

أبرز وظائف الأمن السيبراني:

وظائف للمراحل الابتدائية

المهام	المسمى الوظيفي
<ul style="list-style-type: none">ضمان سلامة البرامج والتطبيقات.بناء أدوات حماية نقاط الضعف في التطبيق المعرض للاختراق والهجمات الإلكترونية.	مسؤول أمن التطبيقات
<ul style="list-style-type: none">تقييم تقنية المؤسسة بحثًا عن المشكلات المحتملة المتعلقة بالأمان والكفاءة والامتثال.	مدقق أمن معلومات
<ul style="list-style-type: none">تصميم الحلول وتوفير المساعدة التقنية.نشر المعرفة حول آخر التقنيات والتحديثات والتوصيات المتعلقة بأمن المعلومات.	أخصائي أمن المعلومات:
<ul style="list-style-type: none">يختبر استمرار شبكات المؤسسة لتحديد نقاط الضعف.	مخترق أخلاقي CEH
<ul style="list-style-type: none">تحليل البيانات والمعلومات المتواجدة داخل الأنظمة وقواعد البيانات بهدف العثور على التعديلات والتحديثات اللازم اتخاذها من أجل تحسين وزيادة كفاءة مستوى الأمن والحماية للشبكات.	محلل أمن المعلومات
<ul style="list-style-type: none">حماية البنى التحتية على الإنترنت وفي مكان العمل.مراقبة البيانات لتحديد النشاط المشبوه.تحديد المخاطر والتخفيف من حدتها قبل حدوث خرق.	محلل SOC
<ul style="list-style-type: none">تطوير الأمان لأجهزة الحاسوب.	مهندس أجهزة أمان الشبكة
<ul style="list-style-type: none">ضمان الامتثال القانوني فيما يتعلق بحماية البيانات.	مسؤول خصوصية البيانات

وظائف للمراحل المتوسطة والمتقدمة

المهام	المسمى الوظيفي
• استخدام الذكاء الاصطناعي لمكافحة جريمة المعلومات.	خبير أمن الذكاء الاصطناعي
• تطوير الترميز لمستقبل المعاملات الآمنة.	مطورو / مهندسو Blockchain
• الدفاع عن مؤشرات / أنظمة تشغيل دفاعية أكثر صرامة.	أعضاء الفريق الأزرق
• كشف نقاط الضعف والأخطاء في الأنظمة الإلكترونية بسبب الأخطاء.	Bug Bounty Hunter
• مراقبة وحماية جميع البيانات.	Network Security Scrum Master
• رئيس قسم أمن المعلومات.	رئيس ضابط أمن المعلومات
• رئيس قسم الأمن الشخصي / المعلومات / الأمن الإلكتروني.	كبير ضباط الأمن
• حماية التطبيقات والبيانات السحابية	Cloud Security Architect
• إحباط التجسس الإلكتروني في البلدان المعادية.	محللو مكافحة التجسس
• فك تشفير البريد المشفر بدون مفتاح التشفير.	التشفير
• تطوير نظام لتشفير المعلومات السرية والحساسة.	عالم التشفير
• استشارة حول مخاطر الإنترنت.	خبير سياسة التأمين على الإنترنت
• تحليل التهديدات الإلكترونية وحماية النظام من التهديدات.	خبير استخبارات الشبكة
• دمج الإجراءات الهجومية الإلكترونية وتنفيذها في آن واحد ضد أنشطة وقدرات العدو. • القيام بأعمال دفاعية لحماية البيانات والشبكات والأنظمة الإلكترونية.	خبراء إجراءات الشبكة

المسمى الوظيفي	المهام
محقق الجرائم الإلكترونية	<ul style="list-style-type: none"> • حل جرائم الأمن السيبراني، من أجل اكتشاف كيفية وصول شخص غير مصرح له إلى نظام أو لجمع الأدلة لأغراض قانونية.
محامي الأمن السيبراني	<ul style="list-style-type: none"> • الدفاع عن الأمن السيبراني والإلكتروني، الجرائم السيبرانية.
مطور / مهندس برنامج أمن الشبكات	<ul style="list-style-type: none"> • تطوير إعدادات الأمان في التطبيقات.
خبير استعادة البيانات	<ul style="list-style-type: none"> • استعادة البيانات المتسربة من الأجهزة الرقمية.
محلل أمن البيانات	<ul style="list-style-type: none"> • حماية المعلومات على أجهزة الحاسوب والشبكات.
خبير التعافي من الكوارث	<ul style="list-style-type: none"> • التخطيط وكيفية التعامل مع الكوارث وكوارث النظام.
مدير الامتثال والحوكمة (GRC)	<ul style="list-style-type: none"> • الإشراف على إدارة المخاطر.
خبير أمن IIOT (الإنترنت الصناعي للأشياء)	<ul style="list-style-type: none"> • حماية أنظمة التحكم الصناعية.
المستجيبون للحوادث	<ul style="list-style-type: none"> • الرد الأولي على القرصنة الإلكترونية وسرقة البيانات.
محلل ضمان المعلومات	<ul style="list-style-type: none"> • تحديد مخاطر نظام المعلومات.
محلل أمن المعلومات	<ul style="list-style-type: none"> • تخطيط وتنفيذ إجراءات أمن المعلومات.
مدير أمن المعلومات	<ul style="list-style-type: none"> • يشرف على فريق أمن تكنولوجيا المعلومات.
مهندس أمن تكنولوجيا المعلومات	<ul style="list-style-type: none"> • تصميم وبناء والإشراف على تنفيذ أنظمة أمن الشبكات والحاسوب للمؤسسات. • إنشاء هياكل أمنية معقدة وضمان تشغيلها، والتعامل مع المعدات الدفاعية المخصصة لهذه الشبكات (مثل اختبار الثغرات الأمنية، وتركيب جدران الحماية، وما إلى ذلك) والاستجابة (على سبيل المثال: الاستجابة لتهديدات الأمن السيبراني).

المسمى الوظيفي	المهام
	<ul style="list-style-type: none"> • إنشاء بنية تحتية للأمن، وتوفير التوجيه الفني، وتقييم التكاليف والمخاطر، وصياغة السياسات والإجراءات الأمنية.
خبراء أمن إنترنت الأشياء	<ul style="list-style-type: none"> • حماية معدات الشبكة.
محلل كشف التسلل	<ul style="list-style-type: none"> • استخدم أدوات الأمان للعثور على الهجمات المستهدفة.
مهندس أمن متنقل	<ul style="list-style-type: none"> • مسؤول عن حماية أنظمة ومعدات الهاتف المحمول.
مسؤول أمن الشبكات	<ul style="list-style-type: none"> • حماية شبكات الحاسوب من التهديدات الداخلية والخارجية.
اختبار الاختراق	<ul style="list-style-type: none"> • تنفيذ الهجمات الإلكترونية عن طريق محاكاة هجمات الشبكة الخارجية.
محلل PKI (البنية التحتية للمفتاح العام)	<ul style="list-style-type: none"> • إدارة الإرسال الآمن للمعلومات الرقمية.
أعضاء الفريق الأحمر	<ul style="list-style-type: none"> • المشاركة في الهجمات السيبرانية المحاكاة.
SCADA(المراقبة واكتساب البيانات) محلل الأمن	<ul style="list-style-type: none"> • نظام لحماية البنية التحتية الحيوية وحمايتها