الدورة التدريبية: أمن الشبكات والوقاية من الاختراقات للشركات



18 - 22 اكتوبر 2026
المنامة
4400 € (للشخص الواحد)
Ref: #CYB6531_397337

مقدمة الدورة التدريبية / لمحة عامة:

في ظل التزايد المستمر للتهديدات السيبرانية، أصبح أمن الشبكات ضرورة حتمية للشركات بجميع أحجامها. تقدم هذه الدورة التدريبية الشاملة للمحترفين الأدوات والمعرفة اللازمة لبناء شبكات آمنة والوقاية من الاختراقات بفعالية. سنتناول في هذه الدورة مفاهيم أمن الشبكات الأساسية والمتقدمة، تصميم الشبكات الآمنة، وتطبيق الدفاعات ضد الهجمات المتطورة. سيكتسب المشاركون مهارات عملية في تكوين جدران الحماية (Firewalls)، أنظمة كشف التسلل (IDS/IPS)، وشبكات VPN. تهدف الدورة إلى تمكين المهنيين من حماية البنية التحتية للشبكة، بيانات الشركات، وضمان استمرارية الأعمال في مواجهة التهديدات السيبرانية المتغيرة. يستند المحتوى إلى أحدث المعايير الصناعية وأفضل الممارسات، مع الاستفادة من خبرات خبراء أكاديميين بارزين مثل البروفيسور ويليام ستالينغز (William Stallings)، مؤلف العديد من الكتب المرجعية في أمن الشبكات والأنظمة الموزعة. يقدم BIG BEN Training Center هذه الدورة لمساعدة الشركات على تعزيز قدراتها الدفاعية السيبرانية وتقليل مخاطر الهجمات الإلكترونية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو الشبكات ومسؤولون الشبكات.
- متخصصو الأمن السيبراني.
- مديرو تكنولوجيا المعلومات ومديرو أمن المعلومات.
- مدققو الأنظمة الأمنية.
- أي مهني مسؤول عن أمن البنية التحتية للشبكة في مؤسسته.

القطاعات والصناعات المستهدفة:

- شركات تكنولوجيا المعلومات والاتصالات.
- القطاع المالي والمصرفي لأمن الشبكات المصرفية.
- القطاع الحكومي والهيئات العامة وما في حكمها لحماية الشبكات الحكومية.
- قطاع الطاقة والمرافق الحيوية.
- شركات التصنيع.
- قطاع التجزئة والتجارة الإلكترونية.

الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- إدارة أمن المعلومات.
- إدارة الشبكات.
- إدارة العمليات.
- إدارة المخاطر.

أهداف الدورة التدريبية:

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

- فهم مبادئ أمن الشبكات وآليات الهجوم الشائعة.
- القدرة على تصميم وتنفيذ شبكات آمنة.
- تكوين جدران الحماية (Firewalls) وأنظمة كشف ومنع التسلل (IDS/IPS).
- إدارة الثغرات الأمنية في الشبكات والوقاية من الاختراقات.
- تأمين الشبكات اللاسلكية والشبكات الافتراضية الخاصة (VPNs).
- مراقبة أمن الشبكات والاستجابة للحوادث الأمنية.
- وضع سياسات وإجراءات أمن الشبكات الفعالة.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية وشاملة، تركز على تزويد المشاركين بالخبرة المباشرة في تأمين الشبكات والوقاية من الاختراقات. سيتمكن المتدربون من خلال ورش العمل المكثفة والمحاكاة الواقعية من تطبيق أدوات وتقنيات أمن الشبكات بشكل عملي. تتضمن المنهجية دراسات حالة مفصلة لاختراقات شبكية حقيقية، مع تحليل كيفية حدوثها وكيفية الوقاية منها. سيتم التركيز على التكوينات الأمنية الصحيحة للأجهزة والبرمجيات، وكيفية تحليل سجلات الشبكة لاكتشاف الأنشطة المشبوهة. يقدم BIG BEN Training Center هذه الدورة لتمكين المهنيين من بناء دفاعات شبكية قوية وفعالة في بيئاتهم التنظيمية. يتم تشجيع التفاعل والنقاش لتبادل أفضل الممارسات والخبرات بين المشاركين.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن الشبكات ومفاهيم الهجوم

- مقدمة إلى مبادئ أمن الشبكات.
- نماذج التهديدات الشبكية وأنواع الهجمات.
- نقاط الضعف الشائعة في الشبكات.
- أمن الطبقات المختلفة في نموذج OSI/TCP-IP.
- المهارات الأساسية لمحلل أمن الشبكات.
- هجمات حجب الخدمة (DoS/DDoS).
- الهندسة الاجتماعية وأثرها على أمن الشبكات.

الوحدة الثانية: جدران الحماية وأنظمة كشف ومنع التسلل

- مفاهيم جدران الحماية (Firewalls) وأنواعها.
- تكوين قواعد جدران الحماية وتطبيقها.
- أنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS).
- تصميم وتنفيذ IDS/IPS.
- تجاوز جدران الحماية وأنظمة IDS/IPS.
- أمن الشبكات في البيئات الافتراضية.
- إدارة السجلات والإنذارات الأمنية.

الوحدة الثالثة: تأمين الشبكات اللاسلكية والشبكات الافتراضية الخاصة

- تحديات أمن الشبكات اللاسلكية (Wi-Fi Security).
- معايير أمن الشبكات اللاسلكية (WEP, WPA, WPA2, WPA3).
- تكوين نقاط الوصول الآمنة.
- مقدمة إلى الشبكات الافتراضية الخاصة (VPNs).
- أنواع VPNs وتكوينها.
- تشفير الاتصالات في VPNs.
- أمن الشبكات اللاسلكية للمؤسسات.

الوحدة الرابعة: تقييم الثغرات وإدارة المخاطر الشبكية

- عملية تقييم الثغرات الأمنية في الشبكات.
- أدوات فحص الثغرات (مثل Nessus, OpenVAS).
- إدارة المخاطر الأمنية للشبكات.
- التعامل مع الثغرات المكتشفة.
- اختبار الاختراق للشبكات الداخلية والخارجية.
- تحليل سجلات الشبكة (Network Log Analysis).
- الاستجابة للحوادث الأمنية في الشبكة.

الوحدة الخامسة: أمن الشبكات المتقدم والاتجاهات المستقبلية

- أمن الشبكات في البيئات السحابية.
- أمن الشبكات المعرفة بالبرمجيات (SDN Security).
- أمن الإنترنت من الأشياء (IoT Security) في الشبكات.
- أمن شبكات التشغيل الصناعية (OT Security).
- الذكاء الاصطناعي في أمن الشبكات.
- الاتجاهات المستقبلية لأمن الشبكات.
- بناء إطار عمل أمني شامل للشبكة.

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 عصر تتزايد فيه تعقيدات الهجمات السيبرانية وتنوع الشبكات (تقليدية، سحابية، IoT)، كيف يمكن للمؤسسات أن تتبنى نهجًا استباقيًا لأمن الشبكات لا يقتصر على الدفاع ضد التهديدات المعروفة، بل يمتد ليشمل بناء بنية تحتية شبكية مرنة قادرة على التكيف مع التحديات المستقبلية غير المتوقعة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل والعميق على أمن الشبكات والوقاية من الاختراقات، وتقديم رؤى عملية تتجاوز المفاهيم النظرية. نغوص في التكوينات الأمنية المتقدمة لجدران الحماية وأنظمة IDS/IPS، مما يميزها عن الدورات التي تقدم نظرة عامة فقط. نقدم أمثلة عملية واقعية لسيناريوهات الاختراق وكيفية بناء دفاعات قوية ضدها. تركز الدورة على تزويد المشاركين بالمهارات العملية في تأمين الشبكات اللاسلكية، والشبكات الافتراضية الخاصة (VPNs)، وإدارة الثغرات. إنها ليست مجرد دورة لتعلم أدوات محددة، بل هي تدريب مكثف يهدف إلى بناء مهندسي شبكات أمنيين قادرين على حماية البنية التحتية الحيوية للشركات بفعالية وكفاءة.