JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة التحليل الجنائي السيبراني والاستجابة للحوادث

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة التحليل الجنائي السيبراني والاستجابة للحوادث

التحليل الجنائي السيبراني والاستجابة للحوادث دورة تدريبية مدتها أسبوع لمستجيبي الحوادث ومحللي مراكز العمليات الأمنية والفنيين الجنائيين الذين يحتوون الهجمات الحية دون إتلاف الأدلة، ويخرج المشاركون منها بدليل إجرائي للاستجابة للحوادث جاهز جنائيا. تتحرك عصابات برامج الفدية والمخترقون اليوم خلال ساعات، لذلك فإن المستجيب الذي يلتقط الذاكرة والسجلات وآثار الشبكة مبكرا يحدد سرعة التعافي وما تستطيع المؤسسة إثباته لاحقا. تقدم جوبيتر برايم للتدريب هذه الدورة في التحليل الجنائي السيبراني والاستجابة للحوادث.

لماذا يهم التحليل الجنائي السيبراني والاستجابة للحوادث الآن

يعتمد المهاجمون بصورة متزايدة على أدوات النظام المدمجة، ويشغلون الشيفرة الخبيثة في الذاكرة فقط، ويمسحون السجلات قبل المغادرة. وفي الوقت نفسه تنتظر شركات التأمين والمدققون والفرق القانونية رواية قابلة للدفاع عما حدث. والمستجيب الذي يعزل الجهاز مبكرا جدا قد يفقد الآثار المتطايرة اللازمة لتحديد نطاق الاختراق، ومن يتأخر كثيرا يسمح بانتشاره. توازن الدورة بين هذين الضغطين، وتربط وظائف الاكتشاف والاستجابة والتعافي في إطار الأمن السيبراني CSF 2.0 NIST بضوابط إدارة الحوادث في المواصفة ISO/IEC 27001:2022.

المستفيدون من التحليل الجنائي السيبراني والاستجابة للحوادث

- المستجيبون الذين يقودون الفرز والاحتواء أثناء الحوادث الأمنية الحية
- محللو مراكز العمليات الأمنية الذين يصعدون التنبيهات إلى تحقيقات
- الفنيون الذين يلتقطون أدلة الذاكرة والحزم والسجلات من الأنظمة المصابة
- صائدو التهديدات الذين يبحثون عن آليات البقاء والتنقل الجانبي عبر الشبكات
- المهندسون الذين يعيدون تشغيل الأنظمة ويتحققون من إخراج المهاجمين

تستفيد فرق العمليات الأمنية في قطاعي الاتصالات والطاقة أكثر عندما يحضر المحللون والمستجيبون معا، لأنهم يتفقون على مسار تصعيد واحد يقدم الأدلة أولا.

قدرات التحليل الجنائي السيبراني والاستجابة للحوادث

يتعلم المشاركون التعامل مع كل إجراء احتواء بوصفه خطوة دفاعية وحدثا ذا أثر في الأدلة معا، فيختارون ما يلتقطونه قبل ما يحجبونه.

- تقييم خطورة التنبيه ونطاقه باستخدام إشارات السجلات والأجهزة الطرفية المترابطة — قائد الحادث
- تطبيق التقاط الذاكرة وتحليلها لكشف العمليات المخفية والشيفرة المحقونة — المسؤول الجنائي
- تحليل التقاطات الحزم وسجلات التدفق لتتبع قنوات القيادة والتحكم — عمليات الشبكة
- اختبار الملفات المشبوهة بالفرز الثابت وبيئة العزل لاستخراج المؤشرات — استخبارات التهديدات
- الموازنة بين خيارات الاحتواء وفقدان الأدلة وتعطل الأعمال — مالكو الخدمات
- تصميم خطوات الدليل الإجرائي التي تحفظ الأدلة في كل مرحلة استجابة — مدير العمليات الأمنية

مصطلحات التحليل الجنائي السيبراني والاستجابة للحوادث الأساسية

- ترتيب التطاير — تسلسل جمع الأدلة من الأقصر عمرا إلى الأطول، بدءا بالذاكرة.
- صورة الذاكرة — نسخة من ذاكرة النظام تكشف العمليات الجارية ومنافذ الشبكة والشيفرة التي لا تكتب على القرص.
- مؤشر الاختراق — أثر ملاحظ مثل بصمة ملف أو نطاق أو مفتاح تسجيل يدل على نشاط خبيث.
- قناة القيادة والتحكم — مسار الاتصال الذي يرسل عبره المهاجمون التعليمات إلى الأجهزة المخترقة.
- استراتيجية الاحتواء — الأسلوب المختار لتقييد وصول المهاجم، من عزل الشبكة إلى تعليق الحسابات.
- الجاهزية الجنائية — الترتيب المسبق للتسجيل والأدوات والإجراءات بما يسمح بجمع الأدلة بسرعة وسلامة.

التحليل الجنائي السيبراني والاستجابة للحوادث يوما بيوم

اليوم 1: مشهد الاختراقات ودورة الاستجابة

- مراجعة أساليب المهاجمين — التعرف على تقنيات أدوات النظام المدمجة والهجمات بلا ملفات
- مراحل دورة الاستجابة — مواءمة الاكتشاف والاستجابة والتعافي مع NIST CSF 2.0
- ترتيب التطاير — تقديم الجمع على إجراءات الاحتواء
- مصفوفة تصنيف الخطورة — تحديد مستويات التصعيد والمستجيبين
- قائمة الجاهزية الجنائية — التأكد من تغطية التسجيل قبل وقوع الحادث

اليوم 2: التحليل الجنائي للذاكرة

- الالتقاط الحي للذاكرة — نسخ الذاكرة دون تنبيه المخترق
- تحليل شجرة العمليات — كشف شذوذ العلاقة بين العمليات الأم والفرعية والتنكر
- كشف الشيفرة المحقونة — تحديد الحمولات المجوفة والمحملة انعكاسيا
- فحص منافذ الشبكة — ربط العمليات بالاتصالات البعيدة
- آثار سرقة بيانات الاعتماد — تقييم انكشاف الأسرار المخزنة مؤقتا

اليوم 3: أدلة السجلات والشبكة

- ترتيب أولوية مصادر السجلات — اختيار سجلات المصادقة والوكيل ونظام أسماء النطاقات
- استعلامات الربط في نظام SIEM — إعادة بناء تنقل المهاجم بين الأجهزة
- مراجعة التقاط الحزم — استخراج الحمولات وتفاصيل الجلسات
- تحليل سجلات التدفق — كشف أنماط الإشارات الدورية وتسريب البيانات
- ربط ضوابط الحوادث — وصل احتياجات الأدلة بالمواصفة ISO/IEC 27001:2022

اليوم 4: فرز البرمجيات الخبيثة وقرارات الاحتواء

- الفرز الثابت للملفات — استخراج النصوص والبصمات والتواقيع بأمان
- تحليل السلوك في بيئة العزل — رصد آليات البقاء والاتصالات العكسية
- تجميع المؤشرات — مشاركة علامات الاختراق مع فرق الاكتشاف
- مصفوفة خيارات الاحتواء — الموازنة بين العزل والحجب وتعليق الحسابات
- التحقق من الإزالة — التأكد من إخراج المهاجم قبل إعادة الخدمات

اليوم 5: ممارسة الدليل الإجرائي للاستجابة للحوادث الجاهز جنائيا

- خطوات الجمع وفق التطاير — دمج التقاط الذاكرة من اليوم 2
- محفزات أدلة الشبكة — تطبيق قواعد السجلات والحزم من اليوم 3
- بوابات قرار الاحتواء — إدراج موافقات مصفوفة الخيارات من اليوم 4
- تمرين محاكاة برامج الفدية — اختبار الخطوات تحت ضغط الوقت
- الدليل الإجرائي للاستجابة للحوادث الجاهز جنائيا — إنهاء الأدوار والمحفزات وخطوات الأدلة

تطبيق التحليل الجنائي السيبراني والاستجابة للحوادث بعد الدورة

- نفذ تمرين التقاط ذاكرة على جهاز اختبار وسجل الوقت والأدوات اللازمة.
- أضف خطوات الجمع وفق ترتيب التطاير إلى أول ثلاثة إجراءات في دليل برامج الفدية الحالي.

أسئلة حول التحليل الجنائي السيبراني والاستجابة للحوادث

ما التحليل الجنائي السيبراني والاستجابة للحوادث ولماذا يهم الآن؟

هو ممارسة احتواء الحوادث الأمنية مع التقاط الأدلة التي تفسرها. ويهم الآن لأن المهاجمين يعملون في الذاكرة ويمسحون السجلات، فالأدلة التي تضيع أثناء الاستجابة لا يمكن استعادتها لاحقا.

ما الأدوار الأكثر استفادة من تدريب التحليل الجنائي السيبراني والاستجابة للحوادث؟

يستفيد أكثر مستجيبو الحوادث ومحللو مراكز العمليات الأمنية والفنيون الجنائيون. ويستفيد كذلك صائدو التهديدات ومهندسو التعافي، لأنهم يعتمدون على أدلة الذاكرة والسجلات والشبكة نفسها لتحديد نطاق الحوادث وإغلاقها.

كيف يختلف التحليل الجنائي السيبراني والاستجابة للحوادث عن دورة التحقيق الجنائي في الحاسوب؟

تعمل هذه الدورة أثناء الحوادث الحية، وتركز على أدلة الذاكرة والشبكة وخيارات الاحتواء. أما دورة التحقيق الجنائي في الحاسوب فتفحص الأقراص المضبوطة بعد الحدث، وتبني خطوطا زمنية وتقارير مفصلة للإجراءات القانونية.

ماذا تعود به من تدريب التحليل الجنائي السيبراني والاستجابة للحوادث؟

تعود بدليل إجرائي للاستجابة للحوادث جاهز جنائيا، مختبر في تمرين محاكاة لبرامج الفدية، يتضمن خطوات الجمع وبوابات الاحتواء والأدوار، وجاهز للتكييف مع مركز العمليات الأمنية لديك.

التحليل الجنائي السيبراني والاستجابة للحوادث: الطريق إلى الأمام

يوجه الدليل الإجرائي للاستجابة للحوادث الجاهز جنائيا أولا القرار التالي بعزل جهاز مصاب. ويستخدمه المستجيبون وقادة مراكز العمليات الأمنية ومالكو الخدمات للاتفاق على ما يلتقط ومن يوافق على الاحتواء. وبعد استخدامه الحي الأول تستحق المراجعة لمعرفة ما إذا كانت أي بوابة احتواء قد أخرت العمل دون داع، ثم تعديل المحفزات حيث ضاعت الأدلة.