الدورة التدريبية: الأمن السيبراني لقطاع الطاقة والخدمات اللوجستية

#CYB8377

الدورة التدريبية: الأمن السيبراني لقطاع الطاقة والخدمات اللوجستية

مقدمة الدورة التدريبية / لمحة عامة:

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

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- 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.
- الهيئات الحكومية وما في حكمها، المسؤولة عن القطاعات الحيوية.
- 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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة في الأمن السيبراني للقطاعات الحيوية

- مقدمة إلى قطاعي الطاقة والخدمات اللوجستية.
- التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية.
- الاختلافات بين أمن تكنولوجيا المعلومات (IT) وأمن العمليات (OT).
- 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.

الوحدة الثالثة: تأمين الشبكات الذكية والبنية التحتية للطاقة

- 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.

الوحدة الرابعة: حماية الخدمات اللوجستية وسلاسل الإمداد

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

الوحدة الخامسة: الاستجابة للحوادث وبناء المرونة السيبرانية

- وضع خطة الاستجابة للحوادث في القطاعات الحيوية.
- اكتشاف الاختراقات والاستجابة السريعة لها.
- التعافي من الكوارث واستمرارية الأعمال.
- التدريب على الأمن السيبراني للعاملين في القطاعات الحيوية.
- بناء ثقافة أمنية قوية في المؤسسة.
- المعايير الأمنية (ISA/IEC 62443, NIST).
- مستقبل الأمن السيبراني للقطاعات الحيوية.

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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