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

#TEL6359

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

مقدمة الدورة التدريبية / لمحة عامة:

يُعتبر قطاع الاتصالات من القطاعات الحيوية التي تشكل العمود الفقري للاقتصادات الحديثة، ولكنها في الوقت نفسه تواجه مخاطر أمنية وتشغيلية متزايدة التعقيد. إن الفشل في تحليل المخاطر وإدارة الأمن بفعالية في مشاريع الاتصالات يمكن أن يؤدي إلى خسائر فادحة، بما في ذلك تسرب البيانات، وتوقف الخدمات، والإضرار بالسمعة. لذلك، أصبح من الضروري للمؤسسات العاملة في هذا القطاع تطوير قدرات قوية في تقييم المخاطر السيبرانية والمادية، وتطبيق استراتيجيات أمنية شاملة. تقدم هذه الدورة التدريبية من BIG BEN Training Center فهمًا شاملاً للمفاهيم الأساسية والمنهجيات المتقدمة في تحليل المخاطر وإدارة الأمن ضمن سياق مشاريع الاتصالات. سنتناول في هذه الدورة إطار عمل إدارة المخاطر، وتقييم التهديدات ونقاط الضعف، وتطوير خطط الاستجابة للحوادث، وتأمين البنية التحتية للاتصالات من الهجمات السيبرانية والتخريب المادي. سيتعرف المشاركون على كيفية بناء برامج أمنية فعالة، والامتثال للمعايير الدولية، وضمان استمرارية الأعمال. تستند محاور الدورة إلى أحدث المعايير الصناعية وأطر العمل المعترف بها عالميًا في إدارة أمن المعلومات والمخاطر، مستلهمة من رؤى أكاديميين وخبراء مثل Matt Bishop في كتابه Computer Security: Art and Science, والذي يُعد مرجعًا في مفاهيم الأمن السيبراني. هذه الدورة هي بوابتك نحو إتقان تحليل المخاطر وإدارة الأمن في قطاع الاتصالات، مما يمكنك من حماية الأصول الحيوية 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 (5G).
- قطاع الطاقة والشبكات الذكية (Smart Grids).
- البنوك والمؤسسات المالية (بسبب اعتمادها على الاتصالات).
- 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:

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

- 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:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات تحليل المخاطر وإدارة الأمن.

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

الوحدة الثانية: تقييم المخاطر في مشاريع الاتصالات.

- منهجيات تقييم المخاطر (ISO 27005, NIST SP 800-30).
- 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.

الوحدة الثالثة: إدارة الأمن وتطوير الضوابط الأمنية.

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

الوحدة الرابعة: الاستجابة للحوادث والتعافي من الكوارث.

- 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.

الوحدة الخامسة: أمن سلسلة التوريد والامتثال والمعايير.

- إدارة مخاطر أمن سلسلة التوريد (Supply Chain Security).
- أمن الأطراف الثالثة والموردين.
- الامتثال للمعايير الدولية (ISO 27001, NIS2 Directive).
- المتطلبات التنظيمية الخاصة بقطاع الاتصالات.
- التدقيق الأمني (Security Auditing).
- قياس وتقييم فعالية الضوابط الأمنية.
- التطورات المستقبلية في المخاطر والأمن.

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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