الدورة التدريبية: أمن المعلومات السيبراني في أنظمة الاتصالات والشبكات المتقدمة للتهديدات الحديثة

مايو ٢٠٢٦ ١٥ - ١١

باريس

(للشخص الواحد) € ٥٧٠٠

Ref: #TEL1272_410301

مقدمة الدورة التدريبية / لمحة عامة:

رفاهية. مع التوسع باستمرار، أصبح أمن المعلومات في أنظمة الاتصالات في عصر تتزايد فيه التهديدات السيبرانية وتتطور
إنترنت الأشياء (IoT)، تتزايد نقاط الهائل في البنية التحتية الرقمية، من شبكات الجيل والشبكات ضرورة قصوى وليست مجرد
BEN المهاجمين. هذه الدورة التدريبية الشاملة منBIG الضعف المحتملة التي يمكن استغلالها من قبل الخامس (G5) إلى
الحيوية من الهجمات السيبرانية. بالمعرفة والمهارات المتقدمة اللازمة لحماية صُممت لتزويد المشاركين Training Center
المخاطر، وتنفيذ حلول أمنية قوية تشمل التشفير، سيتعلم المتدربون كيفية تحديد التهديدات، وتقييم البيانات والأنظمة
أنظمة الاتصالات سيتم التركيز على أحدث التقنيات وأفضل الممارسات في وأمن الشبكات، وإدارة الهوية، والاستجابة للحوادث.
السيبراني مثلBruce Schneier ، الحديثة. تُستلهم هذه الدورة من أعمال أكاديميين مجال الأمن السيبراني المطبقة على
يجمع مرجعًا أساسيًا في مجال التشفير وأمن البيانات. مؤلف كتاب ""Applied Cryptography، الذي يُعد ورواد في مجال الأمن
التهديدات الحالية بين المفاهيم النظرية المتعمقة والتطبيقات العملية يلتزم BIG BEN Training Center بتقديم تدريب
لمواجهة التحديات الأمنية المعقدة في بيئة والمستقبلية، مما يضمن أن يكون المشاركون مجهزين الموجهة نحو سيناريوهات
الاتصالات الرقمية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- متخصصو الأمن السيبراني.
- مهندسو الشبكات والاتصالات.
- مدراء أمن المعلومات.
- مسؤولو الامتثال والمخاطر.
- محللو الأمن ومستشارو الأمن السيبراني.
- مدراء تكنولوجيا المعلومات.
- الاتصالات. المهندسون الذين يعملون على تصميم وتطوير أنظمة
- أي شخص معني بحماية الأصول الرقمية في بيئة الشبكات.

القطاعات والصناعات المستهدفة:

- شركات الاتصالات ومزودو خدمات الإنترنت.
- البنوك والمؤسسات المالية.
- القطاع الحكومي والدفاعي.
- شركات الأمن السيبراني والاستشارات الأمنية.
- قطاع الطاقة والمرافق الحيوية.
- شركات تطوير البرمجيات والمنصات الرقمية.
- قطاع الرعاية الصحية لحماية بيانات المرضى.
- شركات التصنيع التي تعتمد على الشبكات الذكية.

الأقسام المؤسسية المستهدفة:

- أقسام أمن المعلومات والسيبراني.
- إدارات تكنولوجيا المعلومات والشبكات.
- أقسام الامتثال والمراجعة الداخلية.
- أقسام إدارة المخاطر.
- فرق الاستجابة للحوادث الأمنية.
- أقسام الهندسة والتطوير.
- إدارات البنية التحتية.

أهداف الدورة التدريبية:

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

- أنظمة الاتصالات. فهم التهديدات السيبرانية المتقدمة ونقاط الضعف في
- المعلومات الحساسة. تطبيق مبادئ التشفير وأمن البيانات لحماية
- اللاسلكية والسلكية. تصميم وتنفيذ استراتيجيات أمنية قوية للشبكات
- المعقدة. إدارة الهوية والوصول بشكل فعال في بيئات الشبكات
- التخفيف منها. التعرف على هجمات الهندسة الاجتماعية وكيفية
- تنفيذ أنظمة كشف ومنع التسلل المتقدمة (.IDS/IPS)
- الكوارث. تطوير خطط الاستجابة للحوادث الأمنية والتعافي من
- والمحلية (مثل.(ISO ٢٧٠٠١ الامتثال للمعايير واللوائح الأمنية الدولية
- إجراء تقييمات المخاطر الأمنية واختبارات الاختراق.
- بالبرمجيات (.SDN تأمين البنية التحتية السحابية والشبكات المعرفة

منهجية الدورة التدريبية:

العملية المكثفة. تبدأ منهجية تدريبية متعمقة وعملية، تجمع بين المعرفة يعتمد BIG BEN Training Center في هذه الدورة والتهديدات السيبرانية، ثم تنتقل إلى الدورة بمراجعة شاملة للمفاهيم الأساسية لأمن النظرية المتطورة والتطبيقات ورش عمل عملية الهجمات السيبرانية الحديثة على أنظمة الاتصالات تحليل متقدم لدراسات الحالة الواقعية التي تُبرز المعلومات اختراق ودفاع، وتكوين حلول باستخدام أدوات ومحاكيات أمنية متقدمة، حيث سيقومون والشبكات. سيُشارك المتدربون في الجانب العملي من خلال تمارين محاكاة الاختراق، أمنية، وتحليل السجلات الأمنية. سيتم التركيز على بتنفيذ سيناريوهات النقدي وتبادل الخبرات بين للحوادث. تشمل المنهجية مناقشات جماعية مكثفة والتحقيق الجنائي الرقمي، وتخطيط الاستجابة BIG إلى تمكين لضمان فهم عميق للمفاهيم وتنمية المهارات المشاركين. يتم تقديم تغذية راجعة بناءة وفردية لتعزيز التفكير والشبكات من أشد التهديدات المشاركين من اكتساب الخبرة العملية اللازمة لحماية التطبيقية. يهدف BEN Training Center المجال الحيوي. السيبرانية تطورًا، مما يجعلهم خبراء مؤهلين في هذا البنى التحتية للاتصالات

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن المعلومات السيبراني.

- مقدمة في الأمن السيبراني ومفاهيمه الأساسية.
- مبادئ حماية البيانات والخصوصية.
- التهديدات السيبرانية الشائعة وأنواع الهجمات.
- مفاهيم التشفير وأمن المعلومات.
- إدارة المخاطر والضعف.
- الأطر والمعايير الأمنية (مثل NIST, ISO ٢٧٠٠١).
- أهمية الأمن السيبراني في أنظمة الاتصالات.

الوحدة الثانية: أمن الشبكات والاتصالات.

- تأمين البنية التحتية للشبكات (Wired/Wireless).
- بروتوكولات أمن الشبكات (IPSec, SSL/TLS).
- جدران الحماية وأنظمة كشف/منع التسلل (IDS/IPS).
- أمن الشبكات اللاسلكية (Wi-Fi, ٥G).
- أمن إنترنت الأشياء (IoT) والتحكم الصناعي (ICS).
- الشبكات المعرفة بالبرمجيات (SDN) والأمن السحابي.
- أمن الاتصالات الصوتية والمرئية.

المتقدم. الوحدة الثالثة: إدارة الهوية والوصول والتشفير

- مفاهيم إدارة الهوية والوصول (IAM).
- المصادقة متعددة العوامل (MFA).
- أنظمة التحكم في الوصول (ACLs).
- التشفير المتماثل وغير المتماثل.
- البنية التحتية للمفاتيح العامة (PKI).
- التوقيعات الرقمية والشهادات.
- تشفير البيانات أثناء النقل والتخزين.

والاستجابة للحوادث. الوحدة الرابعة: تحليل البرمجيات الخبيثة

- الديدان). أنواع البرمجيات الخبيثة (الفيروسات، الفدية،
- أساليب تحليل البرمجيات الخبيثة.
- مفاهيم الاستجابة للحوادث الأمنية.
- الاستئصال، التعافي). خطوات الاستجابة للحوادث (الاكتشاف، الاحتواء،
- التحقيق الجنائي الرقمي وجمع الأدلة.
- أهمية التخطيط لاستمرارية الأعمال.
- محاكاة الهجمات واختبار الاختراق.

المستقبلية. الوحدة الخامسة: التحديات المتقدمة والتوجهات

- السيبراني. أمن الذكاء الاصطناعي وتعلم الآلة في الأمن
- أمن سلسلة الكتل (Blockchain) في الاتصالات.
- مفاهيم الأمن الكمومي.
- التهديدات السيبرانية الناشئة (.Zero-day exploits)
- أمن الحوسبة السحابية المتقدمة.
- الوعي الأمني والتدريب البشري.
- التعاون الدولي في مكافحة الجرائم 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:

على أقصى كيف يمكن للمؤسسات تحقيق توازن فعال بين الانفتاح مع التوسع الهائل في الرقمنة والترابط بين الأنظمة،

والمعقدة باستمرار؟ درجات الأمن السيبراني ضد التهديدات المتزايدة التكنولوجي الضروري للابتكار وبين الحفاظ

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

الدورات العامة في المعلومات السيبراني المخصص لأنظمة الاتصالات تتميز هذه الدورة بتركيزها الشامل والعميق على أمن بل نغوص في تفاصيل التطبيقات العملية الأمن السيبراني. نحن لا نكتفي بتقديم المفاهيم والشبكات، مما يجعلها مختلفة عن في (IoT) شبكات الجيل الخامس (G٥) وتطبيقات إنترنت الأشياء والأمثلة الواقعية من قطاع الاتصالات، مثل تأمين النظرية، خصيصًا لبيئات الاتصالات المعقدة. العمق، وإدارة المخاطر المتقدمة، وأساليب الاستجابة الحرجة. نركز على استراتيجيات الدفاع سيناريوهات الهجمات الحقيقية على البنية التحتية تتضمن الدورة ورش عمل مكثفة وتمارين محاكاة تحاكي للحوادث المصممة قيادة جهود الأمن بثمن في اكتشاف التهديدات والتصدي لها. نحن نهدف للاتصالات، مما يمنح المشاركين خبرة عملية لا تقدر حساسية في عالم الاتصالات المتطور. السيبراني في مؤسساتهم، وحماية الأصول الرقمية إلى إعداد متخصصين قادرين على الأكثر