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

اغسطس ٢٠٢٦ ٠٧ - ٠٣

باكو - *

(للشخص الواحد) € ٥٠٠٠

Ref: #TEL1751_413671

مقدمة الدورة التدريبية / لمحة عامة:

إلى الخدمات المدنية الاتصالات، شريان الحياة لأي دولة حديثة، فهي تدعم تُعد البنية التحتية الحيوية، بما في ذلك شبكات والتشغيل فحسب، بل تمتد لتشمل والاقتصاد. أصبحت هندسة الاتصالات في هذا السياق لا جميع القطاعات من الدفاع تقدم هذه الدورة التدريبية منBIG BEN Training الأمن القومي والمرونة ضد التهديدات المتزايدة. تقتصر على التصميم سنتناول في هذه الاتصالات المصممة خصيصًا لحماية وتعزيز البنية فهمًا شاملا للمفاهيم المتقدمة في هندسة Center مثل الجيل الخامس (G0) والشبكات الدورة تصميم شبكات الاتصالات المؤمنة، واستخدام التحتية الحيوية والأمن القومي. على تحديات الأمن السيبراني الموجهة ضد المعرفة بالبرمجيات (SDN) في بيئات حساسة. سيتعرف التقنيات الحديثة (Encryption)، المتقدمة، وإدارة المخاطر السيبرانية. كما ستسلط البنية التحتية للاتصالات، واستراتيجيات الدفاع المشاركون الأعمال (Business Continuity) لضمان والتعافي من الكوارث (Disaster Recovery)، الدورة الضوء على أهمية التشفير وخبراء مثل محاور الدورة إلى أحدث المعايير والممارسات صمود الأنظمة الاتصالية في أوقات الأزمات. تستند واستمرارية Cryptography and Network Security Principles and في كتابه William Stallings الدولية، مستلهمة من رؤى أكاديميين تحتية الدورة هي بوابتك نحو إتقان هندسة الاتصالات للأمن يُعد مرجعًا أساسيًا في مجال أمن الشبكات. هذه الذي ,Practice اتصالية مرنة ومحصنة. القومي، مما يمكنك من المساهمة في بناء بنية

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:

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

- فهم مفهوم البنية التحتية الحيوية وأهمية الاتصالات.
- الاتصالات الوطنية. تحديد التهديدات الأمنية التي تواجه شبكات
- 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.
- الأمن. الاستفادة من التقنيات الناشئة (G, SDN0) في تعزيز
- فهم الأطر القانونية والتنظيمية للأمن القومي.
- بناء قدرات وطنية في هندسة الاتصالات الدفاعية.

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

وأمن الاتصالات. الوحدة الأولى: مقدمة إلى البنية التحتية الحيوية

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

والمرنة. الوحدة الثانية: تصميم شبكات الاتصالات المؤمنة

- مبادئ التصميم الآمن للشبكات.
- تقسيم الشبكات (.Network Segmentation)
- تصميم الشبكة. التكرار (Redundancy) وتجاوز الفشل (Failover) في
- البنى التحتية الموزعة والمشفرة.
- أمن الطبقة المادية للاتصالات.
- حماية نقاط التجمع (.Concentration Points)
- تصميم شبكات 0 Gالآمنة.

الاتصالات. الوحدة الثالثة: الأمن السيبراني المتقدم لشبكات

- 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.

الكوارث للأمن القومي. الوحدة الخامسة: استمرارية الأعمال والتعافي من

- 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.
- القومي. الامتثال التنظيمي والمتطلبات القانونية للأمن
- التنسيق بين الجهات في أوقات الأزمات الوطنية.

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 ٢٥٢٠- 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:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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