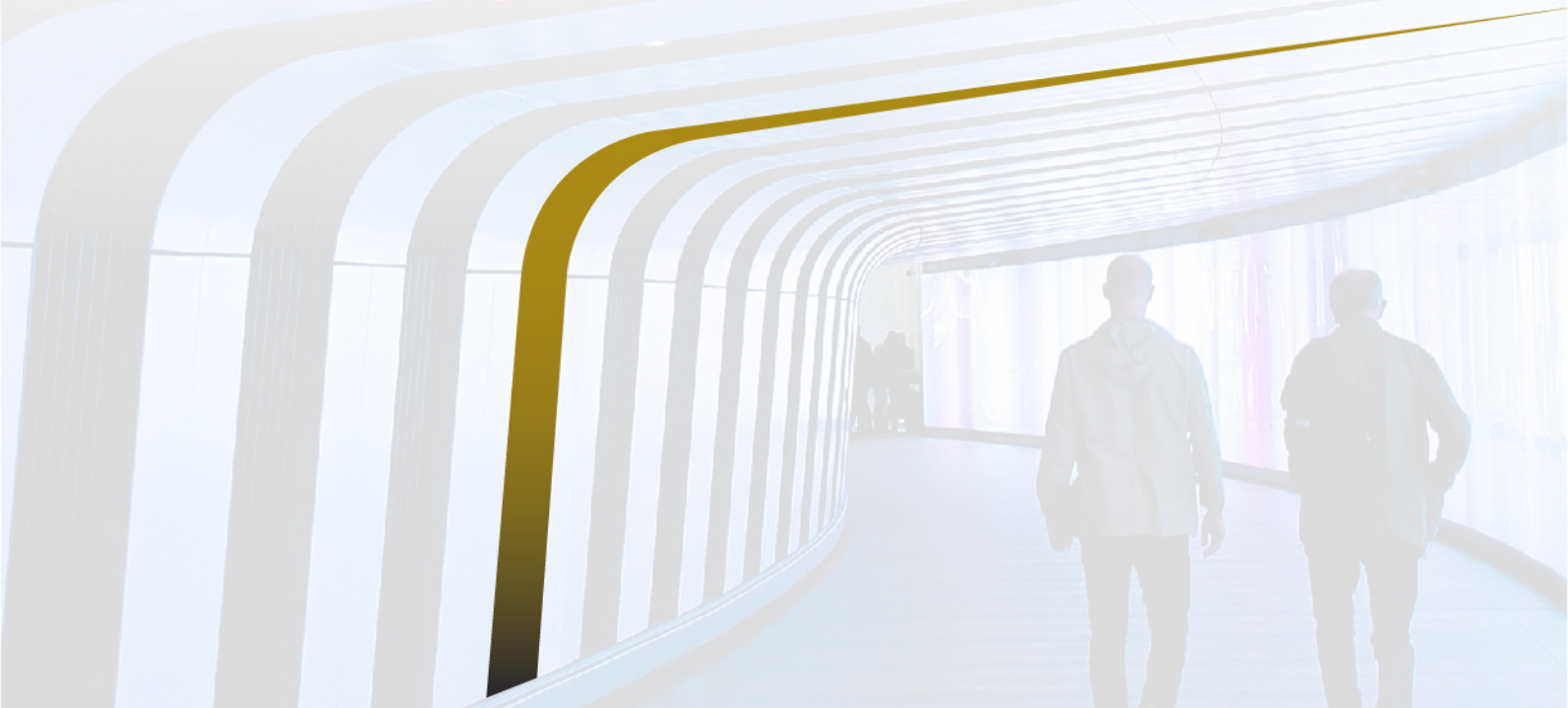
للتهديدات الدورة التدريبية: أمن الشبكات والبيانات المتقدم: استراتيجيات الحماية والتصدي



يوليو ٢٠٢٦ ١٠ - ٠٦

برلين

٤٩٠٠ € (للشخص الواحد)

Ref: #NO9224_388125

مقدمة الدورة التدريبية / لمحة عامة:

استمراريتها وسلامة أمن الشبكات والبيانات ليس مجرد خيار، بل ضرورة في ظل التزايد المستمر للتهديدات السيبرانية، أصبح في أحدث استراتيجيات حماية الشبكات أصولها الرقمية. تقدم هذه الدورة التدريبية الشاملة قصوى للمؤسسات للحفاظ على على تزويد المشاركين السيبرانية وصولا إلى تطبيق آليات الدفاع وتأمين البيانات، بدءًا من فهم أنواع الهجمات منهجًا متعمقًا دفاعية قوية وفعالة. يستعرض BIG BEN Training بالمهارات العملية والنظرية اللازمة لبناء منظومات المتقدمة. يركز التدريب ، المعروف (Anderson المجال مثل البروفيسور روس أندرسون (Ross هذه المفاهيم بعمق، مستنيرًا بأعمال رواد Center ستُمكن الدورة المتدربين من فهم أمن المعلومات، مما يضمن تقديم محتوى أكاديمي وعملي بإسهاماته البارزة في هندسة التطبيقات، الشبكات، والتعامل مع الحوادث الأمنية بفعالية. كيفية تحليل المخاطر، تطبيق أفضل ممارسات أمن رفيع المستوى. التحديات الأمنية المعاصرة أمن السحابة، وإدارة الثغرات لضمان أن يكون المتدرب يتعمق البرنامج في تفاصيل التشفير، أمن والمعقدة. جاهزًا لمواجهة

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مديري أمن المعلومات.
- مهندسي أمن الشبكات.
- محللي الأمن السيبراني.
- مسؤولي تكنولوجيا المعلومات.
- المتخصصين في الامتثال والمخاطر.
- المدققين الأمنيين.
- المطورين المسؤولين عن أمن التطبيقات.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- شركات الاتصالات وتقنية المعلومات.
- الحكومة والدفاع.
- الرعاية الصحية.
- النفط والغاز والطاقة.
- التصنيع.
- قطاع التجزئة والتجارة الإلكترونية.

الأقسام المؤسسية المستهدفة:

- إدارة أمن المعلومات.
- قسم تكنولوجيا المعلومات.
- الامتثال وإدارة المخاطر.
- قسم العمليات الأمنية (SOC).
- قسم تطوير البرمجيات.
- قسم البنية التحتية.
- التدقيق الداخلي.

أهداف الدورة التدريبية:

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

- تحليل وتقييم المخاطر الأمنية للشبكات والبيانات.
- تصميم وتنفيذ حلول أمن الشبكات المتقدمة.
- تطبيق تقنيات التشفير لحماية البيانات.
- منها. التعرف على أنواع الهجمات السيبرانية وسبل الوقاية
- إدارة جدران الحماية وأنظمة كشف التسلل.
- وضع خطط الاستجابة للحوادث الأمنية.
- تطبيق أفضل ممارسات أمن البيانات.
- فهم أمن الحوسبة السحابية والتحديات المرتبطة بها.
- الالتزام بالمعايير التنظيمية لأمن المعلومات.
- إجراء تدقيقات أمنية وتقييمات للضعف.

منهجية الدورة التدريبية:

والبيانات. تبدأ كل وتطبيقية مكثفة، مصممة لتمكين المشاركين من اكتساب تعتمد هذه الدورة التدريبية على منهجية تفاعلية تليها جلسات ورش عمل عملية تُطبق فيها وحدة بمحاضرات نظرية متعمقة تغطي المفاهيم خبرة عملية في أمن الشبكات كيفية تحليل استخدام دراسات حالة مستوحاة من هجمات سيبرانية التقنيات الأمنية على سيناريوهات واقعية. يتم الأساسية، الجماعي والمناقشات Center التهديدات وتطبيق الدفاعات. يشجع BIG BEN Training حقيقية لمساعدة المشاركين على فهم راجعة فردية وجماعية لضمان فهم عميق للمفاهيم لتعزيز تبادل المعرفة والخبرات. تُقدم جلسات تغذية المفتوحة على العمل البيانات الحساسة، والتعامل مع المتدربين بالقدرة على تأمين البنية التحتية وتطوير المهارات. تهدف المنهجية إلى تزويد التهديدات السيبرانية بفعالية وثقة للشبكات، حماية

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الشبكات الوحدة الأولى: أساسيات أمن المعلومات ومفاهيم

- مقدمة إلى أمن المعلومات والتهديدات السيبرانية.
- مبادئ أمن الشبكات الأساسية.
- مكونات الشبكة وتأثيرها على الأمن.
- نموذج OSI ومناطق الهجوم.
- مفاهيم التشفير وأمن البيانات.
- تحليل المخاطر الأمنية.
- القوانين واللوائح المتعلقة بأمن المعلومات.

الوحدة الثانية: تقنيات حماية الشبكات المتقدمة

- جدران الحماية (Firewalls) المتقدمة وتكوينها.
- أنظمة كشف ومنع التسلل (IDS/IPS).
- الاتصالات الشبكات الخاصة الافتراضية (VPN) وتأمين
- إدارة نقاط الضعف وتصحيح الثغرات الأمنية.
- فحص المنافذ واكتشاف نقاط الضعف.
- بروتوكولات التوجيه الآمنة.
- مقدمة إلى أمن الشبكات اللاسلكية.

الوحدة الثالثة: أمن البيانات والتشفير

- مبادئ أمن البيانات.
- أنواع التشفير (Symmetric, Asymmetric, Hashing).
- إدارة المفاتيح والتصديقات الرقمية.
- أمن قواعد البيانات.
- أمن تخزين البيانات.
- التعافي من الكوارث والنسخ الاحتياطي للبيانات.
- حماية البيانات أثناء النقل (Data in Transit).

الوحدة الرابعة: أمن التطبيقات والحوسبة السحابية

- مقدمة إلى أمن التطبيقات.
- ثغرات الويب الشائعة (OWASP Top ١٠).
- أمن البرمجيات والتطوير الآمن.
- أمن الحوسبة السحابية (Cloud Security).
- نماذج أمن السحابة (IaaS, PaaS, SaaS).
- تحديات أمن البيانات في السحابة.
- أمن الحاويات والخدمات المصغرة.

والتحقيق الجنائي الرقمي الوحدة الخامسة: الاستجابة للحوادث الأمنية

- مراحل الاستجابة للحوادث الأمنية.
- أدوات تحليل الحوادث.
- التحقيق الجنائي الرقمي في الشبكات.
- جمع الأدلة الرقمية والحفاظ عليها.
- إدارة السجلات والتدقيق الأمني.
- التخطيط للتعافي من الكوارث.
- التحليل بعد الحادثة والدروس المستفادة.

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:

إعاقة الابتكار أو أقصى درجات أمن الشبكات والبيانات وضمان سهولة كيف يمكن للمؤسسات تحقيق التوازن الفعال بين تطبيق

تجربة المستخدم؟ الوصول والمرونة التشغيلية دون

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

النظرية. يقدم والبيانات من منظور متقدم وعملي، مما يجعلها مختلفة تتميز هذه الدورة بتركيزها الشامل على أمن الشبكات التطبيقية والخبرة العملية، مع التركيز منهجًا يجمع بين BIG BEN Training Center عن الدورات التي تقتصر على المفاهيم مع الحوادث يميز هذه الدورة هو التركيز على كيفية بناء دفاعات على التهديدات السيبرانية الحالية والناشئة. ما الأكاديمية الصناعية، مما يمكنهم من الأمنية بفعالية. يتم تزويد المشاركين بأدوات تحليل قوية، إدارة الثغرات الأمنية، والتعامل ليست مجرد شرح للمفاهيم، بل هي تدريب عملي تطبيق المعرفة المكتسبة فورًا في بيئات عملهم. الأمن وأفضل الممارسات المتزايدة. التحتية الرقمية بكفاءة ومرونة، وضمان استمرارية مكثف يهدف إلى بناء خبراء قادرين على تأمين البنية الدورة الأعمال في مواجهة التحديات السيبرانية