الدورة التدريبية: هندسة الاتصالات المتقدمة للبنية التحتية الحيوية والأمن القومي الشامل

#TEL1751

الدورة التدريبية: هندسة الاتصالات المتقدمة للبنية التحتية الحيوية والأمن القومي الشامل

مقدمة الدورة التدريبية / لمحة عامة:

تُعد البنية التحتية الحيوية، بما في ذلك شبكات الاتصالات، شريان الحياة لأي دولة حديثة، فهي تدعم جميع القطاعات من الدفاع إلى الخدمات المدنية والاقتصاد. أصبحت هندسة الاتصالات في هذا السياق لا تقتصر على التصميم والتشغيل فحسب، بل تمتد لتشمل الأمن القومي والمرونة ضد التهديدات المتزايدة. تقدم هذه الدورة التدريبية من BIG BEN Training Center فهمًا شاملًا للمفاهيم المتقدمة في هندسة الاتصالات المصممة خصيصًا لحماية وتعزيز البنية التحتية الحيوية والأمن القومي. سنتناول في هذه الدورة تصميم شبكات الاتصالات المؤمنة، واستخدام التقنيات الحديثة مثل الجيل الخامس (5G) والشبكات المعرفة بالبرمجيات (SDN) في بيئات حساسة. سيتعرف المشاركون على تحديات الأمن السيبراني الموجهة ضد البنية التحتية للاتصالات، واستراتيجيات الدفاع المتقدمة، وإدارة المخاطر السيبرانية. كما ستسلط الدورة الضوء على أهمية التشفير (Encryption)، والتعافي من الكوارث (Disaster Recovery)، واستمرارية الأعمال (Business Continuity) لضمان صمود الأنظمة الاتصالية في أوقات الأزمات. تستند محاور الدورة إلى أحدث المعايير والممارسات الدولية، مستلهمة من رؤى أكاديميين وخبراء مثل William Stallings في كتابه Cryptography and Network Security Principles and Practice, الذي يُعد مرجعًا أساسيًا في مجال أمن الشبكات. هذه الدورة هي بوابتك نحو إتقان هندسة الاتصالات للأمن القومي، مما يمكنك من المساهمة في بناء بنية تحتية اتصالية مرنة ومحصنة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو الاتصالات والشبكات في القطاع الحكومي.
- أخصائيو الأمن السيبراني والدفاع الإلكتروني.
- مديرو مشاريع البنية التحتية الحيوية.
- المتخصصون في إدارة المخاطر الاستراتيجية.
- قادة الفرق الفنية في قطاعات الدفاع والأمن.
- الجهات التنظيمية في قطاع الاتصالات.
- خبراء التعافي من الكوارث واستمرارية الأعمال.
- صناع القرار في المجالات الاستراتيجية الوطنية.
- الباحثون في أمن الاتصالات.

القطاعات والصناعات المستهدفة:

- القطاع الحكومي (الدفاع، الأمن، الاستخبارات).
- شركات الاتصالات ومزودي الخدمات.
- شركات تطوير البنية التحتية الحيوية.
- مراكز البيانات الحساسة.
- قطاع الطاقة والمياه.
- قطاع النقل (الموانئ، المطارات، السكك الحديدية).
- شركات الأمن السيبراني المتخصصة.
- المؤسسات المالية الكبرى.
- الجهات البحثية والتطويرية في الأمن القومي.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- قسم هندسة الشبكات والاتصالات.
- إدارة البنية التحتية الحيوية.
- قسم التخطيط الاستراتيجي.
- إدارة العمليات والدعم الفني.
- فرق الاستجابة للحوادث الأمنية.
- إدارة المخاطر والامتثال.
- وحدات البحث والتطوير.
- إدارة الأمن المادي والمنطقي.

أهداف الدورة التدريبية:

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

- فهم مفهوم البنية التحتية الحيوية وأهمية الاتصالات.
- تحديد التهديدات الأمنية التي تواجه شبكات الاتصالات الوطنية.
- تصميم بنى تحتية للاتصالات مرنة ومقاومة للهجمات.
- تطبيق تقنيات التشفير المتقدمة لحماية البيانات.
- إدارة مخاطر الأمن السيبراني في أنظمة الاتصالات.
- وضع خطط التعافي من الكوارث لشبكات الاتصالات.
- الاستفادة من التقنيات الناشئة (5G, SDN) في تعزيز الأمن.
- فهم الأطر القانونية والتنظيمية للأمن القومي.
- بناء قدرات وطنية في هندسة الاتصالات الدفاعية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تعليمية متقدمة تجمع بين الشرح النظري المتعمق والمحاكاة العملية، بهدف تزويد المشاركين بالمهارات اللازمة لهندسة الاتصالات في سياق البنية التحتية الحيوية والأمن القومي. ستبدأ الدورة بتحليل دقيق لسيناريوهات التهديد المعقدة، مدعومة بدراسات حالة استخباراتية وأمثلة من الهجمات السيبرانية على الشبكات الحيوية. سيشارك المتدربون في ورش عمل تطبيقية مكثفة تركز على تصميم شبكات مؤمنة، وتكوين الأجهزة الأمنية، واختبار نقاط الضعف باستخدام أدوات المحاكاة. سيتم التركيز على التمارين العملية التي تحاكي بيئات حقيقية، مما يتيح للمشاركين تطبيق تقنيات التشفير، وأنظمة كشف التسلل (IDS)، وجدران الحماية المتقدمة. يقدم المدربون الخبراء في BIG BEN Training Center، الذين يمتلكون خلفيات عسكرية وأمنية وتقنية، تغذية راجعة فورية ومخصصة. تهدف هذه المنهجية إلى بناء قدرات المتدربين على تحليل التهديدات الاستراتيجية، وتصميم حلول اتصالات قوية، وضمان الصمود التشغيلي، مما يمكنهم من حماية أصول الاتصالات الوطنية الحيوية بفعالية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة إلى البنية التحتية الحيوية وأمن الاتصالات.

- مفهوم البنية التحتية الحيوية وأهميتها.
- تصنيف أنظمة الاتصالات الحرجة.
- التهديدات السيبرانية والهجمات الموجهة ضد الاتصالات.
- دور هندسة الاتصالات في الأمن القومي.
- أطر عمل الأمن السيبراني للبنية التحتية.
- دراسات حالة للهجمات على شبكات الاتصالات.
- مفاهيم المرونة (Resilience) والصمود (Survivability).

الوحدة الثانية: تصميم شبكات الاتصالات المؤمنة والمرنة.

- مبادئ التصميم الآمن للشبكات.
- تقسيم الشبكات (Network Segmentation).
- التكرار (Redundancy) وتجاوز الفشل (Failover) في تصميم الشبكة.
- البنى التحتية الموزعة والمشفرة.
- أمن الطبقة المادية للاتصالات.
- حماية نقاط التجمع (Concentration Points).
- تصميم شبكات 5G الآمنة.

الوحدة الثالثة: الأمن السيبراني المتقدم لشبكات الاتصالات.

- هجمات حجب الخدمة الموزعة (DDoS) على الاتصالات.
- الهندسة الاجتماعية والاحتيال الإلكتروني.
- أدوات وأنظمة كشف التهديدات (SIEM, IDS/IPS).
- إدارة الثغرات الأمنية (Vulnerability Management).
- أمن الحوسبة السحابية (Cloud Security) للاتصالات.
- الأمن المادي والوصول غير المصرح به.
- الاستجابة للحوادث السيبرانية في الوقت الحقيقي.

الوحدة الرابعة: التشفير، المصادقة، وإدارة الهوية.

- مبادئ التشفير (Symmetric, Asymmetric).
- خوارزميات التشفير المتقدمة (AES, RSA).
- البنية التحتية للمفاتيح العامة (PKI).
- المصادقة متعددة العوامل (MFA).
- إدارة الهوية والوصول (IAM).
- التوقيعات الرقمية والشهادات.
- أمن الاتصالات الصوتية والمرئية.

الوحدة الخامسة: استمرارية الأعمال والتعافي من الكوارث للأمن القومي.

- تحليل المخاطر وتقييم الأثر الأمني.
- خطط استمرارية الأعمال (BCP) للبنية التحتية.
- خطط التعافي من الكوارث (DRP) لشبكات الاتصالات.
- مراكز العمليات البديلة ومواقع التعافي.
- اختبار وتدريب فرق الاستجابة للطوارئ.
- الامتثال التنظيمي والمتطلبات القانونية للأمن القومي.
- التنسيق بين الجهات في أوقات الأزمات الوطنية.

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 التطور السريع للتهديدات السيبرانية والتقنيات الناشئة، كيف يمكن للمؤسسات المسؤولة عن البنية التحتية الحيوية للاتصالات أن تبتكر استراتيجيات دفاعية استباقية لا تكتفي برد الفعل، بل تستبق التهديدات المستقبلية وتضمن حماية فائقة للأمن القومي في عالم متزايد الترابط؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتقديمها تركيزًا فريدًا وعميقًا على هندسة الاتصالات من منظور البنية التحتية الحيوية والأمن القومي، مما يجعلها مختلفة بشكل جوهري عن الدورات التقليدية. بخلاف الدورات التي تتناول الأمن السيبراني بشكل عام، تتعمق هذه الدورة في التحديات الأمنية الخاصة بقطاع الاتصالات الحساسة، وكيفية تصميم أنظمة قادرة على الصمود في وجه الهجمات المعقدة. يقدم BIG BEN Training Center هذه الدورة بمنهجية تدريبية تجمع بين المعرفة الأكاديمية المتخصصة والتطبيقات العملية الواقعية، مدعومة بدراسات حالة استخباراتية وأمثلة من سيناريوهات التهديد الحقيقية. سيتم تزويد المشاركين بالمهارات اللازمة لتحليل التهديدات الاستراتيجية، وتصميم بنى تحتية اتصالية مقاومة للتعطيل، وتطبيق أحدث تقنيات الأمن السيبراني. هذه الدورة هي الخيار الأمثل للمهنيين الذين يتحملون مسؤولية حماية أمن الاتصالات الوطنية والبنية التحتية الحيوية.