**الدائرة: برنامج الحكومة الإلكترونية**

| 1- معلومات اساسية عن الوظيفة |
| --- |
| 1.1 مسمى الوظيفــة: محلل أمن معلومات |
| 2.1 الادارة/ المديرية: برنامج الحكومة الإلكترونية |
| 3.1 القسم/الشعبة: أمن المعلومات |
| 4.1 مسمى وظيفة الرئيس المباشر: رئيس قسم البنية التحتية وامن المعلومات |

**3-غرض الوظيفة**

- تحليل الحوادث الامنية و الاستجابة لها

**4- المهام والواجبـــات :**

- تحليل سجلات نظام ادارة امن المعلومات و الحوادث (SIEM ) لمختلف الانظمة ( firewall , IPS , proxy , email getaway ..etc ) لتحديد الحوادث الامنية المحتملة.
- انشاء و تعديل و ادارة قواعد (Rules) و واجهات (Dashboards) نظام ادارة امن المعلومات و الحوادث (SIEM)
- تحليل الاشعارات و التنبيهات الامنية لتحديد و ترتيب اولويات التهديدات و الثغرات
- انشاء التذاكر(Ticket) للتنبيهات والتهديدات الامنية
- تحليل وتقييم أنشطة الاستجابة للحوادث الامنية لضمان اتخاذ الإجراءات المناسبة وتقليل احتمالات حدوثها في المستقبل.
- مراجعة و تجميع بيانات الاجهزة ( configuration , running process , ..etc) من النظام من اجل المزيد من التحقيقات
- ادرة المجتوى (content development) وإنشاء الواجهات (dashboard) واعداد التقارير بستخدام ادوات نظام ال (SIEM)
- مهارة إعداد التقارير الفنية والتواصل مع الفريق.
- معهارة كابة التقارير الإدارية وأداء العروض التقديمية.
- تحديد الأنظمة المتأثرة ونطاق الهجوم بالاستفادة من ال ( threat intelligence) مثل ( IOCs , update rules , ..etc )
- التعامل مع مختلف صيغ السجلات ( log format ) لمختلف الانظمة.
- خبرة في تشغيل نظام ادارة امن المعلومات والحوادث (SIEM) مثل ArcSight (preferred), Splunk, IBM QRadar, or McAfee Nitro من حيث انشاء , تعديل و ادارة القواعد (rules) , ترابط الاحداث ( correlation of events ) و الاستعلام (queries )
- خبرة في استخدام و اعداد مختلف ادوات المراقبة و التحليل الامنية

- خبرة في انشاء التعابير ((RegEx) لاستخدامها في الاستعلام (querying)

**المتطلبات الاساسية والاضافية لاشغال الوظيفة**

- **المؤهل العلمي والخبرات:**
  - شهادة البكالوريوس في تكنولوجيا المعلومات أو في أي من الحقول العلمية ذات العلاقة.
  - خبرة 4 سنوات في بيئة مركز عمليات الامن ( SOC ) وكيفية التعامل مع الحوادث
  - سنة خبرة فنية في مجال الشبكات أو أنظمة إدارة الشبكات (MS Infrastructure).

- **2.7 التدريب:**
  - شهادة في إدارة نظام SIEM
  - CEH certified أو ما يعادلها.
  - CCNA Certified
  - CCNA Security is preferred

- **3.7 المعارف والمهارات والقدرات:**
  - معرفة جيدة أو/و خبرة في أمن تكنولوجيا المعلومات في القطاع الحكومي والتجاري.
  - معرفة بآخر المستجدات في القضايا الأمنية الخاصة بتكنولوجيا المعلومات.
  - معرفة بالمعايير الدولية لأمن المعلومات مثل ISO 27001.
  - معرفة بالمعايير الدولية PKI و PCI.
  - فهم عميق للمخرجات الأمنية، و أدواتها، و نظم الشبكات، و أمن الإنترنت .
  - فهم عميق لبيئة العمل من النواحي الأمنية و الفيزيائية، و أنظمة الرقابة على وسائل النفاذ للشبكات.
  - فهم عميق لمبادئ تقييم المخاطر و كذلك لمبادئ إدارة المخاطر، طرق مراجعة التدقيق، و طرق تنفيذ السياسات و الرقابة عليها.
  - فهم جيد بأساليب إدارة الهوية الرقمية، و التوثيق، و تكنولوجيا التشفير .
  - مهارات ممتازة في الاتصال الكتابي والشفهي وباللغتين العربية والانجليزية.
  - مهارة عالية في الاتصالات الكتابية و الشفهية و باللغتين العربية و الإنجليزية

| **8- الاعتمادات:** | | | | |
|---|---|---|---|---|
| **جهة الاعتماد** | **الاسم** | **مسمى الوظيفة** | **التوقيع** | **التاريخ** |
| **1.8 الدائرة المعنية** | | | | |
| **2.8 ديوان الخدمة المدنية** | | | | |