

الصمود السيراني لمهنيي الاتصالات: استراتيجيات الدفاع المتقدمة

3 - 7 يناير 2027

القاهرة (مصر)

UK Traininig

PARTNER



السمود السيبراني لمهنيي الاتصالات: استراتيجيات الدفاع المتقدمة

المرجع: 316358_3254648 التاريخ: 3 - 7 يناير 2027 المكان: القاهرة (مصر) الرسوم: GBP 4900

مقدمة

تركز هذه الدورة على بناء استراتيجيات السمود السيبراني المتينة لمهنيي الاتصالات. سيكتسب المشاركون مهارات متقدمة للدفاع عن شبكات الاتصالات ضد التهديدات السيبرانية المتطورة. تتناول الدورة المبادئ الأساسية للأمن السيبراني وأفضل الممارسات وآليات الدفاع التي تم تصميمها خصيصًا لصناعة الاتصالات. ستتعلم كيفية تحديد الثغرات وتقييم المخاطر وتنفيذ التدابير الوقائية لحماية البنية التحتية الحيوية للاتصالات. بالإضافة إلى ذلك، ستفهم كيفية ضمان استمرارية خدمات الاتصالات في حال حدوث هجوم سيبراني. بنهاية الدورة، ستكون مستعدًا لقيادة منظمتك في حماية البنية التحتية ضد التهديدات السيبرانية.

أهداف الدورة

- فهم مفاهيم السمود السيبراني وأهميته في شبكات الاتصالات.
- تعلم استراتيجيات الدفاع المتقدمة لحماية البنية التحتية للاتصالات.
- تحديد الثغرات وتقييم المخاطر السيبرانية في عمليات الاتصالات.
- تطوير المهارات اللازمة للاستجابة لحوادث الأمن السيبراني والتعافي منها.
- استكشاف تقنيات لضمان استمرارية خدمات الاتصالات أثناء الهجمات السيبرانية.
- فهم المتطلبات التنظيمية و الامتثال المتعلقة بالأمن السيبراني في الاتصالات.
- إتقان أساليب الكشف عن التهديدات و التخفيف منها في بيئات الاتصالات.
- تعلم كيفية تصميم وتنفيذ إطارات الأمن السيبراني لشبكات الاتصالات.
- اكتساب الخبرة في إدارة عمليات الأمن وفرق الاستجابة للحوادث.
- تعلم كيفية دمج استراتيجيات السمود السيبراني في العمليات اليومية للاتصالات.

UK Traininig

PARTNER



محاور الدورة

اليوم الأول: مقدمة في الصمود السيبراني في الاتصالات

- فهم مفهوم الصمود السيبراني وأهمية ذلك في شبكات الاتصالات.
- استكشاف الفرق بين الأمن السيبراني التقليدي و الصمود السيبراني.
- دراسة تأثير الهجمات السيبرانية على البنى التحتية للاتصالات.
- فهم دور المحترفين في مجال الاتصالات في ضمان الصمود السيبراني.
- مراجعة مخاطر البيئة المتغيرة من التهديدات في مجال الاتصالات.
- مناقشة مبادئ إدارة المخاطر في أمن الاتصالات.

اليوم الثاني: تقنيات الكشف المتقدم عن التهديدات ومنعها

- تعلم أساليب متقدمة للكشف عن التهديدات في شبكات الاتصالات.
- استكشاف تقنيات الذكاء الاصطناعي و التعلم الآلي في كشف التهديدات.
- دراسة أهمية مراقبة الشبكة و كشف التهديدات الغريبة.
- تعلم استخدام أنظمة كشف التسلل IDS وأنظمة منع التسلل IPS.
- استكشاف التهديدات الناشئة مثل ثغرات إنترنت الأشياء و هجمات سلسلة التوريد.

اليوم الثالث: تطوير وتنفيذ استراتيجية الصمود السيبراني

- تعلم كيفية تطوير استراتيجية شاملة للصمود السيبراني في شبكات الاتصالات.
- استكشاف كيفية دمج الصمود في تصميم الشبكة وبنيتها.
- مناقشة استراتيجيات ضمان استمرارية الخدمة و توفر الشبكة.
- دراسة التخطيط لاستجابة الحوادث وكيفية التعافي السريع من الهجمات السيبرانية.
- تعلم أفضل الممارسات لتطوير استراتيجيات الاسترداد من الكوارث و استمرارية الأعمال في الاتصالات.

UK Training

PARTNER



اليوم الرابع: الجوانب التنظيمية والتوافقية والقانونية في الصمود السيبراني

- فهم الأنظمة القانونية والتنظيمية المؤثرة في أمن الاتصالات.
- تعلم متطلبات الامتثال لمشغلي الاتصالات مثل GDPR و NIST و ISO 27001.
- استكشاف دور الهيئات التنظيمية في فرض معايير الأمن السيبراني.
- مناقشة قضايا خصوصية البيانات وإجراءات الحماية في خدمات الاتصالات.
- تعلم كيفية دمج الصمود السيبراني في هيكل حوكمة المنظمة.

اليوم الخامس: بناء ثقافة الصمود السيبراني والاستعداد للمستقبل

- تعلم كيفية بناء ثقافة الصمود السيبراني داخل منظمات الاتصالات.
- استكشاف برامج التدريب والوعي للموظفين حول التهديدات السيبرانية.
- فهم دور القيادة في تعزيز ثقافة الأمان السيبراني.
- مناقشة مستقبل الصمود السيبراني في الاتصالات، بما في ذلك التقنيات والاتجاهات المستقبلية.
- دراسة كيفية الاستفادة من أدوات الأتمتة والتنسيق في إدارة الحوادث.
- تطوير خارطة طريق لتحسين الصمود السيبراني في شبكات الاتصالات.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب معرفة متقدمة حول الصمود السيبراني في شبكات الاتصالات.
- تعلم استراتيجيات متقدمة للدفاع لحماية أنظمة الاتصالات من التهديدات السيبرانية.
- إتقان تقنيات الكشف المبكر عن التهديدات ومنعها.
- تحسين مهاراتك في الاستجابة الفعالة للحوادث السيبرانية وضمان استمرارية الخدمة.
- فهم المتطلبات التنظيمية و الامتثال في أمن الاتصالات.
- تعلم كيفية بناء ثقافة الصمود السيبراني داخل منظمتك.
- تحسين قدرتك على إدارة الأمن السيبراني و فرق الاستجابة للحوادث.
- الاستفادة من أحدث التكتيكات الدفاعية لمواكبة التهديدات السيبرانية المتطورة.
- تعزيز فرصك المهنية في مجال أمن الاتصالات و القيادة السيبرانية.

الخاتمة

يعد الصمود السيبراني أمرًا بالغ الأهمية في صناعة الاتصالات. من خلال حضور هذه الدورة، ستكتسب المهارات المتقدمة و الاستراتيجيات اللازمة لحماية شبكات الاتصالات من التهديدات السيبرانية المتطورة. ستتعلم كيفية تصميم وتنفيذ آليات دفاع قوية لضمان استمرارية الأعمال و توفير الشبكة أثناء الهجمات.

PARTNER



بالإضافة إلى فهم الامتثال التنظيمي و استجابة الحوادث وأحدث اتجاهات الأمن السيبراني التي ستجعلك قائدا في
حماية الشبكات في بيئة تتغير بسرعة.

UK Training

PARTNER

