

دورة قيادة الاستجابة للحوادث السيبرانية: الاكتشاف والاحتواء والتعافي





دورة قيادة الاستجابة للحوادث السيبرانية: الاكتشاف والاحتواء والتعافي

ملخص البرنامج

قيادة الاستجابة للحوادث السيبرانية دورة تدريبية تمتد 5 أيام موجهة إلى قيادات الأمن السيبراني على المستويين الإداري والاستراتيجي، ويخرج منها كل مشارك بخطة استجابة للحوادث ومجموعة من أدلة التشغيل لمؤسسته، فبرمجيات الفدية وسرقة البيانات واختراق سلاسل التوريد تختبر اليوم كل مؤسسة، بينما تبقى خطط استجابة كثيرة غير مختبرة وتتداخل الأدوار تحت الضغط. يغطي البرنامج الاستعداد والاكتشاف والاحتواء والتحقيق الجنائي الرقمي والتعافي واستخلاص الدروس. تقدم هذا البرنامج في قيادة الاستجابة للحوادث السيبرانية مارس للتدريب المملكة المتحدة.

المبررات المؤسسية

تتوقف تكلفة الحادث السيبراني على سرعة اكتشافه واحتوائه وعلى جودة تواصل المؤسسة في أثناءه. فالتصعيد البطيء وضياع الأدلة والقرارات الارتجالية تحول حدثًا يمكن احتواؤه إلى انقطاع طويل للخدمات. أما القدرة المعدة مسبقًا والمختبرة بالتمارين فتحد من كل ذلك.

- زمن الاكتشاف والاحتواء: يقصر حين يتفق مسبقًا على المراقبة ومعايير الفرز وأدلة الاحتواء.
- توقف الخدمات وتكلفة التعافي: ينخفضان حين تختبر أولويات التعافي والنسخ الاحتياطية وخطوات الاستعادة قبل وقوع الهجوم.
- التعرض التنظيمي والمخاطر على السمعة: يتراجعان حين تتبع معالجة الأدلة والإبلاغ والتواصل مع أصحاب المصلحة إجراءات محددة.

المبادئ والأساس المعرفي

- NIST SP 800-61 Revision 3، توصيات الاستجابة للحوادث: يربط الاستجابة بإدارة المخاطر السيبرانية وينظم مراجعة القدرات في الجلسة 1.
- NIST Cybersecurity Framework 2.0، إطار الأمن السيبراني: يوفر وظائف الحوكمة والتحديد والحماية والاكتشاف والاستجابة والتعافي لتوزيع المسؤوليات في الجلسات من 1 إلى 4.
- ISO/IEC 27035، معيار إدارة حوادث أمن المعلومات: يوظف عملية إدارة الحوادث وأدوار الفريق ومعالجة الأدلة في الجلسات 2 و3.
- منهجية SANS ذات الخطوات الست: تقدم التسلسل من الاستعداد إلى استخلاص الدروس الذي يتدرب عليه المشاركون في تمرين الجلسة 5.



المشاركون المستهدفون

- القادة المسؤولون عن الدفاع السيرياني وقدرة الاستجابة للحوادث في المؤسسة.
- المديرون الذين يقودون فرق العمليات الأمنية والمراقبة ومعالجة الحوادث.
- المديرون المسؤولون عن خدمات تقنية المعلومات واستعادة البنية التحتية واستمرارية الأعمال.
- كبار الموظفين الذين ينسقون الاستجابة القانونية والإعلامية لحالات الاختراق.

يخدم البرنامج البنوك وشركات التأمين والجهات الحكومية وقطاعي الطاقة والمرافق ومزودي الاتصالات والرعاية الصحية.

مخرجات التعلم

1. سيكون المشاركون قادرين على تقييم نضج قدرة الاستجابة للحوادث مقارنة ب NIST SP 800-61 Revision 3.
2. سيكون المشاركون قادرين على تصميم معايير الفرز ومستويات الخطورة ومسارات التصعيد في مركز العمليات الأمنية.
3. سيكون المشاركون قادرين على ترتيب أولويات إجراءات الاحتواء والاستئصال بالاستناد إلى معلومات التهديدات عن أساليب المهاجمين.
4. سيكون المشاركون قادرين على تبرير إجراءات معالجة الأدلة والتحقيق الجنائي الرقمي التي تحفظ الخيارات التحقيقية والقانونية.
5. سيكون المشاركون قادرين على بناء تسلسل للاستجابة لبرمجيات الفدية والتعافي منها للخدمات الحرجة.
6. سيكون المشاركون قادرين على صياغة إجراءات الإبلاغ والتواصل واستخلاص الدروس بعد الحوادث الكبرى.

هيكل البرنامج

اليوم 1: أسس قيادة الاستجابة للحوادث السيريانية

ما الذي تتطلبه قدرة استجابة فاعلة، وما مستوى نضجها اليوم؟

- تهديدات برمجيات الفدية وسرقة البيانات واختراق سلاسل التوريد
- توصيات NIST SP 800-61 Revision 3 وإدارة المخاطر السيريانية
- وظائف NIST CSF 2.0 وتوزيع مسؤوليات الاستجابة
- نماذج فرق الاستجابة للحوادث وأدوارها وصلحياتها
- تقييم نضج القدرات وتحليل الفجوات

اليوم 2: الاكتشاف والفرز ومعلومات التهديدات

كيف تكتشف الحوادث الحقيقية بسرعة وتميز من الإنذارات العابرة؟



- المراقبة في مركز العمليات الأمنية وحالات الاستخدام
- فرز التنبيهات وتصنيف الخطورة والتصعيد
- مصادر معلومات التهديدات وأساليب المهاجمين
- عملية إدارة الحوادث وفق ISO/IEC 27035
- تسجيل الحوادث وتتبعها وتقارير الوضع

اليوم 3: الاحتواء والاستئصال والتحقيق الجنائي الرقمي

كيف يوقف الاختراق دون إتلاف الأدلة اللازمة لفهم ما حدث؟

- استراتيجيات الاحتواء لأجهزة المستخدمين والشبكات والسحابة
- استئصال آليات البقاء والحسابات المخترقة
- الفرز الجنائي الرقمي وجمع الأدلة
- سلسلة حفظ الأدلة والاعتبارات القانونية
- العمل مع فرق الاستجابة الخارجية وجهات إنفاذ القانون

اليوم 4: برمجيات الفدية والتعافي والتواصل

كيف تستعاد الخدمات ويبلغ أصحاب المصلحة في أثناء هجوم كبير؟

- قرارات الاستجابة لبرمجيات الفدية وسيناريوهات الابتزاز
- سلامة النسخ الاحتياطية وأولويات الاستعادة واختبار التعافي
- الربط مع استمرارية الأعمال وإدارة الأزمات
- الإبلاغ التنظيمي ومتطلبات حالات خرق البيانات
- التواصل مع الإدارة العليا والموظفين والعلماء ووسائل الإعلام

اليوم 5: تطبيق قيادة الاستجابة للحوادث السيبرانية

كيف تختبر القدرات وأدلة التشغيل والقرارات معا قبل وقوع هجوم حقيقي؟

- تمرين محاكاة مكثفي للدورة الكاملة وفق خطوات SANS الست
- صياغة أدلة التشغيل لأنواع الحوادث ذات الأولوية
- مراجعة الدروس المستفادة ومتابعة التحسينات
- مراجعة الزملاء لخطط الاستجابة للحوادث
- عرض خطة الاستجابة للحوادث وأدلة التشغيل



المنهجية

يقوم البرنامج على المحاكاة وتحليل الحالات. إذ يعمل المشاركون على حوادث مستمدة من بيانات مصرفية وحكومية وصحية وصناعية، ويتخذون القرارات كلما ظهرت معطيات جديدة، ثم يطبقون كل أداة على بياناتهم.

- نشاط مقترح: تصنيف سيل من التنبيهات الأمنية وتصعيدها في مركز عمليات افتراضي.
- نشاط مقترح: تحديد خطوات احتواء حساب مسؤول نطاق مخترق.
- نشاط مقترح: قيادة الساعات الأولى لحدث برمجي فدية.

المخرج الختامي

يعد كل مشارك خطة استجابة للحوادث ومجموعة من أدلة التشغيل لمؤسسته، تتضمن أدوار الفريق وصلاحياته، ومعايير الخطورة والتصعيد، وأدلة لأنواع الحوادث ذات الأولوية، وقواعد معالجة الأدلة، وأولويات التعافي، ومصفوفة للتواصل والإبلاغ، وجدولاً للتمارين، جاهزة للاعتماد الإدارة العليا.

الأسئلة الشائعة

هل تناسب دورة قيادة الاستجابة للحوادث السيبرانية مديري تقنية المعلومات ممن لا يملكون خبرة في العمليات الأمنية؟

نعم، فهي تناسب رؤساء أمن المعلومات ورؤساء العمليات الأمنية ومديري الاستجابة للحوادث ومديري تقنية المعلومات، وتفترض الإلمام بعمليات تقنية المعلومات دون خبرة عملية في التحليل أو التحقيق الجنائي الرقمي.

ما المعايير التي تقوم عليها قيادة الاستجابة للحوادث السيبرانية؟

تستند إلى NIST SP 800-61 Revision 3، NIST Cybersecurity Framework 2.0g، ومعايير ISO/IEC 27035 لإدارة الحوادث، ومنهجية SANS ذات الخطوات الست.

كيف تستخدم خطة الاستجابة للحوادث السيبرانية وأدلة التشغيل في العمل؟

تعود بخطة وأدلة تشغيل يمكن للإدارة العليا اعتمادها ولفريقك التدريب عليها، بأدوار واضحة ومعايير تصعيد وأولويات للتعافي.

بم تختلف قيادة الاستجابة للحوادث السيبرانية عن برامج التوعية العامة بالأمن السيبراني؟

تركز على ما يحدث بعد بدء الهجوم؛ الاكتشاف والاحتواء والتحقيق الجنائي الرقمي والتعافي والإبلاغ، لا على التوعية الأمنية العامة أو السياسات.