اللوجستية الدورة التدريبية: الأمن السيبراني لقطاع الطاقة والخدمات

مايو ٢٠٢٦ ٠٨ - ٠٤

كوالالمبور

(للشخص الواحد) € ٥٢٠٠

Ref: #CYB8377_269953

مقدمة الدورة التدريبية / لمحة عامة:

السيبرانية نظرًا لطبيعة العالمي، لكنهما في الوقت ذاته من بين أكثر يمثل قطاعا الطاقة والخدمات اللوجستية عصب الاقتصاد قد يؤدي إلى عواقب وخيمة، من انقطاع بنيتهما التحتية الحرجة. إن أي اختراق أمني في هذا القطاعات عرضة للتهديدات هذين تقدم هذه الدورة التدريبية المتخصصة لمتخصصي الأمن إمدادات الطاقة إلى تعطل سلاسل الإمداد العالمية. المجال اللوجستية. سنتناول في القطاعين، المعرفة والمهارات اللازمة لحماية السيبراني، مديري العمليات، والمهندسين في الصناعية (IOT)، تأمين الشبكات الذكية (Smart) هذه الدورة مفاهيم الأمن السيبراني للأنظمة الأنظمة الصناعية والشبكات التي تستهدف المشاركون القدرة على تحديد المخاطر الأمنية، تطبيق الرقمية. سيكتسب ، وحماية سلاسل الإمداد(Grids في الأمن السيبراني للقطاعات البنية التحتية الحيوية. تهدف الدورة إلى بناء ضوابط حماية فعالة، والاستجابة للحوادث الممارسات الصناعية، مع الاستفادة من إسهامات خبراء الصناعية. يستند المحتوى إلى أحدث المعايير وأفضل كوادر متخصصة BIG BEN ، المعروف بأعماله في أمن أنظمة(Robert Collins) أكاديميين بارزين مثل البروفيسور روبرت كولينز الحيوية واستدامتها. هذه الدورة لتعزيز مرونة البنية التحتية Center التحكم الصناعي (.(ICS يقدم Training

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- متخصصو الأمن السيبراني في قطاع الطاقة.
- مديرو العمليات والتشغيل (OT) في قطاعات حيوية.
- مهندسو الأنظمة الصناعية (ICS) وأنظمة SCADA.
- مديرو المخاطر في شركات الطاقة والخدمات اللوجستية.
- مسؤولو تكنولوجيا المعلومات في القطاعات الحيوية.
- مدققو الأنظمة الداخلية والخارجية.

القطاعات والصناعات المستهدفة:

- قطاع النفط والغاز.
- محطات توليد الطاقة وشبكات الكهرباء.
- شركات النقل والخدمات اللوجستية.
- القطاع الصناعي والبنية التحتية.
- القطاعات الحيوية. الهيئات الحكومية وما في حكمها، المسؤولة عن
- الشركات الكبرى التي تمتلك سلاسل إمداد معقدة.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة العمليات والتحكم الصناعي.
- إدارة المخاطر.
- إدارة تكنولوجيا المعلومات.
- إدارة سلسلة الإمداد.

أهداف الدورة التدريبية:

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

- والخدمات اللوجستية. فهم تحديات الأمن السيبراني في قطاعي الطاقة
- التحكم (ICS/SCADA) القدرة على تأمين الأنظمة الصناعية (OT) وأنظمة
- الطاقة. حماية الشبكات الذكية (Smart Grids) ومحطات
- اللوجستية. تأمين سلاسل الإمداد الرقمية وشبكات الخدمات
- التحتية الحيوية. تحديد المخاطر الأمنية وتقييم الثغرات في البنية
- الحيوية. تطوير خطط الاستجابة للحوادث المتعلقة بالأنظمة
- بالقطاعات الحيوية. الامتثال للوائح والمعايير الأمنية الخاصة

منهجية الدورة التدريبية:

اللوجستية. مصممة لتمكين المشاركين من مواجهة التحديات الأمنية تعتمد هذه الدورة التدريبية منهجية تفاعلية وعملية، على البنية التحتية الحيوية، سيتمكن المتدربون من خلال دراسات الحالة الواقعية المعقدة في قطاعي الطاقة والخدمات الأمن على أنظمة التحكم الصناعي. تتضمن المنهجية وورش العمل العملية، من فهم كيفية تطبيق ضوابط لهجمات سيبرانية الأمان بينهما. سيتم التركيز على المعلومات (IT) والعمليات (OT)، وأفضل مناقشات متعمقة حول الفرق بين أمن تكنولوجيا في الموجهة. يقدم BIG BEN Training Center هذه تحليل المخاطر وبناء دفاعات قوية ضد التهديدات الممارسات لدمج القطاعات الحيوية وضمان استدامة عملياتها. الدورة لتعزيز الخبرة الأمنية لدى العاملين

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الحيوية الوحدة الأولى: مقدمة في الأمن السيبراني للقطاعات

- مقدمة إلى قطاعي الطاقة والخدمات اللوجستية.
- الحيوية. التهديدات السيبرانية التي تستهدف البنية التحتية
- وأمن العمليات (OT). الاختلافات بين أمن تكنولوجيا المعلومات (IT)
- أنظمة التحكم الصناعي (ICS) وأنظمة SCADA.
- هجمات سيبرانية تاريخية على القطاعات الحيوية.
- أهمية الأمن السيبراني في استدامة العمليات.
- الامتثال للوائح الدولية في القطاعات الحيوية.

الوحدة الثانية: أمن الأنظمة الصناعية (OT)

- تقييم المخاطر الأمنية لأنظمة التحكم الصناعي.
- تحديد نقاط الضعف في أنظمة SCADA وPLC.
- أفضل الممارسات في تأمين الشبكات الصناعية.
- تقنيات العزل (Segmentation) للشبكات.
- المصادقة والترخيص في بيئات OT.
- التعامل مع البرامج الضارة الموجهة للأنظمة الصناعية.
- التدقيق الأمني للأنظمة الصناعية.

التحتية للطاقة الوحدة الثالثة: تأمين الشبكات الذكية والبنية

- مقدمة إلى الشبكات الذكية (Smart Grids) وتحدياتها الأمنية.
- أمن محطات الطاقة ومحطات التحويل.
- حماية أجهزة القياس الذكية (Smart Meters).
- تشفير الاتصالات في الشبكات الذكية.
- التحكم في الوصول إلى أجهزة البنية التحتية.
- مراقبة التهديدات في شبكات الطاقة.
- التعامل مع انقطاع الخدمة بسبب هجمات سيبرانية.

الإمداد الوحدة الرابعة: حماية الخدمات اللوجستية وسلاسل

- تأمين سلاسل الإمداد الرقمية.
- حماية أنظمة إدارة المستودعات (WMS).
- أمن أنظمة تتبع الشحنات والمركبات المتصلة.
- تشفير البيانات في سلاسل الإمداد.
- أمن الموانئ والمطارات الذكية.
- والبرية.التحديات الأمنية في الخدمات اللوجستية البحرية
- التعامل مع هجمات التزييف والاحتيال.

السيبرانية الوحدة الخامسة: الاستجابة للحوادث وبناء المرونة

- وضع خطة الاستجابة للحوادث في القطاعات الحيوية.
- اكتشاف الاختراقات والاستجابة السريعة لها.
- التعافي من الكوارث واستمرارية الأعمال.
- الحيوية.التدريب على الأمن السيبراني للعاملين في القطاعات
- بناء ثقافة أمنية قوية في المؤسسة.
- المعايير الأمنية (ISA/IEC ٦٢٤٤٣, NIST).
- مستقبل الأمن السيبراني للقطاعات الحيوية.

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:

كيف يمكن للمؤسسات أن المعلومات (IT) وأنظمة العمليات (OT) في قطاعي في ظل الترابط المتزايد بين أنظمة تكنولوجيا وتخلق بنية تحتية مرنة قادرة على الصمود تبتكر استراتيجيات أمنية متكاملة تتجاوز الحماية الطاقة والخدمات اللوجستية، استمرارية الخدمات الحيوية؟ أمام التهديدات السيبرانية المعقدة مع ضمان التقليدية،

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

لمواجهة التحديات الأمن السيبراني لقطاع الطاقة والخدمات اللوجستية، تتميز هذه الدورة بتركيزها المتخصص والعميق على بشكل عام، نغوص في التطبيق الأمنية الفريدة في هذه القطاعات الحيوية. بدلاً من مما يوفر محتوى مصممًا خصيصًا الشبكات الذكية وسلاسل الإمداد. تقدم الدورة دراسات العملي لتأمين الأنظمة الصناعية (OT)، وحماية تناول الأمن السيبراني IT وOTوبناء خطط مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. حالة واقعية لهجمات سيبرانية على البنية التحتية، استمرارية الأعمال. إنها ليست مجرد دورة نظرية، بل الاستجابة للحوادث، وهي جوانب حاسمة لضمان نركز على الدمج بين أمن للمجتمع. الأمن السيبراني للقطاعات الحيوية قادرين على حماية هي برنامج تدريبي مكثف يهدف إلى بناء متخصصين في الأصول الأكثر أهمية