الدورة التدريبية: إدارة الثغرات الأمنية وتأمين الأنظمة التشغيلية للشركات

يونيو ٢٠٢٦ ٠٥ - ٠١

لشبونة

(للشخص الواحد) € ٤٤٠٠

Ref: #CYB4691_272840

مقدمة الدورة التدريبية / لمحة عامة:

يمكن أن يؤدي إلى مستمرًا وخطيرًا على استمرارية الأعمال. إن الفشل في العصر الرقمي، أصبحت الثغرات الأمنية تهديدًا التشغيلية، مما يسبب خسائر مالية فادحة اختراق الأنظمة، تسرب البيانات الحساسة، وتوقف في إدارة الثغرات بشكل فعال التدريبية ليست مجرد عملية تقنية، بل هي جزء أساسي من الحوكمة وأضرارًا بالغة للسمعة. إن إدارة الثغرات الأمنية العمليات ومهندسي الأنظمة، المعرفة والمهارات المتخصصة لمديري الأمن، متخصصي تكنولوجيا الأمنية للمؤسسة. تقدم هذه الدورة المعالجة سنتناول في هذه الدورة مفاهيم الثغرات الأمنية، اللازمة لبناء برنامج متكامل لإدارة الثغرات. المعلومات، المخاطر، ووضع خطط فعالة للتخفيف والتصحيح. سيكتسب المشاركون القدرة على تحديد أدوات المسح والتقييم، واستراتيجيات إلى في إدارة الثغرات الأمنية، مما يضمن أن المؤسسة من التهديدات. تهدف الدورة إلى بناء كوادر متخصصة الثغرات، تقييم خبراء أكاديميين بارزين مثل أحدث المعايير وأفضل الممارسات الدولية، مع تكون دائمًا في حالة دفاع قوية. يستند المحتوى BIG المعروف بأعماله في تقييم الثغرات الأمنية. يقدم البروفيسور جاكوب ويليامز (Jacob Williams)، الاستفادة من إسهامات المؤسسات من تحويل التهديدات إلى فرص لتعزيز الأمن. هذه الدورة لتمكين BEN Training Center

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مديرو الأمن السيبراني.
- مهندسو الأنظمة والشبكات.
- متخصصو تقنية المعلومات.
- مسؤولو إدارة المخاطر.
- المحللون الأمنيون.
- القيادات التقنية.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- شركات التكنولوجيا.
- الرعاية الصحية.
- الجهات الحكومية وما في حكمها.
- قطاع الاتصالات.
- الشركات الصناعية.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة تقنية المعلومات.
- إدارة العمليات التشغيلية (IT Operations).
- إدارة المخاطر.
- إدارة الامتثال.

أهداف الدورة التدريبية:

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

- فهم مفهوم الثغرات الأمنية ودورة حياتها.
- القدرة على تصنيف الثغرات وتقييم خطورتها.
- استخدام أدوات مسح الثغرات الأمنية وتقييمها.
- وضع خطة متكاملة لمعالجة الثغرات الأمنية.
- تأمين الأنظمة التشغيلية والخوادم.
- دمج إدارة الثغرات في استراتيجية الأمن السيبراني.
- الامتثال للمعايير الأمنية الدولية.

منهجية الدورة التدريبية:

خلال دراسات مصممة لتمكين المشاركين من فهم وتطبيق عمليات إدارة تعتمد هذه الدورة التدريبية منهجية تفاعلية وعملية، التطبيقية، من ممارسة تقييم الثغرات الحالة الواقعية لاختراقات أمنية ناتجة عن ثغرات، الثغرات الأمنية. سيتمكن المتدربون من التشغيل متعمقة حول الفرق بين إدارة الثغرات واختبار وتحديد أولويات المعالجة. تتضمن المنهجية مناقشات وورش العمل المشاركين على التفكير في كيفية المختلفة. سيتم التركيز على الجانب الاستباقي الاختراق، وأفضل الممارسات لتأمين أنظمة هذه الدورة لتمكين المؤسسات من تحصين Center تحسين الدفاعات بشكل مستمر. يقدم BIG BEN Training للأمن، وتشجيع أنظمتها وضمان استمرارية أعمالها.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات إدارة الثغرات الأمنية

- مفهوم الثغرات الأمنية ونقاط الضعف.
- معالجة). دورة حياة الثغرات الأمنية (اكتشاف، تقييم،
- الفرق بين الثغرة الأمنية والتهديد.
- نماذج تقييم الخطورة (CVSS).
- تصنيف الثغرات حسب أنواعها.
- أهمية برنامج إدارة الثغرات للمؤسسات.
- مسؤولية الإدارة في حماية الأنظمة.

الوحدة الثانية: اكتشاف الثغرات الأمنية

- أدوات مسح الثغرات (Nessus, Qualys).
- مسح الشبكات والأنظمة لاكتشاف الثغرات.
- تحليل نتائج المسح وتحديد الثغرات.
- تأثير الثغرات على الأنظمة التشغيلية.
- الاختبار اليدوي للثغرات.
- جمع المعلومات عن الثغرات من المصادر العامة.
- إجراء تقييمات دورية للأنظمة.

الوحدة الثالثة: تقييم المخاطر والمعالجة

- تحليل المخاطر المرتبطة بالثغرات.
- تحديد أولويات المعالجة بناءً على الخطورة.
- استراتيجيات المعالجة (التصحيح، التخفيف).
- بناء خطة للتصحيح وإدارة التغييرات.
- أتمتة عملية التصحيح.
- التخفيف من الثغرات التي لا يمكن تصحيحها.
- التحقق من فعالية المعالجة.

الوحدة الرابعة: تأمين الأنظمة التشغيلية

- أفضل الممارسات لتأمين الخوادم.
- تأمين أنظمة التشغيل (Windows, Linux).
- إدارة التحديثات الأمنية والتصحيحات.
- تقوية إعدادات الأنظمة (Hardening).
- التحكم في الوصول وإدارة الصلاحيات.
- تأمين التطبيقات والبرامج.
- أمن الحوسبة السحابية (Cloud Security).

الوحدة الخامسة: بناء برنامج إدارة الثغرات

- وضع سياسات وإجراءات لإدارة الثغرات.
- دمج برنامج إدارة الثغرات مع فرق العمل.
- التواصل الفعال بين الأقسام.
- الامتثال للمعايير الأمنية (ISO ٢٧٠٠١).
- قياس نجاح البرنامج وتقييم الأداء.
- التحليل الجنائي للثغرات.
- مستقبل إدارة الثغرات.

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:

مجردا التصحيح، بل يُنشئ كيف يمكن للمؤسسات أن تبتكر برنامجًا لإدارة في ظل الانتشار المستمر للثغرات الأمنية المعقدة، السيبرانية؟ المستقبلية، ويُدمج التحليل الاستخباراتي، ويحول نظامًا استباقيًا يُمكنها من التنبؤ بالثغرات الثغرات لا يقتصر على المخاطر إلى فرص لتعزيز المرونة

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

من حماية أنظمتها إدارة الثغرات الأمنية، مما يوفر محتوى مصممًا تتميز هذه الدورة بتركيزها المتخصص والعميق على نغوص في التطبيق العملي لدورة حياة التشغيلية بشكل استباقي. بدلاً من مجرد تناول أدوات خصيصًا لتمكين المؤسسات وخيمة، مع تحليل الاستراتيجيات. تقدم الدورة دراسات حالة واقعية الثغرات، من الاكتشاف والتقييم إلى المعالجة ووضع الأمن، مما يضمن أن المشاركين سيخرجون مفصل للثغرات التي تم استغلالها. نركز على الجانب لاختراقات أمنية أدت إلى عواقب في لإدارة الثغرات. إنها ليست مجرد دورة نظرية، بل هي بمهارات تحليلية قوية وقدرة على بناء برامج فعالة الإداري للأمن، التهديدات. الأمن السيبراني قادرين على حماية المؤسسات من أخطر برنامج تدريبي مكثف يهدف إلى بناء متخصصين