JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة أساسيات الأمن السيبراني للموظفين الجدد في التقنية والأعمال

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة أساسيات الأمن السيبراني للموظفين الجدد في التقنية والأعمال

أساسيات الأمن السيبراني دورة تدريبية مدتها أسبوع للموظفين الجدد في التقنية ومحللي الأعمال والمهنيين المنتقلين إلى أدوار الأمن، يعود منها المشاركون بقائمة التحقق الأمنية الأساسية لفرقهم. فكل إدارة اليوم تتعامل مع حسابات سحابية وأجهزة طرفية عن بعد وسجلات عملاء، ولذلك يمنع الفهم المشترك للسرية والسلامة والتوافر الأخطاء البسيطة التي يستغلها المهاجمون كثيرا. تقدم جوبيتر برايم للتدريب هذه الدورة في أساسيات الأمن السيبراني للموظفين الجدد في التقنية والأعمال.

لماذا تهم أساسيات الأمن السيبراني الآن

ترفع ثلاث قوى أهمية هذا المجال للمنضمين الجدد: التصيد الاحتيالي وسرقة بيانات الدخول اللذان يستهدفان المستخدم العادي لا الخوادم، والعمل الهجين الذي ينشر الحواسيب المحمولة والهواتف خارج شبكة المكتب، والعملاء والمدققون الذين يطلبون دليلا على الضوابط الأساسية قبل توقيع العقود. المؤسسة التي يدرك موظفوها الجدد مسارات الهجوم ويطبقون قواعد النظافة الرقمية تغلق معظم الثغرات السهلة، أما التي تترك الأمن لفريق متخصص صغير فتعيد فتحها باستمرار. وتستند الدورة إلى وظائف إطار NIST Cybersecurity Framework 2.0 المعروف اختصارا NIST CSF 2.0، وإلى محاور الضوابط في معيار ISO/IEC 27001:2022 لنظم إدارة أمن المعلومات.

المستفيدون من أساسيات الأمن السيبراني

- موظفو الدعم التقني المبتدئون الذين ينشئون الحسابات ويجهزون الأجهزة ويعالجون طلبات الصلاحيات
- محللو الأعمال الذين يحددون متطلبات أنظمة تحمل سجلات شخصية أو مالية
- المهنيون المنتقلون من الشبكات أو البرمجة إلى أول وظيفة أمنية
- منسقو المشاريع الذين يتابعون المتطلبات الأمنية في إطلاق الحلول التقنية
- موظفو مكتب الخدمة الذين يتلقون الرسائل المريبة وطلبات إعادة تعيين كلمات المرور

تستفيد الوحدة التقنية أو الرقمية الناشئة أكثر حين ترسل عدة منضمين جدد معا، فيعودون بمفردات واحدة وقائمة تحقق موحدة.

قدرات أساسيات الأمن السيبراني

ينتقل المشاركون من التعرف على التهديدات إلى تطبيق خط الضوابط الأول على الحسابات والشبكات والأجهزة.

- تطبيق ثلاثية السرية والسلامة والتوافر لتصنيف السجلات والأنظمة التي يتعامل معها الفريق — مالكو المعلومات
- تقييم مسارات الهجوم الشائعة مثل التصيد والبرمجيات الخبيثة وكلمات المرور الضعيفة — تصعيد مكتب الخدمة
- تحديد مبدأ الحد الأدنى من الصلاحيات والمصادقة متعددة العوامل لأدوار المستخدمين — مسؤولو الأنظمة
- اختبار تقسيم الشبكة وقواعد جدار الحماية على سيناريوهات بسيطة — قادة البنية التحتية
- بناء خطوات تحصين الحواسيب المحمولة والأجهزة الجوالة — مالكو إدارة الأجهزة
- الإبلاغ عن الحوادث المشتبه بها بوضوح وسرعة — الوظيفة الأمنية والمديرون المباشرون

مصطلحات أساسيات الأمن السيبراني الأساسية

- ثلاثية السرية والسلامة والتوافر — الخصائص الثلاث التي يسعى كل ضابط أمني إلى حمايتها في المعلومات والأنظمة.
- سطح الهجوم — جميع النقاط من حسابات وأجهزة وخدمات مكشوفة التي قد يحاول المتسلل الدخول منها.
- الحد الأدنى من الصلاحيات — منح كل مستخدم أو نظام الوصول اللازم لمهمته فقط دون زيادة.
- المصادقة متعددة العوامل — تسجيل دخول يتطلب إثباتين مستقلين أو أكثر مثل كلمة مرور وتنبيه على الجهاز.
- إدارة التحديثات الأمنية — روتين اكتشاف تحديثات البرمجيات واختبارها وتثبيتها لسد نقاط الضعف المعروفة.
- الهندسة الاجتماعية — التلاعب بالأشخاص لكشف معلومات أو منح وصول، غالبا عبر البريد أو الهاتف أو المراسلة.

أساسيات الأمن السيبراني يوما بيوم

اليوم 1: مبادئ الأمن وصورة التهديدات

- تطبيق ثلاثية السرية والسلامة والتوافر على الأنظمة اليومية — تصنيف ما يحتاج إلى حماية
- أنواع الجهات المهددة ودوافعها — توقع من يستهدف المؤسسة
- نظرة على وظائف NIST CSF 2.0 — تحديد موقع كل دور في دورة الأمن
- أساسيات حصر الأصول — معرفة الأجهزة والحسابات الموجودة فعلا
- قصص اختراقات في التجزئة والخدمات اللوجستية — تتبع الأسباب الجذرية البسيطة

اليوم 2: مسارات الهجوم والعوامل البشرية

- تشريح التصيد والهندسة الاجتماعية — كشف الطعم قبل النقر
- عائلات البرمجيات الخبيثة وبرمجيات الفدية — التعرف المبكر على علامات الإصابة
- هجمات كلمات المرور وحشو بيانات الاعتماد — تقوية ممارسات تسجيل الدخول
- استعراض سلسلة الهجوم — رؤية المواضع التي تقطع فيها الدفاعات الهجوم
- الإبلاغ عن النشاط المريب — اختيار قناة التصعيد الصحيحة

اليوم 3: الهوية والتحكم في الوصول

- دورة حياة الهوية من الانضمام إلى المغادرة — إزالة الحسابات اليتيمة
- الحد الأدنى من الصلاحيات والوصول المبني على الأدوار — اعتماد الصلاحيات بانضباط
- خيارات المصادقة متعددة العوامل — اختيار الأساليب لكل فئة مستخدمين
- التعامل مع الحسابات ذات الامتيازات — فصل صلاحيات الإدارة عن الاستخدام اليومي
- روتين مراجعة الوصول — تأكيد الصلاحيات مع مالكي الأعمال

اليوم 4: أساسيات حماية الشبكة والأجهزة الطرفية

- مفاهيم تقسيم الشبكة وجدار الحماية — الحد من التنقل الجانبي للمهاجم
- الشبكات اللاسلكية الآمنة والوصول عن بعد — حماية العاملين في النمط الهجين
- إعدادات تحصين الأجهزة الطرفية — تقليل تعرض الحواسيب والهواتف
- دورة إدارة التحديثات الأمنية — ترتيب التحديثات حسب الخطورة
- أساسيات النسخ الاحتياطي والاستعادة — صون التوافر بعد برمجيات الفدية

اليوم 5: التطبيق العملي لقائمة التحقق الأمنية الأساسية

- تمرين تصنيف الأصول والبيانات — تطبيق الثلاثية على أنظمة الفريق
- مناقشة نتائج محاكاة التصيد — تطبيق معرفة مسارات الهجوم على رسائل حقيقية
- فحص عشوائي لحقوق الوصول — تطبيق الحد الأدنى من الصلاحيات على حسابات نموذجية
- ربط الفحوص بمحاور ضوابط ISO/IEC 27001:2022 — وصل القائمة بضوابط معترف بها
- قائمة التحقق الأمنية الأساسية — استكمال فحوص الهوية والأجهزة والشبكة والإبلاغ

تطبيق أساسيات الأمن السيبراني بعد الدورة

- إجراء الفحص العشوائي لحقوق الوصول على نظام مشترك واحد وحذف حسابات الموظفين المغادرين.
- تعريف الزملاء بمسار الإبلاغ عن التصيد باستخدام رسالتين احتياليتين وصلتا إلى الفريق مؤخرا.

أسئلة حول أساسيات الأمن السيبراني

ما أساسيات الأمن السيبراني، ولماذا تهم الآن؟

هي المبادئ الجوهرية والضوابط الأساسية التي تحمي الحسابات والأجهزة والشبكات والسجلات. وتهم الآن لأن معظم الاختراقات ما زالت تبدأ برسالة تصيد أو كلمة مرور مكررة أو جهاز غير محدث يستطيع الموظف المدرب اكتشافه.

من أكثر المستفيدين من تدريب أساسيات الأمن السيبراني؟

يستفيد أكثر الموظفون الجدد في التقنية ومحللو الأعمال والمنتقلون إلى الأمن. فقراراتهم اليومية في الوصول والأجهزة والإبلاغ تشكل تعرض المؤسسة منذ البداية.

كيف يختلف تدريب أساسيات الأمن السيبراني عن دورة أمن الذكاء الاصطناعي في قطاع محدد؟

يبني الأساس العام الذي يفترضه كل تخصص لاحق. فالدورة القطاعية تطبق دفاعات تعلم الآلة على أنظمة صناعة واحدة، أما هذا المجال فيعلم المبادئ ومسارات الهجوم والضوابط الأساسية الصالحة لأي مؤسسة.

ماذا تعود به من تدريب أساسيات الأمن السيبراني؟

تعود بقائمة التحقق الأمنية الأساسية. تغطي تصنيف البيانات وحقوق الوصول والمصادقة متعددة العوامل وتحصين الأجهزة والتحديثات والنسخ الاحتياطي ومسار الإبلاغ عن النشاط المريب.

أساسيات الأمن السيبراني: الطريق إلى الأمام

توجه قائمة التحقق الأمنية الأساسية أول قرار حول الحسابات والأجهزة والأنظمة المشتركة التي يعالجها الفريق قبل غيرها. ويستخدمها قادة الفرق والدعم التقني ومالكو المعلومات للاتفاق على تحسينات سريعة ومتابعتها. وبعد أول تطبيق ربع سنوي لها تستحق افتراضات التهديد التي بنيت عليها المراجعة، لأن مسارات الهجوم تتغير وتنضم خدمات جديدة إلى سجل الأصول.