JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في الاستجابة الأولى للحوادث السيبرانية

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في الاستجابة الأولى للحوادث السيبرانية

الاستجابة الأولى للحوادث السيبرانية دورة تدريبية متقدمة مدتها أسبوعين لمحللي مراكز عمليات الأمن السيبراني والمستجيبين للحوادث ومسؤولي أمن تقنية المعلومات الذين يتولون الساعات الأولى من الهجوم، وتنتهي بدليل تشغيل مجرب لمعالجة الحوادث. فالمخترق ينتقل اليوم من موطئ القدم الأول إلى سرقة البيانات خلال ساعات، لذا تحدد جودة التحرك المبكر حجم الخسارة. وتقدم جوبيتر برايم للتدريب هذه الدورة لمستجيبين يتحركون بالدليل والسرعة وضبط النفس.

لماذا تهم الاستجابة الأولى للحوادث السيبرانية الآن

تتشكل الاستجابة الأولى اليوم تحت ثلاثة ضغوط: مجموعات برمجيات الفدية التي تشفر وتبتز خلال نوبة عمل واحدة، وبيئات هجينة تتوزع فيها سجلات السحابة والأجهزة الطرفية والهويات على منصات منفصلة، وقيادات تنتظر تقديرا واضحا للأثر قبل اكتمال الحقائق. المستجيب الذي يحسن الفرز يقلص مدة بقاء المهاجم ويحفظ أدلة مقبولة ويبقي التعافي منظما، أما الخطوة الأولى الخاطئة فقد تمحو الذاكرة المتطايرة أو تنبه المخترق. وتستند الدورة إلى دورة حياة معالجة الحوادث في الإصدار الخاص NIST SP 800-61 NIST Special Publication 800-61 من مرحلة الاستعداد حتى ما بعد الحادث.

المستفيدون من الاستجابة الأولى للحوادث السيبرانية

- كوادر عمليات الأمن التي تراقب التنبيهات وتضبط قواعد الكشف وتصعد حالات الاختراق المشتبه بها
- معالجو الحوادث الذين يحددون نطاق الاختراق ويعزلون الأجهزة وينسقون الاستئصال
- مسؤولو أمن تقنية المعلومات المعنيون بتحصين الأجهزة الطرفية والخوادم والهويات بعد الهجوم
- مدافعو الشبكات الذين يقرؤون حزم البيانات الملتقطة وسجلات التدفق وجدران الحماية أثناء الاختراق
- المساهمون في استخبارات التهديدات الذين يثرون المؤشرات ويتتبعون سلوك الخصوم

يجني مركز العمليات الأمنية الفائدة الكبرى حين يوفد محلليه ومعالجي الحوادث ومدافعي الشبكات معا، لأن الدليل المشترك يزيل تأخير التسليم بين النوبات.

قدرات الاستجابة الأولى للحوادث السيبرانية

يغادر المشاركون قادرين على الانتقال من تنبيه منفرد إلى حادث محتوى وموثق دون فقدان الأدلة أو الوقت.

- تقييم موثوقية التنبيه باستخدام استخبارات التهديدات وربط السجلات — قرارات التصعيد لدى قائد النوبة
- تحليل حركة الشبكة والحزم الملتقطة لرصد أنماط القيادة والتحكم — نطاق الاحتواء لدى مالكي الشبكة
- تطبيق فرز الأجهزة الطرفية على الذاكرة والعمليات ونقاط الاستمرار — قرارات عزل الأجهزة
- حفظ الأدلة الرقمية بسلسلة حيازة موثقة — المستشار القانوني والمحققون
- تحديد خطوات الاحتواء والاستئصال والتعافي لكل فئة من الحوادث — مالكو الأنظمة ومديرو الخدمات
- إيصال حالة الحادث وأثره والدروس المستفادة — القيادة التنفيذية وقائد الحادث

مصطلحات الاستجابة الأولى للحوادث السيبرانية الأساسية

- مؤشر الاختراق — أثر يمكن رصده مثل بصمة ملف أو نطاق أو عنوان شبكي يدل على احتمال تعرض نظام للاختراق.
- مدة البقاء — الفترة الممتدة بين أول دخول للمخترق ولحظة اكتشاف المدافعين لوجوده.
- الفرز — ترتيب سريع للتنبيهات والأصول المتأثرة حسب الخطورة كي يعالج المستجيبون الأكثر إلحاحا أولا.
- سلسلة الحيازة — سجل موثق لمن جمع كل دليل ومن تعامل معه وأين حفظ ومتى.
- الاحتواء — إجراءات توقف انتشار الحادث مثل عزل الأجهزة وتعطيل الحسابات وحجب الحركة مع الحفاظ على الأدلة.
- الحركة الجانبية — أساليب ينتقل بها المهاجم من الجهاز المخترق الأول إلى أنظمة أخرى داخل الشبكة.

الاستجابة الأولى للحوادث السيبرانية يوما بيوم

اليوم 1: مشهد التهديدات أمام المستجيب

- أساليب برمجيات الفدية والابتزاز — إلحاح الاستجابة والأثر على الأعمال
- نماذج سلسلة الهجوم — مواضع اعتراض الاختراق بالكشف
- دورة حياة NIST SP 800-61 — الأدوار من الاستعداد إلى التعافي
- مصفوفة خطورة الحوادث — عتبات التصعيد ومحفزات المناوبة
- جرد أدوات المستجيب — الثغرات قبل التنبيه التالي

اليوم 2: استخبارات التهديدات للاستجابة الأولى

- مصادر الاستخبارات ومجتمعات المشاركة — موثوقية المصدر وملاءمته
- مسار إثراء المؤشرات — ثقة التنبيه ومعدلات الإنذار الكاذب
- ملفات سلوك الخصوم — التحركات المرجحة بعد الدخول الأول
- فرضيات صيد التهديدات — بحث استباقي يسبق التنبيهات
- سجل متطلبات الاستخبارات — الأسئلة التي تحتاج القيادة إلى إجاباتها

اليوم 3: مصادر السجلات وربط الأحداث

- سجلات أحداث Windows وأداة Sysmon — رؤية العمليات وعمليات الدخول
- سجلات التدقيق والمصادقة في Linux — كشف إساءة استخدام الصلاحيات
- قواعد الربط في منصة SIEM — حجم التنبيهات مقابل نطاق التغطية
- مسارات تدقيق السحابة وسجلات الهوية — نطاق الاختراق على مستوى المستأجر
- الاحتفاظ بالسجلات ومزامنة الوقت — موثوقية الخط الزمني للحادث

اليوم 4: تحليل حركة الشبكة

- التقاط الحزم بأداة Wireshark — أدلة تسريب البيانات والاتصالات الدورية
- سجلات NetFlow والاتصالات — مسارات الحركة الجانبية
- مراجعة سجلات DNS والوكيل — كشف نطاقات القيادة والتحكم
- تواقيع كشف التسلل — الضبط في مواجهة الحركة السليمة
- البيانات الوصفية للحركة المشفرة — حدود الفحص ومقايضات الخصوصية

اليوم 5: فرز الأجهزة الطرفية والبيانات المتطايرة

- ترتيب التطاير — ما يجمع قبل العزل
- اقتناء الذاكرة ومراجعة العمليات — الشيفرات الخبيثة في الأنظمة العاملة
- آليات الاستمرار والمهام المجدولة — اكتمال الاستئصال
- بيانات منصات الكشف والاستجابة الطرفية — قرارات عزل الأجهزة
- نصوص الاستجابة الحية — السرعة مقابل سلامة الأدلة

اليوم 6: الأدلة الرقمية والتعامل الجنائي

- نسخ الأقراص والتحقق بالبصمة — مقبولية الأدلة المجمعة
- نماذج سلسلة الحيازة — المساءلة عن كل أثر
- إعادة بناء الخط الزمني — تسلسل أفعال المهاجم
- التعامل مع عينات البرمجيات الخبيثة وبيئات العزل — فهم السلوك بأمان
- الحفظ القانوني وتخزين الأدلة — توقعات المستشار القانوني وشركات التأمين

اليوم 7: قرارات الاحتواء والاستئصال

- الاحتواء قصير المدى مقابل طويل المدى — الأثر على استمرارية الأعمال
- تعطيل الحسابات وإعادة تعيين بيانات الاعتماد — نطاق اختراق الهوية
- تجزئة الشبكة وقواعد الحجب — خطر انكشاف الدفاع للمهاجم
- تحديد السبب الجذري — الثغرة أو الإعداد الخاطئ الواجب إغلاقه
- فحوص التحقق من الاستئصال — الثقة قبل إعادة الربط

اليوم 8: التعافي وتنسيق الحادث

- استعادة الأنظمة من نسخ احتياطية موثوقة — منع إعادة الإصابة
- هيكل قيادة الحادث — صلاحيات القرار أثناء الأزمة
- قوالب التواصل مع أصحاب المصلحة — رسائل القيادة والموظفين والعملاء
- التنسيق مع الأطراف الثالثة والموردين — المسؤولية المشتركة في الاستجابة
- المراقبة بعد التعافي — علامات عودة المهاجم

اليوم 9: التقارير والدروس المستفادة

- هيكل تقرير الحادث — الوقائع والأثر والأسئلة المفتوحة
- تيسير مراجعة ما بعد الحادث — نتائج تحسين بلا لوم
- مقاييس الاستجابة ومتوسط زمن الاحتواء — أولويات الاستثمار في القدرات
- تحليل فجوات الكشف — قواعد جديدة ومصادر بيانات إضافية
- مراجعة حالات من الرعاية الصحية والخدمات المالية — أنماط الاستجابة القطاعية

اليوم 10: ممارسة دليل تشغيل معالجة الحوادث

- محاكاة اختراق حي من التنبيه الأول — الفرز تحت ضغط الوقت
- تطبيق تحليل السجلات والحركة والأجهزة الطرفية — تحديد نطاق الاختراق المحاكى
- تمرين جمع الأدلة — سلسلة الحيازة في التطبيق
- تمرين الاحتواء والإحاطة — تحديث للقيادة خلال ساعة واحدة
- استكمال دليل تشغيل معالجة الحوادث — الخطوات والمسؤولون ومسارات التصعيد

تطبيق الاستجابة الأولى للحوادث السيبرانية بعد الدورة

- إدارة تمرين محاكاة مكتبي لسيناريو برمجيات الفدية باستخدام مصفوفة الخطورة وخيارات الاحتواء التي جرى التدرب عليها
- تدقيق مصادر السجلات ومدد الاحتفاظ بها في ضوء احتياجات الربط والخط الزمني التي ظهرت في تحليل الحركة والأجهزة الطرفية

أسئلة حول الاستجابة الأولى للحوادث السيبرانية

ما الاستجابة الأولى للحوادث السيبرانية ولماذا تهم الآن؟

الاستجابة الأولى للحوادث السيبرانية هي كشف الهجوم وفرزه واحتواؤه في ساعاته الأولى. وتهم الآن لأن المخترقين يتحركون بسرعة، والقرارات المبكرة بشأن الأدلة والعزل تحدد كلفة التعافي ومدته.

من يستفيد أكثر من دورة الاستجابة الأولى للحوادث السيبرانية؟

يستفيد أكثر محللو مراكز العمليات ومعالجو الحوادث ومسؤولو أمن المعلومات ومدافعو الشبكات. وتزداد فائدتك إن كنت تتلقى التنبيهات أو تحدد نطاق الاختراق أو تعزل الأجهزة، وتتضاعف حين يحضر عدة أعضاء من فريق الاستجابة نفسه.

كيف تختلف دورة الاستجابة الأولى للحوادث السيبرانية عن دورة التحليل الجنائي الرقمي؟

تغطي الدورة مسار الاستجابة كله من التنبيه حتى الدروس المستفادة بدلا من التحليل الجنائي المخبري المعمق. ويقدم التعامل مع الأدلة بالقدر الذي يحتاجه المستجيب لحفظ الآثار للمختصين، إلى جانب الاستخبارات وتحليل الحركة والاحتواء.

ماذا تعود به من دورة الاستجابة الأولى للحوادث السيبرانية؟

تعود بدليل تشغيل مجرب لمعالجة الحوادث في بيئتك. ويحدد خطوات الفرز وجمع الأدلة وخيارات الاحتواء وجهات التصعيد وصيغ التقارير التي يستطيع فريقك اعتمادها في الأسبوع التالي.

الاستجابة الأولى للحوادث السيبرانية: الطريق إلى الأمام

يوجه دليل تشغيل معالجة الحوادث أولا طريقة تصعيد التنبيه التالي عالي الخطورة ومن يعزل الجهاز المصاب. ويستخدمه محللو النوبات ومعالجو الحوادث وقائد الحادث أثناء الأحداث الحية، ويستخدمه مالكو الخدمات أثناء التعافي. وبعد أول استخدام فعلي تستحق عتبات الاحتواء وخطوات الأدلة مراجعة جديدة، إذ تكشف الحوادث الأولى مواضع التعارض بين السرعة والحفظ.