مركز إرنست ويونغ لخدمات مراقبة الأمن السيبراني (DSOC)

منصة مراقبة التحليلات الالكترونية الأولى في الشرق الأوسط والتي تستخدم المحاكاة والتعلم التلقائي والحائزة على جائزة عالمية.

EY

نبني عالماً أفضل للعمل

قائمة المحتويات

فوائد التحول الرقمي ومخاطره

أصبحت الشركات في وقتنا الحالي تعتمد بشكل متزايد على التقنيات الرقمية لتشغيل عملياتها لخدمة العملاء، وأصبحت التقنيات الرقمية تحقق فوائد كبيرة لمثل هذه الشركات، منها تقنية إنترنت الأشياء (IoT) أو تقنية اتصال النظم السلكية واللاسلكية بأنظمة أخرى (M2M) وتقنية التعاملات الرقمية (بلوك تشين) وإمكانية التنقل والحوسبة السحابية وتحليلات البيانات المعقدة وغيرها.

بالإضافة إلى ذلك فإن التوافق مع النظم الحالية يحظى بأولوية، لا سيّما اعتماد تقنية انترنت الأشياء الصناعية لتوفير ميزة تنافسية أو تشغيلية. وهذا التقارب في تكنولوجيا المعلومات والتقنيات التشغيلية وتقنية انترنت الأشياء يُساهم في زيادة المخاطر الأمنية. نتيجةً لذلك؛ أصبحت المراقبة الإلكترونية، التي تتصف بقدرتها على الإحساس بالمخاطر، تكتسب أهمية متزايدة وواقع وجب على المؤسسات والشركات اعتماده.

المخاطر الرقمية قد تُشكل عائقاً رئيسياً لتجربتكم

تعترف الشركات في مختلف القطاعات بأن الهجمات الالكترونية تُشكل واحدة من أبرز المخاطر الرقمية التي تواجهها في الوقت الحالي، كما أن تقنيات الأمن التقليدية لم تعد مناسبة لمواجهة مثل هذه المخاطر، لا سيّما أن الشركات تسعى إلى جعل أنظمتها ذكية وتلقائية، وهذا يُشير بشكل أساسي إلى أهمية التقارب بين النظم وجعلها أكثر ترابطاً وإلى ضرورة تبادل البيانات. وبالتالي، أصبحت أكثر عُرضةً للهجمات الإلكترونية بسبب اتساع تواجدها الرقمي بغض النظر عن الحدود الجغرافية.

استبيان إرنست ويونغ حول أمن المعلومات العالمي لعام2016

57% تعرضوا لحادثة كبيرة في مجال الأمن الالكتروني مؤخراً.

ولمواجهة هذه الحوادث، يجب على الشركات أن تكون قادرة على الابتكار وأن تُطوّر نهج الحماية الالكترونية لديها من مجرد محاولته منع التهديدات إلى قدرته على الإحساس بشكل فعّال باقتراب التهديدات والتعافي منها. وحسب توقعات شركة «Gartner» فإنه بحلول عام 2020 سيتم تخصيص60٪ من ميزانيات أمن المعلومات المؤسسية لنهج الكشف عن الهجمات والاستجابة السريعة، وهذه النسبة أكثر بـ30٪ مما كان عليه في عام 2016.

الاعتماد الكبير على التقنيات الرقمية يزيد احتمالية التعرض للهجمات الالكترونية

مركز إرنست ويونغ لخدمات مراقبة الأمن السيبراني (DSOC)

مركز إرنست ويونغ لخدمات مراقبة الأمن السيبراني (DSOC) لمواجهة التهديدات الالكترونية في المنظومة الرقمية الخاصة بكم

نظراً لأهمية تطوير وتطبيق قدرات رقابية واستشعارية على الأنظمة الالكترونية حيثما كانت؛ أطلقنا في شركة إرنست ويونغ مشروعاً لتطوير وبناء هذه القدرات كضمان يُمكّن الشركات والمؤسسات من اعتمادها.

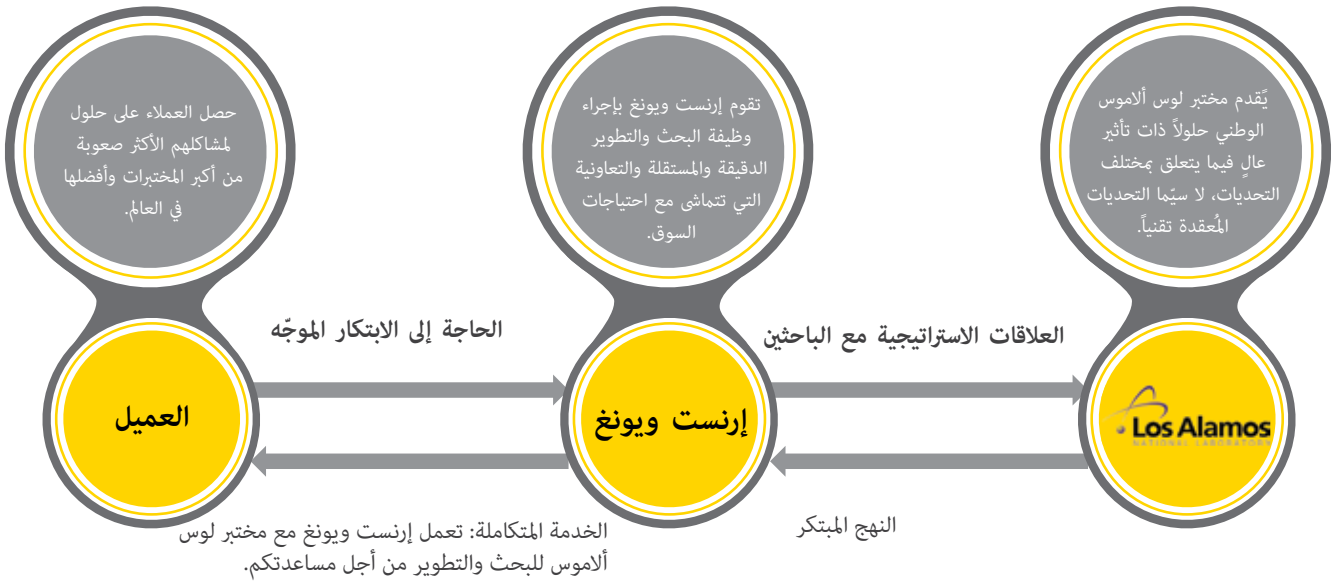
يقدم مركز إرنست ويونغ لخدمات مراقبة الأمن السيبراني (DSOC) خدمة مراقبة الأمن الإلكتروني على مدار الساعة، كما يوفر إمكانيات لمركز العمليات الأمنية التقليدية من خلال استخدام تحليلات متقدمة، إضافةً إلى قدرته على التصدي للهجمات الإلكترونية المتقدمة الناشئة عن التقنيات الرقمية الحالية والنظم الإيكولوجية الرقمية المتقاربة.

وتحقق إرنست ويونغ ذلك من خلال استخدام منصة تحليل إلكتروني حصرية قائمة على بُنية تحتية كبيرة لمعالجة البيانات.

وتساعد منصة التحليل الإلكتروني الشبكة من خلال استخدام تقنية (PathScan) التي تقوم بالكشف عن الحالات الغريبة والمُشتبه بها. وقد تم مؤخراً في مؤتمر البحث والتطوير 100 لعام 2016 منح جائزة إلى إرنست ويونغ ومختبر لوس ألاموس الوطني (LANL) لتطوير هذا الحل الرائد في العالم والذي يجمع بين مجموعات البيانات ومعالجتها في الوقت المُحدد؛ الأمر الذي يُوفر إمكانيات الكشف عن الحالات المُشتبه بها بناءً على التحليلات الحسابية والإحصائية. ولذلك مركز إرنست ويونغ لخدمات مراقبة الأمن السيبراني يُساعد في تسهيل الكشف المُسبَق عن أي اختراق من خلال مقاربة علوم البيانات مع العمليات الأمنية، وبالتالي دعم الشركات من أجل إطلاق مؤشرات مُسبقة لرصد المخاطر المحتملة.

ينفرد مركز إرنست ويونغ لخدمات مراقبة الأمن السيبراني (DSOC) بقدرته السريعة على كشف الهجمات المتقدمة في مراحلها الأولية بواسطة استخدام تقنية تحليل بيانات حاصلة على براءة اختراع تعرف بـPathScan، حيث تقوم هذه التقنية بالتعرف على المراحل الرئيسية للهجمات الإلكترونية كمرحلة الاستطلاع ومرحلة التنقل غير المسموح بين أجهزة الشبكات ومرحلة تجميع البيانات.

ويستطيع المحللون في العاملون في المركز في منطقة الشرق الأوسط وشمال أفريقيا مراقبة الهجمات الإلكترونية على نحو فعال طوال الوقت لتوفير معلومات ذات أهمية لأخذ التدابير المضادة للهجمات في وقت قياسي.



قامت إرنست ويونغ بتطوير مركز خدمات مراقبة الأمن السيبراني (DSOC) الذي يُعزّز الشراكة مع مختبر لوس ألاموس الوطني لمواجهة التحديات التالية:

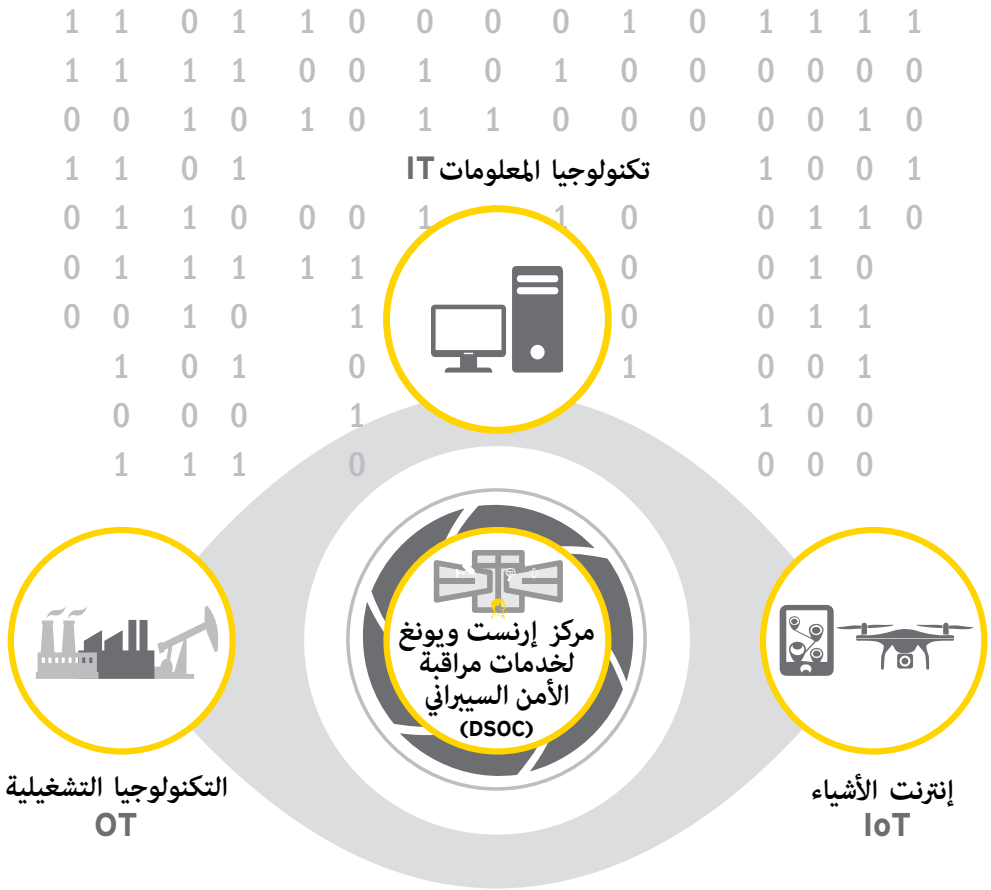
النطاق	المشكلة	الحلول التي يقدمها المركز
مراقبة الأمن	عدم وجود مراقبة مُسبَقة تركز بشكل أساسي على التهديد والمخاطر.	◄ الكشف عن التنقلات غير المصرح بها داخل الشبكة والاستطلاع وتصنيف البيانات. ◄ تغطية شاملة للمنظومة الرقمية.
	عدم تركيز فريق المراقبة الإلكترونية على كشف وتحليل التهديد.	
	عدم ضبط قواعد المراقبة بشكل كاف، مع وجود الكثير من الأنماط الخاطئة.	
	عدد التنبيهات الأمنية يفوق قدرة فرق المراقبة.	
	عدم وجود مصدر لتجميع البيانات وتمكين المراقبة الأمنية الفعّالة، بما في ذلك ارتباط الحوادث ببعضها البعض.	
	التغطية غير المُكتملة (على سبيل المثال، تتم مراقبة بعض نقاط الخروج وليس كافتها).	
الاستجابة للحادث	التعامل غير المُتسق مع الحوادث عبر المؤسسة (على سبيل المثال، تعمل بعض فرق الاستجابة للحوادث بمعزل عن الأخرى).	◄ التركيز على الاستجابة للحوادث. ◄ تزويد الفِرَق بالتحليلات البحثية لتسريع عملية الاستجابة.
	الافتقار إلى وجود الإجراءات والتدريب فيما يتعلق باتخاذ الإجراءات من قِبَل المستجيب الأول.	
	عدم تعريف اجراءات الاستجابة للحوادث.	
	سجل البيانات غير متاح لإجراء تحقيق فعّال و/ أو كامل.	
	الافتقار إلى قدرات التحليل الجنائي لإجراء تحقيق شامل وفعال.	
	الافتقار إلى خطط التواصل الخارجية ,بما في ذلك التواصل مع البائعين و العملاء و عامة الناس.	
المعلومات الاستباقية عن الأحداث والتهديدات الأمنية	وجود الكثير من البيانات غير المصنفة؛ مما يزيد من صعوبة التعرف على مؤشرات الاختراق بشكل سهل وفعال.	◄ السماح بالكشف عن التهديد و تحديد مصادر التهديد الأمني للبيئة. ◄ السماح بالكشف عن التهديد وتتبع الجهات التي تقوم بالتهديد في البيئة المُحيطة.
	عدم ترجمة مؤشرات الإختراق بما يتناسب مع طبيعة عمل المنظمة.	
	التنبيهات الواردة بشأن ظروف التهديد تنظر في التوجهات الخارجية وليس في القدرات الحالية لمواجهتها.	
	تقنيات المهاجم تتغير باستمرار على نحو ذكي سيتخطى يتخطى الإمكانات الحالية.	
	مرور فترة زمنية طويلة على المعلومات مما يُنهي صلتها بالحوادث بشكل سريع.	

القدرة على كشف المخاطر والاستجابة ومقاومة الهجمات الإلكترونية المتقدمة عبر المنظومة الرقمية الخاصة بكم

لمواجهة التحديات المستمرة بسبب اندماج هذه التقنيات واتساع رقعة واحتمالية الهجمات الالكترونية، وبدلاً من بناء مركز متكامل داخل المنشأة قد تكون تكاليف بناءه وتشغيله باهظة؛ فإن خيار التوجه الى الاشتراك بخدمات مُدارة مع مركز إرنست ويونغ الاقليمي لخدمات الأمن السيبراني سيكون الحل الأمثل والأنسب، حيث سيضمن ذلك التصميم التقني للنظام وبقاء المعلومات داخل المؤسسة وعدم نقلها إلى الخارج مع إمكانية المراقبة المستمرة واكتشاف التهديدات والاستفادة من خدمات المركز.

يـمكن للشركات تحقيق عدة فوائد عن طريق اختيار الترتيبات الداخلية الخاصة بالمركز، حيث يُمكن له أن يزيد من قدرة الشركة من خلال التكامل مع موظفي الأمن الإلكتروني الحاليين لضمان التغطية المستمرة على مدار الساعة.

وخلال عملنا في المركز قمنا بإعادة تعريف تشغيل وإدارة أمن المعلومات ليتماشى مع التوجهات الحديثة والمتطورة في الهجمات الالكترونية في العالم الرقمي. وسيقوم المركز بإعطاء القيمة القصوى لعملكم من خلال استكمال المكونات التقنية مع وجود المهام المُدارة والقابلة للتطوير من حيث «الموظفين» و«العمليات». وسوف تساعدكم خدمات المركز كذلك على تحقيق المراقبة الأمنية المكتملة في غضون بضعة أسابيع مع تغطية شاملة للمنظومة الرقمية لديكم.



مميزات العمل في مركز إرنست ويونغ لخدمات مراقبة الأمن السيبراني (DSOC):

- الكشف المسبق عن عمليات الاستطلاع المشبوهة والتنقل غير المصرح بين الشبكات و تصنيف البيانات.
- إعداد البيئة و تنصيب الأدوات في غضون ثمانية أسابيع.
- استخدام منصة التحليلات الالكترونية الرائدة عالمياً والحائزة على جائزة عالمية.
- انخفاض التكاليف وانخفاض الاحتياجات من الموارد.
- المرونة وقابلية التطوير.
- زيادة الامتثال للمتطلبات القانونية والمعايير الصناعية.
- استخدام البنية الأساسية الحديثة وأفضل أنواع التكنولوجيا.
- الوصول الى بيانات استخبارات المصادر المفتوحه والتهديدات التجارية.
- وجود مجموعة متنوعة من المهارات في المركز لضمان قيام الموظفين بعملهم وسعيهم إلى التطوير دوماً؛ مما ساهم في انخفاض معدل تبديل الموظفين أو خسارة العملاء.
- الفعالية (على مدار الساعة) وكفاءة الأداء (استجابة أسرع للمخاطر).

نموذج التسليم في مركز إرنست ويونغ لخدمات مراقبة الأمن السيبراني (DSOC)

يشتمل المركز على نظام رقمي متكامل، وذلك من خلال القدرة على الكشف والاستجابة عبر أنظمة تكنولوجيا المعلومات التقليدية وأنظمة التكنولوجيا التشغيلية الأساسية وتقنية إنترنت الأشياء، ويتألف نموذج التنفيذ من العناصر الأساسية التالية:

1

التحليلات الإلكترونية المتقدمة — يتم استكشاف الشبكة وتحديد التنقل غير المصرح بين الشبكات وتصنيف البيانات باستخدام تقنية (PathScan)، التي تقوم بالكشف عن الحالات المُشتبه بها وغير الاعتيادية، وقامت إرنست ويونغ بدمج تقنية (PathScan) ضمن خدماتها التقنية الأساسية في اكتشاف التهديدات المتقدمة.

2

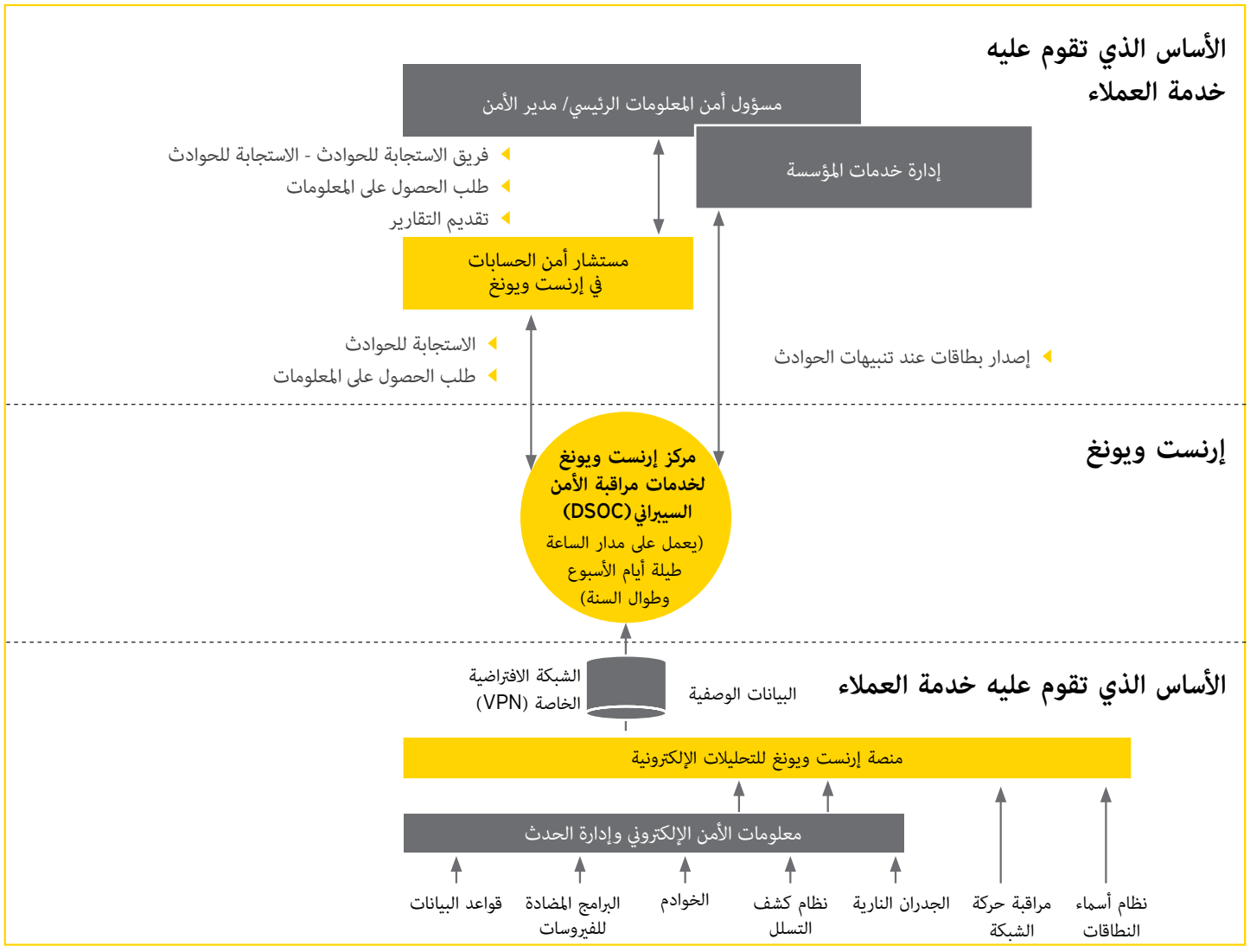
منصة التحليل — تستخدم إرنست ويونغ منصة البيانات المُعقدة «Hadoop» لجمع تحليلات «PathScan»، والتي يتم حفظها من قبل إرنست ويونغ لتوفير التكامل المُحايد بين التقنيات، وهي بيئة قابلة للتوسع بسهولة ومصممة لتناسب احتياجات العملاء المتزايدة في البيئة الخاصة بهم.

3

منصة التحقيق في التهديدات الإلكترونية وإدارة المخاطر — تُجري إرنست ويونغ، إلى جانب التحليلات الإلكترونية، المزيد من التحقيق في التهديدات من خلال فريق متخصص يعمل في المركز. ويستخدم فريق إدارة المخاطر التحليلات الإلكترونية للبحث عن الهجمات المخطط لها عن قصد وتحديد الجهات الفاعلة الخفيّة والقضاء عليها، إضافةً إلى استخدام وسائل تضليل مُصممة خصيصاً لهذا الغرض.

4

الاستجابة للحوادث الإلكترونية — يعمل في المركز محللون متخصصون ومدربون في الأمن الإلكتروني، حيث يقوموا بإجراء التحليلات الإلكترونية التي تُساهم في تحقيق المراقبة الأمنية الفعالية والفرز والاستجابة للحوادث على مدار الساعة، كما يلعب المركز دوراً كبيراً في الاستجابة للحوادث وتوفير الوقت والتكلفة والمال؛ وهو أمر في غاية الأهمية عند وقوع الحوادث الكبيرة.



مميزات عمل إرنست ويونغ في الرقابة الأمنية

مميزات عمل إرنست ويونغ في المجال الرقمي	كيف نحقق ذلك؟	القيمة
منصة إرنست ويونغ للتحليلات الإلكترونية	◀ لدى إرنست ويونغ ترتيبات فريدة من نوعها مع مختبر لوس ألاموس الوطني فيما يتعلق بتحليلات الإنترنت الرائدة في العالم. ◀ حازت هذه التقنية على جائزة عالمية في النظم الإيكولوجية، وتقوم إرنست ويونغ بتنفيذها من أجل توفير تغطية كاملة تكشف عن الهجمات الأكثر تقدماً بطريقة فعّالة من حيث التكلفة، إضافةً إلى سهولة دمجها في مختلف البيئات. ◀ تستند عملية المراقبة على متغيرات الهجوم التالية: ◀ التنقل غير المسموح بين الشبكات ◀ الكشف عن المخاطر (عن طريق المسح الأفقي والعامودي). ◀ تصنيف البيانات. ◀ تمكين الاستجابة للحوادث الكبيرة.	◀ التنبؤ المسبق عن الهجمات الإلكترونية بواسطة تقنية التعلم الذاتي من خلال التحليل الإحصائي للمعلومات والتي لا يمكن لتقنيات المراقبة الإلكترونية التقليدية القيام بها في الوقت الحالي. ◀ توظيف التعلم الآلي وعلوم البيانات الإلكترونية. ◀ سهولة الدمج والتكامل مع أنظمة مراقبة حركة الشبكات Netflow وأنظمة النطاقات DNS دون الحاجة إلى أنظمة وسيطة.
إدارة الخدمة عن طريق مستشار خدمة الحسابات في إرنست ويونغ	◀ وجود مستشار متخصص بأمن المعلومات ذا معرفة واسعة في مجال العمل ونطاق العمل الخاص بكم.	◀ تكنولوجيا متكاملة و خدمات متبادلة. ◀ عقد اجتماعات تنفيذية للتحقق من الحوادث بشكل فعّال. ◀ الإشراف على أهداف مستوى الخدمة والتعاون عند تصعيد كافة القضايا المتعلقة بالخدمة.
تسريع التشغيل	◀ وجود منصة مُجهّزة مسبقاً لتسريع التنظيم والتنفيذ. ◀ استخدام تقنيات التعلم الآلي لتفعيل وتسريع المكونات التشغيلية. ◀ توفير الحلول دون الحاجة إلى وكيل.	◀ نخفاض تكاليف نقل المشروع. ◀ الجاهزية التشغيلية. ◀ تهيئة وتنصيب الأدوات بوقت زمني قصير وبأقل تغيير ممكن للبيئة التشغيلية الحالية.
التغطية الشاملة	◀ وجود منظومة رقمية متكامل من خلال التركيز على توافق التقنيات بين كافة المصادر، مثل نظم تكنولوجيا المعلومات التقليدية ونظم التكنولوجيا التشغيلية الأساسية وإنترنت الأشياء. ◀ إجراء التحليلات البحثية باستخدام إمكانية إعادة تمثيل الهجمات.	◀ تعزيز عملية التحقيق في سلسلة الهجوم.

مميزات عمل إرنست ويونغ في المجال الرقمي	كيف نحقق ذلك؟	القيمة
التركيز على الأصول الأكثر أهمية	◀ القدرة على كشف التهديدات من خلال مراقبة الحالات الخفية والمُشتبه بها. ◀ وجود تقنية فريدة من نوعها وحائزة على براءة اختراع تم اختبارها في حماية شبكات الحكومة الأمريكية الأكثر سرية . ◀ الاستجابة المخصصة للحوادث والتي تعكس مخاطر الأعمال الفريدة من نوعها.	◀ التركيز على التهديدات الفعلية حتى لا يتم إمضاء الوقت على تحليل أحداث مشتبه بها ولكن غير صحيحة. ◀ القدرة على تتبع الهجوم لفهم المسار الذي يأخذه المهاجم والأصول التي يبحثون عنها.
وجود أساس قابل للتجديد والتطوير	◀ تثبيت واختبار قواعد البيانات المعقدة. ◀ منصة الأجهزة المحايدة. ◀ الاستعداد للتخزين الإضافي الذي يسهم في رفع كفاءة و ثبات النظام. ◀ استيعاب بيانات شاملة وكبيرة وإمكانيات تخزين على المدى الطويل.	◀ تحسين استخدام الأجهزة للعملاء الحاليين. ◀ زيادة فعالية قدرات التخزين الموجودة. ◀ تتيح أنظمة البيانات المعقدة إلى زيادة الفعالية ورفع مستوى الثقة .
وجود خبراء متخصصين في التكنولوجيا التشغيلية وإنترنت الأشياء	◀ وجود المعرفة الواسعة والفهم العميق لتقنيات وبروتوكولات التكنولوجيا التشغيلية وإنترنت الأشياء. ◀ مراكز التميز والشركات الصغيرة والمتوسطة الإقليمية في التكنولوجيا التشغيلية وإنترنت الأشياء.	◀ القدرة على اكتشاف عمليات الهجمات المخصصة في التكنولوجيا التشغيلية وتقنية إنترنت الأشياء.

مراقبة الأمن العالمي

استثمرت إرنست ويونغ في العديد من مراكز التميز في جميع أنحاء العالم، بما في ذلك:

- مراكز العمليات الأمنية.
- مراكز التميز المتخصصة في إنترنت الأشياء والتكنولوجيا التشغيلية.
- المراكز الأمنية المتقدمة.
- مراكز التحليلات الرقمية.
- المختبر الوطني «لوس ألاموس».

- تم الاعتراف بإرنست ويونغ في هذا القطاع بأنها الرائدة في مجال الفكر وأمن المعلومات في أحدث تقارير "Forrester Wave" الخاصة بالخدمات الاستشارية في مجال أمن المعلومات، كما حازت مؤخراً على أعلى الجوائز العالمية في البحث والتطوير والتحليلات الإلكترونية. ونقدم في إرنست ويونغ خدمات استشارية أمنية شاملة لعملائنا بما يتفق مع معايير الصناعة الرائدة والمبادئ التوجيهية.
- تقتصر الخدمات التي نقدمها على المعرفة فحسب؛ بل لدينا عدة أساليب ومناهج، كما لدينا قاعدة أصول كبيرة وفريق عمل يصل عدده إلى 7000 من المتخصصين في الأمن الإلكتروني العالمي، بالإضافة إلى أننا نوفر قيادة الأمن الإلكتروني على النحو الصحيح.

«نجمع بين أفضل المتخصصين في الأمن الإلكتروني العالمي لمساعدة عملائنا على نجاح أعمالهم وإيجاد الحلول المُناسبة لتحديات العصر التحويلي».

الرؤى

إن التصدي الفعّال للهجمات الإلكترونية هو السبيل الوحيد للمضي قدماً ومواجهة مجرمي الإنترنت وكسب ثقة العملاء، وتعد الرؤى المتعلقة بالأمن الإلكتروني سلسلة مستمرة من تقارير قيادة الفكر التي تركز على تكنولوجيا المعلومات والتكنولوجيا التشغيلية وإنترنت الأشياء، وغيرها من مخاطر الأعمال والعديد من التحديات والفرص ذات الصلة. وقد تم تصميم هذه المنشورات لمساعدتكم على فهم أهم المشكلات ذات الصلة ولتوفير رؤى قيّمة فيما يتعلق بوجهة نظرنا.

لمعرفة المزيد عن الجهود التي تبذلها إرنست ويونغ في تحديد المخاطر المُسبقة وإدارة التهديدات المتعلقة بالهجمات الإلكترونية، يرجى زيارة الرابط التالي: http://www.ey.com/gl/en/services/advisory/ey-cybersecurity

الأمن الإلكتروني وإنترنت الأشياء

http://www.ey.com/SOC

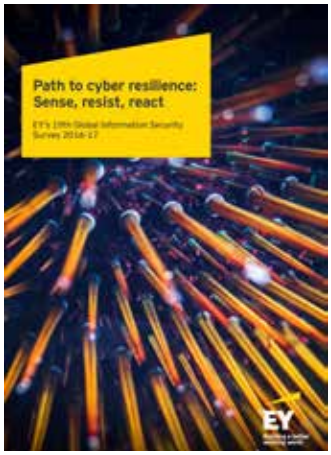
إدارة مركز العمليات الأمنية

مركز إرنست ويونغ الأمني المتقدم، وهو مركز أمني عالمي نعمل فيه من أجلكم.

http://www.ey.com/SOC

استخدام التحليلات الإلكترونية لمساعدتكم في التصدي للجريمة الإلكترونية

www.ey.com/3SOC



إعداد مخطط حول المرونة الإلكترونية ومقاومة المخاطر والاستجابة واتخاذ إجراءات بشأن ذلك.

www.ey.com/GISS

تشمل اختصاصاتنا ما يلي:

- تغطية شاملة للنظام الإيكولوجي.
- سرعة النشر – نستغرق 8 أسابيع للعمل والتنفيذ.
- الذكاء الاصطناعي الإلكتروني.
- التركيز على أهم الحالات المُشتبه بها والخارجة عن المعتاد في بيئة العمل.

إرنست ويونغ | (EY) التدقيق المالي | الاستشارات الضريبية | المعاملات التجارية | الخدمات الاستشارية

نبذة عن إرنست ويونغ (EY)

إرنست ويونغ (EY) هي شركة رائدة عالميًا في مجال التدقيق المالي والاستشارات الضريبية والمعاملات التجارية والخدمات الاستشارية، وتساعد الخدمات عالية الجودة التي نقدمها لعملائنا في شتى المجالات على زيادة الثقة في أسواق المال والمساهمة في بناء الاقتصادات حول العالم. ونحن نعمل على تطوير القادة المتميزين الذين يتعاونون معاً من أجل الوفاء بالوعود التي قطعناها لكافة مساهمينا. ومن أجل تحقيق ذلك، فقد لعبنا دوراً حاسماً في بناء عالم أفضل للعمل لموظفينا وعملائنا ومجتمعاتنا.

تُشير EY إلى المؤسسة العالمية أو إلى احدى الشركات الأعضاء في إرنست ويونغ العالمية المحدودة، حيث تعتبر كل شركة كياناً قانونياً مستقلاً، وكونها شركة بريطانية محدودة بالتضامن فإنها لا تقدم أية خدمات للعملاء. للمزيد من المعلومات حول منظمتنا يُرجى زيارة الموقع الإلكتروني :ey.com

بدأت EY العمل في منطقة الشرق الأوسط وشمال أفريقيا عام1923 ، وعلى مدى أكثر من 90 عاماً، واصلت الشركة النمو حتى وصل عدد موظفيها إلى أكثر من6,000 موظف في 20 مكتب موزعاً في 15 دولة تجمعهم قيم مشتركة والتزام ثابت بأعلى معايير الجودة. ونحن مستمرون في تطوير قادة أعمال مميزين لتقديم خدمات استثنائية لعملائنا وللمساهمة في دعم المجتمعات التي نعمل بها، كما أننا فخورين بما حققناه على مدى الأعوام الماضية؛ لنؤكد من جديد على مكانة EY الرائدة باعتبارها أكبر مؤسسة للخدمات المهنية المتخصصة والأكثر رسوخاً في المنطقة.

EYG no. 05953-172GBL
ED None

ey.com/mena

جهات الاتصال فيمركز إرنست ويونغ لخدمات مراقبة الأمن السيبراني(DSOC)

كلينتون فيرث

رئيس قسم الأمن الإلكتروني، منطقة الشرق الأوسط وشمال افريقيا

clinton.firth@ae.ey.com
+971 50 213 7094

رداد أيوب

شريك مسؤول، إرنست ويونغ

البريد الإلكتروني
raddad.ayoub@ae.ey.com
+966 59 447 8654

جهات الاتصال الإقليمية

المملكة العربية السعودية غلين توماس

غلين توماس
glen.thomas@ae.ey.com
+966 59 447 8654

الإمارات العربية المتحدة

سام فوروتاني
sam.foroutani@ae.ey.com
+971 50 625 2263

قطر

عمر شيرن
omar.sherin@qa.ey.com
+974 666 10746

سلطنة عُمان

محمد نياز
mohamed.nayaz@om.ey.com
+968 99429679

مصر

أكرم رضا
akram.reda@eg.ey.com
+202 272 60260

الكويت/ البحرين

سوراب شارما
sourabh.sharma@kw.ey.com
+965 9400 2430

الأردن/ لبنان

سلام شومان
salam.shouman@jo.ey.com
+962 6 580 0777