المركز الوطني للأمن السيبراني
National Cyber Security Center

# بطاقة الوصف الوظيفي التحليلي

| ١. المعلومات الأساسية | | | |
|---|---|---|---|
| ١,١ معلومات اساسية عن الوظيفة | | | |
| مسمى الوظيفة | محلل عمليات سيبرانية مساعد | نوع الوظيفة | |
| الدائرة | المركز الوطني للأمن السيبراني | الفئة الوظيفية | الأولى |
| الادارة/المديرية | مديرية العمليات السيبرانية | المجموعة النوعية | |
| القسم/الشعبة | المراقبة والتحليل | المستوى | الثالث |
| مسمى وظيفة الرئيس المباشر | رئيس قسم المراقبة والتحليل | المسمى القياسي الدال | محلل أمن سيبراني مساعد |
| رمز الوظيفة | | مسمى الوظيفة الفعلي | محلل عمليات سيبرانية مساعد |
| حجم الموارد البشرية* | | حجم موازنة الدائرة* | |
| *تعبأ لشاغلي وظائف المجموعة الثانية من الفئة العليا فقط. | | | |
| | | | |
| ١,٢ موقع الوظيفة في الهيكل التنظيمي للدائرة | | | |
| تقع الوظيفة في قسم المراقبة والتحليل في مديرية العلميات السيبرانية وترتبط إرتباطاً مباشر اً في رئيس قسم المراقبة والتحليل. | | | |
| ٢. الغرض من الوظيفة | | | |
| المهمة الرئيسية للوظيفة ( الهدف من الوظيفة) | | | |
| تختص الوظيفة بضمان الجاهزية الفورية لإدارة حوادث الامن السيبراني والاستجابة لها والتعامل مع الأضرار الناتجة عنها بهدف الاكتشاف المبكر لحوادث الامن السيبراني بناءاً على عمليات المراقبة والتحليل من خلال العمل على تحسين أنشطة المراقبة وضمان التعامل والاستجابة للحوادث السيبرانية في الوقت المناسب وبفعالية وفقاً لدليل عمليات مديرية العمليات السيبرانية. | | | |
| ٣. المهام والواجبات المسؤوليات الرئيسية | | | |
| المهام التفصيلية والمسؤوليات | | | |
| ١. يراقب الشبكات الحكومية وشبكات البنية التحتية الوطنية الحرجة لاكتشاف الحوادث الأمنية لغايات حماية الشبكات والأنظمة الحكومية من التهديدات السيبرانية وفقا لقانون الامن السيبراني رقم (١٦) لسنة ٢٠١٩. | | | |
| ٢. يتحقق من وصول سجلات الحركات على مركز عمليات المراقبة (SOC) من خلال عملية المراقبة الصحية ( Health Check Monitoring) لضمان استمرارية المراقبة وفقاً لدليل عمليات مديرية العمليات السيبرانية. | | | |
| ٣. يحلل الحوادث الأمنية المكتشفة بشكل أولي لغايات التحقق فيما إذا كانت حادثة فعلية أو لا وتسجيلها على نظام إدارة الحوادث الأمنية وفقاً لدليل عمليات مديرية العمليات السيبرانية. | | | |

المركز الوطني للأمن السيبراني
National Cyber Security Center

**بطاقة الوصف الوظيفي التحليلي**

٤. يقيم ويصنف الحوادث الامنية المكتشفة لغايات تحديد ماهية إجراءات التعامل مع الحادث الامني وفقاً لتعليمات تصنيف حوادث الأمن السيبراني ٢٠٢٣.

٥. يبلغ الجهات المعنية بالحادث الأمني المكتشف من خلال قنوات الاتصال المعتمدة ونظام إدارة الحوادث الأمنية لتقديم التوصيات الفنية اللازمة وفقاً لتعليمات تصنيف حوادث الأمن السيبراني للعام ٢٠٢٣ ودليل عمليات مديرية العمليات السيبرانية.

٦. يعمل على مسح مؤشرات الاختراق (IOC's) الواردة من التقارير الأمنية (من داخل المركز أو خارجه) على أنظمة المراقبة والمشاركة في اعداد التقارير بذلك للتحقق من عدم وجودها في شبكات المؤسسات الحكومية أو البنى التحتية الحرجة وفقاً لدليل عمليات مديرية العمليات السيبرانية والتوجيهات الصادرة بذلك.

٧. يقوم بأية مهام أخرى يكلف بها ذات علاقة بطبيعة العمل.

## ٤. مكونات الوظيفة

### ٤,١ اتصالات العمل

| ماهية وغرض الاتصال | جهات ومستوى الاتصال | مدى التكرار |
|---|---|---|
| ○ تبادل معلومات روتينية متصلة بالعمل مباشرة.<br>○ تنسيق العمل.<br>○ توضيح أساليب العمل وطرقه أو تفسير البرامج والأعمال. | ○ زملاء العمل المباشرين.<br>○ موظفين الوحدات الأخرى الوزارة/المؤسسة.<br>○ موظفي الدوائر الحكومية الأخرى. | ○ يومياً. |

### ٤,٢ المتطلبات الذهنية لحل مشكلات العمل.

قدرة بسيطة على التطبيق المباشر للمعرفة الأساسية بالعمل و تذكر بسيط لتتابع خطوات انجاز العمل، أو استعياب حل المشاكل و الربط بين عناصر مختلفة والمسببات والنتائج و تحليل الظواهر أو المشاكل الى مكوناتها الأساسية أو تحليل المعلومات للتوصل الى نتائج و جمع أفكار متعددة لوضع فكرة جديدة أو التوصل الى الاستنتاجات من معطيات.

### ٤,٣ مجال العمل وتأثيره

أثر فادح على أهداف التنظيم وعلاقته الداخلية والخارجية والأموال والممتلكات.

### ٤,٤ الصعوبة والتعقيد

أعمال معقدة تتطلب إجراءات وأساليب وإجراءات وقواعد معرفة و ذات خطوات متعددة ومتداخلة ومتكررة

### ٤,٥ المسؤولية الاشرافية

| المسميات الوظيفية للمرؤوسين | درجة الوظيفة | أعداد الموظفين |
|---|---|---|
| - | - | - |
| - | | |

المركز الوطني للأمن السيبراني
National Cyber Security Center

## بطاقة الوصف الوظيفي التحليلي

| ٤,٦ المجهود البدني | |
|---|---|
| نوعية المجهود البدني (شدة المجهود البدني) | النسبة المئوية من وقت العمل |
| جالس | ٪١٠٠ |
| **٤,٧ ظروف العمل** | |
| بيئة العمل | النسبة المئوية من وقت العمل |
| عادية (داخل المكتب) | ٪١٠٠ |

### ٥. المؤهلات العلمية والخبرات العملية

**٥,١ متطلبات إشغال الوظيفة (الحد الأدنى من المؤهلات العلمية والخبرات العملية والتدريب)**

**٥,١,١ المؤهل العلمي المطلوب (التعليم الأكاديمي، المهني، الخ)**

البكالوريوس كحد أدنى في مجال الأمن السيبراني أو أمن الشبكات أو أمن المعلومات أو علم الحاسوب أو هندسة الحاسوب أو أي تخصص له علاقة بطبيعة العمل.

**٥,١,٢ الخبرة العملية المطلوبة**

| نوع الخبرة العملية ومجالها | مدة الخبرة العملية |
|---|---|
| خبرة عملية في مجال الأمن السيبراني أو أمن المعلومات. | سنة واحدة |

**٥,١,٣ التدريب الفني أو الإداري أو التخصصي المطلوب (ويقصد التدريب الرسمي اللازم لممارسة عمل او مهنة معينة قبل شغل الوظيفة)**

| مستوى التدريب ومجاله | مدة التدريب |
|---|---|
| يفضل دورة تدريبية في مجال الامن السيبراني أو أمن المعلومات. | لا تقل عن ٢٠ ساعة تدريبية |

**٥,٢ الكفايات الوظيفية**

| الكفاية المطلوبة | وصف الكفاية | مستويات اتقان الكفاية ( اساسي، متوسط، متقدم، خبير) |
|---|---|---|
| الكفايات الفنية | تحليل الحوادث الأمنية | أساسي |
| | تقييم وتصنيف الحوادث الأمنية | أساسي |
| | مسح مؤشرات الاختراق | أساسي |
| | اكتشاف الحوادث الأمنية | أساسي |
| | أدوات SIEM وتحليل السجل | أساسي |
| الكفايات القيادية | - | - |

المركز الوطني للأمن السيبراني
National Cyber Security Center

## بطاقة الوصف الوظيفي التحليلي

| ( لشاغلي الوظائف الإشر افية والقيادية) | | |
|---|---|---|
| الكفايات العامة (السلوكية والإدارية) | احتر افية الأداء | اساسي |
| | التعاون والعمل بروح الفريق | اساسي |
| | الالتزام | اساسي |
| | بناء العلاقات | أساسي |
| | الاتصال الفعال | اساسي |