

الصمود السيرياني لمهنيي الاتصالات: استراتيجيات
الدفاع المتقدمة

UK Traininig

PARTNER



السمود السيبراني لمهنيي الاتصالات: استراتيجيات الدفاع المتقدمة

مقدمة

تركز هذه الدورة على استراتيجيات بناء مرونة سيبرانية قوية للمهنيين في قطاع الاتصالات. سيكتسب المشاركون مهارات متقدمة للدفاع عن شبكات الاتصالات ضد التهديدات السيبرانية المتطورة. تغطي الدورة المبادئ الأساسية للمرونة السيبرانية، وأفضل الممارسات، وآليات الدفاع المصممة خصيصًا لصناعة الاتصالات. سيتعلم المشاركون كيفية تحديد الثغرات، وتقييم المخاطر، وتنفيذ تدابير استباقية لحماية البنية التحتية الحيوية لقطاع الاتصالات. كما سيكتسبون فهمًا حول كيفية ضمان استمرارية خدمات الاتصالات في حال وقوع هجوم سيبراني. في نهاية الدورة، ستكون لديك المهارات اللازمة لقيادة مؤسستك في مجال المرونة السيبرانية وحمايتها من المخاطر والاضطرابات.

أهداف الدورة

- فهم مفهوم المرونة السيبرانية وأهميتها في شبكات الاتصالات.
- تعلم استراتيجيات دفاع متقدمة لحماية البنية التحتية في قطاع الاتصالات.
- تحديد الثغرات وتقييم المخاطر السيبرانية في عمليات الاتصالات.
- تطوير مهارات عملية للرد على الحوادث السيبرانية والتعافي منها.
- استكشاف تقنيات لضمان استمرارية خدمات الاتصالات أثناء الهجمات السيبرانية.
- فهم متطلبات التنظيم والامتثال للأمن السيبراني في الاتصالات.
- إتقان أساليب اكتشاف التهديدات وطرق التخفيف منها في بيئات الاتصالات.
- تعلم كيفية تصميم وتنفيذ إطار الأمن السيبراني لأنظمة الاتصالات.
- اكتساب الخبرة في إدارة العمليات الأمنية وفرق الاستجابة للحوادث.
- تعلم كيفية دمج استراتيجيات المرونة السيبرانية في العمليات اليومية لقطاع الاتصالات.

UK Training

PARTNER



محاورة الدورة

اليوم الأول: مقدمة في المرونة السيبرانية في قطاع الاتصالات

- فهم مفهوم المرونة السيبرانية وأهميتها في قطاع الاتصالات.
- استكشاف دور المهنيين في قطاع الاتصالات في ضمان المرونة السيبرانية.
- دراسة تأثير الهجمات السيبرانية على البنية التحتية في الاتصالات.
- مراجعة المشهد المتطور للتهديدات لمشغلي الاتصالات.
- مناقشة مبادئ إدارة المخاطر في سياق أمن الاتصالات.

اليوم الثاني: تقنيات متقدمة لاكتشاف التهديدات والوقاية منها

- تعلم كيفية اكتشاف التهديدات في شبكات الاتصالات باستخدام أساليب متقدمة.
- استكشاف أدوات الذكاء الاصطناعي والتعلم الآلي لاكتشاف التهديدات.
- دراسة دور مراقبة الشبكات واكتشاف الأنماط الشاذة.
- تعلم عن أنظمة اكتشاف التسلل IDS وأنظمة منع التسلل IPS.
- مناقشة التهديدات الناشئة مثل الثغرات في إنترنت الأشياء وهجمات سلسلة التوريد.

اليوم الثالث: تطوير وتنفيذ استراتيجية للمرونة السيبرانية

- تطوير استراتيجية مرونة سيبرانية شاملة لشبكات الاتصالات.
- تعلم كيفية دمج المرونة السيبرانية في تصميم وبنية الشبكة.
- استكشاف استراتيجيات لضمان استمرارية الخدمة وتوافر الشبكة.
- دراسة ممارسات التعافي من الكوارث و استمرارية الأعمال في قطاع الاتصالات.
- تعلم عن أنظمة النسخ الاحتياطي والازدواجية لبناء بنية تحتية مرنة.

اليوم الرابع: الجوانب التنظيمية والقانونية والامتثال في المرونة السيبرانية

- فهم الإطار القانوني والتنظيمي الذي يؤثر على أمن الاتصالات السيبراني.
- استكشاف متطلبات الامتثال لمشغلي الاتصالات مثل GDPR, NIST, و ISO 27001.
- مناقشة قضايا الخصوصية وحماية البيانات لخدمات الاتصالات.
- مراجعة دور الهيئات التنظيمية في فرض معايير أمن الشبكات في الاتصالات.
- تعلم كيفية دمج المرونة السيبرانية في الحوكمة والهيكل التنظيمية.

UK Traininig

PARTNER



اليوم الخامس: بناء ثقافة للمرونة السيبرانية والتحضير للمستقبل

- تعلم كيفية تعزيز ثقافة المرونة السيبرانية داخل منظمات الاتصالات.
- تطوير برامج تدريبية للموظفين لتحسين الوعي السيبراني.
- استكشاف الاتجاهات المستقبلية في المرونة السيبرانية داخل قطاع الاتصالات.
- دراسة إمكانيات الأتمتة وأدوات التنسيق في إدارة الحوادث.
- التفكير في دراسات حالة ناجحة للمرونة السيبرانية في قطاع الاتصالات.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب معرفة متقدمة في المرونة السيبرانية في شبكات الاتصالات.
- إتقان استراتيجيات دفاع متقدمة لحماية أنظمة الاتصالات من التهديدات السيبرانية.
- تعلم كيفية اكتشاف التهديدات وتنفيذ تدابير الوقاية المبكرة.
- فهم كيفية ضمان توفر الشبكة أثناء الحوادث السيبرانية.
- تطوير المهارات للرد بفعالية على الحوادث السيبرانية واضطرابات الخدمة.
- تحسين الامتثال للإطارات التنظيمية في مجال أمن الاتصالات.
- بناء الخبرة في إدارة العمليات الأمنية وقيادة فرق الاستجابة للحوادث.
- تطوير خطط التعافي من الكوارث واستمرارية الأعمال لقطاع الاتصالات.
- البقاء في الصدارة من خلال استراتيجيات الدفاع المتقدمة في أمن الاتصالات.
- تمهيد الطريق لتكون قائدًا في أمن الاتصالات السيبراني.

الخاتمة

المرونة السيبرانية أمر بالغ الأهمية لصناعة الاتصالات. من خلال حضور هذه الدورة، ستكتسب المهارات المتقدمة والاستراتيجيات اللازمة لحماية شبكات الاتصالات من التهديدات السيبرانية المتطورة. ستتعلم كيفية بناء وتنفيذ آليات دفاع قوية تضمن استمرارية الخدمة وتوافر الشبكة أثناء الهجمات. إن فهم متطلبات التنظيم والامتثال، والاستجابة للحوادث، وأحدث الاتجاهات في الأمن السيبراني سيؤهلك لقيادة قطاع الاتصالات بثقة.

من خلال إتقان المرونة السيبرانية، ستكون مستعدًا لحماية شبكات الاتصالات في ظل المشهد المتطور للتهديدات.

UK Training

PARTNER

