الدورة التدريبية: الشبكات والخوادم: حماية البنية التحتية الرقمية الحيوية



18 - 22 اكتوبر 2026
عمان
3800 € (للشخص الواحد)
Ref: #SM1213_401075

مقدمة الدورة التدريبية / لمحة عامة:

في عصر التحول الرقمي، أصبحت الشبكات والخوادم: حماية البنية التحتية الرقمية الحيوية هي الركيزة الأساسية لأي مؤسسة تسعى لضمان استمرارية أعمالها وسلامة بياناتها. هذه الدورة التدريبية الشاملة مصممة لتزويد المتخصصين في تقنية المعلومات والأمن السيبراني بالمعرفة والمهارات اللازمة لتأمين الشبكات والخوادم ضد التهديدات المتزايدة والمعقدة. سنتناول أحدث الممارسات في تصميم الشبكات الآمنة، إدارة الخوادم، اكتشاف الثغرات، وتنفيذ إجراءات الحماية المتقدمة. تستند الدورة إلى أعمال خبراء أكاديميين بارزين في مجال أمن الشبكات وأنظمة التشغيل، مثل البروفيسور Andrew Tanenbaum Andrew Tanenbaum، الذي يُعرف بإسهاماته الكبيرة في هندسة أنظمة الحاسوب. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين المهنيين من بناء دفاعات قوية، وتقليل مخاطر الاختراق، وضمان موثوقية وأمان البنية التحتية الرقمية. سيركز التدريب على الجوانب العملية والتطبيقية، مع تقديم أمثلة واقعية ودراسات حالة وتمارين عملية، لمساعدة المشاركين على تطبيق المفاهيم النظرية في بيئات عملهم الحقيقية، وتعزيز قدراتهم على مواجهة التحديات الأمنية بفعالية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو الشبكات.
- مسؤولو أنظمة الخوادم.
- محللو الأمن السيبراني.
- مديرو تقنية المعلومات.
- مسؤولو أمن المعلومات.
- مدققو الأمن.
- المطورون.

القطاعات والصناعات المستهدفة:

- قطاع تقنية المعلومات والاتصالات.
- القطاع المصرفي والمالي.
- الحكومة والدفاع.
- مراكز البيانات ومزودو الخدمات السحابية.
- الشركات الصناعية الكبرى.
- الرعاية الصحية.
- التجارة الإلكترونية.

الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- إدارة أمن المعلومات.
- العمليات الفنية.
- إدارة الشبكات.
- إدارة الأنظمة والخوادم.
- قسم الدعم الفني.
- فرق البحث والتطوير.

أهداف الدورة التدريبية:

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

- فهم بنية الشبكات والخوادم وتكويناتها الأمنية.
- تطبيق أفضل الممارسات لتأمين الشبكات والخوادم.
- اكتشاف الثغرات الأمنية ومعالجتها.
- تكوين جدران الحماية وأنظمة كشف التسلل (IDS/IPS).
- إدارة الوصول والامتيازات على الخوادم.
- التعامل مع هجمات الشبكات والخوادم (مثل DDoS).
- تنفيذ آليات النسخ الاحتياطي والاستعادة الآمنة.
- مراقبة أداء وأمن الشبكات والخوادم.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية وعملية تهدف إلى تزويد المشاركين بفهم عميق ومهارات تطبيقية في مجال الشبكات والخوادم: حماية البنية التحتية الرقمية الحيوية. تبدأ المنهجية بمحاضرات متعمقة يقدمها خبراء متخصصون في أمن الشبكات والخوادم، يليها جلسات نقاش حيوية لتبادل الأفكار والتحديات. يتم التركيز بشكل كبير على دراسات الحالة الواقعية، حيث يقوم المشاركون بتحليل سيناريوهات هجمات شبكات وخوادم، وتحديد الثغرات، واقتراح حلول أمنية. تتضمن المنهجية ورش عمل تطبيقية ومختبرات افتراضية، تتيح للمتدربين تكوين جدران الحماية، وإدارة أنظمة كشف التسلل، وتأمين الخوادم بأنظمة تشغيل مختلفة. يشجع BIG BEN Training Center العمل الجماعي والتعاون بين المتدربين لتعزيز التفكير النقدي وقدرات حل المشكلات. يتم تقديم تغذية راجعة فردية ومستمرة لضمان تحقيق أقصى استفادة من الدورة. تهدف هذه المنهجية إلى تمكين المشاركين من العودة إلى مؤسساتهم وهم مسلحون بالمعرفة والأدوات والخبرة العملية اللازمة لحماية البنية التحتية الرقمية بفعالية وكفاءة عالية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الشبكات والخوادم وتحديات الأمن

- مراجعة لمفاهيم الشبكات الأساسية (OSI Model، TCP/IP).
- أنواع الشبكات (LAN، WAN، VPN) وهيكلها.
- مكونات الخوادم وأنواعها (ويب، قاعدة بيانات، تطبيق).
- أهمية حماية البنية التحتية الرقمية.
- التهديدات الشائعة التي تستهدف الشبكات والخوادم.
- مبادئ الأمن السيبراني للشبكات والخوادم.
- دور ضوابط الأمن في حماية الأنظمة.

الوحدة الثانية: تأمين الشبكات: جدران الحماية وأنظمة كشف التسلل

- تصميم الشبكات الآمنة وتقسيمها (VLANs).
- مفاهيم جدران الحماية (Firewalls) وأنواعها.
- تكوين سياسات جدران الحماية الفعالة.
- أنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS).
- نشر وإدارة IDS/IPS.
- أمن الشبكات اللاسلكية (Wi-Fi Security).
- تقنيات أمن الشبكات المتقدمة (NAC، DLP).

الوحدة الثالثة: حماية الخوادم: أنظمة التشغيل والتصلب

- تأمين أنظمة تشغيل الخوادم (Windows Server، Linux).
- تقنيات تصلب الخوادم (Server Hardening).
- إدارة الثغرات الأمنية وتصحيحات النظام (Patch Management).
- إدارة المستخدمين والامتيازات على الخوادم.
- أمن تطبيقات الخوادم والخدمات.
- مراقبة سجلات الأحداث (Event Logs) على الخوادم.
- أمن البيانات المخزنة على الخوادم.

الوحدة الرابعة: أمن التطبيقات وقواعد البيانات على الخوادم

- أمن تطبيقات الويب على الخوادم.
- الثغرات الشائعة في تطبيقات الويب (OWASP Top 10).
- تأمين قواعد البيانات (SQL Injection، Access Control).
- تشفير البيانات في قواعد البيانات وأثناء النقل.
- إدارة المفاتيح والتصاريح لقواعد البيانات.
- مراقبة أداء وأمن قواعد البيانات.
- أمن واجهات برمجة التطبيقات (APIs) في الخوادم.

الوحدة الخامسة: الاستجابة للحوادث والتعافي في بيئات الشبكات والخوادم

- مخطط الاستجابة للحوادث الأمنية في الشبكات والخوادم.
- تقنيات الاحتواء والاستعادة بعد الهجمات.
- النسخ الاحتياطي واستراتيجيات التعافي من الكوارث.
- اختبار خطط التعافي من الكوارث.
- التعامل مع هجمات حجب الخدمة الموزعة (DDoS).
- أمن السحابة والبنية التحتية كخدمة (IaaS).
- الاتجاهات المستقبلية في أمن الشبكات والخوادم.

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 الاعتماد المتزايد على البنية التحتية السحابية والشبكات المعقدة، كيف يمكن للمؤسسات أن تضمن حماية متكاملة للشبكات والخوادم مع الحفاظ على مرونة وكفاءة العمليات التشغيلية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العملي والشمولي على الشبكات والخوادم: حماية البنية التحتية الرقمية الحيوية، مما يميزها عن الدورات التي تركز على جانب واحد فقط. نحن لا نكتفي بتقديم المفاهيم النظرية، بل نغوص في التطبيقات العملية من خلال ورش عمل مكثفة وتمارين مختبرية، مما يمنح المشاركين خبرة مباشرة في تأمين الأنظمة الحساسة. يضمن المحتوى الأكاديمي المتقدم، المقدم من BIG BEN Training Center، أن يكون المشاركون على اطلاع بأحدث التهديدات والحلول الأمنية في هذا المجال الحيوي. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا خبراء قادرين على تصميم، وتنفيذ، وصيانة بنية تحتية رقمية آمنة وموثوقة، مما يعزز مرونة المؤسسات وقدرتها على مواجهة التحديات السيبرانية بفعالية استثنائية.