المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT I info@ainfct.com I www.ainfct.com

Security Information and Event Management (SIEM) Training

فكرة الدورة

أصبحت أنظمة إدارة المعلومات والأحداث الأمنية SIEM عنصراً محورياً في بناء قدرات الرصد والتحليل والاستجابة داخل بيئات الأمن السيبراني الحديثة. ومع تزايد حجم السجلات الأمنية وتنوع مصادرها بين الشبكات والأنظمة والتطبيقات والخدمات السحابية، تحتاج المؤسسات إلى منهجية واضحة لجمع البيانات، وتطبيعها، وربطها، وتحويلها إلى مؤشرات قابلة للتحليل واتخاذ القرار.

يركز هذا البرنامج التدريبي من AINFCT على تمكين المشاركين من فهم دورة عمل SIEM من منظور تشغيلي ومهني، بدءاً من مصادر السجلات وهندسة الجمع، مروراً بقواعد الربط والتنبيه، وصولاً إلى التحقيق في الحوادث، وقياس جودة الكشف، وتحسين حالات الاستخدام. كما يتناول البرنامج العلاقة بين SIEM ومركز العمليات الأمنية، ومؤشرات الاختراق، وأطر الهجوم، وإدارة الإنذارات، والاحتفاظ بالسجلات، والتقارير الأمنية.

يوفر البرنامج قيمة عملية واضحة من خلال ربط مفاهيم الرصد الأمني بسيناريوهات تشغيلية واقعية تساعد المشاركين على تحسين جودة الكشف وتقليل الضوضاء وتعزيز كفاءة الاستجابة.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- شرح دور SIEM ضمن منظومة العمليات الأمنية.
- تحديد مصادر السجلات والأحداث ذات الأولوية.
- تصميم حالات استخدام للكشف والتحليل الأمني.
- تحليل التنبيهات وربطها بمؤشرات الاختراق.
- تحسين جودة القواعد وتقليل الإنذارات الكاذبة.
- إعداد تقارير أمنية تدعم القرار التشغيلي.

منهجية الدورة

- عروض تفاعلية لشرح المفاهيم التشغيلية الأساسية.
- تمارين تحليل سجلات وتنبيهات افتراضية.
- سيناريوهات عملية لبناء حالات استخدام.
- مناقشات موجهة حول تحسين جودة الكشف.
- مراجعات قصيرة لترسيخ المفاهيم اليومية.

أثر الدورة على المنظمة

يمكن تعزيز فعالية الرصد الأمني المؤسسي من خلال:

- تحسين رؤية المؤسسة للأحداث الأمنية الحرجة.
- رفع كفاءة اكتشاف التهديدات والاستجابة لها.

- تقليل الضوضاء التشغيلية والإنذارات غير المهمة.
- دعم الامتثال عبر إدارة سجلات منظمة.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم دورة عمل SIEM من البداية للنهاية.
- تحليل الأحداث الأمنية بمنهجية تشغيلية واضحة.
- بناء حالات استخدام قابلة للتطبيق.
- تحسين التنسيق مع فرق العمليات والاستجابة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج العاملين في الأمن السيبراني وتقنية المعلومات ممن يتعاملون مع السجلات والتنبيهات والتحقيقات الأمنية. كما يفيد الفرق التي تسعى إلى تحسين قدراتها في الرصد الأمني وإدارة أحداث SIEM.

- محللو مركز العمليات الأمنية SOC.
- مسؤولو أمن المعلومات والأمن السيبراني.
- مهندسو الشبكات والأنظمة والبنية التحتية.
- مختصو الاستجابة للحوادث والتحقيقات الرقمية.

- مسؤولو الامتثال والحوكمة الأمنية.

موضوعات الدورة

اليوم الأول: مدخل إلى SIEM ومركز العمليات الأمنية

- مفهوم إدارة المعلومات والأحداث الأمنية SIEM.
- دور SIEM داخل مركز العمليات الأمنية.
- الفرق بين الحدث والتنبيه والحادث الأمني.
- العلاقة بين الرصد والتحليل والاستجابة.
- التحديات التشغيلية في بيئات السجلات الكبيرة.

اليوم الثاني: مصادر السجلات والأحداث الأمنية

- سجلات الأنظمة والخوادم وقواعد البيانات.
- سجلات الشبكات والجدران النارية وأنظمة الكشف.
- سجلات التطبيقات والخدمات السحابية والهوية.
- تقييم قيمة المصدر حسب المخاطر وحالة الاستخدام.
- تحديد أولويات الربط بين المصادر الحرجة.

اليوم الثالث: جمع السجلات وإدارتها

- آليات جمع السجلات من المصادر المختلفة.
- الوكلاء والمجمعات وواجهات التكامل.
- اعتبارات التوقيت والتزامن وجودة البيانات.
- حماية السجلات أثناء النقل والتخزين.
- معالجة الانقطاع وفقدان السجلات الحرجة.

اليوم الرابع: التطبيع والفهرسة وإثراء البيانات

- مفهوم تطبيع الأحداث داخل منصات SIEM.
- الحقول المشتركة وربطها بالسياق الأمني.
- الفهرسة والبحث السريع في البيانات الأمنية.
- إثراء الأحداث بمعلومات الأصول والتهديدات.
- تحسين جودة البيانات لدعم التحليل.

اليوم الخامس: قواعد الربط والتحليل المنطقي

- مفهوم الارتباط بين الأحداث المتعددة.
- قواعد الكشف القائمة على الشروط والأنماط.
- الربط الزمني والسلوكي بين الأحداث.
- إدارة العتبات والاستثناءات والقوائم المرجعية.
- اختبار القواعد قبل تشغيلها عملياً.

اليوم السادس: حالات الاستخدام الأمنية

- مفهوم حالة الاستخدام في الرصد الأمني.
- اختيار حالات الاستخدام حسب المخاطر المؤسسية.
- توثيق المنطق والمصادر والمخرجات المتوقعة.
- بناء حالات استخدام للهوية والشبكات.
- مراجعة فعالية حالات الاستخدام دورياً.

اليوم السابع: مؤشرات الاختراق والتهديدات

- أنواع مؤشرات الاختراق وطرق استخدامها.
- مصادر استخبارات التهديدات وتقييم موثوقيتها.
- ربط المؤشرات بالأحداث والتنبيهات.
- مؤشرات السلوك مقارنة بالمؤشرات الثابتة.
- تجنب الاعتماد المفرط على المؤشرات الضعيفة.

اليوم الثامن: مواءمة SIEM مع MITRE ATT&CK

- استخدام التكتيكات والتقنيات في توصيف الكشف.
- ربط التنبيهات بسلوكيات الخصوم المعروفة.
- تحليل تغطية الكشف حسب الأساليب الهجومية.
- تحديد فجوات الرصد وبناء أولويات التحسين.
- توثيق التغطية بطريقة مفهومة للفرق الأمنية.

اليوم التاسع: إدارة التنبيهات وتقليل الضوضاء

- تصنيف التنبيهات حسب الخطورة والسياق.
- أسباب الإنذارات الكاذبة وطرق تقليلها.
- تحسين شروط القواعد والعتبات التشغيلية.
- إدارة القوائم البيضاء والاستثناءات الآمنة.
- قياس جودة التنبيهات بمرور الوقت.

اليوم العاشر: التحقيق في الأحداث الأمنية

- خطوات التحقيق الأولي في التنبيهات.
- تجميع الأدلة من السجلات والمصادر المرتبطة.
- استخدام البحث المحوري والتحليل الزمني.
- ربط الأحداث بسلاسل الهجوم المحتملة.
- توثيق نتائج التحقيق بطريقة قابلة للمراجعة.

اليوم الحادي عشر: التكامل مع الاستجابة للحوادث

- تحويل التنبيه إلى حادث قابل للإدارة.
- التكامل بين SIEM ومنصات إدارة الحوادث.
- إجراءات التصعيد والإشعار وتوزيع المسؤوليات.
- دعم الاحتواء والتحليل بعد الحادث.
- استخلاص الدروس لتحسين قواعد الكشف.

اليوم الثاني عشر: الامتثال والاحتفاظ بالسجلات

- متطلبات الاحتفاظ بالسجلات في البيئات المؤسسية.
- حماية السجلات من التعديل أو الحذف غير المصرح.
- سياسات التخزين والأرشفة والاسترجاع.
- التقارير الدورية لدعم الحوكمة والامتثال.
- موازنة الاحتفاظ بالتكلفة وقابلية التحليل.

اليوم الثالث عشر: لوحات المعلومات والتقارير

- تصميم لوحات معلومات للمراقبة التشغيلية.
- مؤشرات الأداء الأمنية المرتبطة بـ SIEM.
- تقارير الإدارة وتقارير الفرق الفنية.
- عرض الاتجاهات والحوادث والتنبيهات الحرجة.
- تجنب ازدحام التقارير بمقاييس غير مؤثرة.

اليوم الرابع عشر: تحسين النضج التشغيلي

- تقييم نضج استخدام SIEM داخل المؤسسة.
- إدارة دورة حياة القواعد وحالات الاستخدام.
- قياس التغطية والفعالية والاستجابة.
- تحسين التعاون بين فرق الأمن والتقنية.
- بناء خارطة تطوير مستمرة للمنصة.

اليوم الخامس عشر: تطبيقات عملية ومراجعة تكاملية

- تحليل سيناريوهات أمنية متعددة المصادر.
- بناء حالة استخدام من المتطلبات إلى التنبيه.
- مراجعة تنبيه وتحويله إلى مسار تحقيق.
- تقييم جودة القواعد والتقارير الناتجة.
- تلخيص أفضل الممارسات التشغيلية لـ SIEM.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة موجزة للمفاهيم السابقة، ثم عرض للمحور الرئيسي، يتبعه تمرين تطبيقي أو نقاش تشغيلي مرتبط بسيناريوهات SIEM، وينتهي اليوم بخلاصة مركزة تساعد المشاركين على ربط المفاهيم بممارسات الرصد والتحليل داخل بيئة العمل.

course_assessment

يعتمد التقييم على المشاركة الفعالة، وتحليل السيناريوهات، وتمارين بناء حالات الاستخدام، والمراجعات القصيرة المرتبطة بمحاور البرنامج. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- إدارة السجلات الأمنية.
- تحليل الأحداث والتنبيهات.
- بناء حالات الاستخدام.
- ربط التهديدات بالسياق.
- إدارة التحقيقات الأمنية.
- التقارير والقياس التشغيلي.
- (REFERENCES USED)

7 شارع وهران، الطيران، مدينة نصر
+201152466358
info@ainfct.com
ainfct.com
رقم التسجيل الضريبي: 472920235

مكتب مدريد الفرعي

مدريد، إسبانيا
شارع الصحة 3، وسط المدينة، 28013 مدريد
training@ainfct.com
ainfct.com