الدورة التدريبية: الشبكات الخاصة بالبنوك والمؤسسات المالية: تصميم، أمن، وامتثال

#NO9446

الدورة التدريبية: الشبكات الخاصة بالبنوك والمؤسسات المالية: تصميم، أمن، وامتثال

مقدمة الدورة التدريبية / لمحة عامة:

تُعد الشبكات الخاصة بالبنوك والمؤسسات المالية العمود الفقري للقطاع المالي العالمي، حيث تضمن سرعة وأمان المعاملات المالية، وتحمي البيانات الحساسة للعملاء. مع التزايد المستمر للتهديدات السيبرانية وصرامة المتطلبات التنظيمية، أصبح تصميم، أمن، وامتثال الشبكات المالية أمرًا بالغ الأهمية. تقدم هذه الدورة التدريبية الشاملة منهجًا متعمقًا في بنية الشبكات المصرفية، أمن المعلومات في البنوك، وضمان الامتثال للمعايير المالية العالمية، بدءًا من المبادئ الأساسية للبنية التحتية الشبكية الآمنة وصولًا إلى التطبيقات المتقدمة في بيئات الخدمات المالية المعقدة. يركز التدريب على تزويد المشاركين بالمهارات العملية والنظرية اللازمة لبناء، صيانة، وتأمين شبكات قوية، موثوقة، ومتوافقة مع أعلى معايير الصناعة. يستعرض BIG BEN Training Center هذه المفاهيم بعمق، مستنيرًا بأعمال رواد المجال مثل البروفيسور آلان آر. شوموای (Alan R. Shomway)، الذي أسهم في فهم الأنظمة المالية وأمنها، مما يضمن تقديم محتوى أكاديمي وعملي رفيع المستوى. ستُمكن الدورة المتدربين من فهم كيفية تخطيط الشبكات المصرفية الآمنة، إدارة المخاطر السيبرانية المالية، واستكشاف مشكلات الامتثال، مما يؤهلهم لأن يكونوا خبراء في التعامل مع تحديات التحول الرقمي في القطاع المالي.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسي الشبكات في البنوك والمؤسسات المالية.
- مسؤولي أمن المعلومات في القطاع المالي.
- مديري تكنولوجيا المعلومات المصرفية.
- المتخصصين في الامتثال والتدقيق المالي.
- خبراء الأمن السيبراني المالي.
- مديري البنية التحتية المالية.
- فنيي دعم الأنظمة المصرفية.

القطاعات والصناعات المستهدفة:

- البنوك التجارية والإسلامية.
- شركات الاستثمار وإدارة الأصول.
- شركات التأمين.
- شركات التكنولوجيا المالية (FinTech).
- الجهات التنظيمية المالية (البنوك المركزية، هيئات سوق المال).
- صناديق التحوط والأسهم الخاصة.
- شركات الوساطة المالية.

الأقسام المؤسسية المستهدفة:

- قسم تكنولوجيا المعلومات المصرفية.
- إدارة أمن المعلومات.
- قسم الشبكات والاتصالات.
- إدارة المخاطر والامتثال.
- قسم التدقيق الداخلي.
- إدارة العمليات المصرفية.
- قسم البنية التحتية التقنية.

أهداف الدورة التدريبية:

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

- فهم معمق لمفاهيم الشبكات الخاصة بالبنوك والمؤسسات المالية.
- تصميم بنية شبكية مالية آمنة ومرنة.
- تأمين البنية التحتية الشبكية المصرفية ضد الهجمات السيبرانية.
- ضمان امتثال الشبكة للمعايير المالية العالمية (PCI DSS, SWIFT CSP).
- إدارة أداء الشبكات المالية وضمان التوفيرية.
- استكشاف أخطاء الشبكة وإصلاحها في البيئات المالية.
- تطبيق أفضل ممارسات أمن المعلومات المالية.
- تخطيط استمرارية الأعمال والتعافي من الكوارث للشبكات المالية.
- تنفيذ حلول الشبكات المتقدمة في القطاع المالي.
- إدارة دورة حياة الشبكة في المؤسسات المالية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية عملية وتطبيقية مكثفة، مصممة لتمكين المشاركين من اكتساب خبرة مباشرة في الشبكات الخاصة بالبنوك والمؤسسات المالية. تشمل الدورة مزيجًا من المحاضرات النظرية المتعمقة، وورش العمل العملية التي تركز على تطبيقات الشبكات المالية في سيناريوهات واقعية، مع التركيز على الأمن والامتثال. سيقوم المشاركون بتطبيق المفاهيم المكتسبة من خلال تمارين تصميم شبكات آمنة للبنوك، تكوين أجهزة الشبكة المصرفية، وتشخيص مشكلات الأمن والامتثال في بيئة معملية افتراضية تحاكي أنظمة مالية حقيقية. يتم تشجيع العمل الجماعي والمناقشات التفاعلية لتبادل الخبرات وحلول المشكلات. يقدم المدربون في BIG BEN Training Center، وهم خبراء في مجال الشبكات المصرفية والأمن المالي، تغذية راجعة فورية ودقيقة لضمان فهم عميق للمفاهيم وتطوير المهارات. تهدف المنهجية إلى إعداد المتدربين ليصبحوا قادرين على إدارة وصيانة وتأمين الشبكات المالية بفعالية واحترافية عالية، مما يحمي الأصول الرقمية للمؤسسات.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الشبكات المالية والمتطلبات التنظيمية

- مقدمة إلى الشبكات في القطاع المالي وأهميتها.
- مكونات البنية التحتية للشبكات المصرفية.
- المتطلبات القانونية والتنظيمية (PCI DSS, GDPR, SWIFT CSP).
- معايير أمن المعلومات (ISO 27001, NIST) في المالية.
- تصنيف البيانات المالية وأثرها على تصميم الشبكة.
- نظرة عامة على الأنظمة المالية الأساسية (Core Banking Systems).
- مخاطر الأمن السيبراني في القطاع المالي.

الوحدة الثانية: تصميم وهندسة الشبكات المصرفية الآمنة

- مبادئ تصميم الشبكات الآمنة للمؤسسات المالية.
- هندسة الشبكات المصرفية ذات التوفيرية العالية.
- تجزئة الشبكات (Network Segmentation) للفصل الأمني.
- اختيار أجهزة الشبكة المتوافقة مع المعايير المالية.
- تنفيذ الشبكات الافتراضية الخاصة (VPN) المصرفية.
- تصميم الشبكات لمراكز البيانات المالية.
- البنية التحتية السحابية الآمنة في البنوك.

الوحدة الثالثة: أمن الشبكات المالية والامتثال

- تهديدات الأمن السيبراني المتقدمة في القطاع المالي (APT, Ransomware).
- تقنيات الحماية المتقدمة (Firewalls, IDS/IPS, SIEM, DLP).
- إدارة الثغرات الأمنية والتصحيحات الأمنية.
- المصادقة والتحكم بالوصول (IAM) في البيئات المالية.
- الامتثال للمعايير الدولية (Basel III, SOX).
- التدقيق الأمني للشبكات المالية.
- التعامل مع حوادث الأمن السيبراني المالي.

الوحدة الرابعة: إدارة وتشغيل الشبكات المالية

- أدوات إدارة ومراقبة الشبكات المالية.
- تحليل أداء الشبكة وإدارة النطاق الترددي.
- إدارة التكوينات والتغييرات في الشبكة.
- صيانة وتحديث أجهزة الشبكة المصرفية.
- إدارة جودة الخدمة (QoS) للأنظمة المالية الحرجة.
- التوثيق والتقارير في البيئة المالية.
- استمرارية الأعمال والتعافي من الكوارث للشبكات المصرفية.

الوحدة الخامسة: استكشاف الأخطاء، التحسين، والتوجهات المستقبلية

- منهجيات استكشاف أخطاء الشبكات المالية.
- تشخيص مشكلات الاتصال والأداء في البنوك.
- حل مشكلات الامتثال.
- تحسين الشبكات المالية لزيادة الكفاءة والأمان.
- الشبكات المعرفة بالبرمجيات (SDN) في البنوك.
- الحوسبة السحابية الآمنة والخدمات المالية.
- مستقبل التقنيات المالية (FinTech) وتأثيرها على الشبكات.

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 التحديات المتزايدة للأمن السيبراني والضغط المستمر للتحول الرقمي في القطاع المالي، كيف يمكن للمؤسسات المالية الموازنة بين الحاجة إلى الابتكار وتبني التقنيات الحديثة، وبين الالتزام الصارم باللوائح والمعايير الأمنية لضمان حماية أصول العملاء وسلامة الأنظمة المالية الحيوية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل على الشبكات الخاصة بالبنوك والمؤسسات المالية من منظور متعمق وعملي، مما يجعلها مختلفة عن الدورات التي تقتصر على المفاهيم العامة للشبكات. يقدم BIG BEN Training Center منهجًا فريدًا يجمع بين أسس تصميم الشبكات الآمنة والتطبيق العملي المكثف لمعايير الامتثال المالي، مع التركيز على التحديات الأمنية والتشغيلية الفريدة التي تواجه القطاع المالي. ما يميز هذه الدورة هو التركيز على تأمين المعاملات المالية الحساسة، ضمان الالتزام بالمتطلبات التنظيمية الصارمة (مثل PCI DSS وSWIFT CSP)، وإدارة المخاطر السيبرانية بفعالية. يتم تزويد المشاركين بأدوات مراقبة الشبكات المالية والممارسات الصناعية الرائدة، مما يؤهلهم لتصميم، تأمين، وإدارة شبكات مالية فعالة وموثوقة. هذه الدورة ليست مجرد تدريب، بل هي تجربة تعليمية تحويلية تهدف إلى بناء خبراء قادرين على قيادة مشاريع البنية التحتية الشبكية في القطاع المالي، مما يجعلهم قيمة مضافة حقيقية لأي مؤسسة مالية تسعى لتحقيق أعلى مستويات الأمن والمرونة.