19

سياسة مراقبة الأحداث الأمنية

م/ سيف السياغي

بنود السياسة

- يجب على الجهات الحكومية تطبيق آلية لتحديد الحوادث ومراقبتها بهدف احتواء ومنع الحوادث الأمنية.
- يجب أن تكفل الجهات الحكومية أن سجلات الأنظمة ومعلومات الدعم الأخرى محفوظة لغرض إثبات وتتبع الحوادث الأمنية.
- يجب إجراء خطوات فورية في حال وجود احتمال اختراق لأي نظام وفقاً لخطوات معالجة الحوادث الأمنية الموثقة.
- يجب على الجهات الحكومية أن تنشئ وتوثق وتحفظ خطوات معالجة الحوادث الأمنية لأنظمة المعلومات التابعة لها.

عناصر السياسة

- المقدمة
- الاهداف
- النطاق
- بنود سياسة الأمن المادي والبيئي
- الأدوار والمسئوليات

المقدمة

هي مجموعة أجراءات وخطوات يتم اتباعها في الجهة الحكومية لحماية المعلومات . تضمن سير إجراءات الامن والحماية على جميع سجلات الأنظمة المعلوماتية والسجلات الخاصة بالأجهزة التقنية وعلى كل ما يختص بموار الشبكة وقواعد البيانات والتي يتم من خلالها الكشف عن وقوع الاحداث الأمنية التي نفذت على كل موارد الأنظمة المعلوماتية.

تتضمن

- مراقبة ورصد الأنشطة للكشف عن أي أنشطة غير عادية أو هجمات.
- اكتشاف التهديدات ومحاولات الاختراق.
- الاستجابة السريعة عند اكتشاف حادث أمني.
- تحليل وتقييم الحوادث لفهمها والتصدي لها.
- متابعة وتحسين الأمان المعلوماتي بشكل دوري.
- توثيق وإبلاغ عن الحوادث.

الهدف

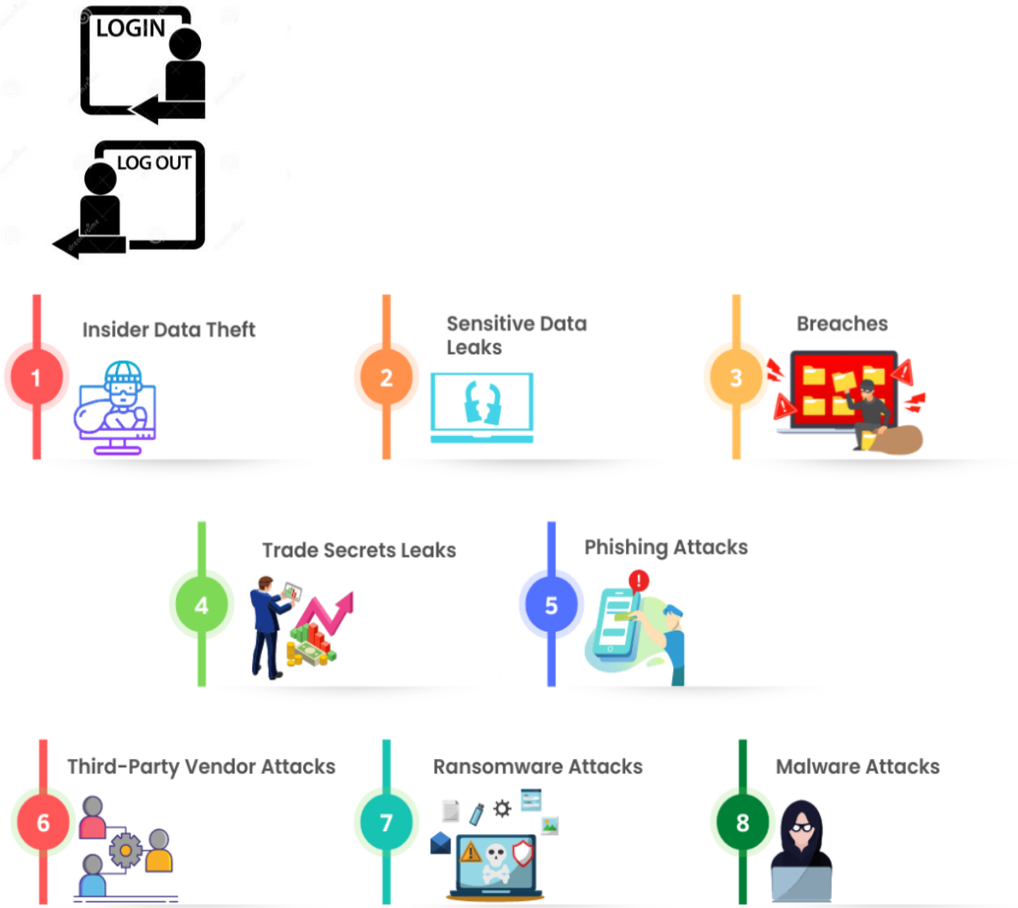
اكتشاف الأحداث الأمنية في وقت مبكر

تخفيف الأثر الضار للأحداث الأمنية

النطاق

تغطي هذه السياسة جميع الأحداث الأمنية التي يمكن أن تؤثر على الجهات الحكومية، بما في ذلك:

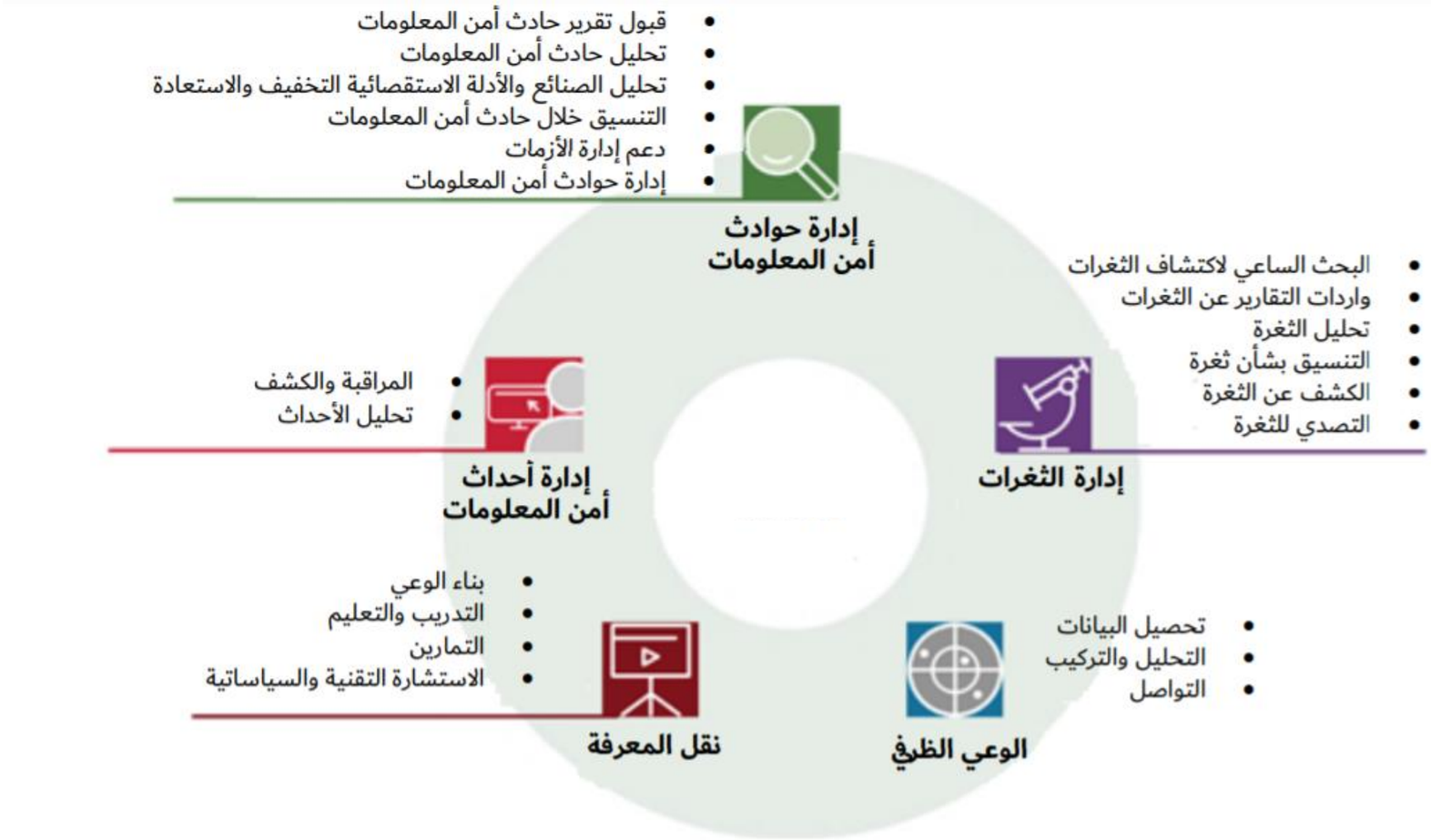
- **الاختراقات الأمنية:** أي وصول غير مصرح به إلى الأنظمة أو البيانات.
- **البرمجيات الضارة:** أي برنامج مصمم لإلحاق الضرر بالأنظمة أو البيانات.
- **فقدان البيانات:** أي فقدان أو تلف للبيانات.
- **الهجوم على البنية التحتية:** أي هجوم على الأنظمة أو الشبكات أو البنية التحتية الأخرى.
- **التهديدات البشرية:** أي نشاط ضار من قبل شخص، مثل سرقة المعلومات أو التلاعب بها.



الادوات التي تساعد في مراقبة الأحداث الأمنية:

- استخدام أحد انظمة إدارة الأحداث الأمنية: يمكن استخدام نظام إدارة الأحداث الأمنية لجمع وتحليل البيانات من أجل اكتشاف الأحداث الأمنية.
- استخدام أدوات المراقبة: يمكن استخدام أدوات المراقبة، مثل أدوات المراقبة للشبكة، وأدوات المراقبة للتطبيقات، لاكتشاف الأحداث الأمنية.
- استخدام أدوات التحليل: يمكن استخدام أدوات التحليل، مثل أدوات تحليل البيانات، وأدوات تحليل السلوك، لاكتشاف الأحداث الأمنية.
- تدريب الموظفين: يجب تدريب الموظفين على كيفية اكتشاف الأحداث الأمنية وكيفية الإبلاغ عنها

دورة حياة إدارة حوادث أمن المعلومات



الأدوار والمسئوليات

مسئولية الجهة على سبيل المثال

يجب أن تضمن الجهة على أن كل الانظمة محفوظة بشكل كامل وبصورة دورية لأجل تتبع الحوادث الأمنية للعمل على حلها واسترجاعها وقت الحاجة.

يجب أن تضمن الجهة أن سجلات الأنظمة وموارد المعلومات الأخرى محفوظة لغرض إثبات، تتبع الحوادث الأمنية فقط.

يجب على الجهة إنشاء آلية لتحديد الحوادث ومر اقبتها لمنع الحوادث الأمنية.