# مغالطات استخبارات التهديدات تقود إلى ثغرات في أوضاع أمن المؤسسات

تتبع المؤسسات تعريفات غير دقيقة لاستخبارات التهديدات تؤدي إلى وضع تصورات رديئة لبرامج استخبارات التهديدات. توصل الشركات تعريفات لاستخبارات التهديدات تدعم عروضهم التي تروج لمغالطة أن استخبارات التهديدات تحل الكثير من المشاكل الأمنية.

تقوم وظائف استخبارات تهديدات الفضاء الإلكتروني على قاعدة غير مدعومة من المهنية التقليدية للاستخبارات. تدعم العديد من البرامج جزء ضئيل من الاحتياجات الاستخباراتية، إلا أن أصحاب المصلحة يحملون توقعات غير واقعية بناءً على نفقاتهم.

لقد تطورت إمكانيات مجال أمن المعلومات بصورة ضئيلة مع الارتفاع الباهظ في النفقات والتطور المحدود في الأوضاع بعد اكتشاف الحقائق التي يتم التعريف بها على أنها إجراءات وقائية.

عمليات الشراء المحمومة لأدوات "استخبارات التهديدات" بناءً على فرضية المشاهدة والاكتشاف والقبض تضمن حدوث تحسن بطيء وعدم التوسع في البيانات. تركز صناعة البرامج الاستخباراتية على تعدد القدرات التكنولوجية والمشاكل التاريخية لأمن المعلومات عندما كانت الجدران النارية وبرامج مكافحة الفيروسات تمثل صلب البرامج الأمنية.
التوصيات والفرص الموجودة في هذا التقرير عن الأوضاع تندرج تحت قسم *تغيير السلوكيات*.

الوصول إلى المؤسسات التي قد تكون أكثر تطوراً في فجوات البيانات متاح لهذا المقال. وقد بنينا الأدلة بناءً على الدخول المباشر على عدد من مؤسسات Fortune 500، ومناقشات أثناء فصول التدريب على استخبارات الفضاء الإلكتروني والأنشطة الفعلية لصناعة برامج الاستخبارات.

ملحوظة: يتبع التقرير المذكور أعلاه باستثناء الفقرات التحليلية وتحليل البدائل أسلوب كتابة يتميز بحرفية التحليل الاستخباراتي.

## التصنيف العام

عند إجراء بحث عام على الإنترنت عن "استخبارات التهديدات" نحصل على 11 مليون نتيجة في 0.36 ثانية ما يدل على الانتشار المتعمد للمصطلح والذي يهدف إلى تحقيق عائدات.
تستخدم شركات المعلومات وأمن الفضاء الإلكتروني ومؤسسات التدريب الشهيرة والشركات الأخرى المصطلح بشكل متكرر لدرجة أفقدته معناه الحقيقي.
تستخدم معظم الشركات المصطلح كما لو كانت الاستخبارات شيء سهل الصنع، ومتاح بسهولة. يباع المنتج على أمل أن استخبارات التهديدات هي العلاج الحاسم الذي سعى إليه كبار ضباط أمن المعلومات لسنوات.
وهذه بشكل عام تسمية مغلوطة ومتكررة عند صياغة واستخدام الكلمات الرنانة والعبارات الشائعة التي تتغير كل عام. تبني الشركات سنوات من القدرات بناءً على المصطلحات الرنانة التي كانت مستخدمة بالأمس وحتى أن أحداً لا يعلم أنها كانت موجودة. أحد هذه المصطلحات الرنانة هو استخبارات التهديدات.

ما هي استخبارات التهديدات؟ تشير مؤسسة غارتنر Gartner إلى أنها:

*استخبارات التهديدات هي المعرفة القائمة على الدليل بما في ذلك السياق والآليات والمؤشرات والتعقيدات والنصائح العملية حول المخاطر والتهديدات القائمة أو الناشئة للقواعد التي يمكن استخدامها في اتخاذ قرارات مدروسة فيما يتعلق بتعامل المواطنين مع التهديد أو الخطر.*
*(غارتنر، 2013) ب 3*

تستخدم شركة Solutionary (NTT) هذا التعريف من وكالة الاستخبارات المركزية:
*عند صياغة المصطلح في أبسط صورة نجد أن الاستخبارات هي المعرفة الحالية والمعرفة المسبقة بالعالم من حولنا وشروع صناع السياسة الأمريكية في اتخاذ قرارات وإجراءات. توفر مؤسسات الاستخبارات هذه المعلومة بطريقة تساعد العملاء سواءً كانوا زعماء مدنيين أو قادة عسكريين من أجل النظر في اعتبارات الخيارات البديلة والنتائج.*
*الاستخبارات*
*هي عملية تتضمن الاجتهاد والمثابرة وبشكل عام الجمع العشوائي والشاق للحقائق وتحليلها وتقييمها بسرعة ووضوح وعمل تقييم لنتائج الاستخبارات ونشرها للعملاء في التوقيت المناسب.*


*وفوق كل ذلك يجب أن تكون العملية التحليلية وفي التوقيت المناسب ومرتبطة بالاحتياجات والمشاكل السياسية. (مجلة سكيورتي، 2016).*
*قمة هرم مؤسسة* A1 NTT Security *يذهب للقول أنه بدلاً من تقديم استخبارات عسكرية أو سياسية للحكومات أصحاب المصلحة يجب أن يكون التركيز الحالي داخل قطاع أمن المعلومات قائم على تقديم خدمات استخبارات التهديدات لأصحاب المصلحة في المؤسسة بشأن التهديدات الرقمية لنظم شركاتهم.*
(مجلة سكيورتي 2016) ب 2

## إساءة فهم التعريفات

هنا تكمن واحدة من أكثر المشاكل المتأصلة التي تعيق عمل العديد من المؤسسات في الوقت الحالي. النظرة القصيرة هي أن كل ما نحتاجه هو استخبارات تهديدات فنية أو تقنية من أجل حماية المؤسسة. سوف نضيف إلى هذه المغالطة مغالطة أخرى لاحقاً. المغالطات التي تخلق ثغرات هائلة في أوضاع أمن الفضاء الإلكتروني لدينا تضمن الوصول إلى توقعات غير منطقية وفجوات في البرامج.

تتراوح تعريفات الاستخبارات في نطاقها وعمقها بناءً على من يستخدم المصطلح. نحن نميل إلى أن نظل بالقرب من التعريفات المهنية التقليدية مثل التعريفات التالية:

المنتج الناتج من جمع ومعالجة ودمج وتقييم وتحليل وترجمة وتفسير المعلومات المتعلقة بالأعداء (الهجمات الصبيانية، وهجمات المبتدئين وجرائم الفضاء الإلكتروني وهجمات الدول والحكومات والقراصنة النشطاء والأنشطة السياسية والمتطفلين والقراصنة أصحاب القبعات البيضاء / القبعات السوداء، وإرهابيي الفضاء الإلكتروني والمنافسين والتقارير الاستقصائية والأكاديمية) والعناصر العدائية على الفضاء الإلكتروني أو التي من المحتمل أن تكون عدائية أو مناطق العمليات الفعلية أو المحتملة.

(الحكومة، الاستخبارات المشتركة، 2013) كما أن A1 أحد هيئات استقصاء الأدلة والاستنتاجات القائمة على ما تم الحصول عليه وتنقيحه استجابة للمتطلبات المعروفة أو المحتملة للعملاء. وعادةً ما يستمد ذلك من معلومات سرية أو لا يقصد منها أن تكون متاحة للاستخدام من قبل من يحصلون عليها. (الحكومة، 2013) A1 كما أن البيانات والمعلومات التي يمكن الحصول عليها من مصادر مفتوحة عندما توضع في عملية تفكيك وتحليل وإعادة تركيب وتخليق تصبح معلومات استخباراتية.

أصبح الأمر محير جداً. ما هو التعريف الذي يجب علينا إتباعه؟ من ناحية اصطلاحية بحتة، فإن MWR InfoSecurity في المملكة المتحدة يبدو أن لها قبضة قوية في تعريف مصطلح استخبارات التهديدات. تفترض MWR نموذجاً يعمل على تقسيم استخبارات التهديدات إلى أربع قطاعات مميزة بناءً على الاستهلاك والعمليات الاستراتيجية والتكتيكية والفنية والتشغيلية والتقنية. (InfoSecurity، 2015) نموذج B3 MWR (شكل 1) واضح ومحدد ومفصل جيداً وهو شيء يجب على المؤسسات أن تقرأ عنه وتتعرف عليه.

المشكلة في هذا النموذج هي تركيزه بشكل حصري على استخبارات التهديدات. واستخبارات التهديدات هي فرع من الاستخبارات. تستخدم استخبارات التهديدات قدر محدد من المعلومات والبيانات التي يتم جمعها في إنشاء الاستخبارات التي يتم الجمع بينها وبين المخاطر المؤسسية بعد ذلك. لا تتضمن استخبارات التهديدات البيانات الصحيحة بشكل دائم. في أغلب الأحوال تكون البيانات ذات طبيعة تكتيكية وتقنية أو فنية ما يؤدي إلى فجوات هائلة. في أحيان أخرى يكون هناك انحراف في البيانات نتيجة للانحياز المتأصل في التقنيات التي يتم من خلالها جمع وتصفية وفلترة البيانات. وفي النهاية فإنها تفتقر إلى العمق والاتساع والنطاق وتفتقر أيضاً إلى المهنية والحرفية.

## ما هي المهنية؟

مع الأسف فإن معظم ما يتم إنتاجه هو بيانات وفي أفضل الأحوال معلومات. وهذا يبدأ بسوء الفهم بشأن ما هي البيانات مقارنةً بالمعلومات على عكس الاستخبارات العادية. هذا المصطلح مكون رئيسي للمبيعات مع تجاهل صعوبة عملية خلق الاستخبارات، مع عرض البيانات والمعلومات كمعلومات كافية للتدخل. خلق الاستخبارات عملية تتطلب الجمع الشاق للبيانات والانتباه للتفاصيل عند إنتاج البيانات والمعلومات والطرق الهيكلية والفنية والوعي بالتفكير الحرج والانحياز المعرفي. واستخدام الطرق التحليلية والصبر والمثابرة اللذان يصاحبان خلق المعرفة. في هذا البحث نطلق على هذه العملية مصطلح المهنية.

دعونا لا نخلط بين المهنية كونها جزء من الاستخبارات العسكرية. يعتقد الكثيرون أن المهنية عسكرية في شكلها ووظيفتها. وهذا غير صحيح.


مهنية وحرفية الاستخبارات التي أتحدث عنها متأصلة في قدرات وإمكانيات وكالة الاستخبارات المركزية التي اكتسبتها عبر سنوات من التجربة والخطأ والخطايا والانتصارات.

كتابات شيرمان

في الماضي كان السيد كنت تعتبر ولفترة طويلة هو الأب الروحي للتحليل الاستخباراتي ولطرق التحليل الاستخباراتي المعترف بها والمستخدمة في الوقت الحالي. يجب تطبيق معايير كنت التحليلية ومعتقداته وممارساته في الوقت الحالي في إطار وظائف تهديدات استخبارات الفضاء الإلكتروني. (دافيس، 2007) A1 تحدد كتابات ريتشاردز جيه هوير جونيور كخبير في وكالة الاستخبارات المركزية على مدار 45 عام مشاكل التفكير الحرج والانحياز المعرفي والأساليب التحليلية والتنظيمية المستخدمة في الوقت الحالي أيضاً. يمكن تطبيق كتابات كلا الرجلين على مجهودات أمن المعلومات من أجل إنشاء مجال استخبارات التهديدات.

استخدامها يمكن المؤسسات من الرؤية وراء المفهوم المحدود لمصطلح "المشاهدة والاكتشاف والقبض" مع الانتقال إلى جمع البيانات وتحليلها وخلق الأعمال الاستخباراتية واستخدامها في منع أعمال الأعداء وفي بعض الأحيان التنبؤ بها. كما أن هذه المهنة هي إطار العمل المحدد للاستخبارات الذي يجب أن تقوم عليه صناعة البرامج العسكرية وغير العسكرية.

ترتبط العديد من المغالطات التي نواجهها كاختصاصيين في مجال أمن الفضاء الإلكتروني بالافتقار إلى فهم ما يجب التسلح به لكي تصبح محترف في مجال الاستخبارات. هذين الشيئين ليس بينهما ارتباطاً قوياً. مراكز العمليات الأمنية لا ينتشر فيها أخصائيي الاستخبارات.

لا ينتشر فيها المحللين الذين يتمتعون بمهارات الفنون التي وضع علومها شيرمان كنت ووثقها ريتشاردز هيور. في الواقع يشعر الكثير من أخصائيي أمن الفضاء الإلكتروني أن هذه المهنة مهنة بغيضة ومضيعة للوقت بشكل عام.

هذا الاستنتاج مستوحى من العديد من المشاركات حول العالم مع أخصائيي أمن الفضاء الإلكتروني. عندما نذهب لهم في مقر عملهم من أجل المساعدة في صناعة برنامج استخباراتي فإننا نواجه على الفور بمقاومة إن لم يكن التركيز على الأنشطة الفنية والتقنية منخفضة المستوى.

إلا أن الكثيرين ليس لديهم أدنى فكرة أو يحيطون بشكل جيد بالحاجة لبرنامج استخباراتي مصنوع بشكل جيد من أوله إلى آخره على عكس البرامج التقليدية التي تصنع من أسفل لأعلى. لم يكن لدى الكثيرين برامج تدريبية في مجال التحليل الاستخباراتي أو المهنية. يخضع محللو الاستخبارات على أرض الواقع لتدريبات شاقة هيكلية ومركزة متخصصة في مجال التحليل الاستخباراتي. الوظيفة الأساسية لأي مؤسسة استخباراتية. هي أنهم يتعلمون كيفية التفكير والكتابة والإيجاز. لأنهم يدرسون الأدوات التحليلية ومشاكل مكافحة التجسس ومفهوم الإنكار والخداع ومهارات التحليل والإنذار والتحذير. (الوكالة، 2007) A1
المغالطة الأخرى هي أن جنود الاستخبارات العسكرية السابقين وفريق العمل في وكالة الأمن الوطني على درجة عالية من المهنية. غني عن القول أنهم ليست لديهم القدرات أو لم يحصلوا على دورات دراسية في مجال الاستخبارات ولكن الدورات تركز بصورة كبيرة على العمليات العسكرية والطبيعية. تدرب وكالة الأمن الوطني كوادرها من جامعي المعلومات على جمع المعلومات والمحللين على تحليل البيانات في أغلب الأحوال. ولن يلتقي الاثنان أبداً. لدينا معرفة مباشرة بهذه الطرق.
بروتوكول العمل هو تصنيف وفصل المهام كأولوية قصوى على حساب استمرار الجهود والفهم. الهدف هنا هو الإشارة إلى أن هذه المهارات مركزة على نحوٍ كبير في العديد من المجالات المختلفة المرتبطة بالاستخبارات. سواء كانت طبيعة هذه الاستخبارات تعتمد على الاستخبارات أو العامل البشري، لا تشمل الطرق النطاق الشامل لمهنة الاستخبارات التقليدية. ما وجدناه هو أن تبني هذه الطرق أسرع بكثير وفهمها للنموذج أكثر شمولاً من أخصائيي أمن الفضاء الإلكتروني. بصفة عامة فإن القدرة على تكييف وملائمة ودمج نموذج الحرفية لا يناسب هؤلاء الرجال والنساء نظراً لخلفياتهم.

## الأزمات اليومية

نحن نقضي عدد ساعات لا حصر لها في إعداد التقارير اليومية والاستجابة للحوادث اليومية والتعامل مع المشاكل اليومية. يطلق الكثيرين على الاجتماعات اليومية التي نقوم بها ونحن واقفين والتي يتبعها تعقب الكثير من البيانات مصطلح الاستخبارات.
لقد قمنا بعمل تقارير بأرقام مسلسلة نقوم فيها بتسليم تقرير يومي عن التهديدات وفي كل أسبوع تقرير مجمع عن الأسبوع وفي كل شهر تقرير مجمع عن الشهر وهكذا.
نمضي الكثير من الوقت في جمع البيانات الحالية ومكافحة المشكلات اليومية ولا نصل على الإطلاق للمرحلة التي نقوم فيها بأداء أعمال ذات طبيعة استخباراتية وهذا يؤثر علينا بالسلب بصورة كبيرة.


هذه المغالطة في عملياتنا تضمن أننا لن نمتلك على الإطلاق القدرة على تحليل البيانات بناءً على جمعها تاريخياً. جميع البيانات التي يتم جمعها بيانات حديثة. مجال البيانات مجال وقتي. لا يتم ترتيب البيانات بالطريقة التي تيسر تحليلها على المدى الطويل. وبالطبع هناك حاجة لموازنة بين التحليل طويل الأمد وبين التقارير قصيرة الأمد. المغالطة هنا هي أن التقارير قصيرة الأمد يتم الإبلاغ عنها كمنتج تحليل استخباراتي بينما هي على الأغلب استعادة للبيانات مفتوحة لمصدر وتقارير الشركات المتاحة بالفعل.

## جعل العدو يعرف ما نعرفه

تقارير الشركات التي لها أسماء لطيفة تغطي على الوثائق العريضة التي توثق تكتيكات وأساليب وإجراءات الأعداء (TTPs). القوائم التفصيلية لمؤشرات الأعداء معرضة للخطر. تعمل القوائم التفصيلية لمؤشرات الأعداء (IoCs) على نشر التقارير المذكورة. توضح التقارير إمكانيات الشركات بالتفصيل وتؤكد شجاعتهم في كشف الأعداء. يتم الكشف عن أخطاء الأعداء وإعلانها بكل فخر.
تذكر التقارير قائمة بالعديد من الاستنتاجات بدون تفاصيل، مع مناقشة بسيطة للاحتمالات والقليل من الاتصالات التي تتمتع بمستويات ثقة مرتفعة، وبدون مناقشة ثغرات عملية جمع وإنتاج وتحليل البيانات. يترك القارئ لكي يثق ثقة تامة في التقرير من مظهره.
ينظر للتقارير على أنها مطلقة في منهجها إلا أن صياغة مهنية المنطق قد تكون ضعيفة. مسح الاستنتاجات التي تبالغ في تبسيط المشكلة هي السمة المميزة للتقارير. ويعمل تكرار عبارات التورية المستخدمة في إقناع القارئ يضغط بقوة على الحاجة لشراء المنتجات من هذه الشركات.

هذه التقارير كتبت من أجل السوق وبيع المنتجات والخدمات، لا تناقش التقارير احتمال الاحتيال والإنكار.

هل يمكن تزييف أو تلفيق البيانات قبل استحواذ الشركات عليها؟ من المحتمل أن طرق الجمع التي يستخدمونها خاطئة أو وجود أخطاء في المستشعرات أو سوء تفسير؟ كيف تمكنت الشركات من تحديد مصداقية وموثوقية المصدر؟ هل هناك أي انحياز في التقنيات المستخدمة أو التحليل البشري للبيانات التي يتم جمعها؟ هل يستخدم الأعداء أساليب لخداع الشركات والوصول بها لمستويات ثقة ثابتة كل ذلك بينما هم يخدعون الشركات باستخدام طرق الخداع الروسية، وهي طرق الخداع المعروف أن روسيا تستخدمها في هذا الأمر؟
الاعتقاد لدينا أن الإجابة على هذا السؤال هي نعم، يتم خداع الشركات والوصول بها لمستويات ثقة زائفة. عندما نقوم بالإبلاغ عما نعرفه عنهم، يطور أعدائنا طرقاً جديدة للإنكار وخداعنا كل ذلك بينما هم يواصلون إبراز الأنشطة التي تعكس TTPs القديمة. على العكس نحن نسعى ونضلل تماماً كما كان الحال في الأزمنة القديمة. حصان طروادة والعملاء المزدوجين والخداع التكتيكي هي إستراتيجية تحول مسار المعارك. (هامس 2014 A1)

ممارسة الخداع من أجل تحفيز عمل معين طريقة أساسية في تخليق البيانات التي يمكن تحويلها إلى استخبارات. عملية التحفيز تؤدي إلى جمع البيانات ليس فقط في الموجة الأولى فيما يعرف بالبركة، ولكن منذ تفعيل الأمر الثاني والثالث. أحد التكتيكات القديمة التي كانت تستخدمها القوات الجوية الأمريكية هي التحليق بدائرة من الطائرات النفاثة المقاتلة على مقربة من مسافة 12 ميل من الحدود البحرية للدولة التي يتم مهاجمتها.

تحلق الطائرات النفاثة على شكل دوائر تتكرر بينما تقترب طائرة RC-135 من أجل جمع البيانات.

ثم تحلق طائرة نفاثة أو أكثر على مكان الحريق وتعبر الحدود. ويتم تشغيل رادار الاستحواذ على البيانات وتضيء مواقع إطلاق الصواريخ كل ذلك يحدث بينما طائرة RC-135 لكي تجمع البيانات.

يتم جمع كنز دفين من المعلومات بينما أجهزة تشويش الراديو تملأ موجات الهواء. تعود الطائرات النفاثة إلى أدراجها ثم تتلاشى عملية الجمع ببطء. الهدف هنا واضح. تم جمع البيانات، رائع. يستخدم أعدائنا نفس التكتيكات في بيئة الفضاء الإلكتروني من أجل تحديد مدى جاهزية استعداداتنا وإمكانياتنا الفنية والتقنية والطرق الدفاعية لدينا.

### ما هي الاضطرابات؟

الاشتباك الحقيقي مع تقارير التهديدات الخاصة بالشركات هو أن هذه التقارير في الواقع منشورة في العلن. حرب الفضاء الإلكتروني علينا. يمحو الأعداء والخصوم المدونات والمنتديات وغرف الدردشة والمواقع الشخصية من أجل جمع أجزاء المعلومات معاً والتي تستخدم في الإضرار بالحكومات والمؤسسات التجارية والأفراد.

أنهم يستخدمون طرق الاحتيال في استخلاص البيانات الحساسة بمعدلات غير مسبوقة.
وعند اكتشافهم تشعر شركات أمن الفضاء الإلكتروني إلى نشر كل TTP وكل IoC، وبرامجهم الخبيثة والدورات التدريبية العملية للقراصنة الأفراد على مستوى العالم. الضرر الناتج عن هذه العملية هو عملية استخباراتية خالصة. المدهش حقاً هو أن الحكومات لا تطلب من الشركات إخفاء التفاصيل.
إذا كانت واحدة منها سوف تعلن عن هذه البيانات فقد نقرأ تقارير عن تهم الخيانة.

تعمل التقارير على تعزيز مبيعات الشركات بينما تخبر الأعداء بما نعرفه عنهم وعن TTPs الخاصة بهم.
العديد من هذه التقارير تذكر تقارير الشركات الأخرى حول نفس الموضوع كتقارير مرجعية وتمثل مغالطة تعزز وتقوي استنتاجاتهم بطريقة خاطئة (هذا ظاهر بوضوح في التقارير حول مجموعة قراصنة Rocket Kitten).
يعمل هذا السلوك على توجيه العدو باستمرار نحو الطرق المبتكرة التي لا يمكن اكتشافها للمسح والاختراق وحجب البيانات.

*Figure 2 Admiralty Code - Hansen*

يقومون بتغيير هذه الطرق مراراً وتكراراً في ضوء الحجب المستمر لتقارير الشركات، وكان توقيت العديد منها إما قبل مؤتمرات أمن الفضاء الإلكتروني المعروفة مباشرةً أو أثنائها.


قد تفقد الشركات التي قامت باختراق المنتديات وغرف الدردشة لدى الأعداء وطرق التواصل والاتصال الجديدة مع الاستعانة بوسائل الدخول من أجل معرفة المزيد عنهم، قد تفتقر إلى "التغير المستمر" بسبب تقارير الشركات.
أقصد بمصطلح التغير المستمر الطرق القديمة في تغيير ترددات الراديو ومعرفة أمور عن العدو بما فيها الترددات البديلة، وإجراء تغيير على هذه الترددات عندما يكون المطلوب بث إذاعي. الطرق الحديثة اليوم أكثر ديناميكية بكثير لأن الاتصالات في كثير من الأحين تكون مشفرة والتغيير طفيف جداً.

## المغالطات التي تخلق ثغرات

كما ذكرنا سابقاً، نحن نعتقد أن المغالطات في استخبارات التهديدات تنبع من الافتقار إلى قاموس مصطلحات وتصنيف متفقُ عليه، قبول العملاء لحلول الشركات من أجل توفير استخبارات فعلية، فإن تقارير الشركات يتم التعامل معها على أنها ذات قيمة حقيقية بدون التحقق من المصدر أو المعلومة، وضع المؤسسات للاستخبارات في إطار أمن المعلومات مرات كثيرة تكون الاستجابة للحادث أو التعامل معه والفهم الدقيق لماهية مهنة الاستخبارات، وعدم قدرة المؤسسات على رؤية ما وراء الإجراءات الدفاعية البحتة من أجل أمن المعلومات.
نحن ندرك أن هذه المغالطات غير دقيقة وتخلق ثغرات متأصلة في البرامج الأمنية.

## تغيير السلوك

ما الذي يمكننا القيام به من أجل إصلاح مسار المغالطات التي نختار إتباعها باستمرار؟

أولاً ( وبغير تحديد واضح للأولويات) يجب
علينا تثقيف الجميع في مجال تقنية المعلومات
وأمن المعلومات وحزمة برامج C- Suite
حول التصنيف القياسي للاستخبارات. وهذا
يوفر فهماً مشتركاً وقاموس مصطلحات
أساسي تُبنى عليه الاتصالات.

ثانياً، يجب علينا التعامل مع كل تقرير من تقارير الشركات على أنه ليس أكثر من مجرد مصدر للبيانات. يجب تقييم البيانات للتأكد من مصداقيتها وموثوقيتها ومدى مناسبتها. للقيام بذلك يمكننا استخدام شفرة الناتو الأدميرالية (NATO Admiralty Code) (شكل 2). (هانسون، 2015) A1 المستخدمة في هذه المقالة من أجل تقييم مصادر المعلومات (A1، B2،B3 ، الخ.). هذا الكود يساعد المؤسسات على تقييم مصادر البيانات ومصداقية المعلومات التي يوفرها هذا المصدر. يجب تقييم كل شركة باستخدام هذا الكود أثناء توثيق سهولة استخلاص البيانات، ومدى مناسبتها للمشاكل الأمنية لمؤسستك وأهميتها في حل المشاكل الأمنية لديك.

ثالثاً، ابدأ بتنمية وزيادة برامج برنامجك الاستخباراتي. تضيف طرق تعلم إخفاء الهوية وجمع البيانات مفتوحة المصدر وإدارة وتخطيط عملية الجمع وإدارة نتاج وظائف الاستخبارات وتحليلها والكتابة التحليلية والتصنيف كل ذلك يضيف قيمة وقتية لمؤسستك. إدراك أن الاستخبارات ليست هي الاستجابة للحوادث والتعامل معها أو مكون رئيسي لمراكز العمليات الأمنية.
هذه مهارات مميزة ويجب مشاركتها إلا أن دفنها في هذه المجالات خطأ.

وقد واجهنا ذلك لسنوات (وما زلنا نفعل) إدراج أمن المعلومات تحت مجال تقنية المعلومات والتعامل معه على أنه مشكلة تقنية وفنية فقط. ينبغي علينا ألا نرتكب نفس الخطأ مع الاستخبارات. وظائف الاستخبارات تحتاج إلى تعامل مباشر مع أصحاب المصلحة في المؤسسة.

رابعاً، إيجاد عمليات قياسية من أجل السعي وراء الأعمال الضارة داخل بيئة تقنية المعلومات لديك. استخدام TTPs الخاصة بالأعداء في قيادة أعمال "الملاحقة والاكتشاف" مع إدراك أن لها قيمة كبيرة وليست وظيفة استباقية. لأنهم بالفعل داخل الشرك ويجب التخلص منهم. يجب على المؤسسات القيام بذلك من أجل التطهير السليم.

خامساً، تطوير طرق داخل نموذج المخاطر المؤسسية من أجل جمع البيانات مفتوحة المصدر بانتظام. وكما هو الحال مع النقطة الثالثة سالفة الذكر يجب علينا تنمية هذه الوظيفة لكي نتمكن من جمع البيانات والمعلومات وتطوير الاستخبارات المرتبطة بأصحاب المصلحة وبالمؤسسة. التمسك بأولويات متطلبات الاستخبارات وخلق متطلبات المعلومات وترتيب أولوياتها مع التركيز على جميع مصادر المعلومات بما في ذلك جمع المعلومات مفتوحة المصدر. وتطوير طرق إدارة المهام التي تقود أهداف جمع المعلومات عن طريق الرصد.

كتابة ملاحظة أن العديد من تقارير الشركات القائمة على اشتراكات توفر معلومات وبيانات عامة وعادية في طبيعتها. بشكل دوري الاستخبارات جزء من التقرير. وفي بعض الأحيان يدرج فيها جزء متعلق بمؤسستك. في أغلب الأحوال تكون التقارير مكتوبة لمرة واحدة ويتم توزيعها بالعديد من أنماط الصياغة والتنسيق.

سادساً، عمل نموذج لأعدائك وقدراتهم يرتكز على الهدف. زيادة جمع المعلومات لتشمل كل ما هو مصدر لدى أعدائك. الطريقة الوحيدة لفهم ما يهدد مؤسستك هو فهم عدوك بشكل كامل وفهم دوافعه وقدراته ومهاراته وإلا فسوف تستمر المؤسسة في لعب مبارياتها على أساس الدفاع بدون عبور خط منتصف الملعب مطلقاً. وهذه وصفة لخسارة مؤكدة.

سابعاً، اكتب تقرير تحليل استخباراتي مختصر. ليس لدى أصحاب المصلحة الكثير من الوقت. أن تجعلهم يسعون وراء الإجابات يضمن لك الفشل. استخدم الدليل في شكل 3 لمساعدتك في كتابة تقرير التحليل الاستخباراتي.

ثامناً، ضع خطة إستراتيجية يعقبها خطة برنامج للاستخبارات داخل مؤسستك. حدد ما فيها وما ليس فيها. أصدر رؤية ومهمة مع المبادئ الإرشادية. طور مجموعة من الأهداف التي لها ثلاث أو أربع غايات من أجل تحديد كيفية تحقيق هذه الأهداف. احصل على الموافقة واتبع الخطط.

تاسعاً، حدد جولات استماع لفروع النشاط لديك وأصحاب المصلحة في المؤسسة. أحصل على الإذن بحضور اجتماعاتهم مع إدراك أنك هناك من أجل الاستماع والتعلم. لا تعرض خدماتك واستمع إلى ملخصات واكتسب المعرفة بأصحاب المصلحة لديك. لا تستمع لكي تجهز رداً. احصل على هذه المعلومة وعد بها إلى مؤسستك للمساعدة على الارتقاء ببرنامجك. قد تعتقد أنك تعرف شركتك لكن معرفتك بأستاذك تضمن لك التفوق والامتياز.

عاشراً، أتح لمؤسستك الوقت من أجل تنفيذ وظائف استخباراتية. حدد ما هو المهم لمؤسستك وما هو الإطار الزمني اللازم لتنفيذه.


ضع أسس برامج تعليمية كعملية لتحسين الأداء وليس تقييم الخطأ. (غابارد، 2008) B1 أتح لمؤسستك الاستخباراتية الوقت لكي تتعلم. ارتكاب الأخطاء هو المراحل الأولى للنضج المتوقع.

فقط لا ترتكب نفس الأخطاء مراراً وتكراراً. امنح مؤسستك الاستخباراتية السلطة لاتخاذ قرارات والوصول لأصحاب المصلحة لمعرفة المتطلبات والتعريف بالإمكانيات.

حدد أهدافاً وغايات عملية ويمكن تحقيقها فعلياً. وسع الأهداف عند تحديد الوظيفة التي يمكن أن تؤدي إلى الفشل الذي لا داعي له. القيادة والمستوى المناسب للقيادة لازمان من أجل إدارة المحللين. اعرف المستوى المناسب لمؤسستك. عن إضافة وظيفة استخباراتية للمؤسسة التي لم تكن بها هذه الوظيفة من قبل على الإطلاق تحكم في التوقعات. من الناحية العملية فريق العمل المدرب جيداً وقيادة المجموعة يمكن أن تضيف قيمة كبيرة لمؤسستك.

وأخيراً، ورغم أنها غير شاملة، جهز مؤسستك للخطوات التالية. تتضمن هذه الخطوات التالية مكافحة التجسس، التي على الرغم من النظر إليها في الوقت الحالي على أنها منطقة مرتفعة المخاطر في المؤسسات، إلا أن اعتقادي أننا سوف نتبنى بالفعل مبادئ معينة مرتبطة بهذه المهنة. في الواقع، تستخدم العديد من المؤسسات طرقاً مرتبطة بمكافحة التجسس، سواء على المستوى السلبي أو النشط. في 2011، أدرجنا الوصايا العشر لمكافحة التجسس في قائمة تركز على الفضاء الإلكتروني وهي:

1. كن مهاجماً
   a. لا تخف من جمع المعلومات مع إخفاء هويتك عن أعدائك. في الكثير من الأحوال يختفون عن مرأى الجميع. يجب عليك فقط أن تعرف أين تنظر.
   b. استخبارات الفضاء الإلكتروني هي أساس مكافحة التجسس في الفضاء الإلكتروني. أعرف أن أعدائك يعدون مؤسستهم للقيام بهجوم معادي على أساس الإنكار والخداع.
2. احترم مهنتك
   a. تعرف على التحليل الاستخباراتي. وغادر المنطقة الأمنية المريحة لديك.
   b. تعلم من خلال دورات التفكير الحرج. لم يفت الأوان على الإطلاق.
3. امتلك الشارع
   a. أسس لك تواجداً على نفس مواقع أعدائك.
   b. اخلق لك شخصيات عديدة عند القيام بذلك.
4. اعرف تاريخك
   a. القول المأثور "اعرف تاريخك أو التاريخ يكرر نفسه حتماً" لا تأثير له.
   b. اعرف ما الذي قام به أعدائك لكي يقرروا ما الذي ينبغي عليهم فعله.
5. لا تتجاهل التحليل
   a. التحليل لا ينبع من الخادم ولكنه يكمن في المهارات البشرية.
   b. إلى حين أن يصبح الذكاء الاصطناعي حقيقة واقعية معنا، سوف يظل العقل البشري يعمل كأفضل حل للتحليل الاستخباراتي (في حالة تدريبه بشكل احترافي).
6. لا تكن محدود أو ضيق الأفق.
   a. شارك البيانات حتى لو كنت مضطراً لذلك عبر القنوات الخلفية. نحن لا ندافع عن انتهاك قواعد الشركات من خلال مشاركة البيانات الحساسة.
   b. المقايضة مطلوبة.
7. درّب العاملين معك.
   a. افهم احتياجاتك وافهم توقيت هذه الاحتياجات واسعَ لزيادة ميزانيات التدريب.
   b. أفضل استثمار يمكنك القيام به هو في نفسك.
8. لا تنحرف عن المسار.
   a. ادفع مسيرتك برفق نحو الاجتماعات من أجل تأسيس "جولات استماع"
   b. توضيح ماهية الاستخبارات وما ليس فيها.
9. لا تبق مدة طويلة جداً
   a. التوثيق الكامل لأعمالك مع تغيير مهام الاستهداف بشكل دوري لكي تظل على دراية بأحدث المستجدات.


b. تغيير المهام من أجل معرفة جميع الجوانب الاستخباراتية

10. لا تستسلم أبداً (باردين، 2011) B2

a. الصبر والمثابرة مطلوبان.

b. أعداؤنا لا يعملون وفق نفس قواعد الاشتباك التي تعيق عملنا.

تماماً كما هو الحال مع القصور الحادث في مجال أمن المعلومات على مدار 15 سنة مضت، ما زال أمن الفضاء الإلكتروني في بداياته ويساء فهمه على نحو كبير. لدينا الكثير من المغالطات، والتعريفات غير الدقيقة والاستخدام الخاطئ للمصطلحات. يجب عدم الخلط بين مجال الاستخبارات وبين مجال الأمن ويجب ألا يشوش علينا التقارير السيئة والمنحازة. الطريقة الوحيدة لتغيير المشاكل المتأصلة في الاستخبارات في الوقت الحالي هي قيادة التغيير داخلياً مع إجبار السوق على التغير والتحول. وقد أدركت وكالة الاستخبارات المركزية هذا منذ سنوات مضت وسعت جاهدة من أجل خلق وإيجاد مجال التحليل الاستخباراتي. يمكن أن يكون إطار عمل الاستخبارات هو المعيار الأساسي للتخطيط الاستراتيجي الاستخباراتي وصناعة البرامج وينبغي أن يكون كذلك.

وهذا يأتي مع النقد البناء المتكرر من الشركات المنتجة للخدمات والمنتجات. وقد قلت دائماً أن أفضل استثمار يمكنك القيام به في حياتك هو الاستثمار في نفسك. يجب على المؤسسات أن تضع في اعتبارها القيام بنفس الشيء. تثقيف وتعليم فريق العاملين معك. وصناعة برنامجك. وقيادة التغيير من الداخل.

للإطلاع على ملخص لهذا المقال انظر الجزء الأول

جيف باردين
Treadstone 71


Agency, C. I. (2007, April 25). *Offices of the CIA*. Retrieved from Central Intelligence Agency - Training Resources: https://www.cia.gov/offices-of-cia/intelligence-analysis/training-resources.html

Bardin, J. (2011). *The Ten Commandments of Cyber Counterintelligence.* Boston: CSO Online.

Davis, J. (2007, April 21). *Sherman Kent and the Profession of Intelligence Analysis*. Retrieved from CIA Library: https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm

Gabbard, T. a. (2008). *Assessing the Tradecraft of Intelligence Analysis.* Retrieved from Rand Corporation Published Research: https://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR293.pdf

Gartner. (2013, May 13). *Threat Intelligence*. Retrieved from Gartner Definition: Threat Intelligence: https://www.gartner.com/doc/2487216/definition-threat-intelligence

Government, U. (2013, October 22). *Joint Intelligence*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

Government, U. (2013, February 21). *Office of the Director National Intelligence*. Retrieved from www.dni.gov

Hames, J. (2014, September). *Strategic Trickery: The U.S. Army's Use of Tactical Deception*. Retrieved from Soldiers - The Official U.S. Army Magazine: http://soldiers.dodlive.mil/2014/09/strategic-trickery-the-u-s-armys-use-of-tactical-deception/

Hanson, J. (2015). *The Admiralty Code - A Cognitive Tool for Self-Directed Learning.* Sydney: JM Hanson. Retrieved from www.ijlter.org/index.php/ijlter/article/download/494/234


InfoSecurity, M. (2015). *Threat Intelligence: Collecting, Analysing, Evaluating.* London: MWR InfoSecurity. Retrieved from https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf

Security, N. (2016, September 9). *Threat Intelligence Defined - 1260wp.* Retrieved from Threat Intelligence Defined - Solutionary: https://www.solutionary.com/_assets/pdf/white-papers/threat-intelligence-defined-1260wp.pdf