتيجيات للتميز في أمن مشاريع الاتصالات. هذه الدورة هي الخيار الأمثل للمهنيين الذين يسعون حماية الأصول الحيوية لمؤسستك