Cyber Security Careers Summary

هذا الملف يلخص أهم مجالات السيكيوريتي، مع شرح لكل وظيفة ومسؤولياتها ومسارات التعلم.

1️⃣ Security Analyst

الوظيفة: حماية البيانات وبناء خطط أمنية للشركة. **الشرح:** محلل الأمن السيبراني يعمل على فحص الشبكات والبنية التحتية للشركة لإيجاد ثغرات، ثم يوصي بالحلول لتفادي الهجمات. هذا الدور يحتاج لفهم السياسات الأمنية والتواصل مع الفرق المختلفة. **المسؤوليات:** - تحليل الأمن السيبراني للشركة - إعداد تقارير عن سلامة الشبكات والمشاكل الأمنية - تطوير خطط أمنية وفق أحدث التهديدات **مسار التعلم:** Pre Security, Cyber Security 101, SOC Level 1

2️⃣ Security Engineer

الوظيفة: تطوير وتنفيذ حلول أمان ضد الهجمات والثغرات. **الشرح:** مهندس الأمان يعمل على تصميم الأنظمة والسياسات الأمنية، ويقوم باختبار البرامج والشبكات لضمان أقصى حماية ضد التهديدات. **المسؤوليات:** - اختبار الحلول الأمنية في البرامج - مراقبة الشبكات وتحديث الأنظمة لتقليل الثغرات - تنفيذ أنظمة حماية متقدمة **مسار التعلم:** SOC Level 1, JR Penetration Tester, Offensive Pentesting

---

3️⃣ Incident Responder

الوظيفة: الاستجابة للهجمات فور وقوعها وحماية البيانات. **الشرح:** مسؤول الاستجابة للحوادث يعمل في المواقف العاجلة لإيقاف الهجمات وتقليل الضرر، ويعد خطط الاستجابة للمستقبل. **المسؤوليات:** - تطوير خطط استجابة للحوادث - دعم الممارسات الأمنية الأفضل ومتابعة التدابير - إعداد تقارير بعد الحوادث لتحسين الاستجابة مستقبلاً **مسار التعلم:** SOC Level 1

4️⃣ Digital Forensic Specialist

الوظيفة: استخدام الأدلة الرقمية للتحقيق في الحوادث أو الجرائم. **الشرح:** خبير الأدلة الرقمية يعمل على جمع وتحليل البيانات الرقمية بطريقة قانونية لفهم طبيعة الحوادث وحل القضايا. **المسؤوليات:** - جمع الأدلة الرقمية قانونياً - تحليل الأدلة لإيجاد معلومات عن الحادث - توثيق النتائج وإعداد التقارير

5️⃣ Malware Analyst

الوظيفة: تحليل البرمجيات الخبيثة لمعرفة سلوكها والتعامل معها. **الشرح:** محلل البرمجيات الخبيثة يفك شفرات البرامج الضارة ويحلل سلوكها لمعرفة كيفية اكتشافها وحماية الأنظمة منها. **المسؤوليات:** - تحليل البرمجيات الخبيثة بشكل ثابت وديناميكي - إعادة هندسة البرامج لتحويلها إلى كود قابل للقراءة - توثيق وتحليل النتائج

6️⃣ Penetration Tester (Pentester)

الوظيفة: اختبار أنظمة الشركة لكشف الثغرات الأمنية. **الشرح:** يقوم باختبار الشبكات والأنظمة والتطبيقات بشكل قانوني لمحاكاة هجوم حقيقي، بهدف تحسين دفاعات الشركة. **المسؤوليات:** - إجراء اختبارات على الأنظمة والشبكات والتطبيقات - تقييم السياسات الأمنية وإعداد تقارير - تقديم توصيات لمنع الهجمات **مسار التعلم:** JR Penetration Tester, Offensive Pentesting

---

7️⃣ Red Teamer

الوظيفة: محاكاة دور المهاجم لتقييم دفاعات الشركة. **الشرح:** يعمل كفريق هجوم داخلي أو خارجي، يحاكي طرق الهجوم الحقيقية لاختبار استجابة الشركة وقدرتها على اكتشاف الهجمات. **المسؤوليات:** - تقليد المهاجمين لكشف الثغرات والحفاظ على الوصول - تقييم ضوابط الأمن واستجابة الحوادث - تقديم تقرير بالنتائج مع نصائح لتجنب الهجمات **مسار التعلم:** JR Penetration Tester, Offensive Pentesting