



الكتيب 10.4: نشاط تقييم احتمال وقوع هجوم

الغرض:

تقديم معلومات ونموذج للمساعدة في تقييم احتمالات وقوع هجوم صادر عن تهديد تم تحديده

الجزء 1: تقييم احتمال وقوع هجوم

مقدمة

بمجرد استكمال أوراق العمل للتعرف على التهديدات الداخلية والخارجية تكون الخطوة التالية هي تقييم احتمالات وقوع هجوم من هذه التهديدات. ستقوم باستخدام ميزان التقييم التالي للتعبير عن احتمالات وقوع الهجوم: منخفض جداً، منخفض، متوسط، مرتفع، مرتفع جداً.

ستقوم بتحليل فئات متعددة وتطبيق درجة التقييم المناسبة. سيقوم المشاركون بعد ذلك باستكمال ورقة العمل الخاصة بتقييم احتمالات الهجوم لكل نمط من أنماط التهديد. لإتمام تقييم ورقة العمل الخاصة باحتمالات الهجوم، يحتاج المشاركون إلى المعلومات التالية عن كل خصم:

- نمط التهديد
- القدرة
- التاريخ والنوايا
- الجاذبية النسبية للهدف

ورقة عمل لتقييم احتمال وقوع هجوم

بعد أن يناقش المشرف فئات ورقة العمل، يقرأ المشاركون سيناريو آخر للمساعدة في فهم كيفية استكمال ورقة العمل الخاصة بتقييم احتمالات وقوع الهجوم. سيستخدم المشاركون المعلومات في هذا السيناريو الجديد لاستكمال الجدول 1: ورقة عمل لتقييم احتمال وقوع هجوم

الجدول 1: ورقة عمل لتقييم احتمال وقوع هجوم

ورقة عمل لتقييم احتمال وقوع هجوم (L _A)				
التاريخ:		تم التوثيق عن طريق:		
المسؤول عن تقييم المنشأة:				
نمط التهديد:				
الإمكانية:				
هل جماعة الخصوم لها القدرة على القيام بهجوم ناجح على تلك المنشأة؟ للإجابة على هذا السؤال، يجب إعتبار الآتي: هل الخصم يتميز بالخصائص التالية: هل يقع بالقرب من المنشأة وهل له قدرة النفاذ إليها؟ هل من المتوقع حصوله على الموارد المادية اللازمة لشن هجوم على المنشأة؟ هل من المتوقع حصوله على المهارات التقنية اللازمة لشن هجوم على المنشأة؟ هل من المتوقع حصوله على المهارات التخطيطية والتنظيمية المطلوبة لشن هجوم على المنشأة؟	إذا كان الجواب نعم، إستمّر	إذا كان لا، ضعيف جدا - توقف		
تعليمات للقسم التالي: بتعين إنتقاء من الأعمدة الثلاثة الوسطى الإجابة التي تصف بأكثر درجات الدقة البند الوارد في عمود الفئة الخاصة بكل صف (سطر). لاحظ القيمة الرقمية المرتبطة بالإجابة و عليك إدخال تلك القيمة الرقمية بالعمود الخاص بتقييم "الدرجات".				
التاريخ والنوايا:		القيمة بالدرجات		
الفئة المصالح (الإهتمامات) التاريخية	إذا لم ترد أية أدلة موثقة تاريخيا تفيد أن هذه المجموعة من الخصوم قد أبدت اهتماما خاصا بهذا النوع من المنشآت أو هذه المنشأة بالتحديد	إذا كانت هناك تكهنات ولكن بدون أدلة موثقة تاريخيا تفيد أن هذه المجموعة من الخصوم قد أبدت اهتماما خاصا بهذا النوع من المنشآت أو هذه المنشأة بالتحديد	إذا لم يكن هناك أية أدلة موثقة تاريخيا تفيد أن هذه المجموعة من الخصوم قد أبدت اهتماما خاصا بهذا النوع من المنشآت أو هذه المنشأة بالتحديد	القيمة الرقمية =
	الدرجات = 5	الدرجات = 3	الدرجات = 1	

ورقة عمل لتقييم احتمال وقوع هجوم (L _A)				
القيمة الرقمية=	إذا لم تكن هناك أية أدلة موثقة تاريخياً تفيد أن هذه المجموعة من الخصوم قد شنت هجمات مماثلة على هذا النوع من المنشآت أو هذه المنشأة بالتحديد الدرجات = 1	إذا كانت هناك تكهنات ولكن بدون أدلة موثقة تاريخياً تفيد أن هذه المجموعة من الخصوم قد شنت هجمات مماثلة على هذا النوع من المنشآت أو هذه المنشأة بالتحديد الدرجات = 3	إذا لم ترد أية أدلة موثقة تاريخياً تفيد أن هذه المجموعة من الخصوم قد قامت بهجمات مماثلة على هذا النوع من المنشآت أو هذه المنشأة بالتحديد الدرجات = 5	الفئة الهجمات الثابتة تاريخياً
القيمة الرقمية=	إذا لم ترد أية معلومات حالية توحى بوجود اهتمام بالمنشأة. قيمة الدرجات = 2	لا ينطبق	إذا توافرت معلومات حالية توحى بوجود اهتمام إرهابي بالمنشأة. الدرجات = 10	الفئة الإهتمام الحالي بالمنشأة
القيمة الرقمية=	إذا لم تتناول الاستخبارات الراهنة المنشأة بعينها أو أية منشآت مماثلة في البلاد أو بالخارج. الدرجات = 2	إذا كانت الاستخبارات الراهنة تحققت من المسح الخاص بموقع معين أو أية منشآت مماثلة في البلاد أو بالخارج. الدرجات = 6	إذا تحققت الاستخبارات الراهنة من المسح بموقع محدد الدرجات = 10	الفئة المراقبة (المسح) الحالية

ورقة عمل لتقييم احتمال وقوع هجوم (L _A)				
القيمة الرقمية =	إذا كان هذا الموقع لم يتعرض لتهديدات هجومية موثقة من هذا النمط التهديدي ولا من أية مجموعات معادية أخرى الدرجات = 2	إذا كان هذا الموقع قد تعرض لتهديدات هجومية موثقة ولكن ليست من هذا النمط التهديدي الدرجات = 6	إذا كان هذا الموقع قد تعرض لتهديدات هجومية موثقة من هذا النمط التهديدي الدرجات = 10	الفئة التهديدات الموثقة
القيمة بالدرجات	الجاذبية النسبية للهدف			
القيمة الرقمية =	إذا كان مستوى التبعات التقديرية للهجوم غير متسق البتة مع أهداف هذا النمط من التهديدات. الدرجات = 2	إذا كان مستوى التبعات التقديرية للهجوم ليس متسقا بكل تأكيد مع أهداف هذا النمط من التهديدات ولكن هناك احتمال قائم. الدرجات = 6	إذا كان مستوى التبعات التقديرية للهجوم متسق مع أهداف هذا النمط من التهديدات. الدرجات = 10	الفئة التبعات
القيمة الرقمية =	إذا كان الهجوم على هذا الموقع لا يتسق البتة مع الأيديولوجية ولا الدوافع الخاصة بهذا النمط من التهديد. الدرجات = 2	إذا كان الهجوم على هذا الموقع لا يتسق مع الأيديولوجية ولا معالدوافع الخاصة بهذا النمط من التهديد، ولكن هناك احتمال قائم. الدرجات = 6	إذا كان الهجوم على هذا الموقع يتسق مع الأيديولوجية والدوافع الخاصة بهذا النمط من التهديد. الدرجات = 10	الفئة أيديولوجية

نمط التهديد

نمط التهديد هو وصف نوع الخصم ونمط الأفعال المطلوب تحليلها. يتعين على كل المشاركين استكمال ورقة العمل الخاصة بكل نمط من أنماط التهديد المحتملة التي تم التعرف عليها في ورقة عمل المعلومات المتعلقة بتهديد العناصر الداخلية، وورقة عمل المعلومات الخاصة بتهديد العناصر الخارجية. تذكر أن نمط التهديد هو وصف موجز للخصم، بما في ذلك اسم الجماعة والعمل المحتمل القيام به. يتعين استكمال ورقة عمل منفصلة لكل مجموعة وعمل محتمل.

القدرة

وبمجرد تحديد نوع التهديد موضع التقييم في ورقة العمل، يتعين إجراء أول تقييم بغرض تحديد ما إذا كان هذا النمط التهديدي قادراً على شن هجوم ناجح على الهدف أم لا. يتلخص هذا التحديد بنعم أم لا، مع وضع المعلومات التالية في الاعتبار. هل نمط تهديد الخصم يتميز بالخصائص التالية:

- هل يقع بالقرب من المنشأة وهل له قدرة النفاذ إليها؟
- هل من المتوقع حصوله على الموارد المادية اللازمة لشن هجوم على المنشأة؟
- هل من المتوقع حصوله على المهارات التقنية اللازمة لشن هجوم على المنشأة؟
- هل من المتوقع حصوله على المهارات التدريبية والتنظيمية المطلوبة لشن هجوم على المنشأة؟

إذا كانت الأجوبة على الأسئلة آنفة الذكر **نعم**، يتعين على المشاركين الإستمرار في استكمال بقية الأجزاء الخاصة بورقة العمل. إذا كانت الإجابة لا في جميع الأسئلة، عندئذ فلا حاجة للإستمرار في استكمال باقي عناصر ورقة العمل الخاصة بالهجوم حيث تكون احتمالاته ضعيفة جداً.

التاريخ والنوايا

إذا كان تقييم القدرات (الخاصة بالخصم) يستدعي قيامك باستكمال ورقة العمل، فالقسم التالي سيساعدك على النظر في تاريخ ونوايا التهديد الذي تقوم بتقييمه. تحتوي ورقة العمل على تصريحات تساعدك على عمل تقييم رقمي لكل منطقة أو جانب من الجوانب الموصوفة فيما يلي. ستقرأ هذه التصريحات في ورقة العمل ثم تختار القيمة الرقمية المناسبة لكل جانب.

المصالح (الاهتمامات) التاريخية

يتعين على المشاركين البحث عما إذا كانت هناك أية أدلة موثقة أو إرهابيات التي تشير إلى أن هذه المجموعة من الخصوم قد أبدت اهتماماً خاصاً بهذا النوع من المنشآت أو نمط محدد من المرافق الحيوية بعينها.

الهجمات الثابتة تاريخياً

يتعين البحث عن وجود الأدلة الموثقة أو التكهّنات التي تشير إلى أن هذه المجموعة من الخصوم قد أبدت اهتماماً خاصاً بهذا النوع من المنشآت أو نمط محدد من المرافق الحيوية.

الاهتمام الحالي بالمنشأة

يتعين التحري عن وجود أية معلومات حالية توحى بوجود اهتمام إرهابي بالمنشأة.

المراقبة الحالية

يتعين تحديد ما إذا كانت الإستخبارات الراهنة تحققت من المسح الخاص بموقع معين أو مراقبة أية منشآت مماثلة في البلاد أو بالخارج.

التهديدات الموثقة

يجب تحديد ما إذا كان هذا الموقع قد تعرض لتهديدات هجومية موثقة من هذا الخصم بالذات أو من جماعة مشابهة.

الجاذبية النسبية للهدف

يتعين أيضاً اعتبار الجاذبية النسبية للتهديد موضع التقييم والذي يتم تحديده وفقاً لمستوى العواقب التقديرية، والأيدولوجية، أو سهولة الهجوم. تحتوي ورقة العمل على تصريحات تساعدك على عمل تقييم رقمي لكل منطقة أو جانب من الجوانب الموصوفة فيما يلي. ستقرأ هذه التصريحات في ورقة العمل ثم تختار القيمة الرقمية المناسبة لكل جانب.

التبعات

يتعين اعتبار ما إذا كان مستوى التبعات التقديرية للهجوم متسقاً مع أهداف هذا النمط من التهديدات.

الأيدولوجية

يتعين النظر لتحديد ما إذا كان الهجوم على هذا الموقع يتسق مع الأيدولوجية والدوافع الخاصة بهذا النمط من التهديد.

سهولة الهجوم

يتعين اعتبار ما هو الإدراك الرصدي لنظام الأمن المادي فيما يتعلق بوجوده (وجود التهديد بالهجوم) وما مدى سهولة التغلب عليه.

وبمجرد استكمال جمع المعلومات الكافية، يتعين تقييم الخصم في كل فئة باستخدام الأوصاف الواردة في ورقة العمل. تسجيل القيمة الرقمية في عمود الدرجات الوارد في ورقة العمل. وبعد تحديد القيمة الرقمية للدرجات الخاصة بكل منطقة، يتعين جمع كل الدرجات. تسجيل القيمة الإجمالية لمجموع درجات نوع التهديد.

مقارنة إجمالي الدرجات مع المقياس الوارد في أسفل ورقة العمل. إذا كان المجموع الكلي للدرجات التي حصل عليها هذا النمط من التهديد:

- 60 درجة أو أكثر، فإحتمالات الهجوم مرتفعة جداً.
- أقل أو يساوي 59، وأكثر أو يساوي 47، فإحتمالات الهجوم مرتفعة.
- أقل أو يساوي 46، وأكثر أو يساوي 32، فإحتمالات الهجوم متوسطة.
- أقل أو يساوي 31، وأكثر أو يساوي 19، فإحتمالات الهجوم منخفضة.
- 18 درجة أو أقل، فإحتمالات الهجوم منخفضة جداً.

الغرض: تقديم مثال للمساعدة في تقييم احتمالات وقوع هجوم صادر عن تهديد تم تحديده

المدة: 25 دقيقة (20 دقيقة للنشاط، و 5 دقائق لاستخلاص المعلومات)

تشكيل المجموعة: مجموعات الطاولة

استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة

الجزء 2: توجيهات النشاط:

1. اقرأ المعلومات التي يقدمها سيناريو القاعدة الجوية
2. استخدم تلك المعلومات في الجدول 1: ورقة عمل لتقييم احتمال وقوع هجوم.
 - تستخدم ورقة العمل الخاصة بتقييم احتمال وقوع الهجوم تحديدا رقميا للمستوى يتراوح في نطاق ما بين 1 إلى 10، حيث يشير رقم "10" إلى أقصى درجة من الأهمية الحرجة.
 - افحص كل فئة أثناء انتقالك عبر مراحل ورقة العمل مع مجموعتك.
 - استخدم خبراتك ومهاراتك التدريبية بالإضافة إلى معلومات نشاط السيناريو لتطبيق الدرجات المناسبة وفقاً للمعلومات المذكورة عن كل نمط من أنماط التهديد.
 - وربما ترغب في تغيير أو تعديل القيم العددية لكل فئة، ولكن أي تعديل جاد تجريه يجب أن يكون له مبررات قوية ويكون الغرض منه هو الوفاء بمتطلبات خاصة.
3. أمامك 20 دقائق لإتمام هذا النشاط.
4. كن مستعداً للتشارك في تقييم الدرجات مع بقية أعضاء الصف.

سيناريو القاعدة الجوية

- أعلنت إحدى العصابات الإجرامية المنظمة (مشتبته أن يكون لها طابع إرهابي) عبر السنوات السابقة أنها بصدد التخطيط لسرقة أملاك حكومية ثمينة من قواعد القوات الجوية.
- نجد أن هذه الجماعة الإجرامية المنظمة قد قامت فعلاً باستهداف 3 قواعد عسكرية للقوات الجوية في الشهر الماضي ببلد مجاور، ونجحت بالفعل في سرقة معدات حيوية مملوكة للجيش. يحصل هذا الجانب على تقييم رقمي (5) بالنسبة لفئة المصالح والهجمات التاريخية.
- لاحظت قوات إنفاذ القانون فرد يشتبه أنه عضو في جماعة إجرامية منظمة يحوم حول القاعدة الجوية التي تعمل بها. ولم تنجح محاولة إيقاف الهدف والتعرف على هويته. ولكن الشرطة العسكرية المحلية تمكنت من التعرف على الهدف والتأكد من انتمائه كفرد من تلك الجماعة المشبوهة.
- عاد أعضاء العصابة إلى قاعدة القوات الجوية ببلدك. لاحظ سكان المنطقة أولئك الأفراد وهم يلتقطون الصور للمنشأة العسكرية ويسجلون البيانات في دفتر الملاحظات. ولم تتمكن السلطات المحلية من الاتصال بالأهداف قبل أن يغادروا المنطقة.
- سنفترض جدلاً أن وحدة الاستخبارات الخاصة بالقوات الجوية في بلدك قد راجعت التقارير الاستخباراتية السابقة واكتشفت أن جماعة إرهابية مماثلة، قد تكون خلية إرهابية أخرى، قد حاولت بالفعل سرقة معدات حيوية من موقع عسكري منذ خمس سنوات.
- كانت المعدات الحيوية المسروقة تتضمن أحدث صيحة في أجهزة الاتصالات والرادارات الأرضية المستخدمة لرصد وتتبع الطائرات المقاتلة.
- وفقاً للتقارير الاستخباراتية الحالية، لم تحاول العصابة الإجرامية المنظمة بيع تلك المعدات. وبالتالي، هناك اعتقاد قوي لدى وحدة الاستخبارات أن هذه العصابة هي منظمة إرهابية، وأنها

- بعينها هي التي أعلنت في الماضي أن هدفها هو إيقاف الطائرات الحربية من القوات الجوية التابعة لبلدك من التحليق في سماء دولتهم، حيث يعتبرونها طائرات دولة معادية.
- حتى الآن، لم يتم اعتراض الهجمات من جانب السلطات العسكرية. ولم يتم تحديث أنظمة الأمن المادي على مدار 15 سنة، والتكنولوجيا المستخدمة في حماية المعدات الحيوية تحتاج إلى صيانة.

تم ترك هذه الصفحة فارغة عمداً.