UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

القدرات الأساسية لمركز العمليات الأمنية

الإصدار 3.0

مايو 2023

تنبيه

اعتُمدت هذه الوثيقة ووافق مجلس الوزراء في دولة الإمارات العربية المتحدة عليها، وهي ملكية حصرية وخاصة للمجلس الأمن السيبراني.

ويحتفظ مجلس الأمن السيبراني بحقه في تعديل، أو إضافة، أو حذف أي بند أو قسم من هذه السياسة.

لا يُمكن استخدام هذه الوثيقة أو أي جزءٍ منها دون الحصول على الموافقة الخطية المسبقة من مجلس الأمن السيبراني.

ضوابط الإصدار

الإصدار	0.1
التاريخ:	11 مايو 2022
جهة الإعداد:	مجلس الأمن السيبراني
التعديل:	وثيقة المسودة الأولية

الإصدار	0.2
التاريخ:	...
جهة الإعداد:	...
التعديل:	...

الإصدار	0.3
التاريخ:	...
جهة الإعداد:	...
التعديل:	...

	جهة المراجعة	جهة الموافقة
المسمى الوظيفي:	xxxxxxxxx	xxxxxxxxx
الاسم:	xxxxxxxxx	xxxxxxxxx
التوقيع:	xxxxxxxxx	xxxxxxxxx
التاريخ:	xxxxxxxxx	xxxxxxxxx

جدول المحتويات

جدول المحتويات

1

القسم

المقدّمة

المقدّمة

استناداً لظهور التهديدات سريعة التطوّر، بالإضافة إلى العدد الهائل من التقنيات الجديدة والممارسات التجارية تسعى المؤسسات إلى الرفع من مستوى قدراتها ومهاراتها، مع ضمان التحديث المستمر لقدراتها في كشف التهديدات ذات الصلة، والتعزيز المستمر لتلك القدرات على الاستجابة لمثل هذه التهديدات. ويُعد مركز العمليات الأمنية عنصراً أساسياً ومحورياً لتحقيق هذه القدرات، حيث يعمل المركز على تنبيه المعنيين بالحوادث والأحداث الأمنية المهمة، كما يعمل على تفعيل مفاهيم المركزية من خلال إيجاد وحدة متخصّصة لإطلاق التنبيهات، ويوفّر القدرة على تنسيق الاستجابة لجميع الأحداث الناشئة، وبذلك، يساهم المركز في الحد من أثر الحوادث السيبرانية.

وتمتلك مراكز العمليات الأمنية الحديثة مجموعة واسعة من تقنيات منع الهجمات، واكتشافها والاستجابة لها، بالإضافة إلى قدرات رفع التقارير بالمعلومات الاستخبارية السيبرانية، وقدرة الوصول إلى مجموعة متنامية من الموارد البشرية المتخصّصة ذات الكفاءة العالية والمثبتة في المجالات السيبرانية. ولذلك فمن الضروري بمكان أن تحدّد القدرات الأساسية لمراكز العمليات الأمنية وتوضع ضمن البنية التحتية للمعلومات الحيوية، بالإضافة إلى وضع مستهدفات الجاهزية التي تساهم في تطوير التكنولوجيا، والأدوات، وتدعم الأفراد المعنيين والعمليات المتبعة.

وضمن سياق بناء قدرات المراقبة الوطنية، فيمن المُتوقع أن تتماشى مهام مراكز العمليات الأمنية مع الجهات المتخصّصة في البنية التحتية للمعلومات الحيوية وأن تعمل على دعم وتعزيز الوعي بأهميتها من خلال تفعيل تصنيف معتمد للأحداث والحوادث الأمنية، وتوحيد مجهودات الاستجابة للحوادث والهجمات السيبرانية على المستوى الوطني.

أسس مجلس الأمن السيبراني هذه القدرات الأساسية لغاية تحديد الحد الأدنى لمتطلبات البنية التحتية للمعلومات الحيوية الخاصة بمراكز العمليات الأمنية، ووضع مستهدفات الجاهزية لتعزيز المرونة والقدرات السيبرانية الوطنية. وتعزز هذه المبادرة من مكانة الدولة وريادتها على مستوى العالم في المجال ذاته، كما تعمل أيضاً على تحسين الوضع الأمني للمؤسسات والأفراد داخل الدولة.

1.1 الهدف

يتمثّل الغرض من هذه الوثيقة في توضيح المنهجية المتّبعة لقياس نسبة جاهزية وقدرات مركز العمليات الأمنية للبنية التحتية للمعلومات الحيوية، من خلال توفير الجاهزية للحد الأدنى من القدرات ضمن قطاعات البنية التحتية للمعلومات الحيوية. وهو ما يضع خارطة الطريق المتعلقة بتطوير وتحسين مراكز العمليات الأمنية عبر جميع البنى التحتية الحيوية في الدولة.

وفي الوقت الذي ستحتاج فيه كل مؤسسة وكل قطاع إلى تخصيص الدرجة الخاصة بهم من مستوى جاهزية مركز العمليات الأمنية، وهو ما يأخذ بعين الاعتبار مستوى تحملهم للمخاطر السيبرانية، والحد الأدنى من القدرات الأساسية، وكما هو موضّح في هذه الوثيقة، جميع ما سبق سيساهم في تحسين القدرة والمرونة السيبرانية الوطنية.

1.2 النطاق ومدى قابلية التطبيق

توفّر هذه الوثيقة الحد الأدنى الإلزامي من مستوى جاهزية مراكز العمليات الأمنية عبر كل قطاع من قطاعات البنى التحتية للمعلومات الحيوية. كما ستوضّح أيضاً القدرات الأمنية الواجب توفيرها وتضمينها في البيئة الخاضعة للمراقبة، والتي يجب اعتمادها عبر جميع البنى التحتية للمعلومات الحيوية في الدولة.

ويحدّد إطار العمل أيضاً إرشادات تطبيق القدرات والتدابير الأمنية لمركز العمليات الأمنية، ويُمكن استخدامه في تقييم مدى الامتثال لدى المؤسسات الفردية للمتطلبات. وبينما تحدّد هذه الوثيقة وتوضّح اللمتطلبات والإرشادات عبر العناصر المختلفة لقدرات مركز العمليات الأمنية، ومستوى الجاهزية، فإنها تفعل ذلك بطريقة حيادية من الناحية التكنولوجية.

تُعد هذه الوثيقة قابلة للتطبيق على جميع الجهات المتخصّصة في البنية التحتية للمعلومات الحيوية، والتي تُحدّد ضمن هذه الفئة في سياسة البنى التحتية للمعلومات الحيوية، كما أنها قابلة للتطبيق على مقدّمي الخدمات المُدارة الذين يقدّمون خدمات مراكز العمليات الأمنية للبنى التحتية للمعلومات الحيوية في الدولة.

2

القسم

تعريف الأثر

2.1 حدث مهم مقابل حادث

يعرّف الحادث على أنه انقطاع (أو انخفاض في مستوى الجودة) غير مخطط له يحدث لخدمات تكنولوجيا المعلومات، بينما يُمكن تفسير الحدث على أنه أي واقعة يُمكن اكتشافها أو تمييزها وتكون ذات أهمية في إدارة البنية التحتية لتكنولوجيا المعلومات أو تقديم خدمة تكنولوجيا المعلومات، إلّا أنه لا ترتقي هذه التعريفات إلى مستوى التعريف الدقيق للأحداث والحوادث الأمنية، حيث أن المراحل الأولى لعملية التعطل لا تحمل أي أثرٍ جوهري، إلّا أنها تكون أكثر أهمية من مجرد حدث أمني بسيط. وبناءً على ما تقدّم، فقد اعتمدنا التعريفات الثلاثة التالية:

- **الحدث الأمني**: أي حدث ملموس ذي علاقة بأمن المعلومات، مثال: مستخدم يدخل إلى النظام باستخدام بروتوكول النقل الآمن (SSH).
- **الحدث الأمني المهم**: حدث أمني ذو أهمية محدّدة لمركز العمليات الأمنية، حيث أنه يحمل تبعات ذات طابع تهديد أمني ضمن المنظومة أو البيئة مثال تسجيل دخول مستخدم إلى خادم عبر برتوكولا النقل الآمن (SSH)
- **مثال**: حظر أحد حلول مكافحة الفيروسات لأحد البرامج الضارة التي جرى تنزيلها مؤخراً.
- **الحادث الأمني: حدث أمني ذو أهمية عالية**، حيث أنه إما أن يؤدي بصورة مباشرة إلى إحداث خطر أمني، أو أنه ينطوي عليه حدوث هذا الخطر الأمني المباشر، ويكون له أثرٌ على المؤسسة، أو أصولها، أو على معلوماتها.

مثال: برمجية فدية أو الابتزاز تتكاثر بشكل متسارع ضمن بيئة أو منظومة ما.

والفارق الأساسي هنا هو الأثر المترتب. فالأثر هو ما يميّز بين الأحداث التي وإن كانت خبيثة فهي قد لا تكون ذات أثر على عمليات وأعمال المؤسسة، وبين الحوادث التي تفرض التعطيلات المكلفة مادياً والتي تستهلك الكثير من الوقت الثمين أيضاً، والتي تُعد ذات أهمية عالية جداً وتوجِد الحاجة للتحري عنها بالشكل المناسب والخروج بحلول ناجحة للتعامل معها. فعلى سبيل المثال: يجب التخلص من البرمجيات الخبيثة (الباب الخلفي) إن وجدت على النظام، ولكن إذا لم تنجح عملية إزالتها، وإذا لم تنجح هذه البرمجية الخبيثة في الاتصال بخادم الأوامر والتحكّم (C&C)، فهل تعتبر في الواقع بأنها حادث أمني، أم حالة بسيطة تتعلق بتطبيق الممارسات الجيدة للحفاظ على الأمن السيبراني (cyber hygiene)؟ وفي الوقت الذي يطرح فيه هذا السؤال مستوى أهمية الأصول أو مدى حساسيتها، إلّا أنه وفي معظم الحالات يصنّف هذا الموقف على أنه حدث أمني مهم.

2.2 التعريف الرسمي للأثر

يعرَّف الأثر على أنه أي ضرر أو خطر على السرّية، أو مدى توفّر، أو سلامة المعلومات، والأصول، والعمليات.

ومع ذلك، فقد تم التوسع في التعريف ضمن مراكز العمليات الأمنية الحديثة، ولما تجاوز نموذج السرّية، ومدى التوفّر، والسلامة أو ما يدعى (CIA Triad). حيث يُعد الحفاظ على السيطرة والسلامة من الضرورات الرئيسية في البيئات التي توجد فيها أنظمة التحكّم الصناعية (ICS)، أو التكنولوجيا التشغيلية (OT)، أو إنترنت الأشياء (IoT)، كما يؤدي دوراً مهماً، ويتطلب المستوى نفسه من الاهتمام.

يُعد وضع الأولويات للتعامل مع الحوادث جزءاً مهماً من مرحلة التصنيف الأولية لمركز العمليات الأمنية، حيث أنه يحدّد مستوى الاستجابة، ومستوى التنسيق، ومدى تكرار إطلاق التنبيهات للمعنيين ذوي العلاقة أثناء وقوع الحادث. ومع التفريق بين الحدث المهم والحادث، بناءً على الأثر المحتمل، يتحتم علينا استخدام عامل الأثر بصورة أساسية لتقييم مستوى الأولوية. ومع الوضع في عين الاعتبار أن هذا الأسلوب يتيح إقصاء معيار منفصل، ألا وهو مستوى الخطورة، والذي يشكّل عادةً مقياساً تقديرياً مصاحباً لنوع التهديد. وللتأكيد على ما سبق، فإن طبيعة التهديد ليست ذات صلة مقارنة بأثره المحتمل. وسيسمح لنا هذا النهج بإسقاط أي مصفوفة أولوية أو خطورة تضيف القليل من القيمة لإدارة الحادث. وبدلاً من ذلك، سيكون العامل الحاسم في هذه المعادلة هو مدى اقتراب منفذ الهجمات من تحقيق هدفه في إحداث الأثر على المؤسسة.

2.2 التعريف الرسمي للأثر

وُضعت الأولويات التالية ضمن الخطوات الواردة في إطار عمل MITRE ATT&CK. وتتيح عملية وضع الخطوات هنا المجال أمام تحقيق التكامل مع إطار عمل حالات الاستخدام الهرمي، حيث يتم توجيه التنبيهات الصادرة عن نظام إدارة المعلومات والحوادث الأمنية أو نظام الكشف والاستجابة الممتدة إلى المحلل وفقاً للأولويات التالية:

الأولوية	إطار عمل MITRE ATT&CK
الحوادث المهمة: المستوى الابتدائي والهجمات غير الناجحة	الاستطلاع، والوصول الأولي، وتطوير الموارد
الأولوية الثالثة: المرحلة المبكرة	الأوامر والتحكّم، والتنفيذ، والاستمرارية، وتجنب الإجراءات الدفاعية
الأولوية الثانية: المرحلة المتوسطة	تصعيد الامتيازات، والبرمجيات الخبيثة، والوصول إلى المعرفات، والاستكشاف
الأولوية الأولى: المرحلة المتأخرة والأصول الحيوية	الجمع، والأثر، والنقل غير المصرّح ملاحظة: يجب في هذه المرحلة البدء بإطلاق تنبيهات بخصوص الأصول التي تعتبر حساسة
الأولوية القصوى: الهجمات الناجحة	غير مُحدّدة ملاحظة: خُصّصت هذه الأولوية للحوادث التي تُكتشف بعد وقوعها، ومثال عليها عمليات الاختراق، بالإضافة إلى الحوادث التي يكون الأثر التراكمي فيها مرتفعاً من حيث النوع، وبحيث يفرض إيلاء أكبر قدر من الاهتمام.

3

القسم

الجاهزية والقدرات والمنهجية المتبعة

يستقي إطار العمل هذا إلى حدٍ كبير من إطار عمل نموذج جاهزية القدرات لمركز العمليات الأمنية SOC-CMM، والذي بدوره يمثل نموذج تكامل جاهزية القدرات CMMI. وعملت جامعة كارنيغي ميلون على وضع نموذج تكامل جاهزية القدرات، حيث يهدف إلى تحسين العمليات عبر جميع مراحل المشاريع، والأقسام، والمؤسسة بأكملها. ويعرِّف هذا النموذج مستويات الجاهزية التي يُمكن استخدامها لتقييم العمليات، كما يعمل على الاستفادة منها للتحسين من تلك العمليات. استخدام نموذج جاهزية القدرات لمركز العمليات الأمنية الذي طوره "روب فان أوس" على نحوٍ واسع من قبل القطاع المصرفي الهولندي، ومن ثم جرى التوسع في مفاهيمه لتصل إلى مركز العمليات الأمنية.

3.1 الجاهزية

تمثّل الجاهزية خبرة ملموسة، كما وتشكّل نهجاً قابلاً للتوقع وإعادة الإنتاج، والتطبيق عبر العديد من العمليات المختلفة والمتطلبات ذات العلاقة بعمليات مركز العمليات الأمنية. وهناك عاملان أساسيان لتحقيق الجاهزية وهما: التوثيق، ومن ثم اعتماد ذلك التوثيق ضمن ثقافة المؤسسة. تعتمد أطر نموذج تكامل جاهزية القدرات على ثبات مجموعة الإنجازات، والتي توفّر منظوراً عن التقدّم العام نحو الجاهزية. ونظراً لصعوبة تقييم الثقافة، تركّز أطر العمل على جانب **التوثيق**.

المستوى	الاسم	الوصف
0	**غير موجودة**	في هذا المستوى، يتعلق الجانب بوقت الحاجة إلى حدٍ كبير، أو أنه غير مكتمل. ولذلك، فمن غير المؤكد تنفيذ عملية التنفيذ.
1	**أولية**	يُنفّذ الجانب في وقت الحاجة.
2	**مُدارة**	يوثّق الجانب ويُنفّذ بطريقة مستمرة
3	**محدّدة**	يُدار الجانب باستخدام الملاحظات الواجب إبدائها في وقت الحاجة بخصوص الجودة والجداول الزمنية للمُخرجات، وتعنى هذه الخطوة تحديداً بالتحسين المستمر. ويُعاد النظر بالوثيقة مرة واحدة في السنة على الأقل، مع وجود النية في الحفاظ على دقتها، وتنفيذ التحسينات اللازمة عليها.
4	**مُدارة كمياً**	يُقاس هذا الجانب بأسلوب منهجي من حيث الجودة، والكمية، والجداول الزمنية للمُخرجات. وكما هو الحال في المستوى الثالث، يُعاد النظر في الوثيقة مرة واحدة على الأقل في السنة، إلّا أن الاختلاف هنا يكمن في السبب الذي يدفع بالحاجة إلى تنفيذ عملية التغيير، وتُعد الآن بأنها مدفوعة من خلال المقاييس ومؤشرات الأداء الرئيسية.
5	**التحسين**	يجري تعزيز هذا الجانب وتحسينه باستمرار. كما يتم البحث باستمرار وفاعلية عن فرص لتحسينه ومراقبته. وتجري عملية مراجعة الأداء شهرياً، أو أسبوعياً، أو أكثر، وتنفّذ التغييرات ليس فقط بحسب الحاجة، بل كمحاولة لاختبار طرق جديدة لتحقيق الكفاءة.

3.2 القدرات

تمثّل القدرات عملية تفعيل للإرادة. وفي مركز العمليات الأمنية، يترجم هذا التعريف على أنه القدرة على الاتصال، والتنسيق، والمنع، وعلى الاكتشاف، والتحليل، والاحتواء، والتصحيح أو الإصلاح. ويستثمر مركز العمليات الأمنية العديد من التقنيات، والمنهجيات، والخبرات، والعمليات لتحقيق هذه الأهداف.

وكما هو الحال في الجاهزية، تصنّف القدرات اعتماداً على مستوى ثبات مجموعة الإنجازات، والتي توفّر منظوراً عن التقدّم العام نحو تحقيق الحد الأقصى من القدرات المرغوبة. ونظراً لصعوبة تقييم المنهجية، تركّز أطر العمل بصورة أساسية على الجانب **التكنولوجي**.

المستوى	الاسم	الوصف
0	**غير مكتملة**	في هذه المرحلة، يُعد الجانب غير مكتمل. ولذلك، لا يمتلك مركز العمليات الأمنية القدرات الكافية على تنفيذ هذا الجانب.
1	**منجزة**	توجد قدرات كافية لتنفيذ هذا الجانب ضمن المستوى الأساسي. وفي هذا المستوى، فأنت تمتلك القدرات إلى حدٍ ما، وهي قابلة للتطبيق ضمن المجالات التي تحتاجها.
2	**مُدارة**	تُنفّذ القدرات لهذا الجانب باستمرار. وقد وصلت القدرات إلى مستوى التغطية الكاملة، كما أن جودة القدرات تُعد ضمن المستوى الجيد.
3	**محدّدة**	وصلت القدرات ضمن هذا الجانب إلى مستويات عالية، وموثّقة على نحوٍ جيد، وهي تقدّم قيمة حقيقية. كما أن هذه القدرات ذات جودة جيدة، وتخضع للتحسين المستمر (أسبوعياً، أو شهرياً، أو غير ذلك) بناءً على المقاييس المعتمدة.

3.3 منهجية التقييم

يوفّر إطار العمل هذا أداة يُمكن استخدامها لتقييم التحسين المستقبلي والتخطيط لتنفيذه، كما يوفّر خارطة طريق فعّالة لجميع الوثائق التي توجد الحاجة لإنشائها، والموافقة عليها، وتحديثها، وتُعد هذه المنهجية أساسية من بين جميع القدرات التي يحتاج مركز العمليات الأمنية إلى امتلاكها، وذلك ليصل إلى وضع نفسه ضمن أفضل المراكز والمستويات العالمية.

وبصورة أساسية، يُمكن استخدام هذه الوثيقة والأدوات المصاحبة لها لتنفيذ التقييم لمراكز العمليات الأمنية الموجودة، وللمساعدة في التعرّف على المجالات التي تحتاج إلى المزيد من التطوير فيها لتحقيق الأهداف المرجوة والمتوقعة من المؤسسة. ويتطلب تنفيذ التقييم جمع النسخ من جميع الوثائق التي تحتوي على إثبات لمستوى جاهزية أو قدرات كل بند من البنود الخاضعة للتقييم.

وبالنسبة للقدرات، فإن عملية التقييم ستحتاج في العادة إلى توفير نظرة عامة أو استخراج الإعدادات المصاحبة للتكنولوجيا. ويجب أن تثبت هذه الإعدادات أن القدرات ليست متوفّرة أو موجودة فحسب، بل أنها مطبّقة لتحقيق المستوى المطلوب من التغطية.

4

القسم
مستهدفات القطاع

يُتوقع أن تلبي القطاعات الحيوية المتطلبات الإلزامية التي تُحدّد في الوثائق خلال مدة ثلاث سنوات من بدء تطبيق هذه القدرات الأساسية.

وتحتسب المستهدفات باعتبارها المتوسط (المعدل) للجاهزية والقدرات عبر جميع مراكز العمليات الأمنية القابلة للتطبيق.

القطاع	المعايير	الهدف الإلزامي	الهدف المُوصى به
الطاقة	الجاهزية	4	5
	القدرات	2	3
النقل	الجاهزية	3	4
	القدرات	2	2
القطاع المالي	الجاهزية	3	4
	القدرات	2	2
الصحة	الجاهزية	3	4
	القدرات	2	2
المياه والكهرباء	الجاهزية	4	5
	القدرات	2	3
البنية التحتية الرقمية	الجاهزية	3	4
	القدرات	2	2
الخدمات الحكومية	الجاهزية	3	4
	القدرات	2	2
الدفاع	الجاهزية	4	5
	القدرات	2	3
التعليم	الجاهزية	3	4
	القدرات	2	2
الفضاء	الجاهزية	3	4
	القدرات	2	2
الصناعات الغذائية	الجاهزية	3	4
	القدرات	2	2

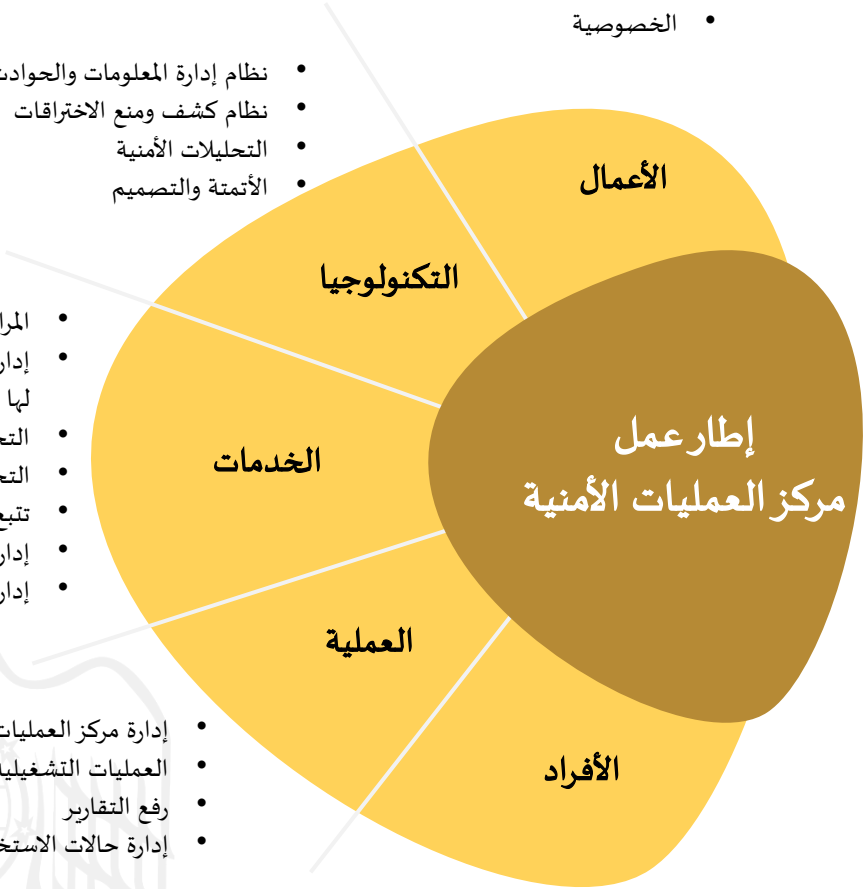
القسم 5

إطار عمل مركز العمليات الأمنية

يعتمد إطار مركز العمليات الأمنية بصورة أساسية على التوثيق. ويُمكن النظر إلى كل قسم من الأقسام التالية على أنه وثيقة منفصلة، مع إيجاد ضوابط الإصدار، وتوقيع الجهة المعنية لتحقيق الاعتماد الرسمي. ومن المقبول تماماً أن تُجمع العديد من هذه الأقسام ضمن وثيقة واحدة، عندما تقتضي الحاجة ذلك. وتجدر الإشارة هنا أنه بينما يجب أن يعتمد المدققون على المعاملات الورقية لتقديم دليل على وجودها، فإن الجوانب التي تُقاس هنا يجب أن تكون حقيقية، وأن تشكّل جزءاً من المهام اليومية لمركز العمليات الأمنية.

- محفزات الأعمال
- العملاء
- الميثاق
- الحوكمة
- الخصوصية

- نظام إدارة المعلومات والحوادث الأمنية/ نظام الكشف والاستجابة الممتدة
- نظام كشف ومنع الاختراقات
- التحليلات الأمنية
- الأتمتة والتصميم



- المراقبة الأمنية
- إدارة المعلومات والحوادث الأمنية والاستجابة لها
- التحقيقات الأمنية الجنائية
- التحليل الذكي للمخاطر
- تتبع التهديدات
- إدارة الثغرات الأمنية
- إدارة السجلات

- إدارة مركز العمليات الأمنية
- العمليات التشغيلية والمنشآت
- رفع التقارير
- إدارة حالات الاستخدام

- الموظف
- الأدوار والهيكلية
- إدارة الأفراد
- إدارة المعرفة
- التدريب والتعليم

5.1 الأعمال

تمثّل مركز العمليات الأمنية مؤسسة في أساس عملها، وتوجد في صميم كل مؤسسة مجموعة من الوثائق التي تحدّدها وتعمل على تعريفها. وعملية إدارة العمل ما هي إلّا عبارة عن تنفيذ عمليات التنسيق والتنظيم لنشاطات العمل، وذلك لتحقيق الأهداف المنصوص عليها لهذا العمل. وفي الوقت الذي قد تكون فيه الأهداف بديهية عند النظر إلى القطاع الأمني، إلّا أن الأسباب الحقيقية وراء تخصيص مراكز العمليات الأمنية وبرامج الأمن السيبراني لتخدم قطاعات محدّدة يرجع إلى التركيز المحدّد الذي تتطلبه هذه القطاعات.

5.1.1 محفزات الأعمال

الهدف

تحديد الأنشطة الرئيسية، والمُدخلات، والضرورات التي تحفز المتطلبات التشغيلية لمركز العمليات الأمنية، وتوثيق محفزات الأعمال المحدّدة على هذا النحو وضمان ملاءمتها المستمرة.

التوجيه

تتمثّل الخطوة الأولى في تحديد النشاطات، والمُدخلات والضرورات الأساسية التي تحفز المُخرجات التشغيلية لمركز العمليات الأمنية، وتسجيلها ضمن وثيقة مخصّصة. ويُمكن أن تمتلك مؤسستك العديد من محفزات الأعمال، كما يُمكن لهذه المحفزات أن تتغير أو أن تنمو وتتطوّر مع مرور الوقت. وفيما يلي قائمة غير شاملة، يجب تحديدها جنباً إلى جنب مع المعنيين من قطاع الأعمال.

رقم محفز الأعمال	محفزات الأعمال
المحفز الأول	الحفاظ على قدرة الوصول إلى المعلومات
المحفز الثاني	الحفاظ على سرّية المعلومات
المحفز الثالث	الحفاظ على سلامة المعلومات
المحفز الرابع	الحفاظ على التحكّم في العمليات التشغيلية
المحفز الخامس	الحفاظ على أمن المستخدمين
المحفز السادس	الحفاظ على خصوصية المستخدمين
المحفز السابع	المساهمة في الحفاظ على مرتبة دولة الإمارات العربية المتحدة عالمياً بالنسبة للوضع العام للأمن السيبراني.
المحفز الثامن	بناء المرونة والقدرة على مواجهة منفذي الهجمات الغريبة.
...	...

يجب دائما المواءمة والتوفيق بين محفزات الأعمال الموثقة وبين الاستراتيجية المؤسسية وأهدافها، كما يجب تحديث كتيب خدمات مركز العمليات الأمنية بما يتماشى مع محفزات الأعمال.

5.1 الأعمال

5.1.2 العملاء

الهدف

تحديد عملاء مركز العمليات الأمنية، وتحديد احتياجاتهم وتوقعاتهم، والتوثيق الرسمي لاتفاقيات مستوى الخدمات.

التوجيه

يتعامل مركز العمليات الأمنية عادة مع أكثر من جهة معنية واحدة، لذا فمن المهم تحديد عملاء مركز العمليات الامنية رسمياً، وتوثيق العلاقات معهم. كما يجب مواءمة هذا التوثيق الرسمي مع التزامات العملاء، ومُدخلاتهم، ومُخرجاتهم، ويجب توثيق اتفاقية مستوى الخدمات، وتحديد نقاط الاتصال لديهم.

وعادة، تتضمن مجموعة العلاقات مع مركز العمليات الأمنية ما يلي على سبيل المثال لا الحصر:

- الأعمال
- العملاء الخارجيون
- الإدارة العليا
- مركز العمليات الأمنية المحلي
- مركز العمليات الأمنية الوطني
- الشؤون القانونية
- الموارد البشرية
- التدقيق
- أمن العمليات التشغيلية
- الهندسة / البحث والتطوير
- تكنولوجيا المعلومات

يجب تحديد عملية التواصل مع العميل، ويجب أن تخضع هذه العمليات على أقل تقدير لتحديثات دورية بخصوص مراقبة مستوى الخدمات، بالإضافة إلى قياس ومراقبة مدى رضا العميل.

5.1 الأعمال

5.1.3 الميثاق

الهدف

توثيق الميثاق الرسمي لمركز العمليات الأمنية والذي يوضّح صلاحياته ومهمته الأساسية.

التوجيه

يستقي مركز العمليات الأمنية صلاحياته من الميثاق، والذي يوضّح تفويضه الرسمي ويبيّن مهمته الأساسية في نفس الوقت. ويحدّد الميثاق مسؤوليات المركز، ويبيّن الصلاحيات المسندة إليه بهدف السعي في تنفيذ هذه المهام.

ومن المهم جداً أن تُحدّث هذه الوثيقة دورياً، وأن تتضمن توقيع جميع الأطراف المعنية وموافقتهم على منح المركز الصلاحيات الموكلة إليه.

ويتضمن الميثاق البنود والأقسام التالية:

- الرسالة: يجب توضيح مهمة مركز العمليات الأمنية لتوفّر نظرة شمولية حول أسباب تأسيس هذا المركز
- الرؤية: يصف هذا القسم الأهداف بعيدة المدى لمركز العمليات الأمنية
- الاستراتيجية: يجب وضع استراتيجية لتوضيح كيفية تحقيق الأهداف والمستهدفات التي توضّحها الرسالة والرؤية
- نطاق الخدمات: يُوثّق نطاق الخدمات لتوفير نظرة شمولية على الخدمات التي يقدّمها مركز العمليات الأمنية
- المُخرجات: المُخرجات التي يقدّمها مركز العمليات الأمنية، على سبيل المثال: التقارير، والحوادث، والتحريات، والاستشارات، وغير ذلك
- المسؤوليات: قائمة بالأنشطة التي يتولى مركز العمليات الأمنية المسؤولية عن تنفيذها
- المساءلة: قائمة بالأنشطة التي يكون مركز العمليات الأمنية مسائلاً ومحاسباً عن تنفيذها
- ساعات العمل: ساعات العمل لمركز العمليات الأمنية والخدمات التي يقدّمها
- الجهات المعنية: قائمة بالمؤسسات، والأدوار، والأفراد التي يتبع لها مركز العمليات الأمنية، والتي يستقي منها رسالته ورؤيته
- الغايات والأهداف: يجب أن تكون الغايات والأهداف واضحة وراسخة، وأن تكون قابلة للقياس بهدف استخدامها لغايات رفع التقارير.
- بيان النجاح: يستخدم بيان النجاح لتحديد مدى نجاح مركز العمليات الأمنية، ويجب أن يكون البيان متسقاً مع الغايات والأهداف.
- التواقيع: تواقيع الجهات المعنية.

5.1 الأعمال

5.1.4 الحكومة

الهدف

توثيق نموذج الحوكمة المعتمد لدى مركز العمليات الأمنية، وبما يتضمن التفاعلات العامة، والتقييم، والمراقبة لتكليفاته، ورفده بالموارد اللازمة لتنفيذ مهمته بكفاءة عالية.

التوجيه

يجب توثيق الاستراتيجية لمركز العمليات الأمنية، حيث تعنى الحوكمة بالتعامل بالمستوى العالي لمركز العمليات الأمنية، وخططه الموضوعة على المدى البعيد. وإلى جانب المهمة المنوط بتنفيذها، فمن المطلوب أن يعزز مركز العمليات الأمنية من كفاءة أداءه، كما يجب أن يحدّد المعايير الأساسية لرفع التقارير، وهيكلية التبعية الإدارية والعملية. وسيؤثر مدى التحكّم في الحوكمة على المستوى الاتحادي على المُخرجات، والمُدخلات والعمليات المنفذة داخل مركز العمليات الأمنية.

يجب تحديد العناصر التالية ويجب مراجعتها باستمرار:

- نطاق التحكّم
- المواءمة مع الجهات الوطنية، والمحلية، والإقليمية
- مؤشرات الأداء الرئيسية لمركز العمليات الأمنية
- التدقيق الخارجي والتقييم لمركز العمليات الأمنية
- المساءلة
- الرعاية
- المهمة
- التعامل مع المورّدين أو الجهات الخارجية
- إدارة البرامج
- عملية التطوير المستمر

وتُعد الميزانية وتوفير الموارد عوامل أخرى تؤخذ بعين الاعتبار، حيث يجب تطبيق الإجراءات المناسبة لإدارة التكاليف في مركز العمليات الأمنية، وبما يتضمن وضع الميزانية، ونشاطات المراقبة عبر العناصر التالية:

- توقعات الميزانية
- توافق الميزانية
- العائد على الاستثمار
- تكاليف الأفراد
- تكاليف العمليات
- تكاليف التكنولوجيا
- تكاليف الخدمات

5.1 الأعمال

5.1.5 الخصوصية

الهدف

توضيح سياسة الخصوصية لمركز العمليات الأمنية فيما يتعلق بالمراقبة الأمنية للعملاء والموظفين، وبما يتماشى مع القوانين والأنظمة السارية، بالإضافة إلى تلبية جميع متطلبات الخصوصية اللازمة.

التوجيه

تؤثر عمليات جمع المعلومات، وإدارتها، ومعالجتها كجزء من مركز العمليات الأمنية بصورة مباشرة على خصوصية العملاء، والموظفين، والزوار. وتعمل جميع مراكز العمليات الأمنية ضمن حدود سياسات المؤسسة التابعة لها، وضمن حدود القوانين والأنظمة السارية أيضاً، ولذلك يجب أخذ الاحتياطات اللازمة للتوثيق الدقيق بشأن النهج المتبع في تلبية هذه المتطلبات.

وبناءً على ما سبق، يجب تطبيق العناصر التالية المرتبطة بالخصوصية:

- تحديد القوانين والأنظمة السارية والتعاون المشترك مع الفرق القانونية ضمن الجهات المعنية
- إجراءات التعامل مع عمليات التحري ذات العلاقة بالخصوصية
- تحديد المعلومات التي يعالجها مركز العمليات الأمنية والتي تكون خاضعة للقوانين المؤسسة للخصوصية
- تقييم أثر الخصوصية
- ضوابط الخصوصية التي تُحدّد من خلال تقييم أثر الخصوصية (تقييد قدرة الوصول إلى المعلومات الشخصية، وموافقة مالك البيانات، وحيثما ينطبق؛ وإرشادات الاحتفاظ بالبيانات، وسيناريوهات استخدام البيانات، والتدريب على خصوصية البيانات).

5.2 الأفراد

يمثّل الأفراد المورّد الأساسي لمركز العمليات الأمنية. وفي الوقت الذي تتطوّر فيه قدرات الذكاء الاصطناعي باستمرار، إلّا أنه ما زال لا يوجد هناك بديل للقدرات والإمكانات التي يضيفها المحلل الأمني فيما يتعلق بتجميع البيانات وتحليلها والتحري بخصوصها. ويتطلب النموذج المتطوّر لإدارة الأفراد وضع عمليات مُحكمة، بالإضافة إلى استقطاب المواهب وتعزيزها واستبقائها. فقطاع الأمن ليس قطاعاً ينتج منتجات ملموسة، كما أن الوقت اللازم لاستقطاب المواهب ذات الخبرة والكفاءة العالية يُعد وقتاً طويلاً، وبالتالي، يجب الحرص على تحفيز وتوجيه، وتدريب الموظفين الحاليين لتعزيز قدرات مركز العمليات الأمنية على تحقيق المتطلبات المتعددة والواسعة في المجالات المعرفية المحدّدة.

5.2 الأفراد

5.2.1 الموظفون

الهدف

بناء القوى العاملة ذات الكفاءة العالية لتحقيق متطلبات الأداء الفعّال لمركز العمليات الأمنية، وبما يتضمن تعيين الموظفين بدوام كامل، وتحقيق متطلبات المهارات اللازمة، وعملية استقطاب المواهب.

التوجيه

يعتمد عدد الموارد التي يحتاجها مركز العمليات الأمنية على ساعات العمل المعتمدة، وعلى القدرات المطلوبة من المركز، بالإضافة إلى الحجم الكلي للمؤسسة الخاضعة للمراقبة. ويحتاج التشغيل على مدار الساعة عدد 12 موظفاً لتغطية متطلبات المراقبة فقط وفي الغالب ما ينتج عن النقص في الموارد البشرية ذات التكلفة المقبولة ضمن القطاع الأمني اضطرار مراكز العمليات الأمنية لتوظيف الموارد من خلال التعاقد مع جهات خارجية. وحيث أن الاعتماد على المورّدين الخارجيين عادةً ما ينتج عنه فرض معتمدات متنوعة، بالإضافة إلى إيجاد عامل المخاطرة، تصبح لذلك عملية إدارة نسبة التعيين بين عدد الموظفين بدوام كامل من العاملين لدى مراكز العمليات الأمنية وأولئك المعينين عن طريق جهات خارجية عبارة عن هدف مستمر. وفيما ما يلي أُدرجت بعض التوصيات بخصوص أعداد الموظفين، مع الأخذ بعين الاعتبار أن البند الأول وهو "أقل من الحد الأدنى" والبند الثاني وهو "الحد الأدنى" يُعدان غير مناسبين لإدارة البنية التحتية الحيوية للمؤسسات.

الفئة	الحد الأعلى لحجم المؤسسة	ساعات العمل	الدعم خارج ساعات العمل	التحليل - الموظفون بدوام كامل	الحد الأدنى من معدل التوطين
أقل من الحد الأدنى	100	9 إلى 5*	موظف مناوب واحد	2	%0
الحد الأدنى	500	9 إلى 5*	موظف مناوب واحد	6	%40
الحد المُوصى به	1000	على مدار الساعة طيلة أيام الأسبوع	موظف مناوب واحد للاستجابة للحوادث	14 إلى 16	%60
النتيجة الأمثل	5000	على مدار الساعة طيلة أيام الأسبوع	موظفان مناوبان . للاستجابة إلى الحوادث	20	%80

يُستحسن إلى حدٍ كبير استخدام جهات خارجية لتوفير متطلبات المراقبة على مدار الساعة

يجب أن تُشغل جميع الوظائف المدرجة ضمن مركز العمليات الأمنية، كما يجب أن تدعم عمليات استقطاب المواهب وعمليات التعيين متطلبات القوى العاملة لدى المركز. وتجب الإشارة هنا إلى أن ما سبق يمثّل توصيات فقط، حيث يجب وضع مهام القطاع في مقدّمة جميع العوامل المحدّدة لأي قرار يُتخذ بخصوص الموارد الفعلية التي تشكّل مركز العمليات الأمنية.

وحيثما استخدمت الموارد الخارجية، يبقى مركز العمليات الأمنية مسؤولاً عن تحقيق مستوى الجاهزية المتوقع وتقديم درجة القدرات المدرجة في **القسم الرابع: مستهدفات القطاع**. وبناءً على ما تقدّم، نوصي بشدة بإلزام المورّدين بتحقيق الأهداف التي يشاركون فيها، أو تلك المستهدفات التي يتحملون المسؤولية الوحيدة عن تحقيقها من خلال شروط تعاقدية محدّدة بوضوح.

5.2 الأفراد

5.2.2 الأدوار والهيكلية

الهدف

إنشاء هيكلية مبنية على الأدوار الوظيفية ضمن مؤسسة مركز العمليات الأمنية، وتوضيح مسؤوليات ومهام كل دور من هذه الأدوار.

التوجيه

يجب أن توثّق الهيكلية المبنية على الأدوار ضمن مركز العمليات الأمنية بوضوح وذلك لتوضّح التوقعات، وبما يتضمن الوصف الوظيفي لكل دور، ومسؤولياته، والمهام الموكلة إليه، والمهارات الفنية المطلوبة لشغله، والمستوى التعليمي لمن يشغله، وجميع الشهادات المطلوبة بالخصوص. كما يجب أن تُراجع الأدوار الوظيفية وتعدّل دورياً، وحسبما تقتضي الحاجة.

5.2 الأفراد

5.2.3 إدارة الأفراد

الهدف

تطبيق نهج متسق وواضح في إدارة الأفراد وبما يبيّن منهجية استقطاب المواهب وتعزيزها واستبقائها لدى مركز العمليات الأمنية.

التوجيه

يجب أن تبدأ دورة الحياة المتعلقة بالموظف من خلال اعتماد عملية متطورة لإدارة المواهب، الأمر الذي يعزز من تحقيق تطلعات وتوقعات الموارد البشرية لدى مركز العمليات الأمنية. على أن يتم إلحاق هذه الدورة بالعملية المطلوبة لتحقيق عملية التعيين الإلحاق بالعمل للموظفين الجدد. ويُحتمل أن توجد الحاجة لتلبية متطلبات التنوع والشمول أو مستهدفات التوطين المعتمدة أو كلاهما لدى المؤسسة، والتي يجب دراستها وتطبيقها بعناية.

وحيث أن نقص الموارد البشرية الماهرة يبقى عاملاً مؤثراً في المستقبل المنظور، ستساعد عمليات التدريب والتدريب المشترك في الإجابة عن المخاوف المتعلقة بمعدل دوران الموظفين في المستقبل، فضلاً عن زيادة معدل الموظفين بدوام كامل من داخل المؤسسة بالنسبة إلى خارج المؤسسة.

وللرفع من معدل استبقاء الموظفين، يجب تطبيق تخطيط المسار الوظيفي، وتحقيق معايير رضا الموظفين.

كما يجب تنفيذ العمليات الأخرى التي تهدف إلى تضمين الأمان عبر دورة حياة الموظف، مثل: الفحص والتناوب الوظيفي والرصد الدوري والتقييم.

5.2 الأفراد

5.2.4 إدارة المعرفة

الهدف

إعداد ممارسات رسمية لإدارة المعرفة ضمن عمليات مركز العمليات الأمنية.

التوجيه

قد تكون المجموعة الأوسع من المهارات والقدرات المطلوبة لإنجاز مهمة مراكز العمليات الأمنية معقدة على نحوٍ خاص لإدارتها. وتمثّل إدارة المعرفة مستوى إجادة مركز العمليات الأمنية وقدرته على إدارة مجموعة المعارف والمهارات المرغوبة، بالإضافة إلى الوضع الحالي المتوفّر ضمن المؤسسة. كما ستتناول كيفية جمع المعارف، وتنظيمها، وتشاركها، وتعزيزها.

يجب استخدام مصفوفة محدّدة لمهارات مركز العمليات الأمنية، بالإضافة إلى تنفيذ التقييمات الدورية التي تلبي المهارات الفنية وغير الفنية، وهو ما يحفز الأفراد وأعضاء الفرق في جميع أقسام مركز العمليات الأمنية على التحسن المستمر.

كما يجب وضع واستخدام مصفوفة تغطي جميع الموارد البشرية ومجالات المعرفة، وذلك لتحديد متطلبات التدريب والمتطلبات الأكاديمية ذات العلاقة.

وسيساهم مدى تغطية المهارات والمعرفة عبر موارد مركز العمليات الأمنية المتاحة، بالإضافة إلى التحديث المنتظم لمصفوفة المهارات والمعرفة فيها إلى التحديث المستمر لهذه المصفوفة، كما سيضمن استمرار أهميتها.

ويجب استخدام الأدوات اللازمة لدعم توثيق المعارف وتوزيعها.

5.2 الأفراد

5.2.5 التدريب والتعليم

الهدف

تطبيق برنامج التدريب والتعليم المخصّص للموارد البشرية العاملة لدى مركز العمليات الأمنية، وذلك لتلبية متطلبات المهارات والمعارف اللازمة ولسد الفجوات فيها.

التوجيه

يجب أن يكون البرنامج التدريبي لمركز العمليات الأمنية مبنياً على الأدوار الوظيفية، وبما يتضمن تعزيز المهارات الشخصية، كما يجب أن يأخذ بعين الاعتبار منهجيات متعددة، مثل: التدريب أثناء العمل، والتدريب المتخصّص على منتجات محدّدة، والتعليم الأكاديمي الرسمي.

وبالإضافة إلى ذلك، يجب تطوير مجموعة من مسارات التأهيل الوظيفي العملي والشهادات المعتمدة، بحيث تربط كل دور من الأدوار والدرجات الوظيفية داخل المؤسسة مع مجموعة من الدورات والمتطلبات التدريبية، وذلك لتبيان امتلاك شاغل هذا الدور الوظيفي لمجموعة المهارات والمعارف اللازمة، الأمر الذي يبيّن مستوى جاهزية مؤسسة مركز العمليات الأمنية.

كما يجب ربط البرنامج التعليمي والتدريبي بمعايير تقييم الأداء، والتطوّر الوظيفي. ولتحقيق برنامج تدريبي وتعريفي فعّال، يُعد تخصيص الميزانية المالية والوقت الكافي أمام الموارد البشرية من العوامل الحاسمة، جنباً إلى جنب مع تنفيذ عمليات المراجعة والتحديث الدوري للبرنامج التدريبي والتعليمي.

5.3 العملية

العمليات هي مجموعة من الخطوات والنشاطات التي تحقّق غاية مرجوة، وتكمن أهمية العمليات في أنها تساهم في استقرار العمليات التشغيلية لمركز العمليات الأمنية. وتُعد خطوات تصميم وتنفيذ العملية المناسبة للهيكلية من الخطوات الحاسمة التي تساهم في مواءمة العمليات النهائية مع الأهداف الاستراتيجية للمؤسسة.

5.3.1 إدارة مركز العمليات الأمنية

الهدف

تنظيم العلاقات المتعددة اللازمة للحفاظ على استمرارية عمل مركز العمليات الأمنية، بالإضافة إلى تحمل مسؤولية التحسين والتطوير المستمر للعمليات، وذلك من خلال إعداد المنهجيات اللازمة لتنفيذ العمليات المطلوبة التي تضمن استمرارية العمليات التشغيلية اليومية.

التوجيه

يجب وضع الإجراءات الإدارية التي تحدّد بوضوح مجموعة العوامل التالية المطلوبة للإدارة الناجحة والمطلوبة لمركز العمليات الأمنية:

- إدارة العلاقات الداخلية والخارجية
- إدارة شؤون المورّدين
- التحسين المستمر للخدمات
- منهجية المشاريع
- توثيق العمليات ووضع مخططاتها
- مصفوفة الأدوار والمسؤوليات
- دليل الخدمات
- إجراءات تطبيق الخدمات الجديدة
- إجراءات إيقاف الخدمات
- مراقبة الامتثال

يجب أن تراجع إجراءات إدارة مركز العمليات الأمنية وتحديثها دورياً. ويُمكن أيضاً مشاركة هذه العمليات مع المعنيين ذوي العلاقة.

5.3 العملية

5.3.2 العمليات التشغيلية والمنشآت

الهدف

التأكد من توفّر الخدمات، والأفراد، والعمليات، والأدوات اللازمة في جميع الأوقات لتحقيق توفّر الخدمات.

التوجيه

في الوقت الذي قد لا يتحمل فيه مركز العمليات الأمنية مسؤولية عمليات المركز وصيانته منشآته، إلّا أنه يشارك في مسؤولية الحفاظ على توفّر الخدمات. وعلى هذا النحو، فإن ضمان وجود مجموعة واسعة من الخدمات والأفراد والعمليات والأدوات في جميع الأوقات يُعد جزءاً من مهمة مركز العمليات الأمنية.

وبالإضافة إلى ما سبق، يجب الحرص على التطرق إلى المتطلبات التالية:

1. توحيد عمليات تقديم الخدمة: يجب توثيق العمليات الإجرائية اليومية ضمن مركز العمليات الأمنية بوضوح في كتيب تشغيلي، يحتوي على مخطط سير العمل، والإجراءات التشغيلية القياسية، وقائمة النشاطات المتكررة. وعلى هذا النحو، يجب تنفيذ تمارين العمليات الأمنية دورياً على وجه الخصوص
2. تكامل العمليات: يجب تضمين العمليات التالية على نحوٍ جيد ضمن مهام مركز العمليات الأمنية، وهي: إدارة التغيير، وإدارة الإعدادات، وإدارة المشكلات، وإدارة الحوادث، وإدارة الأصول.
3. منشآت مركز العمليات الأمنية: حيثما أمكن، يجب وضع الجوانب التالية في عين الاعتبار ضمن منشآت مركز العمليات الأمنية: موقع مخصّص لمركز العمليات الأمنية مع تفعيل الضوابط والإجراءات الأمنية للدخول، وشبكة مخصّصة للمركز، وحائط مخصّص لشاشات الفيديو لتنفيذ عمليات المراقبة، وقدرات مركز الاتصال، ومحطات عمل مخصّصة للمحللين.
4. المناوبات اليومية: يجب أن يوضع جدول واضح يبيّن المناوبات اليومية، كما يجب تفعيل آليات لمراقبة هذه المناوبات (يدوياً أو آلياً أيهما أمكن). ويجب وضع نموذج مخصّص لتسليم المناوبات، والذي يتضمن على سبيل المثال لا الحصر:

- تفاصيل التغيير
- تفاصيل الطلب
- تسليم المهام
- المشاكل المستمرة
- أي تنبيهات للمراقبة
- فحص التطبيقات الحيوية
- تفاصيل الحوادث

5. إدارة المعرفة: يجب أن يعمل مركز العمليات الأمنية على إعداد نظام إدارة الوثائق، وأن يستفيد من منصة متخصّصة للتعاون والمعرفة.
6. إدارة بيئة العمل: يتم في الكثير من المواقف إغفال مجموعة محدّدة من جوانب إدارة مركز البيانات، إلّا أن هذه الجوانب تُعد غاية في الأهمية لضمان استمرار عمل وقدرات مركز العمليات الأمنية، ومن هذه الجوانب تمديدات الكهرباء، والتدفئة، والتهوية، والتكييف (HVAC). ويجب توثيق جميع جوانب مسؤولية وإدارة هذه المتعلقات المهمة، فضلاً عن وصف تفاصيل مخطط الطوابق الموجودة في المؤسسة.

5.3 العملية

5.3.3 رفع التقارير

الهدف

ضمان إعداد التقارير ضمن آلية زمنية محدّدة مبنية على نوع هذه التقارير والجهات المستلمة لها، وضمان مراجعة هذه التقارير والموافقة عليها حسبما تقتضي الحاجة.

التوجيه

قد يُعد مركز العمليات الأمنية تقارير يومية، أو أسبوعية، أو شهرية، أو ربع سنوية، أو سنوية، وذلك بالاعتماد على الجهة المستلمة لهذه التقارير. وفيما يلي بعض الأمثلة على أنواع التقارير، والجهات المستلمة لها، ومدى تكرار إعدادها، ولكن يُحتمل أن تختلف هذه المتغيرات اعتماداً على متطلبات المؤسسة.

نوع التقرير	الجهة المستلمة	الوتيرة
التقارير العملياتية	الفريق الأمني	يومياً أو أسبوعياً
تقارير الحوادث	الفريق الأمني، وفريق تكنولوجيا المعلومات	يومياً أو أسبوعياً
التقارير الأمنية الفنية	الفريق الأمني، وفريق تكنولوجيا المعلومات، وفريق التطبيقات	شهرياً
تقارير التوجهات	الفريق الأمني، وفريق تكنولوجيا المعلومات، وفريق التطبيقات	شهرياً
النشرات الإخبارية أو الملخصات	كافة الجهات	شهرياً
تقارير مؤشرات الأداء الرئيسية	الفريق الأمني، وفرق إدارة الأعمال، والإدارة العليا	فصلياً
التقارير الأمنية التنفيذية	الفريق الأمني، وفرق إدارة الأعمال، والإدارة العليا	فصلياً وسنوياً

حيثما أمكن، يجب أن تستخدم هذه التقارير المقاييس الكمية والنوعية، ومقاييس الحوادث والحالات، وبيانات اتفاقيات مستوى الخدمة.

5.3 العملية

5.3.3 رفع التقارير

وبالإضافة إلى ذلك، يجب إعداد تقرير الحادث الأمني بعد الحوادث ضمن الفئات من الأولوية القصوى إلى الأولوية الثالثة. وحيث أن الفئات المتمثّلة في الأولويتين الثالثة والثانية قد تكون اعتيادية ودورية، فمن المهم أن يعتمد في إعداد هذه التقارير على نموذج بسيط وموحّد وأن يهدف النموذج إلى أن يكون موجزاً. ويُمكن الزيادة في الانتباه إلى التفاصيل والمحتوى عند الحاجة، وذلك في الحالات للتقارير من الفئات المتمثّلة في الأولويتين القصوى والأولى.

ويجب أن يشتمل التقرير المناسب بالحادث الأمني على الحقول التالية:

- تاريخ ووقت بدء الحادث
- تاريخ ووقت انتهاء الحادث
- الأولوية
- الفئة
- العنوان
- تاريخ ووقت الكشف
- الكشف وآلية إعداد التقارير
- فريق التحقيق
- الوصف
- الإطار الزمني
- الإثبات والتحليل
- التصحيحات
- الخلاصة والتوصيات

5.3 العملية

5.3.4 إدارة حالات الاستخدام

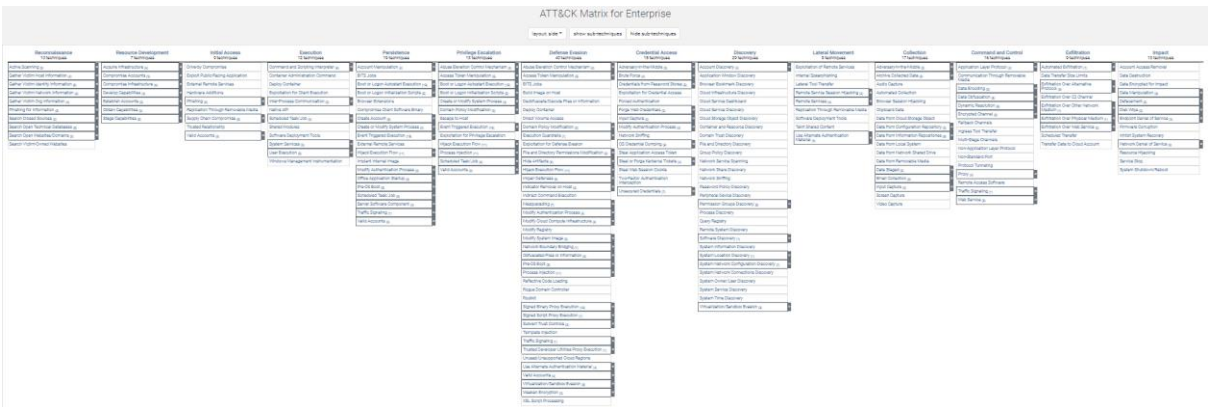
الهدف

توفير أسلوب منهجي للمراقبة الأمنية، ولنشاطات المتابعة المطلوبة، والتي ترتبط بمحفزات الأعمال.

التوجيه

تُعتبر حالة الاستخدام رسمياً أكثر من مجرد آلية للكشف، فهي الأنشطة التقنية المجمعة والتقنيات والعمليات التي تعمل على تحويل أحد المُدخلات إلى المُخرجات أو حالة مرغوبة. وفي سياق مركز العمليات الأمنية، فإن الهدف الكلي يتمثّل في الانتقال من البيئة غير الآمنة إلى بيئة آمنة ومحمية. وعلى هذا النحو، ستشمل معظم حالات استخدام مركز العمليات الأمنية على تقديم محفزات عمل محدّدة من خلال اكتشاف سلوك مشبوه أو غير مرغوب فيه، بحيث يُمكن التحري فيه أولاً، ثم الاستجابة إليه أو الرد عليه على النحو المناسب.

وحيث يقع وصف إطار عمل إدارة حالة الاستخدام الكامل خارج الهدف المعلن لهذه الوثيقة، فإن النهج المناسب أمر بالغ الأهمية للتشغيل الناجح لمركز العمليات الأمنية، بحيث يجب اتباع بعض الإرشادات. وفي الوقت الذي -وكما أُشير إلى ذلك سابقاً- تؤثر فيه العمليات والتكنولوجيا في حالات الاستخدام، إلّا أن حالات الاستخدام الفنية هي محور هذه الممارسة. وتوجد حالات الاستخدام الفنية هذه بصورة أساسية داخل نظام إدارة المعلومات والحوادث الأمنية أو نظام الكشف والاستجابة الممتدة لدى المؤسسة، وبالرغم من المستوى المحدود من القدرة والأداء لهذه الأنظمة، إلّا أنها يجب أن تغطي مجموعة كبيرة من القدرات لتحديد الأساليب والتكتيكات والاجراءات من السجلات المجمّعة. وبالإضافة إلى ذلك، فلا يُمكن تجاهل العامل البشري، حيث أن للمحللين الأمنيين قدرة محدودة على معالجة التنبيهات.



يجب تنظيم حالات الاستخدام ضمن إطار عمل هرمي، واعتماد نهج تنازلي عند العمل على تحقيق أهداف الاكتشاف المتوقعة. حيث ومن الأخطاء الشائعة التي قد تتخذ في مراكز العمليات الأمنية هي أن تُحدّد حالات استخدام فردية تستهدف ثغرات أمنية محدّدة أو حملات من البرمجيات الخبيثة. لذا توصي هذه الوثيقة إلى حدٍ كبير في اعتماد إطار عمل أكثر شمولية.

5.4 التكنولوجيا

بالرغم من الانتشار الواسع للتكنولوجيا، وتضمنها لجميع المجالات، إلّا أننا في هذه الوثيقة نتناول على وجه التحديد التكنولوجيا التي من المفترض أن تساعدنا في تحقيق مرحلة من المراحل الأساسية لدورة حياة الأمن السيبراني، وهي: الوقاية، والكشف، والتحري، والاحتواء، والإصلاح.

تُقاس التقنيات بمعايير جاهزيتها وقدراتها. ويجب تسجيل كل فئة تقنية على الأقل ضمن وثيقة مخصّصة تغطي الأقسام التالية:

- الملكية الفنية
- الملكية الوظيفية
- الوصف الفني
- الوصف الأدائي
- حالة التدريب
- حالة الدعم
- التوفّر والسلامة
- حالة السرّية

يجب أن تكون القدرات شمولية في تغطيتها. وفقط في حال غطت مجموعة صغيرة من الشبكة، أو إذا كانت إمكانية تحديد نمط معيّن منخفضة، فيجب عند ذلك التركيز إلى حدٍ كبير على تحديد المستوى المرتبط بالقدرات.

5.4 التكنولوجيا

5.4.1 نظام إدارة المعلومات والحوادث الأمنية/ نظام الكشف والاستجابة الممتدة

الهدف

توفير إدارة السجلات وقابلية الارتباط، والتي يُستفاد منها لتحقيق مفاهيم المركزية لجميع التنبيهات والإشارات وتوجيهها إلى نقطة محورية واحدة للإدارة باستخدام نظام إدارة المعلومات والحوادث الأمنية أو نظام الكشف والاستجابة الممتدة.

التوجيه

يُعد نظام إدارة المعلومات والحوادث الأمنية ونظام الكشف والاستجابة الممتدة عبارة عن جيلين من الأنظمة المبنية على النهج المفاهيمي نفسه. فهما أدوات أساسية لمركز العمليات الأمنية، ومن خلالهما يحافظ المركز على نظرته الشمولية للوضع الأمني للمؤسسة. وفي هذين النظامين تُحدّد معظم حالات الاستخدام الفنية، وفي الغالب ما يكون بهدف توفير لوحة المعلومات، والتقارير، ومعظم التنبيهات المهمة، والتي تعالجها بعد ذلك خدمة المراقبة الأمنية. ويشكّلان أيضاً مستودعاً للقياسات التي تستخدمها الإدارة لتقييم الخدمات.

يجب توفير القدرات التكنولوجية التالية:

- التجميع
- الارتباط
- التجزئة المخصّصة
- تكامل التحليل الذكي للمخاطر
- الكشف الدقيق عن الأحداث
- التنبيه الآلي
- الإقرار بالتنبيه
- الاستجابة الآلية للتهديدات
- الارتباط متعدد المراحل
- اكتشاف الأنماط
- نظام إدارة الحالات
- تكامل إدارة الأصول
- تكامل سياق الأعمال
- تكامل سياق المعرفات
- تكامل سياق الأصول
- تكامل سياق الثغرات الأمنية
- القوانين المعيارية
- القوانين المخصّصة
- نموذج الشبكة
- التقارير المخصّصة لنظام إدارة المعلومات والحوادث الأمنية أو نظام الكشف والاستجابة الممتدة
- لوحات المعلومات المخصّصة لنظام إدارة المعلومات والحوادث الأمنية أو نظام الكشف والاستجابة الممتدة
- ضوابط الدخول الدقيقة
- الدعم والصيانة الخاضعان للمراقبة
- تكامل واجهة برمجة التطبيقات
- النقل الآمن للأحداث
- الدعم لتقنيات نقل الأحداث المتعددة

5.4 التكنولوجيا

5.4.2 نظام كشف ومنع الاختراقات

الهدف

تمكين عمليات الكشف، والحجب التلقائي لمؤشرات الاختراق (IoC) والمؤشرات السلوكية باستخدام التكنولوجيا.

التوجيه

عادة ما يشير مصطلح نظام كشف ومنع الاختراقات (IDPS) إلى عائلة أو مجموعة من الأجهزة التي يُمكن استثمارها لمراقبة نسبة استخدام الشبكة والتحري عن أي نشاطات مشبوهة، وحجب مثل هذه النشاطات من خلال التدخل الآلي أو اليدوي. وفي هذه الوثيقة، تم التوسع في هذا التعريف ليشمل جميع التقنيات التي يُمكن أن تساهم بصورة مباشرة في الكشف، والحجب التلقائي لمؤشرات الاختراق والمؤشرات السلوكية.

وتشتمل على سبيل المثال لا الحصر، على الفئات التالية من الأجهزة:

- نظام كشف ومنع الاختراقات المبنية على الشبكات
- نظام كشف ومنع الاختراقات اللاسلكية
- نظام تحليل سلوك الشبكة
- حلول مضادات الفيروسات، ونظام كشف ومنع الاختراقات المبني على خدمات المضيف
- حلول مكافحة هجمات الحرمان من الخدمة الموزعة
- محرك جمع الحزمة
- نظام ضبط الدخول إلى الشبكة
- برمجية القائمة البيضاء للتطبيقات
- نظام وبرمجيات الحماية من تسريب المعلومات
- جدار الحماية الخاص بتطبيق الويب
- كشف الأجهزة الطرفية وتصحيحها
- بيئة اختبار الشبكات
- اكتشاف الشبكات والاستجابة لها بدلاً من تحليل سلوك الشبكة
- تصفية البريد الإلكتروني والويب

وهناك ثلاثة أساليب أساسية يشيع استخدامها في جميع حلول نظام كشف ومنع الاختراقات، وهي:

- المستندة إلى التوقيع
- المستندة إلى الحالات الشاذة
- المستندة إلى البروتوكول

5.4 التكنولوجيا

5.4.2 نظام كشف ومنع الاختراقات

وبعيداً عن مشاركتها في الحد من الاختراق، والتخفيف من ملف المخاطر للمؤسسة، تمثّل حزمة نظام كشف ومنع الاختراقات الأساليب الأساسية لتدخل مركز العمليات الأمنية أثناء وقوع الحادث.

يجب توفير القدرات التكنولوجية التالية:

- كشف الاختراق المستند إلى الشبكة
- كشف الاختراق المستند إلى المضيف
- فحص سلامة المستندات
- القائمة البيضاء للتطبيقات
- المصائد
- التوقيعات المخصّصة
- كشف الحالات الشاذة
- التنبيه الآلي
- وحدة الإدارة المركزية
- الجمع الكامل للحزمة لنسبة الاستخدام الوارد والصادر عبر الإنترنت
- الجمع الكامل للحزمة للمجموعات عالية القيمة ضمن الشبكات الداخلية
- الجمع الكامل للحزمة للشبكات الداخلية الأخرى
- ضوابط الدخول الدقيقة
- الدعم والصيانة الخاضعان للمراقبة
- تكامل نظام إدارة المعلومات والحوادث الأمنية أو نظام الكشف والاستجابة الممتدة
- تكامل واجهة برمجة التطبيقات
- تكامل التحليل الذكي للمخاطر
- الحماية من هجمات الحرمان من الخدمة الموزعة
- حماية التطبيقات من هجمات الحرمان من الخدمة
- جدار الحماية الخاص بتطبيق الويب
- تصفية البريد الإلكتروني والويب
- كشف الأجهزة الطرفية وتصحيحها
- القدرات السحابية (وسيط أمان الوصول إلى السحابة، وإدارة وضع الأمان السحابي، ومنصة حماية عبء العمل السحابي)

5.4 التكنولوجيا

5.4.3 أدوات التحليلات الأمنية

الهدف

لتحقيق حالات الاستخدام التي قد تكون كبيرة جداً في نطاقها، أو أنها تلك التي تكون ذات مستوى تعقيد بالنسبة لحلول نظام إدارة المعلومات والحوادث الأمنية، وذلك من خلال استخدام حلول التحليلات الأمنية المناسبة (مثل: تحليل البيانات الكبيرة) والتحليل الذكي للمخاطر.

التوجيه

في أكثر حالاتها تقدّماً، قد تكون هذه القدرات التقنية مرتفعة التكلفة إلى حدٍ كبير، كما أنها قد لا تكون مناسبة لمراكز العمليات الأمنية الأصغر حجماً. ومع ذلك، تُعد هذه القدرات من القدرات المهمة والتي لا يُمكن الاستغناء عنها في البيئات مرتفعة البيانات، مثل: بيئة مزوّدي خدمات الإنترنت، وشبكات النقل، ومراكز البيانات، حيث تستخدم هذه الأدوات الصلاحية الخاصة للوصول، والتي توفّرها هذه البيئات للكشف عن وجود أي بنية تحتية خبيثة. ويشكّل ذلك نوعاً ما الفارق بين نظام إدارة المعلومات والحوادث الأمنية وبين نظام الكشف والاستجابة الممتدة الذي يغطي العديد من المهام الوظيفية المدرجة هنا.

وتكون هذه القدرات التكنولوجية بشكل عام مسؤولة عن إدارة مجموعة القدرات التالية:

- محرك تحليلات قابل للتطوير
- التسوية الآلية للبيانات
- التحليل المستند إلى الأنماط
- تكامل إدارة الحوادث الأمنية
- تكامل المراقبة الأمنية
- تكامل التحليل الذكي للمخاطر الخارجية
- البحث والاستعلام المتقدّم
- تقنيات التصوير المرئي للبيانات
- البحث والتنقيب عن البيانات
- مسارات التدقيق المفصّلة لأنشطة المحللين
- كشف النشاطات السابقة
- جمع البيانات المنظّمة
- جمع البيانات غير المنظّمة
- تحديد المعايير الأساسية للمستخدم
- تحديد المعايير الأساسية للتطبيقات
- تحديد المعايير الأساسية للبنية التحتية
- تحديد المعايير الأساسية للشبكة
- تحديد المعايير الأساسية للنظام
- وحدة التحليل المركزية
- مستودع البيانات الأمنية
- البنية المرنة للبيانات
- ضوابط الدخول الدقيقة
- الدعم والصيانة الخاضعان للمراقبة
- تكامل واجهة برمجة التطبيقات

5.4 التكنولوجيا

5.4.4 الأتمتة والتصميم

الهدف

تمكين استخدام الأتمتة كأسلوب لربط الأدوات الأمنية مع بعضها لتصبح حلاً متكاملاً واحداً.

التوجيه

من الطبيعي أن يتعرض مركز العمليات الأمنية لكم كبير من الحوادث والأحداث الأمنية ذات المستوى المنخفض. وعند ذلك، تأخذ عمليات الأتمتة الأمنية دوراً محورياً في أداء المهام بالنيابة عن المحللين، أو ببساطة تعمل لتخفيف العبء في بعض الحالات، أو العمل على الاستجابة لهذا الحدث بصورة مستقلة تماماً. وعادة ما تتضمن هذه المراحل في منتج يدعى نظام تنسيق الأمن والأتمتة والاستجابة (SOAR). وفي الوقت الذي لا يتحدّد فيه هذا النظام بالعمل على سيناريو واحد، فإن تنسيق الأمن والأتمتة والاستجابة عادة ما يتم تفعيله من خلال حالات الاستخدام لنظام إدارة المعلومات والحوادث الأمنية أو نظام الكشف والاستجابة الممتدة. وبعد ذلك، يعمل هذا النظام على صياغة دليل المبادئ، يعمل من خلاله على تحصيل سير العمل المستخدم في التعامل مع حالة الاستخدام المنظورة. ومن الممكن أتمته هذه الأدلة بشكل كامل، أو جزئي، حيثما وجدت الحاجة للتدخل من قبل المحلل.

كما يجب أن تكون حيازة هذه الأدلة، وتطويرها، وتحسينها من المقاييس النوعية المهمة التي تبين مستوى أداء هذه التكنولوجيا ومدى جاهزيتها.

وتكون هذه القدرات التكنولوجية بشكل عام مسؤولة عن إدارة مجموعة القدرات التالية:

- تكامل نظام إدارة المعلومات والحوادث الأمنية أو نظام الكشف والاستجابة الممتدة
- تكامل التحليل الذكي للمخاطر
- تكامل إدارة الأصول
- تكامل إدارة المستخدمين
- تكامل إدارة الثغرات الأمنية
- مطابقة الأحداث السابقة
- تكامل قاعدة المعرفة
- وضع أولويات الأحداث استناداً إلى مستوى الخطر
- تكامل جدران الحماية
- تكامل نظام كشف ومنع الاختراقات
- تكامل حماية البريد الإلكتروني
- تكامل الحماية من البرمجيات الخبيثة
- تكامل بيئات الاختبار
- تكامل الدليل النشط / إدارة الوصول والتحقّق من الهوية
- دعم طلبات الخدمة
- ضوابط الدخول الدقيقة
- الدعم والصيانة الخاضعان للمراقبة
- تتبع الأداء

5.5 الخدمات

تعمل جميع أقسام مركز العمليات الأمنية وتخصّصاته على توفير الدعم لإنشاء الخدمات التي يقدّمها المركز. وتُعد جميع هذه الأقسام بأنها القيمة الأساسية التي يقدّمها المركز، والتي يمثّلها تجاه المؤسسة. وتعرّف جميع هذه الأقسام والتخصّصات على أنها مجموعة النشاطات العامة والتي تفعّل مجتمعة لتوفير القدرة على حماية البيئة التي تقع ضمن مهام مركز العمليات الأمنية.

وتُقاس الخدمات بمعايير جاهزيتها وقدراتها. حيث يجب تسجيل كل خدمة من الخدمات بصورة منفصلة، ضمن وثيقة مخصّصة تغطي الأقسام التالية:

- مؤشرات الأداء الرئيسية
- مؤشرات الجودة
- الاعتمادات الخدمية
- مستويات الخدمات
- ساعات العمل
- عملاء الخدمات والمعنيون بها
- الغرض
- مُدخلات ومحفزات الخدمات
- مُخرجات الخدمة والمنجزات الناتجة عن تقديمها
- نشاطات الخدمات
- أدوار ومسؤوليات الخدمات

يجب أن تكون القدرات شمولية في تغطيتها. و في حال غطت مجموعة صغيرة من الشبكة، أو إذا كانت إمكانية تحديد نمط معيّن منخفضة، و بذلك فأنه سيأثر على مستوى الجاهزية المرتبط بالقدرات بشكل ملحوظ.

5.5 الخدمات

5.5.1 المراقبة الأمنية

الهدف

إعداد عملية لجمع وتحليل السجلات والإشارات، بهدف تحديد الحوادث الأمنية المحتملة، والتي يجري بعد ذلك التحقّق منها، وتصنيفها، وتصعيدها إلى خدمة إدارة الحوادث.

التوجيه

معظم الحوادث التي تديرها خدمة إدارة الحوادث أو تستجيب لها هي في الواقع حوادث تم الإبلاغ عنها من قبل خدمة المراقبة الأمنية. وتركّز هذه الخدمة على مستوى الوضوح، حيث يشكّل الاكتشاف والمراقبة المستمرة والتنبيه الفوري بالحوادث السبيل في تحقيق القدر الأكبر من تلك الشفافية.

وتتولى هذه الخدمة مسؤولية إدارة مجموعة القدرات التالية:

- الكشف المبكر
- كشف الاختراق
- كشف النقل غير المصرّح
- الكشف الدقيق عن الأحداث
- اكتشاف البرمجيات الخبيثة
- كشف الحالات الشاذة
- الكشف في الوقت الفعلي
- التنبيه والإشعارات
- مراقبة الحالة
- مراقبة الشبكة الفرعية
- مراقبة المستضيف
- مراقبة الشبكة ونسبة استخدام الشبكة
- مراقبة الدخول والاستخدام
- مراقبة المستخدم
- مراقبة التطبيقات والخدمات
- مراقبة السلوك
- مراقبة قاعدة البيانات
- مراقبة فقدان البيانات
- مراقبة فقدان الأجهزة وتعرضها للسرقة
- مراقبة الجهات الخارجية
- مراقبة البيئة المادية
- الحد من الإنذارات الكاذبة
- الضبط والتعديل المستمر
- التغطية
- مراقبة الحوسبة السحابية
- مراقبة الأجهزة المتحركة

5.5 الخدمات

5.5.2 إدارة المعلومات والحوادث الأمنية والاستجابة لها

الهدف

وضع العمليات والإجراءات التي ستُستخدم في التعامل مع الأحداث الأمنية المهمة، والحوادث الأمنية، وعمليات التحري قبل حدوث الاختراق، وذلك للتخفيف من حدة أثر مثل هذه الوقائع، ولتوفير مستوى من الوضوح بخصوصها، ولإصلاح الأصول التي تعرضت للاختراق، ولتوفير التوصيات التي تثمر في تجنب وقوع أحداث مشابهة في المستقبل.

التوجيه

إدارة الحوادث الأمنية تمثّل عملية الاستجابة وتنسيق الرد على التهديدات الأمنية التي يُحتمل أن تتسبب في إحداث أثرٍ سلبي على المؤسسة.

وتتولى هذه الخدمة مسؤولية إدارة مجموعة القدرات التالية:

- إجراءات تسجيل الحادث
- إجراءات التعامل مع الحادث
- إجراءات التحري عن الحادث
- إجراءات التصعيد
- إجراءات جمع الأدلة
- إجراءات تغيير كلمة المرور
- التدريب على الاستجابة للحوادث
- تمارين المحاكاة العملية
- تمارين الفريق الأحمر/ الفريق الأزرق
- مصفوفة الأدوار والمسؤوليات
- التخويل بالرد
- نموذج الحادث
- نظام تتبع الحادث
- الحد من الإنذارات الكاذبة
- تعيين الأولويات
- تعيين مستوى الخطورة
- التصنيف
- جسر الاتصالات الحساس
- غرفة العمليات المركزية
- خطة التواصل ونماذج البريد الإلكتروني
- تكنولوجيا وسائل الاتصال الاحتياطية
- قنوات الاتصالات الآمنة
- المنصة (المخصّصة) لتبادل المعلومات
- تكامل إدارة التغيير
- استخراج وتحليل البرمجيات الخبيثة
- الاستجابة للحوادث في الموقع
- الاستجابة للحوادث عن بُعد
- التصعيد للجهات الخارجية
- نموذج التقييم
- نموذج رفع التقارير
- إغلاق الحادث
- استخراج الدروس المستفادة بهدف تحسين العمليات
- اتفاقيات دعم الحوادث الأمنية الخارجية
- التمارين مع الفرق الأخرى المتخصّصة في الاستجابة للحوادث
- تحليل الأسباب الجذرية

5.5 الخدمات

5.5.3 التحريات الأمنية والتحقيقات الجنائية

الهدف

توفير قدرات المراقبة الأمنية مع تعزيز القدرة على التفريق بين الحوادث الصحيحة وبين الإنذارات الكاذبة، بالإضافة إلى القدرة على تأسيس أطر زمنية سليمة جنائياً فيما يتعلق بخدمات إدارة الحوادث، والرفع من مستوى المعرفة بالحوادث وصولاً إلى تحقيق المعرفة الكافية بطرق الحل والإجابات عن الأسئلة الجوهرية، مثل: الماهية، والسبب، والطرف المعني، والتوقيت، ومكان وقوع الحدث، والكيفية.

التوجيه

تتضمن عمليات التحليل الأمنية إجراءات التحقيقات الجنائية الرقمية للأجهزة وتنفيذ تحليل الذاكرة، بالإضافة إلى التحليل المتقدّم للشيفرات الثنائية. وبعد تحديد تهديد معين، يجب أن يمر هذا التهديد في عملية الاختبار، فأولاً لتحديد ما إذا كان إنذاراً كاذباً أو إذا كان برمجية أو حدثاً خبيثاً ومن ثم لتحديد طبيعة هذا التهديد. وبعد تحقيق هذه العملية والانتهاء منها، سيكون عند ذلك من الممكن استنباط المعلومات اللازمة لاكتشاف أي عمليات اختراق أخرى تعرضت لها المؤسسة إن وجد أي منها. وتمثّل هذه الخدمة مجموعة الإمكانات التحليلية لمركز العمليات الأمنية، بداية من المراجعة اليدوية المتقدّمة للسجل، ووصولاً إلى المعالجة المتقدّمة لتحليل البيانات الكبيرة.

وتتولى هذه الخدمة مسؤولية إدارة مجموعة القدرات التالية:

- تحليل الحدث
- أدوات تحليل الحدث
- تحليل التوجهات
- تحليل الحوادث
- التحليل المرئي
- التحليل الثابت للبرامج الخبيثة
- التحليل الديناميكي للبرمجيات الخبيثة
- تحليل المهارات
- التحليل السابق
- تحليل الشبكات
- تحليل الذاكرة
- تحليل الأجهزة المتحركة
- جمع المعلومات الحساسة
- جمع الأدلة عن بُعد
- أدوات التحقيقات الجنائية للأجهزة
- الأدوات البرمجية لتحليل الأدلة الجنائية
- محطات التحليل المتخصّصة
- كتيب التحليل الأمني والتحقيقات الجنائية
- سير عمل التحليل الأمني والتحقيقات الجنائية
- نظام إدارة الحالات
- نماذج التقارير
- إجراء ضبط الأدلة
- إجراء نقل الأدلة
- إجراء الحفاظ على سلامة سلسلة حيازة الأدلة

5.5 الخدمات

5.5.4 التحليل الذكي للمخاطر

الهدف

توفير مستوى من الاستيعاب والفهم لمؤشرات الاختراق، بالإضافة إلى معالجتها، وإدارتها، وتحليلها ورفع التقارير بشأنها، وذلك من خلال إعداد موجزات بيان التهديد والإحاطات عن التهديد (والتي قد تشتمل على عناوين بروتوكول الإنترنت، والنطاقات، وتجزئة الملفات، أو حتى أن تحتوي على المؤشرات السلوكية)، ولإنشاء روابط وثيقة مع المؤسسات الأخرى وللمشاركة الطوعية أو الإلزامية للمعلومات.

التوجيه

سيعمل أكثر برامج التحليل الذكي للمخاطر جاهزية على نحوٍ وثيق مع المحللين الأمنيين ومتخصّصي خدمة تتبع التهديدات لبناء قدرات التهديدات الاستخبارية الخاصة بهم.

وتتولى هذه الخدمة مسؤولية إدارة مجموعة القدرات التالية:

- الجمع المستمر للمعلومات الاستخبارية
- الجمع والمعالجة الآلية للمعلومات الاستخبارية
- الجمع والتوزيع المركزي
- جمع المعلومات الاستخبارية من المصادر العلنية والمفتوحة
- جمع المعلومات الاستخبارية من المجتمعات المغلقة
- جمع المعلومات الاستخبارية من مزوّدي المعلومات الاستخبارية
- جمع المعلومات الاستخبارية من شركاء الأعمال
- جمع المعلومات الاستخبارية من القوائم البريدية
- جمع المعلومات الاستخبارية من المصادر الداخلية
- تحليل البيانات المنظّمة
- تحليل البيانات غير المنظّمة
- تحليل الحوادث السابقة
- تحليل التوجهات
- التنبيه الآلي
- تتبع تحركات الخصوم
- تحديد المهاجمين
- تحديد التهديدات
- توقع التهديدات
- الإجراءات التشغيلية القياسية المتعلقة بالتحليل الذكي للمخاطر
- الأدوار والمسؤوليات
- مراقبة الثغرات الأمنية والإبلاغ عنها
- استخراج الأساليب والتكتيكات والاجراءات
- إلغاء الازدواجية
- إثراء البيانات
- الوضع ضمن السياق
- تحديد الأولويات
- رفع التقارير بالتحليل الذكي للمخاطر
- التقديرات والتنبؤات
- المشاركة داخل الشركة
- المشاركة ضمن القطاع
- المشاركة خارج القطاع
- المشاركة باستخدام صيغة مشتركة (مثال: STIX)

5.5 الخدمات

5.5.5 تتبع التهديدات

الهدف

تمكين البحث الاستباقي والمتكرر عبر الشبكات والأصول لاكتشاف أدلة على وجود التهديدات غير المكتشفة.

التوجيه

في الوقت الذي تُعد فيه المراقبة الأمنية المُدخل الأساسي لعملية إدارة الحوادث، فإن خدمة تتبع التهديدات يُمكن أن تأتي في المرتبة الثانية. ويُمكن تنفيذ عمليات تتبع التهديدات يدوياً من خلال التنقل بين السجلات، أو بمساعدة الآلات والأجهزة المتخصّصة. ويُمكن أن يكون تتبع التهديدات منظّماً أو غير ذلك. وستتبع الخدمات الأكثر جاهزية إطار عمل مثبت لتتبع التهديدات، ومثال عليه إطار عمل TaHiti.

وتتولى هذه الخدمة مسؤولية إدارة مجموعة القدرات التالية:

- تتبع قيم التجزئة
- تتبع عناوين بروتوكول الإنترنت
- تتبع أسماء النطاقات
- تتبع الخلل في بيانات الشبكة
- تتبع الخلل في البيانات المستندة إلى المستضيف
- تتبع أدوات الخصوم
- تتبع الأساليب والتكتيكات والإجراءات
- تتبع التهديدات الواردة
- تتبع التهديدات الصادرة
- تتبع التهديدات الداخلية
- كشف القيمة الخارجية
- تغطية التتبع
- استثمار الأدوات المتاحة
- التتبع المخصّص للنصوص والأدوات
- منصات التتبع المخصّصة
- الجمع المستمر للمعلومات حول التتبع
- التتبع السابق
- التتبع الآلي
- التنبيه بعمليات التتبع
- تكامل معلومات الثغرات الأمنية
- تكامل التحليل الذكي للمخاطر

5.5 الخدمات

5.5.6 إدارة الثغرات الأمنية

الهدف

تقليص مساحة الهجمات من خلال تحديد وتقييم وإصلاح الثغرات الأمنية ورفع التقارير بشأنها.

التوجيه

الثغرات الأمنية هي نقاط ضعف يُمكن أن يستغلها منفذ الهجمات بهدف إساءة استخدام منتج ما أو خدمة ما. وقد تكون إساءة الاستخدام هذه غير ضارة نسبياً، أو أنه قد ينتج عنها السماح للمستخدمين غير المخولين باستخدام الشبكات أو الصلاحيات الممنوحة للغير. وتتسبب الثغرات الأمنية في وقوع الحوادث الأمنية، أي أن الثغرات الأمنية تشكّل الركائز الأساسية للحوادث الأمنية، وعادة ما يقوم منفذ الهجمات بربطهما ببعضهما في سبيل تحقيق الأهداف النهائية لمنفذ الهجمات تلك. وغالباً ما يظهران كخطأ في قاعدة التعليمات البرمجية للتطبيق، أو في إحدى المكتبات الخاصة به، أو كخطأ في الإعدادات نفسها. وكنتيجة لذلك، غالباً ما تعتمد المؤسسات على المورّدين لتحديد الإصدارات الضعيفة من التطبيقات، ولتوفير التصحيحات أو الأساليب أو الحلول المؤقتة للعمل.

ولا تتعلق إدارة الثغرات الأمنية بالتصحيحيات فقط، حيث أنها ترتبط أيضاً بالحفاظ على قدرة اكتشاف المخاطر ضمن المؤسسة.

وتتولى هذه الخدمة مسؤولية إدارة مجموعة القدرات التالية:

- تخطيط الشبكة
- تحديد الثغرات الأمنية
- تحديد المخاطر
- قبول المخاطر
- المسح الأمني الأولي
- المسح المخول
- تكامل إدارة الحوادث
- تكامل إدارة الأصول
- تكامل إدارة الإعدادات
- تكامل إدارة التصحيح
- تحديد التوجّهات
- مستودع الثغرات الامنية لدى المؤسسة
- مخزن تطبيقات المؤسسة
- إجراءات إدارة الثغرات الأمنية
- تعديل سياسة المسح
- التقارير المفصّلة بالثغرات الأمنية
- التقارير الإدارية
- المسح المجدول
- المسح المتخصّص
- جمع وتحليل المعلومات عن الثغرات الأمنية

5.5 الخدمات

5.5.7 إدارة السجلات

الهدف

ضمان تفعيل الأنشطة المتعلقة بالجمع المستمر للسجلات، ومعالجتها، وتخزينها، وتنفيذ عملات المعالجة اللاحقة لها، بالإضافة إلى التحليل المنتظم لجودة السجلات ولضبط المعايير والمعلمات المشتقة.

التوجيه

لإدارة السجلات تأثير مباشر على تحقيق مستوى الوضوح المطلوب والمحافظة عليه، وذلك بهدف ضمان استمرارية عمل خدمة المراقبة الأمنية على النحو المناسب.

وتتولى هذه الخدمة مسؤولية إدارة مجموعة القدرات التالية:

- جمع بيانات السجلات من الأجهزة الطرفية
- جمع بيانات السجلات من التطبيقات
- جمع بيانات السجلات من قواعد البيانات
- جمع بيانات تدفق الشبكة
- جمع بيانات سجل الأجهزة التي تستخدم الشبكة
- جمع بيانات سجل الأجهزة الأمنية
- التجميع والتخزين المركزي
- فترات الاستبقاء المتعددة
- نقل السجل الأمني
- الدعم للتنسيقات متعددة السجل
- دعم أساليب النقل المتعددة
- تسوية البيانات
- البحث والتصفية في السجلات
- التنبيه
- لوحات المعلومات والتقارير
- اكتشاف التلاعب بالسجلات
- سياسة جمع السجلات
- سياسة التسجيل
- سياسة الاحتفاظ بالبيانات
- سياسة إدارة الخصوصية والبيانات الحساسة

القسم 6

البيئة الاتحادية والمركز الوطني للعمليات الأمنية

6.1 المركز الوطني للعمليات الأمنية

تتمثّل رؤية المركز الوطني للعمليات الأمنية في إيجاد وضوح مركزي، وعمليات تنسيقية، وإجراءات مساءلة للدفاع عن دولة الإمارات العربية المتحدة ضد تهديدات الأمن السيبراني. وسيكون المركز الوطني للعمليات الأمنية مسؤولاً عن توفير المساعدة لجميع قطاعات مراكز العمليات الأمنية ومؤسساته، وذلك من خلال تقديم الخدمات، وقيادة التعاون المشترك بين الجهات الحكومية، والأكاديمية، ومؤسسات القطاع.

ويعمل المركز الوطني للعمليات الأمنية كمركز لجمع المعلومات، وتحليلها، وتوزيعها، ويعتمد في عمله على أعلى المعايير المعتمدة في هذه الوثيقة. كما يتولى المركز مسؤولية النظام الوطني للتوعية بالأمن السيبراني، والذي تستقي منه المؤسسات ومراكز العمليات الأمنية في القطاع معلوماتها حول الوضع العام للأمن السيبراني في دولة الإمارات العربية المتحدة.

ويعمل المركز الوطني للعمليات الأمنية أيضاً على إدارة سياسات وأطر عمل الأمن السيبراني في الدولة. ودورياً، يعمل على تقييم امتثال مراكز العمليات الأمنية في القطاع لإطار العمل والسياسات الموضوعة في هذه الوثيقة بالنيابة عن مجلس الأمن السيبراني. وتقيّم مراكز العمليات الأمنية في القطاع بدورها امتثال الجهات والمؤسسات التابعة لها.

في الوقت الذي يدعم فيه المركز الوطني للعمليات الأمنية معظم المؤسسات الحيوية في دولة الإمارات العربية المتحدة، إلّا أنه مهمته تتمثّل أيضاً في حماية وبناء الجاهزية الأمنية السيبرانية، وتقديم الاستشارات بخصوصها ضمن القطاع العام والتجاري الأوسع. كما يسعى المركز الوطني للعمليات الأمنية جاهداً إلى بناء مجتمع الأمن المحلي، والمساعدة في رفع مستوى الوعي، وتقديم التعليم والتدريب اللازم للمؤسسات التي تحتاجه، وهو معني على وجه التحديد أيضاً بإقامة الشراكات، وتوفير الموارد، وآليات التغذية الراجعة لجميع المؤسسات داخل دولة الإمارات العربية المتحدة.

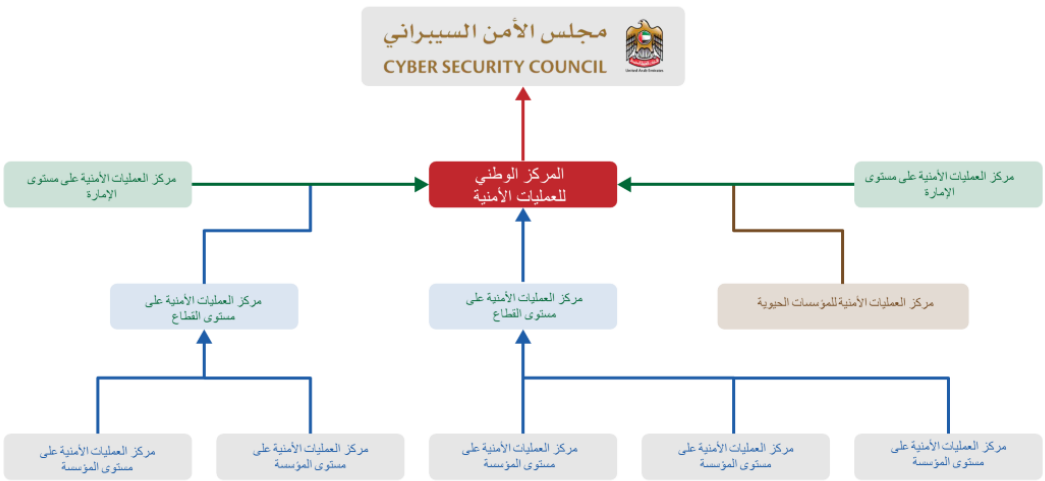
وبشكل عام، يوفّر المركز الوطني للعمليات الأمنية الخدمات التالية:

- الوعي بالموقف العام
- الهندسة العكسية للبرمجيات الخبيثة
- التحليل الأمني والتحقيقات الجنائية
- التحليل الذكي للمخاطر
- تقييم مستوى الامتثال
- الخدمات الاستشارية للأمن السيبراني
- التعليم والتدريب على الأمن السيبراني
- إدارة الاستجابة للحوادث
- تنسيق الاستجابة للأزمات
- اختبارات الاختراق والفريق الأحمر
- إدارة الثغرات الأمنية
- المراقبة الأمنية
- تتبع التهديدات

وفي حال وقوع أحداث سيبرانية أمنية ذات أهمية عالية، سيوفّر المركز الوطني للعمليات الأمنية الدعم بحسب الطلب لأي مؤسسة تحتاجه

6.2 البيئة الاتحادية

تعني البيئة الاتحادية بصورة أساسية استخدام منهجية اتصالات ثنائية الاتجاه، أو الاتصال المتبادل بين الجهات، حيث أن المعلومات يتم تصعيدها من المؤسسة إلى الجهة المسؤولة، بينما تتجه التعليمات بالخصوص من الجهة المسؤولة إلى المؤسسة. ويُتوقع من مراكز العمليات الأمنية في القطاع رفع التقارير بصورة مباشرة إلى المركز الوطني للعمليات الأمنية والإبلاغ عن أي حوادث تُبَلَّغُ بها. وفي المقابل، تلتزم جميع المؤسسات التي تعمل تحت مسؤولية مراكز العمليات الأمنية في القطاع بإبلاغ المركز المسؤول عنها وتزويده بالتقارير عن أي حوادث تتعرض لها.



ويجب أن تحتوي جميع التقارير بالحوادث على البيانات التالية:

- درجة الأولوية المحلية
- مستوى الفئة المخصّص
- العنوان
- الوصف
- الوضع الراهن
- الخلل في البيانات

ويجب إيصال جميع هذه التنبيهات مع اختتام عملية التحقيق، كما يجب رفع التقارير بالتحديثات بشكل دورية مناسبة. و متوقع وقت التنبيه فحين الاعلان أو الإخطار بوقوع الحادث.

6.2 البيئة الاتحادية

الوقت المتوقع للتنبيه

فئة الحادث	متوسط وقت التنبيه
حالة طارئة على مستوى القطاع	30 دقيقة
حادث على مستوى القطاع	60 دقيقة
حادث على المستوى المحلي	1440 دقيقة

الوقت المتوقع للتحديث

فئة الحادث	متوسط وقت التحديث
حالة طارئة على مستوى القطاع	60 دقيقة
حادث على مستوى القطاع	120 دقيقة
حادث على المستوى المحلي	1440 دقيقة

وبهدف تحسين قدرات الكشف لدى المركز الوطني للعمليات الأمنية، يجب مشاركة البيانات التالية مع مراكز العمليات الأمنية في القطاع، ومن جهتها تشارك المراكز هذه المعلومات مع المركز الوطني للعمليات الأمنية

- جدار الحماية الخاص بالشبكة الفرعية
- وكيل توجيه الإنترنت
- تحليل اسم النطاق
- معلومات توجيه بروتوكول البوابة الحدودية

7

القسم
الملاحق

7.1 المعايير الأساسية لرفع التقارير والمراقبة

يجب التركيز على مقاييس ومؤشرات الأداء الرئيسية لتحقيق مراحل الجاهزية والقدرات المتقدّمة. كما يتوجب على المؤسسة تطوير المقاييس الصحيحة والحفاظ عليها ومراجعتها على نحوٍ متكرر حتى تتمكّن من الانخراط في دورة التحسين المستمر الموجودة في مستوى التحسين (المستوى الخامس) من الجاهزية والمستوى المحدّد للقدرات (المستوى الثالث). ونركّز هنا على مؤشرات الأداء الرئيسية المرتبطة بالخدمات والتقنيات الرئيسية الموجودة في مراكز العمليات الأمنية.

مقاييس المراقبة الأمنية

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
عدد الأصول الخاضعة للمراقبة	عدد الأصول المذكورة في السجلات والأحداث الأمنية	يحدّد بشكل عام نطاق النشاط الذي يخضع للمراقبة، ويحدّد المشكلات المحتملة في إدارة التغيير، أو أي مشكلات فنية أخرى في حال تغيّر الرقم بشكل غير متوقع.
نسبة اكتمال قاعدة بيانات الأصول	عدد الأصول الخاضعة للمراقبة مقارنة بعدد الأصول المعروفة والمشمولة في قاعدة بيانات إدارة الأصول.	يحدّد التغيير في المراقبة أو في قائمة الأصول.
عدد الأحداث الخاضعة للمراقبة	إجمالي عدد الأحداث الأمنية التي رصدها الفريق، والتي تشمل أي إجراء أمني ذي صلة، مثل: تسجيل الدخول إلى الأجهزة الطرفية باستخدام حساب المستخدم. ولا تُعد أحداث مشبوهة في طبيعتها، بل إنها الحالات الاعتيادية للاستخدام، والتي توفّر النظرة الشمولية اللازمة لتحديد الأحداث والحوادث المهمة.	يحدّد بدقة نطاق النشاط الذي يخضع للمراقبة، ويُعد الأساس الذي تنبثق منه جميع المقاييس الأخرى.
متوسط وقت اكتشاف الأحداث	الوقت الذي يسبق اكتشاف حدث أمني مهم وتحديده وإخطار مركز العمليات الأمنية	يراقب قدرة الحزمة الأمنية على اكتشاف المعلومات وترحيلها إلى المستخدم النهائي.
متوسط وقت الاستجابة	المدة الزمنية بين اكتشاف حدث مهم وقبل إقرار محلل تابع لمركز العمليات الأمنية استلامه للتنبيه أو قبل تطبيق أي إجراء وقائي تلقائي.	يُحدّد أسلوب القياس هذا سرعة الاستجابة، ويُمكن أن يحدّد إذا كانت مراقبة مركز العمليات الأمنية مشغولة جداً، أو لا تمتلك درجة كافية من الانتباه، أو تفتقر إلى درجة السرعة التي تتطلبها المؤسسة.
عدد الإنذارات الكاذبة المُصَعّدة	عدد الأحداث الأمنية المهمة المحدّدة على أنها حوادث.	يُمكن أن تشير هذه القيمة إلى استقلالية وجاهزية إجراءاتك ودليل المبادئ، إلّا أنه يُمكن أن تكون هذه القيمة أكبر من الواقع بسبب الإنذارات الكاذبة التي يسهل إغلاقها، وتمثّل مشكلة في طبقة إدارة حالات الاستخدام. كما تشير أيضاً إلى قدرة المؤسسة على التعامل مع التهديدات وردعها في مراحلها المبكرة.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

مقاييس المراقبة الأمنية

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
متوسط وقت التنبيه	الوقت بين الإقرار بوقوع حدث مهم، وإرسال التنبيه إلى الجهات المعنية. وينطبق ذلك فقط في الحالات التي يكون فيها التنبيه ضرورياً أو في حالات الأحداث التي تتطلب التصعيد.	وهذا هو المقياس الذي يتم من خلاله قياس كفاءة فريق المراقبة.
عدد الأحداث الأمنية المهمة الواجب معالجتها	عدد الأحداث الأمنية المهمة التي جرى تحديدها وتحليلها وفرزها ومن ثم حلها أو تصعيدها.	يمثّل هذا الرقم العبء التحليلي على فريق المراقبة، أي مدى انشغالهم.
نسبة الأحداث الأمنية المهمة التي تم حلها	عدد الأحداث الأمنية المهمة التي عمل فريق المراقبة على حلها دون الحاجة إلى التصعيد.	يُمكن أن تشير هذه القيمة إلى استقلالية وجاهزية إجراءاتك ودليل المبادئ، إلّا أنه يُمكن أن تكون هذه القيمة أكبر من الواقع بسبب الإنذارات الكاذبة التي يسهل إغلاقها، وتمثّل مشكلة في طبقة إدارة حالات الاستخدام. كما تشير أيضاً إلى قدرة المؤسسة على التعامل مع التهديدات وردعها في مراحلها المبكرة.
عدد الحوادث المُحدّدة	عدد الأحداث الأمنية المهمة المحدّدة على أنها حوادث.	يُمكن أن تشير هذه القيمة إلى استقلالية وجاهزية إجراءاتك ودليل المبادئ، إلّا أنه يُمكن أن تكون هذه القيمة أكبر من الواقع بسبب الإنذارات الكاذبة التي يسهل إغلاقها، وتمثّل مشكلة في طبقة إدارة حالات الاستخدام. كما تشير أيضاً إلى قدرة المؤسسة على التعامل مع التهديدات وردعها في مراحلها المبكرة.
عدد الإنذارات الكاذبة المُصَعّدة	عدد الأحداث الأمنية المهمة المحدّدة على أنها حوادث.	يُمكن أن تشير هذه القيمة إلى استقلالية وجاهزية إجراءاتك ودليل المبادئ، إلّا أنه يُمكن أن تكون هذه القيمة أكبر من الواقع بسبب الإنذارات الكاذبة التي يسهل إغلاقها، وتمثّل مشكلة في طبقة إدارة حالات الاستخدام. كما تشير أيضاً إلى قدرة المؤسسة على التعامل مع التهديدات وردعها في مراحلها المبكرة.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

مقاييس إدارة المعلومات والحوادث الأمنية

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
عدد الحوادث، مصنفة حسب الأولوية	عدد الأحداث الأمنية المهمة المعرفة على أنها حوادث.	يمثّل هذا الرقم العبء التحليلي على فريق إدارة الحوادث، أي مدى انشغالهم.
متوسط وقت استمرار الحادث حسب الأولوية	الوقت بين لحظة بدء الحادث ووقت احتواء الأصل المتأثر أو معالجته.	يمثّل هذا المتوسط الوقت الذي يقضيه منفذ الهجمات في بيئتك، والتعرض الفعلي لمؤسستك لهذا الحادث. يتمثّل الهدف في تقليل هذا الرقم على الدوام.
متوسط وقت التحديث	قد يتطلب كل حادث التواصل ووضع نقاط تنسيق، ويقيس هذا الرقم دقة فريق إدارة الحوادث في الإبقاء على تلك النقاط.	يُعد هذا المتوسط مقياساً للكفاءة والاكتمال. ويجب أن يكون التواصل متكرراً وإلزامياً في الحالات الحرجة، خاصة مع المعنيين.
متوسط وقت الاحتواء	الوقت بين لحظة تحديد وقوع الحادث، ووقت احتواء أو معالجة أثر ذلك الحادث.	يُمكن أن تكون هذه الإحصائيات الأكثر تضليلاً لمركز العمليات الأمنية. وكلما كانت الحادث الأمني أكثر خطورة، كلما استغرق حله وقتاً أطول، وذلك على عكس حوادث تكنولوجيا المعلومات التي قد يؤدي فيها تحديد الأولويات إلى تقليل وقت التعطل. ومع ذلك، يجب مراقبة هذا المقياس، لأنه يوفّر نظرة عامة على الكفاءة الإجمالية لمركز العمليات الأمنية فيما يتعلق بالتخفيف من الأثر، ولكن يجب النظر إليه ضمن سياق الأحداث الفعلية.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

تحليل الأمن السيبراني ومقاييس التحقيقات الجنائية

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
عدد العينات المُجمّعة، مصنفة حسب النوع	عدد العينات من أي نوع: ملف، أو ذاكرة، أو صورة قرص صلب، أو جمع حزمة، وغيرها، والتي تُجمع لغايات التخزين أو المعالجة.	يحدّد بدقة عبء ونطاق النشاط المنجز، ويُعد الأساس الذي تنبثق منه جميع المقاييس الأخرى في هذه الفئة.
عدد العينات المحلّلة	عدد العينات من أي نوع: ملف، أو ذاكرة، أو صورة قرص صلب، أو جمع حزمة، وغيرها، والتي تُجمع لغايات التخزين أو المعالجة.	يمثّل إحدى القيمتين اللتين تشكّلان العبء التحليلي على الخدمة، أي مدى انشغال الفريق المسؤول. وعند مقارنتها بالعينة الإجمالية المجمّعة، فإنها توفّر نظرة على شمولية التحقيق الذي يُمكن تنفيذه بناءً على الموارد المتوفّرة.
عدد مؤشرات الاختراق الناتجة	عدد مؤشرات الاختراق المكتشفة من خلال تحليل العينات	مقياس قيمة خدمة التحليلات الأمنية.
عدد التقارير المعدة	عدد التقارير المعدة ولا تشمل تقرير الحادث.	يمثّل إحدى القيمتين اللتين تشكّلان العبء التحليلي على الخدمة، أي مدى انشغال الفريق المسؤول.
عدد مرات فشل سلسلة الحيازة	عدد المرات التي تكشف فيها مراجعة سلسلة الحيازة عن وجود تناقض، أو عدد المرات التي يتم فيها الإبلاغ عن مثل هذا الحدث ذاتياً.	يوفّر مقياساً لجودة ودقة عمل المحللين.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

مقاييس التحليل الذكي للمخاطر

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
عدد موجزات البيانات الخاضعة للمراقبة	عدد موجزات البيانات الخاضعة للمراقبة عبر جميع الأجهزة سواء كانت مركزية أو غير مركزية.	يُعد الحفاظ على مستوى الوضوح أمراً مهماً، لكن ازدياد هذا الرقم ليس دائماً مؤشراً إيجابياً.
نسبة موجزات البيانات المركزية	نسبة موجزات البيانات المركزية لغايات المراقبة والحماية عبر الحزمة الأمنية كاملاً	يدل على جاهزية فريق التحليل الذكي للمخاطر، ويمثّل الاستخدام الأفضل لجميع البيانات التي تم الحصول عليها.
عدد الإنذارات الكاذبة، حسب موجزات البيانات	عدد المرات التي تسببت بها مؤشرات الاختراق بحدث أو حادث مهم خاطئ	يؤثر على الثقة في مصدر البيانات، ويُمكن استخدامه في عملية اتخاذ قرارات مدروسة حول طرق الاستفادة من استخدام أو عدم استخدام موجز البيانات.
عدد مؤشرات الاختراق الخاضعة للمراقبة، حسب موجزات البيانات	عدد مؤشرات الاختراق الخاضعة للمراقبة عبر الحزمة الأمنية	يقيس مقدار المعلومات الاستخبارية التي توظفها بفاعلية.
متوسط وقت التقادم، حسب موجزات البيانات	المدة الاعتيادية للحفاظ على مؤشرات الاختراق في موجز البيانات.	تتمحور أهمية مؤشرات الاختراق حول الوقت. وعادة ما تكون موجزات البيانات التي لها فترة تقادم أقصر أكثر جاهزية وفائدة.
عدد الحوادث المُحدّدة	عدد الحوادث المُحدّدة بناءً على مؤشرات الاختراق.	تشير هذه القيمة إلى قيمة وأهمية برنامج التحليل الذكي للمخاطر.
عدد مؤشرات الاختراق الناتجة	عدد مؤشرات الاختراق الناتجة نتيجة لبرنامج التحليل الذكي للمخاطر.	يعمل فريق التحليل الذكي للمخاطر المتطوّر على إعداد التحليلات الاستخبارية بنفسه. مقياس ممتاز لقيمة الخدمة.
عدد التوصيات الناتجة	عدد التحسينات على الوضع الأمني العام الناتجة عن الخدمة.	تمثّل هذه القيمة مقياساً لقيمة الخدمة.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

مقاييس تتبع التهديدات

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
عدد عمليات تتبع التهديدات المنجزة	عدد عمليات تتبع التهديدات المنجزة	يمثّل هذا الرقم العبء التحليلي على فريق التتبع، أي مدى انشغالهم ومقدار إنتاجيتهم.
متوسط مدة إكمال عملية تتبع التهديدات	المدة ما بين بدأ عملية التتبع واكتمالها.	على غرار متوسط وقت الاحتواء، يُمكن أن تكون هذه القيمة مضللة، وذلك لأن عمليات التتبع ذات النطاق الواسع تستغرق وقتاً أطول، وقد تتطلب عمليات التتبع الناجحة وقتا طويلاً بسبب الحاجة إلى التمحور والتكرار. مع ذلك، يجب مراقبة هذا المقياس، لأنه يوفّر نظرة عامة على مقدار الوقت المستغرق في عمليات التتبع، كما يجب النظر إلى هذا المقياس ضمن سياق الأحداث الفعلية.
عدد الحوادث المُحدّدة	عدد الحوادث المُحدّدة بسبب عمليات تتبع التهديدات	تشير هذه القيمة إلى قيمة وأهمية برنامج تتبع التهديدات.
عدد التوصيات الناتجة	عدد التحسينات على الوضع الأمني العام الناتجة عن الخدمة.	تمثّل هذه القيمة مقياساً لقيمة الخدمة.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

مقاييس إدارة الثغرات الأمنية

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
وتيرة تنفيذ التصحيحات الداخلية	عدد الحوادث المُحدّدة بسبب عمليات تتبع التهديدات	تشير هذه القيمة إلى قيمة وأهمية برنامج تتبع التهديدات.
متوسط وتيرة إصدار التصحيحات من قبل المورّد	عدد التحسينات على الوضع الأمني العام الناتجة عن الخدمة.	تمثّل هذه القيمة مقياساً لقيمة الخدمة.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

الثغرات الأمنية في الشبكات الفرعية المراقبة

يجب أن يهتم برنامج إدارة الثغرات الأمنية على نحوٍ خاص بالأصول التي يُمكن الوصول إليها مباشرة من الإنترنت، أو تلك الموجودة في المنطقة العازلة منزوعة السلاح (DMZ). إذ يُمكن لمنفذ الهجمات إجراء عمليات مسح للثغرات أو محاولة استغلال هذه الأصول بصورة مباشرة، لذلك فإنه من المهم إعطاء عملية تصحيح هذه الثغرات، وخاصة الثغرات الحرجة، أولوية أكبر من الثغرات التي تواجه الشبكات الفرعية الأخرى.

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
عدد الثغرات الأمنية الموجودة، حسب الأهمية	عدد الثغرات الأمنية الموجودة حالياً في المؤسسة، مصنّفة حسب الأهمية.	تشير هذه القيمة إلى مدى تعرضك الحالي ومدى انشغال فريق إدارة الثغرات الأمنية.
عدد الثغرات الأمنية الحرجة الموجودة	عدد الثغرات الأمنية الحرجة الموجودة حالياً في المؤسسة. يمثّل مقياساً فرعياً مهماً من المقياس السابق.	تمثّل هذه القيمة عدد المشكلات الطارئة التي يجب معالجتها.
عدد الثغرات الأمنية المعالجة مؤخراً	عدد الثغرات الأمنية المعالجة منذ آخر فحص، عادةً ما تكون المدة شهراً واحداً.	تمثّل هذه القيمة إنجازات فريق إدارة الثغرات الأمنية. يُمكن تقييمها لتقدير مقدار الجهد المبذول ونتائجه.
التغيّر الشهري، حسب الفئة	مجموع تراكمي للتغيّر الإيجابي أو السلبي للعدد الإجمالي للثغرات الأمنية.	يوضّح هذا المقياس التقدّم العام الذي حقّقه برنامج إدارة الثغرات الأمنية. هل تتوجّه المؤسسة نحو وضع أكثر أو أقل أمناً؟
التغيّر الأسبوعي	مجموع تراكمي للتغيّر الإيجابي أو السلبي للعدد الإجمالي للثغرات الأمنية على نطاق أصغر.	يتيح هذا المقياس توقع اتجاه التقدّم المُحرز وإعادة الضبط للتأثير على المقياس السابق.
متوسط وقت الاحتواء، حسب الأهمية	المتوسط الحسابي للوقت المستغرق منذ تحديد الثغرة الأمنية حتى اللحظة التي يتم فيها احتوائها أو تصحيحها.	يمثّل هذا المقياس المدة الفعلية للتعرض، ويُعد المقياس الأساسي للخدمة الذي يجب تحسينه باستمرار.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

الثغرات الأمنية في الشبكات الفرعية الخلفية

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
عدد الثغرات الأمنية الموجودة، حسب الأهمية	عدد الثغرات الأمنية الموجودة حالياً في المؤسسة، مصنّفة حسب الأهمية.	تشير هذه القيمة إلى مدى تعرضك الحالي ومدى انشغال فريق إدارة الثغرات الأمنية.
عدد الثغرات الأمنية الحرجة الموجودة	عدد الثغرات الأمنية الحرجة الموجودة حالياً في المؤسسة. يمثّل مقياساً فرعياً مهماً من المقياس السابق.	تمثّل هذه القيمة عدد المشكلات الطارئة التي يجب معالجتها.
عدد الثغرات الأمنية المعالجة مؤخراً	عدد الثغرات الأمنية المعالجة منذ آخر فحص، عادةً ما تكون المدة شهراً واحداً.	تمثّل هذه القيمة إنجازات فريق إدارة الثغرات الأمنية. يُمكن تقييمها لتقدير مقدار الجهد المبذول ونتائجه.
التغيّر الشهري، حسب الفئة	مجموع تراكمي للتغيّر الإيجابي أو السلبي للعدد الإجمالي للثغرات الأمنية.	يوضّح هذا المقياس التقدّم العام الذي حقّقه برنامج إدارة الثغرات الأمنية. هل تتوجّه المؤسسة نحو وضع أكثر أو أقل أمناً؟
التغيّر الأسبوعي	مجموع تراكمي للتغيّر الإيجابي أو السلبي للعدد الإجمالي للثغرات الأمنية على نطاق أصغر.	يتيح هذا المقياس توقع اتجاه التقدّم المُحرز وإعادة الضبط للتأثير على المقياس السابق.
متوسط وقت الاحتواء، حسب الأهمية	المتوسط الحسابي للوقت المستغرق منذ تحديد الثغرة الأمنية حتى اللحظة التي يتم فيها احتوائها أو تصحيحها.	يمثّل هذا المقياس المدة الفعلية للتعرض، ويُعد المقياس الأساسي للخدمة الذي يجب تحسينه باستمرار.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

إدارة السجلات

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
نسبة التغطية، حسب مصدر السجل	ما هي نسبة مصادر السجل المجمّعة من الأجهزة المنتجة لها؟	يمثّل هذا المقياس مقدار الوضوح الشامل للحلول النهائية المتعلقة بنظام إدارة المعلومات والحوادث الأمنية أو نظام الكشف والاستجابة الممتدة
الدقة، حسب مصدر السجل	نسبة السجلات المعدّة كما هو مُتوقع والتي تحتوي على بيانات صحيحة.	يمثّل هذا المقياس موثوقية السجلات المُدخلة. يُمكن أن يختلف تفسير السجلات لمعيار RFC باختلاف الشركة المصنّعة. وبمرور الوقت، يُمكن أن تتسبب المشكلات أيضاً في عدم دقة السجل، على سبيل المثال عندما يصبح المؤقت الداخلي لمصدر البيانات غير دقيق.
القدرة على إدخال السجلات، حسب مصدر السجل	نسبة الوقت المستغرق في جمع البيانات ومعالجتها في الوقت المحدّد، مع وجود مقدار مقبول من التأخير.	تعتمد المراقبة الأمنية الدقيقة والسريعة على وقت ومدى توفّر المعلومات. لذلك يُعد هذا المقياس مؤشراً رئيسياً لخدمة إدارة السجل ككل.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

إدارة حالات الاستخدام

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
عدد حالات الاستخدام	العدد الإجمالي لحالات الاستخدام الموجودة	ازدياد هذا الرقم ليس دائماً مؤشراً إيجابياً، إلّا أن هذا المقياس مفيد على نحوٍ خاص أثناء تحديد حالات الاستخدام لتصل إلى مستوى الاستعداد المطلوب. ومن الجانب الآخر، يُمكن أن يساعد هذا المقياس في تحديد سيناريو يكون فيه تواجد عدد كبير جداً من حالات الاستخدام دليلاً على نقص الكفاءة في الإدارة الشاملة.
معدل الإنذارات الحقيقية، حسب حالات الاستخدام	عدد الإنذارات الحقيقية مقسومة على مجموع الإنذارات الحقيقية والكاذبة. ويشار إلى ذلك غالباً بالحساسية.	يوفّر هذا المقياس معدل دقة حالات الاستخدام. فما مدى ثقتنا بقدرتنا على اكتشاف وقوع حدث ما؟
معدل الإنذارات الكاذبة، حسب حالات الاستخدام	عدد الإنذارات الكاذبة مقسومة على مجموع الإنذارات الحقيقية والكاذبة. ويشار إلى ذلك غالباً بالنوعية.	يعطي هذا المقياس معدل الخطأ في حالات الاستخدام أو القدرة على تحمل نتيجة الإنذارات الكاذبة. فما مدى ثقتنا في صحة تفسيرنا للحدث؟ فما مقدار الإنذارات الكاذبة التي يُمكن أن نقبلها لنقلل احتمالية تجاهل حدث حقيقي؟
دورية حالات الاستخدام	عدد حالات الاستخدام التي تعمل ضمن فئة معينة من الدورية: شبه فوري (أقل من 5 دقائق) # نحو 15 دقيقة # نحو كل ساعة # على نحوٍ يومي # على نحوٍ أسبوعي # على نحوٍ شهري	يساعد هذا المقياس في تخطيط أثر أداء حالات الاستخدام.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

نظام إدارة المعلومات والحوادث الأمنية/ نظام الكشف والاستجابة الممتدة

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
سعة نظام إدارة المعلومات والحوادث الأمنية/ نظام الكشف والاستجابة الممتدة (مساحة قرص التخزين)	نسبة استخدام قرص التخزين	يُعد هذا المقياس **مؤشر على قدرة البنية التحتية لدعم الكشف عن الحوادث.**
أداء نظام إدارة المعلومات والحوادث الأمنية/ نظام الكشف والاستجابة الممتدة (ذاكرة الوصول العشوائي)	نسبة استخدام ذاكرة الوصول العشوائي	يُعد هذا المقياس مهماً لتخطيط دورية وكفاءة حالات الاستخدام، ويساعد في توقع متطلبات التحديث.
أداء نظام إدارة المعلومات والحوادث الأمنية/ نظام الكشف والاستجابة الممتدة (وحدة المعالجة المركزية)	نسبة استخدام وحدة المعالجة المركزية	يُعد هذا المقياس مهماً لتخطيط دورية وكفاءة حالات الاستخدام، ويساعد في توقع متطلبات التحديث.
استخدام الرخص	نسبة استخدام الرخص	يساعد في توقع متطلبات التحديث.
توفّر نظام إدارة المعلومات والحوادث الأمنية/ نظام الكشف والاستجابة الممتدة	النسبة المئوية لفترة تشغيل منصة نظام إدارة المعلومات والحوادث الأمنية/ نظام إدارة المعلومات والحوادث الأمنية/ نظام الكشف والاستجابة الممتدة	يدل هذا المقياس بصورة مباشرة على القدرة على تنفيذ المراقبة الأمنية.

7.1 المعايير الأساسية لرفع التقارير والمراقبة

نظام كشف ومنع الاختراقات

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
معدل الإنذارات الحقيقية، حسب الجهاز الأمني	عدد الإنذارات الحقيقية مقسومة على مجموع الإنذارات الحقيقية والكاذبة. ويشار إلى ذلك غالباً بالحساسية.	يوفّر هذا المقياس معدل دقة الجهاز الأمني. فما مدى ثقتنا بقدرتنا على اكتشاف وقوع حدث ما؟
معدل الإنذارات الكاذبة، حسب الجهاز الأمني	عدد الإنذارات الكاذبة مقسومة على مجموع الإنذارات الحقيقية والكاذبة. ويشار إلى ذلك غالباً بالنوعية.	يعطي هذا المقياس معدل الخطأ في الجهاز الأمني أو القدرة على تحمل نتيجة الإنذارات الكاذبة. فما مدى ثقتنا في صحة تفسيرنا للحدث؟ فما مقدار الإنذارات الكاذبة التي يُمكن أن نقبلها لنقلل احتمالية تجاهل حدث حقيقي؟

7.1 المعايير الأساسية لرفع التقارير والمراقبة

نظام تنسيق الأمن والأتمتة والاستجابة

مؤشر الأداء الرئيسي	الوصف	الغرض المنشود
إجمالي عدد الأدلة	عدد الأدلة المتعلقة بنظام تنسيق الأمن والأتمتة والاستجابة (SOAR)	يمثّل عدد الإجراءات المؤتمتة جزئياً أو كلياً.
عدد الأدلة المؤتمتة كلياً	عدد الأدلة المتعلقة بنظام تنسيق الأمن والأتمتة والاستجابة (SOAR) التي لا تتطلب أتمتة يدوية	يمثّل عدد الإجراءات المؤتمتة كلياً. يُعد مقياساً لمقدار أتمتة البيئة.
معدل النجاح، حسب دليل المبادئ	النسبة المئوية للمرات التي نجح فيها نظام تنسيق الأمن والأتمتة والاستجابة (SOAR) في تنفيذ نشاط ما، عند تنشيطه للقيام بذلك.	يشير هذا المقياس إلى جودة أدلة معدة على نحوٍ جيد، ومدى موثوقية نظام تنسيق الأمن والأتمتة والاستجابة (SOAR).

التقارير التشغيلية

يجب أن تتضمن التقارير التشغيلية التغييرات اليومية والأسبوعية التي تغطي جميع المقاييس المدرجة ذات الصلة، وتستهدف الخبراء في المجال التقني، وتستخدم البيانات لتحديد المشكلات العامة في مراكز العمليات الأمنية ومعالجتها.

التقارير التنفيذية

يجب أن تنقل التقارير التنفيذية صورة واضحة وموجزة للحالة الأمنية السابقة والحاضرة والمستقبلية للمؤسسة، ويجب أن تشمل هذه التقارير ما يلي:

- الثغرات الأمنية: ما الذي نتعرض له؟
- الأحداث الأمنية والمراقبة: ما هو النشاط الخبيث الذي لاحظناه؟
- الحوادث: كيف تعاملنا معها؟
- التحليل الذكي للمخاطر: ما الذي يجب أن نكون مستعدين له؟

تقارير الحوادث

مشمولة في القسم الخامس

7.2 الاعتبارات المتعلقة بالحوسبة السحابية

نالت الحوسبة السحابية شعبية كبيرة لما لها من مزايا مالية واضحة، لذلك لا يُمكن تجاهلها كمتغيّر شائع في التخطيط والامتثال لمراكز العمليات الأمنية، إلّا أنه لا تزال الحوسبة السحابية موضوعاً معقداً. وتغطي الحوسبة السحابية نماذج خدمات متعددة (البرمجيات كخدمة SaaS، والمنصة كخدمة PaaS، والبنية التحتية كخدمة IaaS، وغيرها)، كما توظف أساليب نشر متعددة، وهي: خاصة وعامة ومختلطة ومجتمعية. وينتج عن كل نموذج وخدمة مخاوف أمنية وتحديات هيكلية خاصة بها، ويترتب على ذلك عدة آثار، حيث توظف هذه البيئات نموذج المسؤولية المشتركة الذي يعمل على تقسيم المخاطر والمسؤوليات الأمنية بين مقدّمي الخدمات السحابية والمستخدمين.

ويتولى مقدّم الخدمات مسؤولية الأمن والمخاطر وتعرض البنية التحتية والبيانات والتطبيقات، أما المستخدم فتقع على عاتقه مسؤولية الحفاظ على أمن الشيفرة واستخدام التطبيق وتوظيف خاصية مصادقة قوية. تشمل المخاطر الأمنية الرئيسية الخاصة بالحوسبة السحابية ما يلي:

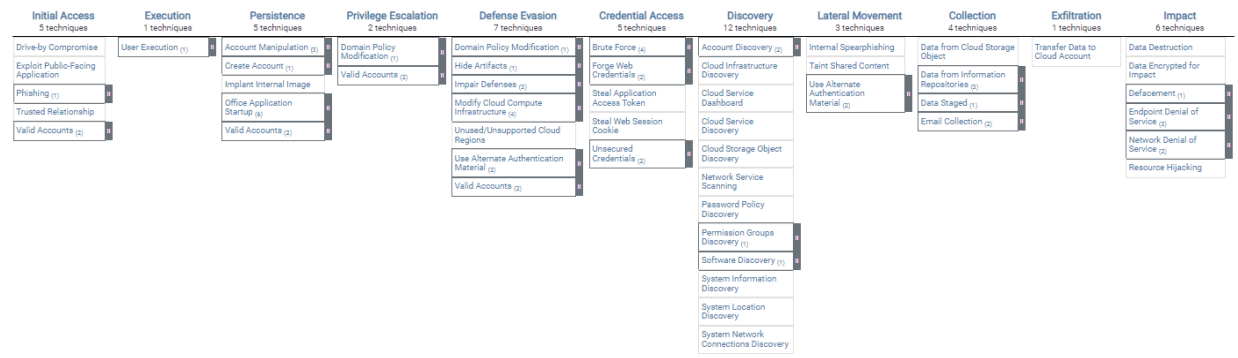
- **التهديد الداخلي:** يُعد هذا النوع من التهديدات أكثرها شيوعاً في أي بيئة، إلّا أنه يمثّل تحدياً كبيراً خاصة في بيئة الحوسبة السحابية لأن مقدّم الخدمات هو الجهة الوحيدة التي تستطيع الوصول إلى البيانات بشكلها المادي.
- **الفشل في عزل البيانات:** يتشارك مستخدمو الحوسبة السحابية بالبنية التحتية للسحابة، لذلك لا تزال هناك مخاوف كبيرة من تمكن مستخدم آخر من الوصول إلى بيانات ليست له.
- **اختراق منصات مراقبة الأجهزة الافتراضية Hypervisor:** على الرغم من إمكانية توقع هذا النوع من المخاطر، إلّا أن هناك تخوف من تعرض منصة مراقبة الأجهزة الافتراضية إلى الاختراق ضمن البنية التحتية السحابية لمقدّم الخدمات، حيث يؤدي ذلك إلى إتاحة الوصول بالكامل إلى البيانات الخاصة بالمؤسسة.

7.2 الاعتبارات المتعلقة بالحوسبة السحابية

من منظور مركز العمليات الأمنية، يتمثّل التحدي المتعلق بالمخاوف المذكورة أعلاه في الافتقار إلى الوضوح والحاجة إلى انتظار استجابة مقدّم خدمة الحوسبة السحابية. ولا توجد قدرات جنائية جيدة، إن وجدت بالأساس، في حالات تطبيق الحوسبة السحابية التجارية، كما لا يوجد عادةً وصول إلى قرص تخزين أو إمكانية جمع ذاكرة الوصول العشوائي لاستخدامها في تحليل تقني أكثر تعمقاً. لذلك، يجب التعامل بعناية فائقة مع عملية تحديد البيانات التي سترفع على البنية السحابية التي تقع خارج نطاق التحكّم المباشر للمؤسسة، كما يجب النظر في إدراج منطقة غير موثوقة أو شبه موثوقة يتم فيها مراقبة جميع عمليات الوصول من خلال نقطة جمع ومراقبة واحدة، مثل: وسيط أمان الوصول إلى السحابة.

وهو برنامج يقع بين المستخدم وحوسبة الحافة، ويعمل على جمع الاتصالات بين الطرفين وفرضها ومراقبتها.

كما تُعد السجلات الناتجة عن وسيط أمان الوصول إلى السحابة إحدى أكثر مصادر البيانات قيمة بالنسبة إلى مركز العمليات الأمنية. سيوفّر أيضاً القدرة على فرض أو إنهاء الاتصال مع السحابة. وعند استخدام السحابة، يجب مواءمة حالات الاستخدام مع مصفوفة الحوسبة السحابية التابعة لإطار MITRE ATT&CK.



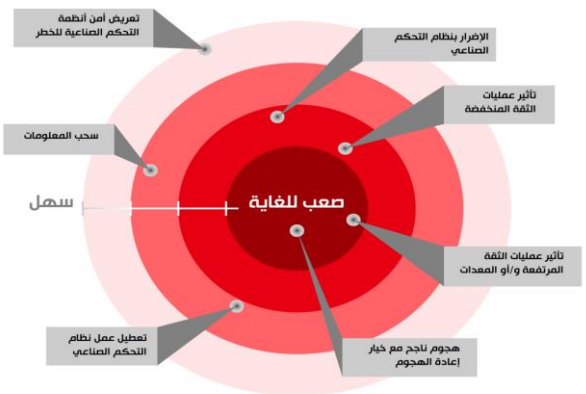
7.3 الاعتبارات المتعلقة بأنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT)

إن الانتشار المتزايد لأنظمة التحكّم الصناعية (ICS) وغيرها من التكنولوجيا التشغيلية (OT) يجعل الاستمرار في التعامل معها كمجال متخصّص منفصل أمراً صعباً، خاصة مع تزايد المؤسسات التي تسعى إلى ربط هذه الأنظمة بتكنولوجيا المعلومات التقليدية الخاصة بها، مما يعرضها إلى مخاطر ناتجة عن منفذي الهجمات عن بُعد. يجب أن تتمكن مراكز العمليات الأمنية الحديثة من تحديد أوجه التشابه والاختلاف بين مراقبة شبكة أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) وحمايتها.

تُعد التكنولوجيا الجنائية وتكنولوجيا الكشف المخصّصة لأنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) قليلة ومحدودة القدرات. لذلك، يعد عزل شبكة أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) والتحكّم بصلاحية الوصول لها النهج الأكثر فاعلية من حيث التكلفة، حيث يعتمد على قدرات مركز العمليات الأمنية المتفوقة من حيث أمن تكنولوجيا المعلومات التقليدية. كما يُعد تتبع تنفيذ شبكة أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) أمراً بالغ الأهمية.

من الجدير بالذكر أن هجمات أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) معقدة للغاية عكس المعتقدات الشائعة وذلك يعود إلى الطبيعة المخصّصة لجميع عمليات التطبيق. يتركّز سوق أجهزة التحكّم المنطقي القابلة للبرمجة (PLCs) على عدد قليل من الجهات الكبيرة، ومع ذلك يوجد أكثر من 250 بروتوكولاً خاصاً بأنظمة التحكّم الصناعية، بالإضافة إلى عدد كبير من الأنواع المختلفة من أجهزة الاستشعار والمشغلات. وغالباً ما تكون بنية وتطبيقات هذه الأجهزة مخصّصة لتلبية متطلبات المستخدم، فيكون من الصعب فهم التفاعلات بين الأجزاء المختلفة من النظام العام بالكامل.

لذلك يجد كل من الطرف المدافع ومنفذي الهجمات صعوبة في التعامل مع هذا التعقيد. يجب أن يقضي أي منفذ الهجمات ينوي استغلال وصولها إلى النظام وقتاً طويلاً داخل الشبكة لدراسة وظيفتها وبنيتها قبل أن يتمكن من التخطيط لهجوم واختباره ثم تنفيذه بنجاح.



صعوبة شن الهجمات على نظام التحكّم الصناعي

7.3 الاعتبارات المتعلقة بأنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT)

على هذا النحو، يُمكننا تقسيم هجمات نظام التحكّم الصناعي إلى مرحلتين منفصلتين، لكل منها سلاسل إيقاف الهجمات السيبرانية مميّزة:

تمثّل المرحلة الأولى وقوع حادث قياسي لأمن تكنولوجيا المعلومات، حيث يتمكّن منفذ الهجمات من الوصول إلى شبكة أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT)، ثم يبدأ في دراسة المرحلة التالية من الهجوم والتخطيط لها. تُعد هذه النقطة أفضل فرصة لاعتراض وإيقاف الهجوم، كما أنها تمثّل التحدي الأقل تعقيداً، حيث يتماشى هذا مع حزمة الكشف والحماية التقليدية، ومع العمليات والخدمات الحالية الخاصة بمركز العمليات الأمنية.

7.3 الاعتبارات المتعلقة بأنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT)

تمثّل المرحلة الثانية تحدياً أكبر، حيث إنها تشتمل على قيود وخصوصيات بيئة أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) التي يجب التعامل معها ضمن النهج المتبع في الكشف عن الحوادث وإدارتها. حيث وفي هذه المرحلة، يستغل منفذ الهجمات وصوله غير المكتشف لمراقبة النظام أو تعديله أو تدميره.

تُعد شبكات أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) ثابتة نسبياً مما يمنح مركز العمليات الأمنية أفضلية أخرى عند التعامل معها، ذلك لأنها لا تتغيّر بنفس الوتيرة الذي تتغيّر بها شبكة تكنولوجيا المعلومات العادية. في هذه الحالة، من الضروري جمع معلومات دقيقة عن نسبة استخدام الشبكة الاعتيادية على الشبكة وإعدادات العُقد. يُتوقع أن توظف جميع عمليات استخدام شبكات أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) في البنية التحتية الحيوية أداة متقدّمة لتحديد أصول النظام التحكّم الصناعي. كما يوصى أيضاً باستخدام هذه الأداة المتقدّمة في البنية التحتية غير الحيوية، مع توفّر مشاريع مفتوحة المصدر كبديل.

نطاق المؤسسة	المستوى الخامس	شبكة المؤسسة
	المستوى الرابع	تخطيط الأعمال والخدمات اللوجستية
نطاق التصنيع	المستوى الثالث	عمليات المواقع والتحكّم
نطاق الخلية/المنطقة	المستوى الثاني	التحكّم الإشرافي بالمنطقة
	المستوى الأول	التحكّم الأساسي
	المستوى التمهيدي	العملية

7.3 الاعتبارات المتعلقة بأنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT)

يجب أن يستخدم كل مركز عمليات أمنية متقدّم كل خدمة من خدماته التقليدية عند تشغيل شبكات أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT)، مع مراعاة الاعتبارات التالية:

المراقبة الأمنية

- يجب إعداد نقاط جمع البيانات ونقاط الخنق في الشبكة ومراقبتها عن كثب.
- يجب مراقبة التغييرات في إعدادات أو بنية شبكة أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) عن كثب.
- يجب أن يكون الانتقال إلى عملية إدارة الحوادث محدوداً ويخضع لموافقة الإدارة العليا. تستهلك الاستجابة للحوادث ضمن بيئة أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) وقتاً طويلاً ويُحتمل أن تتسبب في انقطاع الوصول إلى النظام، لذلك يجب اتخاذ هذا القرار بعناية أكثر مقارنة بشبكات تكنولوجيا المعلومات.
- قد لا يوصى بوضع أجهزة مراقبة مضمنة على شبكة أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) بسبب المخاطر التي يُمكن أن تتعرض لها العمليات، لذا يجب توخي الحذر الشديد في التعامل مع هذا الأمر.

إدارة الحوادث

- الأدوات الجنائية المتوفّرة لشبكة أنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT) محدودة للغاية، إذ أن هذا المجال لا يزال قيد البحث.
- تحتوي كل من وحدات التحكّم المنطقية القابلة للبرمجة (PLC) وأجهزة الاستشعار والمشغلات على ذاكرة صغيرة مباشرة وقرص صلب مما يبسط متطلبات الأجهزة
- يُحتمل أن تؤدي محاولات استخلاص البيانات إلى تعطل الجهاز، لذا يجب الافتراض بأنها ستتسبب بانقطاع الوصول.
- تحدث الغالبية العظمى من الحوادث مباشرة على أنظمة واجهة تفاعل الإنسان والآلة، والتي تعمل عادةً على نظام تشغيل ويندوز قديم، مما يُمكننا من توظيف أساليب الاستجابة التقليدية للحوادث

التحليل الذكي للمخاطر

- يجب الحصول على موجزات متخصّصة لبيانات تهديد شبكة ICS/OT.
- من المهم أن يتم تحديد وتقليل المعلومات الموجودة على الإنترنت حول توظيف شبكة ICS/OT حيث يساعد ذلك على زيادة الوقت الذي يحتاجه منفذ الهجمات داخل الشبكة.

7.3 الاعتبارات المتعلقة بأنظمة التحكّم الصناعية (ICS) والتكنولوجيا التشغيلية (OT)

تتبع التهديدات

- يجب تطوير سلاسل إيقاف الهجمات السيبرانية المخصّصة لعمليات نشر محدّدة لشبكات ICS/OT
- يجب تنفيذ عمليات تتبع التهديدات على سلاسل إيقاف الهجمات السيبرانية إلى حدٍ أكبر مقارنة بشبكات تكنولوجيا المعلومات العادية
- يتمثّل أحد المُخرجات الرئيسية لتتبع التهديدات بتحديد الوضع الاعتيادي والانحراف المتوقع الذي قد تسببه الأساليب والتكتيكات والإجراءات (TTP).
- في البيئات الحساسة جداً للتفاعل، يصبح من الضروري استنساخ بيئة مطابقة (أو شبكة مرجعية) في نطاق سيبراني افتراضي لغايات تنفيذ عمليات تتبع التهديدات.

إدارة الثغرات الأمنية

- يجب توخي الحذر الشديد عند التخطيط والإبلاغ عن التصحيحات ضمن هذه البيئات. حيث أن ما يقدّر بنحو 80% من ثغرات أنظمة التحكّم الصناعية ICS لا يُمكن معالجتها أو من غير الضروري منع ذلك بسبب وجود وضع أكثر خطورة مثل انعدام أمن جهاز معيّن. فعلى سبيل المثال، لا تُعد عيوب التنفيذ عن بُعد مهمة إذا كان الجهاز في تصميمه يسمح بالمصادقة المجهولة. ويتطلب التصحيح غالباً حدوث انقطاع خطير في النظام، لذا يجب أن تعمل خدمة إدارة الثغرات الأمنية على تحديد الحالة الأكثر أهمية، بالإضافة إلى الحالة التي تكون فيها الفائدة الناتجة أكبر من المخاطر المترتبة ومشكلة انقطاع عمل النظام.
- يتمثّل إدارة مسار الهجوم نهج يركّز على تحديد نقاط الخنق الطبيعية التي يجب التعامل معها لضمان نجاح الهجوم، وتُعد مهمة خاصة في بيئات التكنولوجيا التشغيلية. يسمح هذا النهج بالحد من نطاق وتعقيد عمليات التصحيح والتقوية اللازمين لبناء بنية تحتية أكثر قوة ومرونة. ويجب أن يقوم مركز العمليات الأمنية القادر على التعامل مع التكنولوجيا التشغيلية أو مركز حلول الكشف والاستجابة المدارة MDR أو مركز الدمج بتنفيذ هذا النهج لإدارة تعرض البيئة بكفاءة.

إدارة حالات الاستخدام

- يجب توسيع نطاق حالات الاستخدام لتشمل إطار عمل ICS/OT MITRE Att&ck
- يجب تصميم حالات الاستخدام لتشمل بيئة أجهزة المستشعر الذكي/ إنترنت الأشياء سريعة التغيّر داخل شبكات التكنولوجيا التشغيلية

7.4 الوثائق المرجعية

المعايير الدولية

يوضّح الجدول التالي المصادر الدولية المشار إليها في هذه الوثيقة.

الهيئة/ الجهة	الوثيقة
نموذج جاهزية القدرات لمركز العمليات الأمنية	نموذج جاهزية القدرات لمركز العمليات الأمنية
MITRE	ATT&CK

7.5 الاختصارات

الهيئة/ الجهة	الوثيقة
SOC	مركز العمليات الأمنية
CII	البنية التحتية للمعلومات الحيوية
NSOC	المركز الوطني للعمليات الأمنية
C&C	خادم الأوامر والتحكّم
CIA Triad	السرّية والتوفّر والسلامة
ICS	أنظمة التحكّم الصناعية
OT	التكنولوجيا التشغيلية
IoT	إنترنت الأشياء
SIEM	نظام إدارة المعلومات والحوادث الأمنية
XDR	الكشف والاستجابة الممتدة
CMMI	نموذج تكامل جاهزية القدرات
SLA	اتفاقية مستوى الخدمات
KPI	مؤشر الأداء الرئيسي
PIA	تقييم أثر الخصوصية
FTE	موظف بدوام كامل
HVAC	تمديدات الكهرباء، والتدفئة، والتهوية، والتكييف
TTP	الأساليب والتكتيكات والاجراءات
IDPS	نظام كشف ومنع الاختراقات .
IoC	مؤشرات الاختراق
NBA	تحليل سلوك الشبكة
NAC	نظام ضبط الدخول إلى الشبكة
DLP	الحماية من تسريب البيانات
EDR	كشف الأجهزة الطرفية وتصحيحها
API	واجهة برمجة التطبيقات
DDoS	هجمات الحرمان من الخدمة الموزعة
WAF	جدار الحماية الخاص بتطبيق الويب
CWPP	منصة حماية عبء العمل السحابي
CASB	وسيط أمان الوصول إلى السحابة
CSPM	إدارة وضع الأمان السحابي
ISP	مقدّم خدمات الإنترنت
SOAR	نظام تنسيق الأمن والأتمتة والاستجابة
IAM	إدارة الهوية وصلاحية الوصول
IR	الاستجابة للحوادث
RACI	مصفوفة الأدوار والمسؤوليات
TTP	الأساليب والتكتيكات والاجراءات
SOP	الإجراءات التشغيلية القياسية