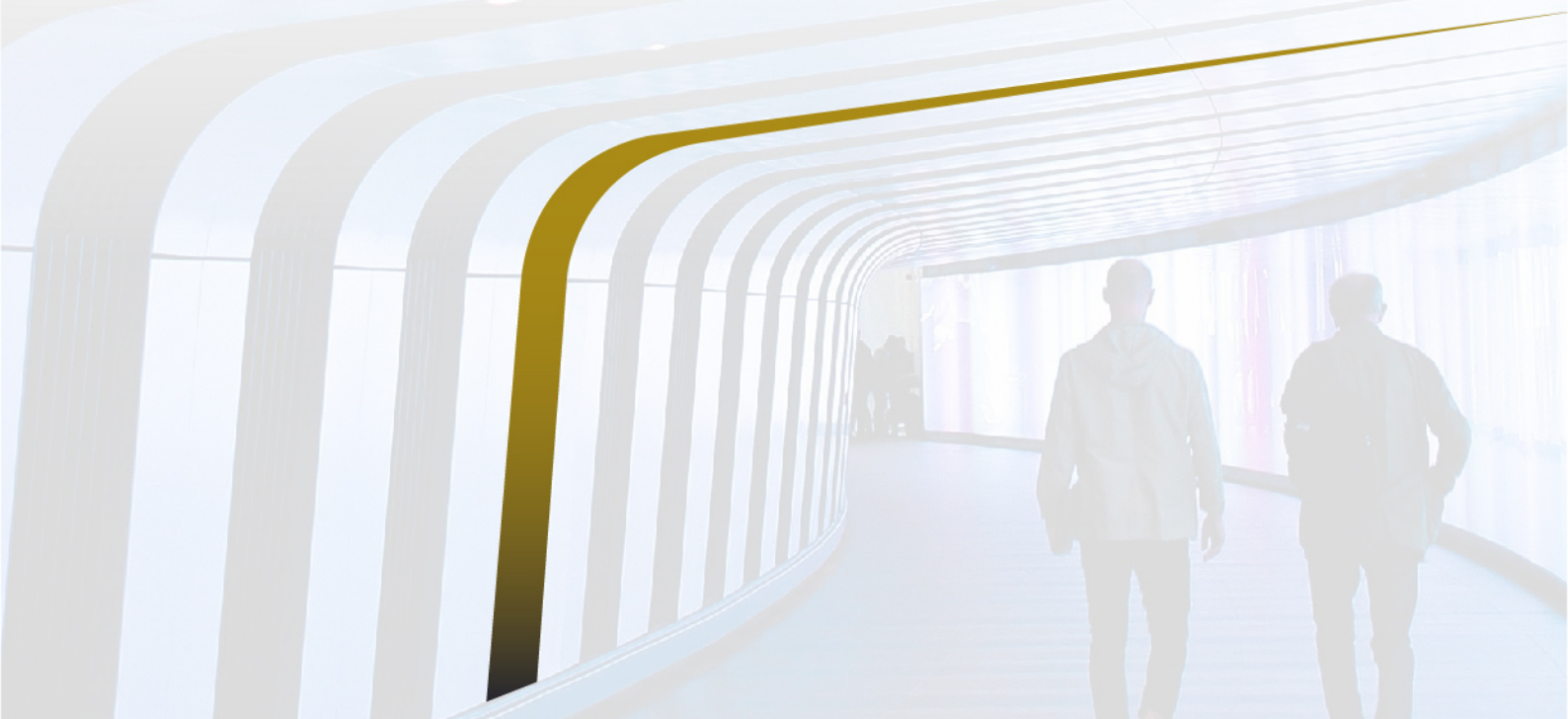
الممارسات الدورة التدريبية: أمن الشبكات اللاسلكية والواي فاي: تهديدات، دفاعات، وأفضل



٠٥ - ٠٩ يوليو ٢٠٢٦

* - الدوحة

00٠٠ € (للشخص الواحد)

Ref: #NO2515_91101

مقدمة الدورة التدريبية / لمحة عامة:

مما يتطلب فهمًا عميقًا حاسمًا في عالمنا المتصل، حيث تتزايد التهديدات أصبح أمن الشبكات اللاسلكية والواي فاي تحديًا التدريبية الشاملة منهجًا متعمقًا في تهديدات أمن لنقاط الضعف وطرق الحماية. تقدم هذه الدورة السيبرانية باستمرار، التشفير اللاسلكي وتطبيق أفضل ممارسات الأمن في بيئات الواي فاي الشبكات اللاسلكية، تقنيات الدفاع ضد الاختراقات، المعقدة. يركز التدريب على تزويد المشاركين وصولا إلى التطبيقات المتقدمة في تأمين الشبكات المتنوعة، بدءًا من أساسيات الأمنية اللاسلكية. يستعرضBIG المخاطر الأمنية، تطبيق الإجراءات الوقائية، بالمهارات العملية والنظرية اللازمة لتحديد رواد المجال مثل البروفيسور ويليام ستالينغز هذه المفاهيم بعمق، مستنيرًا BEN Training Center والاستجابة للحوادث رفيع المستوى. أساسية في مجال أمن الشبكات والشبكات اللاسلكية، ، الذي تُعد كتبه مراجع(William Stallings) بأعمال حماية البيانات عبر الهواء، ستُمكن الدورة المتدربين من فهم كيفية تكوين شبكات مما يضمن تقديم محتوى أكاديمي وعملي يؤهلهم لأن يكونوا خبراء في التعامل مع تحديات واستكشاف نقاط الضعف في بيئات الاتصال اللاسلكي، الواي فاي الآمنة، أمن الفضاء السيبراني اللاسلكي. مما

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مهندسي أمن الشبكات.
- مسؤولي تكنولوجيا المعلومات.
- خبراء الأمن السيبراني.
- مديري الشبكات.
- المتخصصين في البنية التحتية.
- مدققي الأمن.
- أي شخص مسؤول عن أمن الشبكات اللاسلكية في مؤسسته.

القطاعات والصناعات المستهدفة:

- تكنولوجيا المعلومات والاتصالات.
- القطاع المصرفي والمالي.
- الجهات الحكومية والدفاع.
- قطاع الرعاية الصحية.
- التصنيع والخدمات اللوجستية.
- التعليم والبحث العلمي.
- شركات استشارات الأمن السيبراني.

الأقسام المؤسسية المستهدفة:

- قسم الأمن السيبراني.
- إدارة تكنولوجيا المعلومات.
- قسم الشبكات.
- إدارة المخاطر.
- قسم التدقيق الداخلي.
- إدارة البنية التحتية.
- قسم الامتثال.

أهداف الدورة التدريبية:

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

- الضعف. فهم معمق لتهديدات أمن الشبكات اللاسلكية ونقاط
- تصميم وتنفيذ شبكات واي فاي آمنة.
- (WPA٣, ٨٠٢.١X) تطبيق بروتوكولات التشفير والمصادقة اللاسلكية
- حماية الشبكات اللاسلكية من الهجمات الشائعة.
- (Wireless Intrusion Detection/Prevention Systems) إدارة أجهزة الأمن اللاسلكي
- الاستجابة للحوادث الأمنية اللاسلكية.
- اللاسلكية. إجراء تقييمات الضعف واختبارات الاختراق للشبكات
- تطبيق أفضل ممارسات الأمن للشبكات اللاسلكية.
- تكوين جدران الحماية اللاسلكية.
- ضمان امتثال الشبكة اللاسلكية للمعايير الأمنية.

منهجية الدورة التدريبية:

والواي فاي. وتطبيقية مكثفة، مصممة لتمكين المشاركين من اكتساب تعتمد هذه الدورة التدريبية على منهجية عملية التي تركز على تطبيقات الأمن تشمل الدورة مزيجًا من المحاضرات النظرية المتعمقة، خبرة مباشرة في أمن الشبكات اللاسلكية المشاركون بتطبيق المفاهيم المكتسبة من خلال تمارين اللاسلكي في بيئات الأعمال الحقيقية. سيقوم وورش العمل العملية العمل الجماعي اللاسلكية، واستخدام أدوات تحليل الأمن اللاسلكي في تكوين الشبكات اللاسلكية الآمنة، محاكاة الهجمات يقدم المدربون فيBIG BEN Training والمناقشات التفاعلية لتبادل الخبرات وحلول بيئة معملية افتراضية. يتم تشجيع إلى اللاسلكية، تغذية راجعة فورية ودقيقة لضمان فهم في مجال أمن الشبكات والشبكات ، وهم خبراءCenter المشكلات. عالية، مما يحمي إعداد المتدربين ليصبحوا قادرين على تأمين شبكاتهم عميق للمفاهيم وتطوير المهارات. تهدف المنهجية مؤسساتهم من المخاطر السيبرانية المتزايدة اللاسلكية بفعالية واحترافية

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

وتهديداتها الوحدة الأولى: أساسيات الشبكات اللاسلكية

- مراجعة لأساسيات تقنيات الواي فاي (٨٠٢.١١).
- مكونات الشبكة اللاسلكية وأنواعها.
- نقاط الضعف الشائعة في الشبكات اللاسلكية.
- أنواع الهجمات اللاسلكية (Evil Twin, WEP/WPA Cracking, DE authentication)
- المخاطر الأمنية المرتبطة بالشبكات اللاسلكية.
- أهمية أمن الواي فاي للمؤسسات.
- نظرة عامة على البروتوكولات الأمنية اللاسلكية.

الوحدة الثانية: بروتوكولات الأمن اللاسلكي والتشفير

- بروتوكولات التشفير اللاسلكي (WPA٢, WPA٣).
- المصادقة الشبكية (٨٠٢.١X) وخوادم RADIUS.
- إدارة مفاتيح التشفير اللاسلكية.
- تكوين الشبكات اللاسلكية الآمنة على نقاط الوصول.
- فصل الشبكات اللاسلكية (VLANs) لأغراض الأمن.
- تطبيق سياسات كلمة المرور القوية.
- استخدام الشهادات الرقمية في المصادقة اللاسلكية.

الوحدة الثالثة: دفاعات الشبكات اللاسلكية المتقدمة

- أنظمة كشف ومنع التسلل اللاسلكي (WIDS/WIPS).
- جدران الحماية اللاسلكية المتقدمة.
- الشبكات الافتراضية الخاصة (VPN) عبر Wi-Fi.
- أمن الأجهزة الطرفية المتصلة بالشبكة اللاسلكية.
- مراقبة حركة المرور اللاسلكية للنشاط المشبوه.
- تقنيات حماية Wi-Fi Protected Setup (WPS).
- إدارة الثغرات الأمنية في أجهزة الواي فاي.

والاستجابة للحوادث الوحدة الرابعة: إدارة أمن الشبكات اللاسلكية

- أدوات إدارة أمن الشبكات اللاسلكية.
- مراجعة سجلات الأمن اللاسلكي وتحليلها.
- إجراء تقييمات الضعف واختبارات الاختراق اللاسلكية.
- وضع خطط الاستجابة للحوادث الأمنية اللاسلكية.
- إجراء التدريبات الأمنية للموظفين.
- تطبيق التحديثات الأمنية الدورية لأجهزة الواي فاي.
- الامتثال للمعايير الأمنية للشبكات اللاسلكية.

والمستقبل الأمني الوحدة الخامسة: تقنيات الواي فاي الناشئة

- أمن Wi-Fi ٦ (٨٠٢.١١ax) و Wi-Fi ٧ (٨٠٢.١١be).
- أمن شبكات 5G الخاصة (Private 5G).
- الإنترنت اللاسلكي للأشياء (IoT) وأمنه.
- الذكاء الاصطناعي في أمن الشبكات اللاسلكية.
- تقنيات المصادقة المتقدمة (Multi-factor Authentication, Biometrics).
- تحديات الأمن اللاسلكي في البيئات السحابية.
- مستقبل أمن الشبكات اللاسلكية وتطورها.

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:

للمتخصصين في أمن وازدياد اعتمادنا على الاتصال اللاسلكي في كل جانب في ظل التطور المتسارع للتهديدات السيبرانية للمستخدمين، وبين فرض أعلى مستويات الشبكات تحقيق التوازن بين توفير الوصول السهل من جوانب حياتنا، كيف يمكن فاي؟ الحماية والأمان للبيانات الحساسة عبر شبكات الواي والمرونة

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

على المفاهيم اللاسلكية والواي فاي من منظور متعمق وعملي، مما تتميز هذه الدورة بتركيزها الشامل على أمن الشبكات بين فهم التهديدات السيبرانية الأساسية. يقدم BIG BEN Training Center منهجًا يجعلها مختلفة عن الدورات التي تقتصر التركيز على مع التركيز على التحديات الأمنية الفريدة للبيئات المتقدمة والتطبيق العملي المكثف لتقنيات الدفاع، فريدًا يجمع عبر الهواء، والاستجابة الفعالة للحوادث تأمين بروتوكولات الواي فاي الحديثة، حماية اللاسلكية. ما يميز هذه الدورة هو شبكات لاسلكية تحليل الأمن اللاسلكي والممارسات الصناعية الرائدة، الأمنية اللاسلكية. يتم تزويد المشاركين بأدوات البيانات تهدف إلى بناء خبراء قادرين فعالة وموثوقة. هذه الدورة ليست مجرد تدريب، بل هي مما يؤهلهم لتصميم، تأمين، وإدارة قيمة مضافة حقيقية لأي مؤسسة تسعى لتعزيز على حماية البنية التحتية اللاسلكية الحيوية، مما تجربة تعليمية تحويلية دفاعاتها السيبرانية. يجعلهم