JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

# دورة متقدمة في استخبارات التهديدات والاستجابة السيبرانية للطيران

info@jupiterprime.uk

**jupiterprime.uk**

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

# دورة متقدمة في استخبارات التهديدات والاستجابة السيبرانية للطيران

استخبارات التهديدات والاستجابة السيبرانية للطيران دورة تدريبية مدتها أسبوعين لمحللي مراكز العمليات الأمنية والمستجيبين للحوادث وقادة الأمن السيبراني في شركات الطيران والمطارات ومقدمي الملاحة الجوية، يخرج منها المشاركون بدليل الاستجابة للحوادث السيبرانية في الطيران لمنظمتهم. فهجمات الفدية واختراقات الموردين والاعتداءات على أنظمة الركاب والتشغيل تصل اليوم إلى صالات التسجيل وجداول الرحلات خلال ساعات. تقدم الدورة جوبيتر برايم للتدريب.

## لماذا يهم استخبارات التهديدات والاستجابة السيبرانية للطيران الآن

ترفع ثلاث قوى رهانات العمليات الأمنية في الطيران. فالمجموعات الإجرامية والجهات المدعومة تستهدف شركات الطيران والمطارات لأن انقطاعا واحدا يصنع اضطرابا ظاهرا وضغطا للدفع. والمنصات المشتركة والخدمات السحابية ومقدمو المناولة يوسعون سطح الهجوم خارج شبكة أي منظمة منفردة. وتنتظر سلطات الطيران من المشغلين معاملة الأحداث السيبرانية بوصفها مخاطر سلامة وأمن مع إبلاغ سريع واستعادة مجربة. المنظمة التي تحول الاستخبارات إلى رصد مبكر تحمي الرحلات وبيانات الركاب والسمعة، أما التي تتأخر فتواجه إلغاء المغادرات وتعافيا طويلا. تستند الدورة إلى دورة الاستخبارات ودورة حياة التعامل مع الحوادث من التحضير والرصد والاحتواء والاستئصال والاستعادة حتى الدروس المستفادة.

## المستفيدون من استخبارات التهديدات والاستجابة السيبرانية للطيران

- محللو العمليات الأمنية الذين يفرزون التنبيهات في شبكات شركات الطيران والمطارات
- المستجيبون للحوادث الذين يحتوون اختراقات الأنظمة التشغيلية ويحققون فيها
- محللو الاستخبارات الذين يتتبعون الجهات المهاجمة لقطاع الطيران
- قادة الأمن السيبراني الذين يرفعون الحوادث إلى الإدارة العليا والسلطات
- مهندسو التقنيات التشغيلية المسؤولون عن أنظمة الأمتعة والبوابات والمهابط

تستفيد شركة الطيران أو المطار أكثر حين يحضر فريق العمليات الأمنية والاستجابة والتقنيات التشغيلية معا ويتدربون على دليل مشترك واحد.

## قدرات استخبارات التهديدات والاستجابة السيبرانية للطيران

يتدرب المشاركون على ربط ما يعرف عن مهاجمي الطيران بالتنبيهات والقرارات وخطوات الاستعادة التي تبقي الطائرات في الأجواء.

- بناء متطلبات استخبارية تعكس مخاطر الرحلات والركاب والشحن — المسؤول الأول عن أمن المعلومات
- تقييم ملفات الجهات المهاجمة وأساليبها ضد أنظمة الطيران — قادة العمليات الأمنية
- تصميم قواعد رصد لشبكات مراقبة المغادرة والأنظمة التشغيلية للمطار والتقنيات التشغيلية — مهندسو الرصد
- تطبيق قرارات الاحتواء التي توازن بين الأمن واستمرار الرحلات — مديرو المناوبات ومركز التحكم بالعمليات
- اختبار تسلسل استعادة أنظمة الركاب والتشغيل — مالكو خدمات تقنية المعلومات
- نقل حالة الحادثة إلى الإدارة العليا والسلطات والشركاء — فريق إدارة الأزمات

## مصطلحات استخبارات التهديدات والاستجابة السيبرانية للطيران الأساسية

- استخبارات التهديدات السيبرانية CTI — معلومات محللة عن المهاجمين ونواياهم وأساليبهم توجه قرارات الدفاع.
- مؤشر الاختراق IOC — علامة تقنية مثل بصمة ملف أو عنوان شبكي تدل على احتمال اختراق النظام.
- التكتيكات والتقنيات والإجراءات TTPs — أنماط السلوك التي يتبعها المهاجم لبلوغ أهدافه.
- هندسة الرصد — تصميم القواعد التي تحول سجلات الأنظمة إلى تنبيهات أمنية موثوقة واختبارها وضبطها.
- الاحتواء — إجراءات تحد من انتشار المهاجم مع الإبقاء على العمليات الأساسية.
- دليل الاستجابة للحوادث — تسلسل متفق عليه مسبقا للأدوار والخطوات والقرارات لنوع محدد من الحوادث السيبرانية.

## استخبارات التهديدات والاستجابة السيبرانية للطيران يوما بيوم

### اليوم 1: مشهد التهديدات السيبرانية في الطيران

- خريطة سطح الهجوم في الطيران — أنظمة شركات الطيران والمطارات والملاحة
- اتجاهات برمجيات الفدية والابتزاز — الأثر على التسجيل والأمتعة
- حالات اختراق سلاسل التوريد — المنصات المشتركة ومقدمو الخدمات
- انكشاف التقنيات التشغيلية — إضاءة المهابط والبوابات وأنظمة المباني
- الخطر السيبراني بوصفه خطر سلامة — الصلة بالاضطراب التشغيلي

### اليوم 2: متطلبات الاستخبارات وجمعها

- تخطيط دورة الاستخبارات — الأسئلة التي يحتاج القادة إلى إجاباتها
- متطلبات الاستخبارات ذات الأولوية — مخاطر الرحلات والركاب والشحن
- المصادر المفتوحة والتجارية والقطاعية — الموثوقية والتغطية
- مجتمعات تبادل المعلومات — التبادل الموثوق مع نظراء الطيران
- تصنيف المصادر وقواعد التعامل — درجة الثقة وحدود المشاركة

## اليوم 3: تحليل الجهات المهاجمة

- بناء ملفات الجهات المهاجمة — الدوافع والقدرات واستهداف الطيران
- مطابقة أساليب TTPs — ربط سلوك المهاجم بفجوات الدفاع
- تتبع الحملات — ربط الحوادث عبر المنظمات
- أساليب التحليل — الفرضيات المتنافسة وفحص الانحياز
- صيغ تقارير الاستخبارات — منتجات تكتيكية وتشغيلية واستراتيجية

## اليوم 4: هندسة الرصد

- تغطية مصادر السجلات — أنظمة الركاب والشبكات والأجهزة الطرفية
- تصميم قواعد الرصد — تحويل أساليب المهاجم إلى تنبيهات
- مراقبة التقنيات التشغيلية — المستشعرات السلبية وخطوط الأساس
- ضبط التنبيهات — خفض الإنذارات الكاذبة دون نقاط عمياء
- فرضيات مطاردة التهديدات — البحث عن الاختراقات غير المرصودة

## اليوم 5: مسارات عمل مركز العمليات الأمنية

- معايير فرز التنبيهات — الشدة المرتبطة بأثر الرحلات
- مسارات التصعيد — من المحلل إلى قائد الحادثة
- سجلات إدارة الحالات — سلامة الأدلة والتسلسل الزمني
- تسليم المناوبات في المركز — الاستمرارية أثناء الحوادث الطويلة
- مقاييس أداء المركز — زمن الرصد وزمن الاستجابة

## اليوم 6: التعامل مع الحوادث واحتواؤها

- دورة حياة التعامل مع الحوادث — من التحضير حتى الدروس المستفادة
- تصنيف الحوادث — الفئات والشدة لأحداث الطيران
- خيارات الاحتواء — العزل مقابل استمرار التشغيل
- التنسيق مع مركز التحكم بالعمليات — قرارات اللجوء إلى التشغيل اليدوي
- تنسيق حوادث الأطراف الثالثة — الموردون ومنصات المجتمع

## اليوم 7: التحقيق الرقمي والاستئصال

- جمع الأدلة — حفظ الذاكرة والأقراص والسجلات
- فرز البرمجيات الخبيثة — تحليل السلوك لخدمة قرارات الاستجابة
- تحديد السبب الجذري — نقطة الدخول الأولى والتحرك الجانبي
- تخطيط الاستئصال — إعادة تعيين بيانات الاعتماد وإعادة البناء
- سلسلة حيازة الأدلة — الأدلة لأغراض قانونية وتأمينية

## اليوم 8: استعادة أنظمة الطيران التشغيلية

- ترتيب أولويات الاستعادة — الأنظمة الحرجة للرحلات مقابل أنظمة الأعمال
- خطوات الاستعادة والتحقق — نسخ احتياطية نظيفة وفحوص السلامة
- إجراءات التشغيل اليدوي — التسجيل الورقي وأوراق الحمولة
- تنسيق استمرارية الأعمال — شركاء شركات الطيران والمطارات
- معايير العودة إلى الخدمة — الثقة قبل إعادة الربط

## اليوم 9: اتصالات الأزمات والإبلاغ

- نماذج إحاطة الإدارة العليا — الأثر والخيارات والقرارات
- مسار إشعار السلطات — المهل والمحتوى
- رسائل المسافرين ووسائل الإعلام — الدقة تحت الضغط
- عوامل قرار الفدية والابتزاز — الاعتبارات القانونية والأخلاقية
- مراجعة ما بعد الحادثة — دروس تعود إلى دورة الاستخبارات

## اليوم 10: ممارسة دليل الاستجابة للحوادث السيبرانية في الطيران

- تمرين فدية على نظام مراقبة المغادرة — تطبيق خطوات الاحتواء والاستعادة
- تمرين اختراق مورد — تطبيق تنسيق الأطراف الثالثة
- محاكاة مطاردة تهديد — تطبيق قواعد الرصد ومطابقة الأساليب
- تمرين إحاطة الأزمة للإدارة — تطبيق نماذج الإبلاغ
- دليل الاستجابة للحوادث السيبرانية في الطيران — الأدوار والمحفزات وترتيب الاستعادة

## تطبيق استخبارات التهديدات والاستجابة السيبرانية للطيران بعد الدورة

- صياغة ثلاثة متطلبات استخبارية ذات أولوية مع قادة العمليات ومطابقة تغطية الرصد الحالية معها.
- إجراء تمرين مكتبي على هجوم فدية يستهدف أنظمة الركاب مع مركز التحكم بالعمليات ومالكي خدمات تقنية المعلومات.

## أسئلة حول استخبارات التهديدات والاستجابة السيبرانية للطيران

### ما استخبارات التهديدات والاستجابة السيبرانية للطيران، ولماذا تهم الآن؟

استخبارات التهديدات والاستجابة السيبرانية للطيران هي ممارسة تتبع المهاجمين الذين يستهدفون شركات الطيران والمطارات والتعامل مع الحوادث التي يسببونها. وتهم الآن لأن الفدية واختراقات الموردين قادرة على إيقاف التسجيل والأمتعة وتخطيط الرحلات خلال ساعات.

### ما الأدوار الأكثر استفادة من دورة استخبارات التهديدات والاستجابة السيبرانية للطيران؟

يستفيد محللو العمليات الأمنية والمستجيبون للحوادث أكثر من غيرهم، ثم محللو الاستخبارات وقادة الأمن السيبراني ومهندسو التقنيات التشغيلية. وإذا كنت ترصد الهجمات أو تحتويها أو تبلغ عنها فستكتسب طريقة ومصطلحات مشتركة.

### كيف تختلف دورة استخبارات التهديدات والاستجابة السيبرانية للطيران عن دورة عامة في الأمن السيبراني؟

تطبق أساليب الاستخبارات والاستجابة على الأنظمة التي تبقي الرحلات مستمرة. فالدورة العامة تغطي الضوابط بصورة واسعة، أما هذه الدورة فتعالج حوادث مراقبة المغادرة والأنظمة التشغيلية للمطار والتقنيات التشغيلية والتشغيل اليدوي الذي تتطلبه.

### ماذا تعود به من دورة استخبارات التهديدات والاستجابة السيبرانية للطيران؟

تعود بدليل مجرب يحدد الأدوار ومحفزات الرصد وخيارات الاحتواء وترتيب الاستعادة لحوادث الطيران. ويمنح فرق الأمن والعمليات خطة واحدة يتبعونها تحت الضغط.

### استخبارات التهديدات والاستجابة السيبرانية للطيران: الطريق إلى الأمام

يوجه دليل الاستجابة للحوادث السيبرانية في الطيران أولا قرار من يعلن الحادثة وأي الأنظمة تعزل أو تبقى قيد التشغيل. ويستخدمه قادة العمليات الأمنية وقادة الحوادث وموظفو مركز التحكم بالعمليات مع كل تنبيه كبير. وبعد أول تمرين أو حدث فعلي يستحق ترتيب الاستعادة ومحفزات الرصد مراجعة في ضوء ما حدث فعلا.