

## خطة الاستجابة للحوادث / اختراق البيانات

stc

الإصدار 1.0

تاريخ الإصدار: 30 يونيو 2024

التصنيف: عام

## المحتويات

المقدمة.....	3
فهم تأثيرنا الواسع.....	3
قدراتنا في مجال الأمن السيبراني.....	3
نظرة عامة على برنامج الاستجابة للحوادث.....	4
التعرف على الحوادث وفرزها.....	4
تنسيق الاستجابة وتقديم الإرشادات.....	4
التحليل الجنائي.....	5
الإبلاغ عن الحوادث.....	5
عملية الاستجابة للحوادث.....	5
الهيكل التنظيمي - الأدوار والمسؤوليات.....	9
التدريب والتوعية.....	9
الخاتمة.....	10
الملحق: التعريفات.....	10

## المقدمة

يستمر مشهد التهديدات السيبرانية العالمية في التطور والنمو، ويصبح الاكتشاف المبكر والاستجابة السريعة لحوادث الأمن السيبراني واختراق البيانات أمرًا بالغ الأهمية للتخفيف من تأثيرها على عملنا وشركائنا وأصحاب المصلحة وعبر stc .

تعد stc محرك التحول الرقمي في المنطقة، حيث تقدم مجموعة شاملة من الخدمات التي تشمل البنية التحتية الرقمية والحوسبة السحابية والأمن السيبراني وإنترنت الأشياء (IoT) والذكاء الاصطناعي (AI) والمدفوعات الرقمية والإعلام الرقمي والترفيه الرقمي عبر المملكة العربية السعودية ومنطقة الشرق الأوسط وشمال إفريقيا (MENA) وأوروبا. دورنا الهام في تقديم العديد من الخدمات الهامة يعزز التزامنا بممارسات الأمن السيبراني القوية. فهماً لأهمية خدماتنا، قمنا بتطوير خطة شاملة للاستجابة لحوادث الأمن السيبراني تتوافق مع اللوائح الوطنية وأفضل الممارسات الدولية. بالإضافة إلى ذلك، نقوم بدمج الاستدامة في عمليات الأمن السيبراني لدينا للمساهمة بشكل إيجابي في الأهداف البيئية والاجتماعية والحوكمة (ESG) التي نسعى لتحقيقها سنويًا.

## فهم تأثيرنا الواسع

مصنفة كجزء من البنية التحتية الحيوية الوطنية، تدرك stc التأثير الواسع لحوادث الأمن السيبراني على عملنا وشركائنا وأصحاب المصلحة والمملكة العربية السعودية ككل. يضمن نهجنا في الاستجابة للحوادث قدرتنا على إدارة أي حادث بسرعة وفعالية مع تقليل الاضطرابات والحفاظ على الثقة التي وُضعت فينا. نحن نعمل بشكل وثيق مع الجهات التنظيمية لدينا مثل هيئة الاتصالات والفضاء والتقنية (CST) والهيئة الوطنية للأمن السيبراني (NCA) لضمان الامتثال والاستجابات المنسقة.

## قدراتنا في مجال الأمن السيبراني

تحتفظ stc بقدرات قوية في مجال الأمن السيبراني التي تلتزم بأعلى المعايير الدولية للأمن السيبراني، بما في ذلك ISO 27001، ISO 22301، NIST، SANS، CSA، OWASP، GSMA، و ENISA التي توجه نهجنا الشامل في اكتشاف الحوادث، والاستجابة، والتعافي. بالإضافة إلى ذلك، لدينا محترفون معتمدون من CREST لاختبار الاختراق وخدمات الاختراق الأخلاقي، حيث نقوم بالتحقق من أمان أنظمتنا، وتحديد نقاط الضعف، وتنفيذ إجراءات التصحيح لتعزيز دفاعاتنا ضد التهديدات السيبرانية المحتملة. كما أن stc عضو نشط في FIRST.org (متتدى فرق الاستجابة للحوادث والأمن)، حيث نتعاون مع خبراء الأمن السيبراني العالميين لمشاركة معلومات التهديدات، وأفضل الممارسات، واستراتيجيات الاستجابة للحوادث. يعزز مشاركتنا في FIRST من جاهزيتنا للاستجابة للحوادث ويدعم الحماية من حوادث الأمن السيبراني.

## نظرة عامة على برنامج الاستجابة للحوادث

برنامج الاستجابة للحوادث لدينا مُنظم حول أربع وظائف أساسية: تحديد وتصنيف الحوادث، تنسيق الاستجابة والإرشاد، التحليل الجنائي، وتقرير الحوادث. تم تصميم هذه الوظائف لضمان استجابة منهجية وفعالة لأي حادث أمن سيبراني.



## التعرف على الحوادث وفرزها

يقوم فريق إدارة الحوادث الأمنية (SIM) لدينا بإجراء تحقيقات شاملة لتصنيف الحوادث بدقة، وتحديد أوقات الاستجابة والحدود المناسبة. يتعاون فريق SIM مع فرق مراقبة التهديدات وإدارة الثغرات الأمنية لتعزيز فعالية التعامل مع الحوادث.

## تنسيق الاستجابة وتقديم الإرشادات

عمليات الاستجابة والتنسيق والإرشاد تتبع دورة حياة الاستجابة للحوادث وفقاً لمعايير NIST وتشمل عدة مراحل للاستجابة الفعلية للحوادث بهدف تقليل تأثير الحادث، والقضاء عليه والتعافي منه:

- الاحتواء
- القضاء على الحادث
- التعافي
- المتابعة بعد الحادث

## التحليل الجنائي

خلال الحوادث السيبرانية، يقوم فريق الاستجابة للحوادث بالاستعانة بالمحللين الجنائيين لجمع الأدلة وتحليلها وتخزينها (بما في ذلك الحفاظ على سلسلة الأدلة لتلبية المتطلبات القانونية والتنظيمية) وانتهاءً بإعداد تقرير بالنتائج. يتضمن التحليل الجنائي فحصاً شاملاً للحوادث لجمع الأدلة، وفهم الهجوم، وتحسين الاستجابات المستقبلية.

## الإبلاغ عن الحوادث

إجراءاتنا الصارمة للتقارير تضمن إبلاغ أصحاب المصلحة خلال وقت قياسي، والامتثال للمتطلبات التنظيمية، وتنفيذ الإجراءات التصحيحية بكفاءة. يُعد الإبلاغ الشفاف لفريق حماية البيانات والخصوصية في stc والهيئات التنظيمية مثل هيئة الاتصالات والفضاء والتقنية (CST) والهيئة الوطنية للأمن السيبراني (NCA) جزءاً أساسياً من التزامنا بالامتثال والمسؤولية.

## عملية الاستجابة للحوادث

كل استجابة فريدة من نوعها، تهدف عملية الاستجابة للحوادث حماية بيانات العملاء، واستعادة الخدمة في أسرع وقت ممكن، وتلبية المتطلبات التجارية والتنظيمية والتعاقدية. يصف الجدول التالي الخطوات الرئيسية في برنامج الاستجابة للحوادث الخاص بـ stc .

خطوة الاستجابة	الوظيفة الأساسية	الوصف	الأنشطة الرئيسية
التعرف على الحوادث وفرزها	التعرف على الحوادث وفرزها	يستخدم فريق إدارة الحوادث الأمنية (SIM) أدوات ومنهجيات متقدمة للتعرف على الحوادث وتصنيفها بسرعة وفقاً لمستويات الخطورة والتأثير المحددة. تعد هذه المرحلة الأولية مهمة لأنها تضع الأساس لإجراءات استجابة دقيقة وفعالة للحوادث.	<b>كشف الحوادث:</b> استخدام أدوات إدارة معلومات الأحداث الأمنية (SIEM) المتطورة لمراقبة واكتشاف الحوادث الأمنية المحتملة في الوقت الفعلي. <b>الفرز الأولي:</b> التقييم الفوري لخطورة الحادث وتصنيفه، لضمان الأولوية المناسبة وتخصيص الموارد.
			<b>الجاهزية الجنائية:</b> دمج قدرات التحليل الجنائي في وقت مبكر من دورة حياة الحادث، مما يتيح جمع البيانات وحفظها بشكل استباقي للتحليل المفصل.

<p><b>الإخطار والموافقة:</b> عند الاكتشاف، يخطر فريق إدارة الحوادث الأمنية الأطراف الرئيسية ويحصل على الموافقات اللازمة لمتابعة تدابير الاحتواء. يضمن ذلك أن تكون الإجراءات المتخذة مرخصة ومتوافقة مع أهداف استمرارية الأعمال.</p> <p><b>الحلول المؤقتة:</b> يتم اتخاذ إجراءات فورية للتخفيف من التأثير والحد من تقدم الحادث. قد تشمل هذه الإجراءات عزل الأنظمة المتضررة، حظر الوصول إلى الشبكة مؤقتاً، أو تنفيذ قواعد الجدار الناري لمنع الوصول غير المصرح به.</p> <p><b>المراقبة والتقييم:</b> في الوقت نفسه، يقوم الفريق بمراقبة الأنظمة المتضررة لجمع معلومات إضافية عن الحادث، يساعد هذا النهج الاستباقي في فهم نطاق الهجوم وأصله والتأثير المحتمل.</p> <p><b>اتخاذ القرار:</b> بناءً على خطورة وطبيعة الحادث، يقرر فريق إدارة الحوادث الأمنية ما إذا كان يجب الاستمرار في المراقبة أو المتابعة بإجراءات احتواء مشددة. توجه عوامل مثل سرية البيانات وأهمية النظام وتأثير العمليات على عملية اتخاذ القرار.</p>	<p>بعد اكتشاف حادث سببراني، يقوم فريق إدارة الحوادث الأمنية الخاص بstc بسرعة بتنفيذ تدابير الاحتواء لمنع المزيد من الضرر واستعادة العمليات للوضع الطبيعي.</p>	<p>تنسيق الاستجابة وتقديم الإرشادات</p>	<p>الاحتواء</p>
<p><b>الحل الجذري:</b> بعد تحديد وحل السبب الجذري للحادث أمراً بالغ الأهمية، على سبيل المثال، تصحيح الأنظمة الضعيفة أو إزالة البرامج الضارة يضمن عدم تكرار حوادث مماثلة.</p> <p><b>الحلول طويلة الأجل:</b> تنفيذ الإصلاحات الدائمة والتدابير الوقائية لتعزيز الدفاعات ضد الهجمات المستقبلية. قد يشمل ذلك مراجعة سياسات الأمان، وتحديث الاعداد المسبق، وتعزيز تجزئة الشبكة.</p> <p><b>التنسيق مع فرق تقنية المعلومات:</b> التعاون الوثيق مع فرق تقنية المعلومات ودعم الشبكة لضمان تنفيذ سلس لإجراءات القضاء على الحادث دون تعطيل العمليات التجارية.</p>	<p>بمجرد احتواء الحادث، يتحول التركيز إلى القضاء على السبب الجذري واستعادة الأنظمة المتأثرة إلى حالة أمان.</p>	<p>تنسيق الاستجابة وتقديم الإرشادات</p>	<p>القضاء على الحادث</p>
<p><b>استعادة البيانات:</b> استعادة أي بيانات فقدت أو تعرضت للخطر أثناء الحادث من النسخ الاحتياطية الآمنة. يضمن ذلك الحد الأدنى من الاضطراب في العمليات التجارية وخدمة العملاء.</p>	<p>بعد الاحتواء والقضاء على الحادث، يتحول التركيز إلى التعافي - استعادة الأنظمة والعمليات المتأثرة إلى حالتها قبل وقوع الحادث.</p>	<p>تنسيق الاستجابة وتقديم الإرشادات</p>	<p>التعافي</p>

<p><b>إزالة التدابير المؤقتة:</b> عكس التغييرات المؤقتة التي تم إجراؤها خلال مرحلة الاحتواء، مثل قواعد الجدار الناري أو العزل الشبكي، لاستعادة الاتصال الطبيعي للشبكة.</p> <p><b>التحقق والاختبار:</b> التحقق من الأنظمة المستعادة وإجراء الاختبارات لضمان أنها تعمل بشكل كامل وآمن. يشمل ذلك التحقق من سلامة البيانات وإجراء تقييمات الضعف بعد التعافي.</p>			
<p><b>تحليل الحادث:</b> إجراء تحليل شامل للحادث، بما في ذلك كيفية التعامل معه وفعالية الاستجابة. يتم توثيق الدروس المستفادة لتعزيز قدرات الاستجابة للحوادث المستقبلية.</p> <p><b>الإبلاغ والتوثيق:</b> إعداد تقارير الحادث التي تفصل زمن الحادث، والإجراءات المتخذة للاستجابة، والتوصيات للتحسينات. تعد هذه التقارير ضرورية للشفافية والامتثال للمتطلبات التنظيمية.</p> <p><b>التواصل مع أصحاب المصلحة:</b> ضمان التواصل الفوري مع أصحاب المصلحة، بما في ذلك الإدارة التنفيذية، وفرق تكنولوجيا المعلومات، والهيئات التنظيمية حسب الضرورة. تعزز هذه الشفافية الثقة وتظهر المسؤولية في إدارة الحوادث السيبرانية.</p>	<p>بعد التعافي، تقوم stc بإجراء أنشطة شاملة بعد الحادث لمراجعة وتحسين إجراءات الاستجابة للحوادث.</p>	<p>تنسيق الاستجابة وتقديم الإرشادات</p>	<p>المتابعة بعد الحادث</p>
<p><b>التوثيق:</b> يتم إعداد الوثائق قبل إجراء التحقيق الجنائي، مثل طلبات إجراء التحقيقات، ونماذج سلسلة الحفظ، وما إلى ذلك.</p> <p><b>التحضير:</b> ضمان أن الأدوات اللازمة، والأجهزة، والبرمجيات، والمعدات جاهزة وتعمل كما هو مخطط له.</p> <p><b>تقييم الحالة:</b> تحديد نطاق وأهداف التحقيقات والحصول على مزيد من المعلومات المتعلقة بالحادث. يشمل ذلك</p>	<p>يتم عادةً بدء هذه الخطوة خلال مرحلة التعرف على الحادث. يتم تنفيذها بشكل مستمر خلال الاستجابة حيث يجمع المحلل الجنائي الأدلة لتحليلها على خلال رحلة الاستجابة للحادث.</p>	<p>التحليل الجنائي</p>	<p>التحليل الجنائي</p>

<p>أيضًا حل أي مشكلات تقنية أو إدارية قد تعيق إكمال التحقيقات بنجاح.</p> <p><b>جمع الأدلة:</b> بمجرد تحديد الأدلة وجمعها، تكون الخطوة التالية هي استعادة الأدلة. تختلف طريقة جمع الأدلة بناءً على حالة الجهاز.</p> <p><b>التحليل:</b> في هذه الخطوة، يركز فريق التحقيق الجنائي على تحليل البيانات والأدلة التي تم جمعها. يتم إجراء التحليل باستخدام نوع التحليل المناسب.</p> <p><b>تخزين الأدلة:</b> عند الانتهاء من عملية التحليل، يجب تخزين الأدلة (مثل الصور وملفات القضية (سلسلة الحفظ، أوراق عمل تصوير القرص) بشكل صحيح في خزانة مغلقة أو صندوق أمان في مختبر التحقيق الجنائي.</p> <p><b>الإبلاغ:</b> يجب أن يحتوي التقرير على ملخص تنفيذي، النتائج والتوصيات، قائمة بالأدلة التي تم تحليلها، نتائج عمليات البحث المختلفة ووصف البرامج ذات الصلة.</p>			
<p><b>الإبلاغ الداخلي:</b> عند اكتشاف وتقييم أولي لحدث سيبراني، يقوم فريق إدارة الحوادث الأمنية (SIM) في stc ببدء إجراءات الإبلاغ الداخلي. تحدد خطورة الحادث مسار التصعيد:</p> <ul style="list-style-type: none"> <li>• <b>الحوادث الحرجة:</b> يتم الإبلاغ عنها فورًا لفريق إدارة الأزمات (CMT) عبر مكتب إدارة الأزمات لاتخاذ إجراء سريع وحاسم.</li> <li>• <b>الحوادث الكبيرة:</b> يتم الإبلاغ عنها لفريق التعافي التقني (TRT) لإجراء تحليل تقني شامل وتنسيق الاستجابة.</li> <li>• <b>الحوادث المتوسطة إلى المنخفضة:</b> يتم التعامل معها ضمن إدارة الحوادث الأمنية (SIM) أو الدفاع السيبراني، مع التصعيد المناسب حسب الضرورة.</li> </ul>	<p>الإبلاغ عن الحوادث سيكون المرحلة النهائية في إدارة الحوادث الأمنية. بناءً على الأنشطة التي يقوم بها معالجي الحوادث وأخصائيي الاستجابة للحوادث والمحللون الجنائيون، يجب إنهاء المعايير للإبلاغ.</p>	<p>الإبلاغ عن الحوادث</p>	<p>الإبلاغ عن الحوادث</p>

<p><b>الإبلاغ الخارجي:</b> بناءً على خطورة وطبيعة الحادث، تلتزم stc بالالتزامات التنظيمية للإبلاغ عن الحوادث للجهات الخارجية مثل هيئة الاتصالات والفضاء والتقنية (CST) والهيئة الوطنية للأمن السيبراني (NCA) ويتم تنفيذ هذه التقارير بأمان لحماية المعلومات الحساسة والحفاظ على الامتثال التنظيمي.</p>		
--	--	--

## الهيكل التنظيمي – الأدوار والمسؤوليات

تُهيكل فرق الاستجابة للحوادث لدينا بطريقة تعزز ليس فقط حل الحوادث، ولكن أيضاً تقوي وضعنا الأمني العام ضد التهديدات المتطورة. لدعم الأنشطة مثل التحقيق في الحوادث، والاستجابة، والأنشطة الجنائية، يتم تحديد أدوار مختلفة في فرق الاستجابة للحوادث الخاصة بـ stc. يشمل الهيكل التنظيمي مدير قسم إدارة الاستجابة للحوادث الأمنية، ومعالج الحوادث، وأخصائي الاستجابة، ومحللي التحقيق الجنائي. تتعاون الفرق بشكل وثيق مع بعضهم البعض مع أصحاب المصلحة الخارجيين حسب الحاجة لضمان حل سلس للحوادث.



### محللي التحقيق الجنائي لإدارة الحوادث الأمنية

يقوم بالأنشطة الجنائية، ويوثق النتائج، ويشارك التقارير مع أصحاب المصلحة من أجل التحسين المستمر.



### أخصائيي الاستجابة

يدير إجراءات الاستجابة للحوادث، ويجري تحليلات متقدمة، ويوفر توجيهات استراتيجية للاحتواء والقضاء على الحوادث.



### معالج الحوادث

يقود التحقيق في الحوادث وفرزها، ويضمن دقة تصنيفها، وينسق أنشطة الاستجابة.



### مدير قسم إدارة استجابة الحوادث الأمنية

يشرف على وظائف الاستجابة للحوادث، ويدير الموارد، ويضمن الامتثال لاتفاقيات مستوى الخدمة ومبادرات التحسين.

## التدريب والتوعية

في stc، ندرك أن الأمن السيبراني هو مسؤولية الجميع. ولضمان أعلى مستوى من الاستعداد، لدينا برامج تدريبية شاملة وحملات توعوية مصممة لتمكين الموظفين بالمعرفة والمهارات اللازمة للتخفيف من المخاطر وتحديد التهديدات ومعرفة كيفية الاستجابة الفعالة للحوادث السيبرانية. من خلال تزويدهم بالمعرفة والمهارات اللازمة لتحديد وإبلاغ التهديدات المحتملة، نخلق ثقافة الوعي بالأمن السيبراني في جميع أنحاء المنظمة. وتعزز هذه الثقافة قدرتنا على منع الحوادث والاستجابة لها بفعالية.

## الخاتمة

نضع على عاتقنا حماية عملياتنا والحفاظ على الثقة مع أصحاب المصلحة والشركاء والعملاء. تضمن خطة الاستجابة للحوادث والتي تتماشى مع المعايير الدولية والمتطلبات التنظيمية، الحماية الاستباقية ضد التهديدات السيبرانية وتعزز التزامنا بالأمان والشفافية والتحسين المستمر.

## الملحق: التعريفات

- **الحادث السيبراني:** انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني.
- **الحادث السيبراني:** شيء يحدث في مكان محدد (مثل الشبكة والأنظمة والتطبيقات وغيرها) وفي وقت محدد..
- **التهديد:** أي ظرف أو حدث من المحتمل أن يؤثر سلباً على أعمال الجهة (بما في ذلك مهمتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها مستغلاً أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية.
- **الثغرة:** أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يجعل الأمن السيبراني عرضة للتهديد.
- **الخطر السيبراني:** المخاطر التي تمس عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إدارتها أو صورتها أو سمعتها) أو أصول الجهة أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نظم المعلومات.
- **البيئية والاجتماعية والحوكمة (ESG):** وتشير إلى التأثير المستدام والأخلاقي للمنظمة على البيئة والمجتمع وممارسات الحوكمة.
- **السرية:** الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.