# التدريبية: الشبكات والخوادم: حماية البنية التحتية الرقمية الحيوية الدورة

يونيو - ٠٢ يوليو ٢٠٢٦ ٢٨

الدوحة - *

(للشخص الواحد) € ٥٥٠٠

Ref: #SM1213_75111

## مقدمة الدورة التدريبية / لمحة عامة:

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

## لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

- فهم بنية الشبكات والخوادم وتكويناتها الأمنية.
- تطبيق أفضل الممارسات لتأمين الشبكات والخوادم.
- اكتشاف الثغرات الأمنية ومعالجتها.
- (IDS/IPS). تكوين جدران الحماية وأنظمة كشف التسلل
- 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:

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

## خريطة المحتوى التدريبي (محاور الدورة التدريبية):

## الأمن الوحدة الأولى: أساسيات الشبكات والخوادم وتحديات

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

## وأنظمة كشف التسلل الوحدة الثانية: تأمين الشبكات: جدران الحماية

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

## والتصلب الوحدة الثالثة: حماية الخوادم: أنظمة التشغيل

- 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 ١٠).
- 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:

### 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 ٢٠-٢٥ 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:

والخوادم مع الحفاظ السحابية والشبكات المعقدة، كيف يمكن للمؤسسات أن في ظل الاعتماد المتزايد على البنية التحتية

على مرونة وكفاءة العمليات التشغيلية؟ تضمن حماية متكاملة للشبكات

### ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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