الدورة التدريبية: الاستخبارات السيبرانية (CTI)

تحليل التهديدات واتخاذ القرار -

يونيو - ٠٣ يوليو ٢٠٢٦ ٢٩

فيينا

(للشخص الواحد) € ٥٧٠٠

Ref: #CYB1956_272022

مقدمة الدورة التدريبية / لمحة عامة:

BIG BEN TRAINING CENTER

لتمكين المؤسسات من يعد الدفاع السلبي كافيًا. أصبحت الاستخبارات في عالم يزداد فيه تعقيد التهديدات السيبرانية، لم
بأنها المعرفة المكتسبة من خلال جمع اتخاذ قرارات استباقية ومستنيرة. تُعرف الاستخبارات السيبرانية (CTI) أداة حاسمة
التدريبية إنها تمكن المؤسسات من فهم من هو الخصم، وما هي وتحليل البيانات المتعلقة بالتهديدات الرقمية. السيبرانية
التنفيذية، المعرفة والمهارات المتخصصة لمحللي الأمن، مديري فرق الاستجابة دوافعه، وكيف يعمل. تقدم هذه الدورة
تحليل سنتناول في هذه الدورة مفاهيم الاستخبارات اللازمة لبناء برنامج استخبارات سيبرانية فعال. للحوادث، والقيادات
سيكتسب المشاركون القدرة على جمع التهديدات، وتطبيق الاستخبارات لاتخاذ القرارات السيبرانية، دورة حياة الاستخبارات،
فعال لجميع مستويات المؤسسة. تهدف الدورة إلى بناء المعلومات الاستخباراتية، تحليلها، وتقديمها بشكل الاستراتيجية.
وأفضل الممارسات أن المؤسسة تكون دائمًا في طليعة الدفاع. يستند كوادر متخصصة في الاستخبارات السيبرانية، مما يضمن
مثل البروفيسور سكوت جايسون (.J Scott الدولية، مع الاستفادة من إسهامات خبراء أكاديميين المحتوى إلى أحدث المعايير
رؤى استباقية هذه الدورة لتمكين BIG BEN Training Center يقدم ، المعروف بأعماله في تحليل التهديدات.(Jones بارزين
قابلة للتنفيذ. المؤسسات من تحويل المعلومات إلى

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- محللو الأمن السيبراني.
- مديرو فرق الاستجابة للحوادث (IR).
- مسؤولو الأمن السيبراني (CISO).
- القيادات التنفيذية ومديرو المخاطر.
- المهندسون الأمنيون.
- المستشارون الأمنيون.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- شركات الاتصالات وتقنية المعلومات.
- شركات الأمن السيبراني.
- الجهات الحكومية وما في حكمها.
- قطاع الطاقة.
- الرعاية الصحية.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة المخاطر.
- إدارة تقنية المعلومات.
- إدارة الاستجابة للحوادث.
- الإدارة التنفيذية.

أهداف الدورة التدريبية:

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

- الاستراتيجية. فهم مفهوم الاستخبارات السيبرانية وأهميتها
- السيبرانية. القدرة على تطبيق دورة حياة الاستخبارات
- جمع البيانات من مصادر مختلفة (OSINT, TTPs).
- تحليل التهديدات السيبرانية وأنماط الهجمات.
- إنشاء تقارير استخباراتية فعالة وقابلة للتنفيذ.
- اليومية. دمج الاستخبارات السيبرانية في عمليات الأمن
- استخدام الاستخبارات لاتخاذ قرارات استراتيجية.

منهجية الدورة التدريبية:

سيتمكن المتدربون وتشاركية، مصممة لتمكين المشاركين من فهم وتطبيق تعتمد هذه الدورة التدريبية منهجية متقدمة وورش العمل التطبيقية، من ممارسة تحليل من خلال دراسات الحالة الواقعية لـهجمات سيبرانية عمليات الاستخبارات السيبرانية. الاستخباراتية متعمقة حول الفرق بين البيانات والمعلومات التهديدات وتحديد الأنماط. تتضمن المنهجية مناقشات معقدة، للأمن، وتشجيع المشاركين على التفكير للقيادات العليا. سيتم التركيز على الجانب والاستخبارات، وكيفية تقديم الرؤى الأمن. لتعزيز القدرات الدفاعية للمؤسسات وضمان اتخاذ كخصوم. يقدم BIG BEN Training Center هذه الدورة الاستباقي قرارات مستنيرة في عالم

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة في الاستخبارات السيبرانية (CTI)

- مفهوم الاستخبارات السيبرانية وأنواعها.
- دورة حياة الاستخبارات السيبرانية.
- الفرق بين CTI وبيانات التهديدات.
- أهمية الاستخبارات في اتخاذ القرارات.
- مصادر جمع المعلومات الاستخباراتية (OSINT, MISP).
- المهارات الأساسية لمحلل الاستخبارات.
- إطار عمل MITRE ATT&CK.

الوحدة الثانية: جمع وتحليل البيانات الاستخباراتية

- تحديد متطلبات الاستخبارات (PRI).
- أدوات وتقنيات جمع البيانات.
- تحليل مؤشرات الاختراق (IoCs).
- تحليل تكتيكات، تقنيات، وإجراءات الخصوم (TTPs).
- بناء ملفات تعريف للخصوم (Threat Actor Profiling).
- الارتباط بين الحوادث والتهديدات.
- أتمتة عملية جمع البيانات.

الوحدة الثالثة: بناء التقارير وتقديم الرؤى

- صياغة تقارير استخباراتية واضحة وموجزة.
- تخصيص التقارير لمختلف الجماهير (التقنيين، المديرين).
- استخدام النماذج لتسهيل التحليل.
- تحديد مستوى اليقين في المعلومات.
- عرض الرؤى الاستخباراتية للقيادات التنفيذية.
- تقديم توصيات قابلة للتنفيذ.
- أمثلة على تقارير استخباراتية ناجحة.

الوحدة الرابعة: دمج الاستخبارات في عمليات الأمن

- استخدام CTI في اكتشاف التهديدات (Threat Hunting).
- دمج الاستخبارات في أنظمة SIEM وSOAR.
- تحسين الاستجابة للحوادث باستخدام CTI.
- تحديث الدفاعات استنادًا إلى التهديدات الجديدة.
- تطبيق الاستخبارات في إدارة المخاطر.
- التنبؤ بالهجمات المستقبلية.
- بناء دفاعات استباقية.

الوحدة الخامسة: الاستراتيجية والمستقبل

- بناء برنامج CTI فعال.
- الميزانية والموارد اللازمة لبرنامج CTI.
- الاستخبارات المفتوحة المصدر (OSINT) المتقدمة.
- التعاون مع مجتمع الأمن السيبراني.
- تأثير الذكاء الاصطناعي على CTI.
- المرونة السيبرانية والاستخبارات الاستراتيجية.
- التطور المستقبلي لـ CTI.

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:

بل تُنشئ كيف يمكن للمؤسسات أن تبتكر استراتيجيات استخبارات في ظل التطور السريع للتهديدات السيبرانية والخصوم، ويُقدم رؤى استراتيجية للقيادات نظامًا استباقيًا يُمكنها من التنبؤ بالهجمات سيبرانية لا تقتصر على تحليل الماضي، فعالة، ويضمن بقاء المؤسسة في طليعة الأمن؟ العليا، ويحول المعلومات الخام إلى قرارات دفاعية المستقبلية،

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

من الانتقال من الاستخبارات السيبرانية (CTI)، مما يوفر محتوى تتميز هذه الدورة بتركيزها المتخصص والعميق على نغوص في التطبيق العملي لدورة الدفاع السلبي إلى الدفاع الاستباقي. بدلاً من مجرد مصممًا خصيصًا لتمكين المؤسسات باستخدام التقارير وتقديم الرؤى. تقدم الدورة دراسات حالة حياة الاستخبارات، من الجمع والتحليل إلى بناء تناول أدوات الأمن، على الجانب الاستراتيجي للأمن، مما الاستخبارات، مع تحليل مفصل لنتائجها وكيفية واقعية لهجمات معقدة تم الكشف عنها إلى وقدرة على اتخاذ قرارات مستنيرة. إنها ليست مجرد يضمن أن المشاركين سيخرجون بمهارات تحليلية قوية تطبيقها. نركز التهديدات المتزايدة. بناء متخصصين في الاستخبارات السيبرانية قادرين على دورة نظرية، بل هي برنامج تدريبي مكثف يهدف حماية المؤسسات من