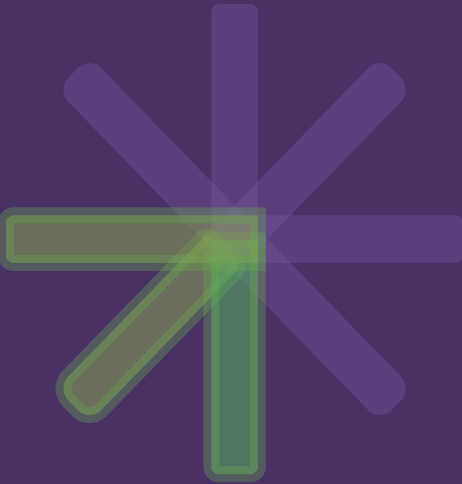


دورة التعامل مع الحوادث الأمنية: الفرز وحفظ الأدلة وإغلاق القضايا

2027 – 16 سبتمبر

كوالالمبور





دورة التعامل مع الحوادث الأمنية: الفرز وحفظ الأدلة وإغلاق القضايا

المرجع: 22572_356 التاريخ: 12 - 16 سبتمبر 2027 المكان: كوالالمبور الرسوم: GBP 4000

ملخص البرنامج

التعامل مع الحوادث الأمنية، بما فيه فرز الحوادث وحفظ الأدلة وإغلاق القضايا، محور دورة تدريبية تمتد 5 أيام لرؤساء الأمن والتحقيقات ومديري الأمن المؤسسي بمستوى إداري، ويخرج منها كل مشارك بخطة للتعامل مع الحوادث في مؤسسة واحدة. فالحوادث تفقد قيمتها دليلاً حين يتأخر تقييمها ويتفاوت تصعيدها وتغلق دون سجل واضح لما تكشف. ويتدرج البرنامج من المبادئ ومعايير التحقيق، إلى تشخيص الفرز ومخاطر الأدلة، ثم إلى تصميم الاستجابة والتحقيق، وصولاً إلى التقارير والإغلاق وخطة عملية. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في التعامل مع الحوادث الأمنية.

المبررات المؤسسية

حين تعالج الحوادث الأمنية كل حالة على حدة، دون سلم مشترك للخطورة ولا مسار ثابت للأدلة، تتعامل المؤسسة مع وقائع متشابهة بطرق مختلفة وتعجز عن الدفاع عن استنتاجاتها. أما القادة الذين يضعون قواعد الفرز ويشترطون مراجعة الإغلاق فيستطيعون بيان كيف حسمت كل حالة.

- تأخر الاستجابة: يقل حين تتفق سلاسل الخطورة ومسارات التصعيد مسبقاً.
- فقدان الأدلة: ينخفض حين تتبع خطوات الحفظ والحيازة بروتوكولا واحداً.
- تكرار الحوادث: يتراجع حين تسجل الأسباب الجذرية والدروس ويعمل بها عند الإغلاق.

المبادئ والأساس المعرفي

- مبادئ ISO/TS 37008 المواصفة الفنية الدولية للتحقيقات الداخلية في المنظمات في الاستقلالية والسرية والموضوعية والتناسب: تشكل بيان التحقيق وقواعد التعامل المبنية في الجلسة 1.
- إرشاد ISO/TS 37008 في تخطيط التحقيقات الداخلية وإجرائها: يوطر قائمة حفظ الأدلة وخطة التحقيق المصممة في الجلسة 3.
- إرشاد ISO/TS 37008 في إعداد تقارير التحقيقات الداخلية وإغلاقها: يوجه قالب التقرير ومعايير الإغلاق المعدة في الجلسة 4.



المشاركون المستهدفون

- القادة الأمنيون الذين يقررون كيف تصنف الحوادث وتصعد وتخصص لها الموارد.
- مدبرو التحقيقات الذين يكلفون بالتحقيقات ويعتمدون نتائجها.
- مدبرو الأمن المؤسسي الذين يتولون الاستجابة الأولى ويحفظون المواد في موقع الحادث.
- مسؤولو الشؤون القانونية والامتثال الذين يعتمدون على سجلات الحوادث وتقارير التحقيق.

يخدم البرنامج الأمن المؤسسي والمؤسسات المالية والمشغلين الصناعيين.

مخرجات التعلم

1. سيكون المشاركون قادرين على تقييم تعامل المؤسسة مع الحوادث في ضوء الإرشاد الدولي للتحقيقات الداخلية.
2. سيكون المشاركون قادرين على تشخيص التأخر وسوء تقدير الخطورة ومخاطر الأدلة في سجل الحوادث.
3. سيكون المشاركون قادرين على بناء بروتوكولات الفرز والتصعيد وحفظ الأدلة.
4. سيكون المشاركون قادرين على تصميم خطة تحقيق بنطاق وضمانات للاستقلالية والسرية.
5. سيكون المشاركون قادرين على تقويم تقارير الحوادث والتحقيقات من حيث الأدلة والسبب الجذري والوضوح.
6. سيكون المشاركون قادرين على تبرير خطة التعامل ومؤشراتها أمام رئيس الأمن.

هيكل البرنامج

اليوم 1: مبادئ التعامل مع الحوادث الأمنية ومعايير التحقيق

من يقرر كيفية التعامل مع الحادث الأمني، وفي ضوء أي مبادئ يجري التحقيق فيه؟

- مراجعة مبادئ ISO/TS 37008
- سلم فئات الحوادث ودرجات خطورتها
- خريطة الأدوار وصلاحيات التصعيد
- بيان استقلالية التحقيق وسريته
- موجز تعريف الحادث وقنوات الإبلاغ

اليوم 2: تشخيص مسار الحوادث والفرز ومخاطر الأدلة

أين تتعثر الحوادث أو يساء تقدير خطورتها أو تفقد أدلتها قبل بدء التحقيق؟



- مراجعة عينة من سجل الحوادث
- تدقيق قرارات الفرز
- تحليل تأخر التصعيد
- فحص مخاطر فقدان الأدلة
- مراجعة تغطية قنوات الإبلاغ

اليوم 3: تصميم الاستجابة وحفظ الأدلة وتخطيط التحقيق

كيف يؤمن الحادث وتحفظ أدلته ويحدد نطاق التحقيق؟

- بروتوكول الفرز والتصعيد
- قائمة فحص تأمين موقع الحادث وحفظ الأدلة
- سجل سلسلة الحيازة
- قالب نطاق التحقيق وخطته
- ورقة تخطيط المقابلات

اليوم 4: إعداد التقارير والإغلاق والتعلم

كيف يتحول التحقيق إلى تقرير، وكيف تغلق القضية ويستفاد منها؟

- مصفوفة النتائج والأدلة
- قالب تقرير الحادث والتحقيق
- مخطط تحليل الأسباب الجذرية
- مراجعة إغلاق القضية
- سجل الدروس المستفادة

اليوم 5: تطبيق التعامل مع الحوادث الأمنية في مؤسسة واحدة

هل خطة التعامل جاهزة ليعتمدها رئيس الأمن؟

- تطبيق تدقيق الفرز من الجلسة 2 على الفريق المختار
- اختيار قائمة حفظ الأدلة من الجلسة 3 على سيناريو حي
- مطابقة تقرير الجلسة 4 مع معايير الإغلاق
- وضع مؤشرات التعامل للفريق
- إنجاز خطة التعامل مع الحوادث الأمنية



المنهجية

يقوم البرنامج على تمارين منظمة في ملفات حوادث مجهولة المصدر من الأمن المؤسسي والمواقع الصناعية والقطاع المالي. يعمل المشاركون في فرق صغيرة بأدوار قائد الحادث ومدير التحقيق والعميل، وينقلون حادثاً واحداً من البلاغ الأول إلى الإغلاق.

- نشاط مقترح: فرز مجموعة من بلاغات الحوادث وتعليل درجة الخطورة لكل منها.
- نشاط مقترح: حصر الأدلة المعرضة للخطر في سيناريو وترتيب الخطوات التي تحميها.
- نشاط مقترح: إعادة كتابة مذكرة إغلاق لتتضح فيها النتائج والسبب الجذري والإجراءات.

المخرج الختامي

يعد كل مشارك خطة للتعامل مع الحوادث الأمنية في مؤسسة واحدة. وتضم سلماً للخطورة، وبروتوكولا للفرز، وإجراءات لحفظ الأدلة وسلسلة الحياة، وقابلاً لخطة التحقيق، ومعياراً للإغلاق، ومؤشرات للتعامل. وتستخدم الخطة في إحاطة رئيس الأمن ومراجعة الحادث التالي.

الأسئلة الشائعة

هل يناسب التعامل مع الحوادث الأمنية المديرين الذين لا يجرون التحقيقات بأنفسهم؟

نعم، فالتعامل مع الحوادث الأمنية بمستوى إداري، ويفترض أنك توجه التحقيقات أو تعتمد عليها لا أنك تجري المقابلات بنفسك.

ما الموصفة التي يقوم عليها التعامل مع الحوادث الأمنية في هذا التدريب؟

يقوم التعامل مع الحوادث الأمنية على ISO/TS 37008 وإرشادها في تخطيط التحقيقات الداخلية وإجرائها والإبلاغ عنها وإغلاقها، ومنه الاستقلالية والسرية والموضوعية والتناسب.

كيف تستخدم خطة التعامل مع الحوادث الأمنية في العمل؟

تستخدم الخطة في إحاطة رئيس الأمن، ووضع قواعد الفرز والأدلة، ومراجعة طريقة إغلاق كل قضية.

بماذا يختلف التعامل مع الحوادث الأمنية عن برنامج في الاستجابة للحوادث السيبرانية؟

يركز التعامل مع الحوادث الأمنية على الحوادث الأمنية المؤسسية والمادية والأدلة والتحقيقات الداخلية، بينما يركز برنامج الاستجابة للحوادث السيبرانية على احتواء الهجمات على الأنظمة والشبكات.