أخصائي الأمن السيبراني الصناعي (Industrial Cybersecurity Specialist)

حماية المصانع والأنظمة الذكية من هجمات العالم الرقمي

مقدّمة

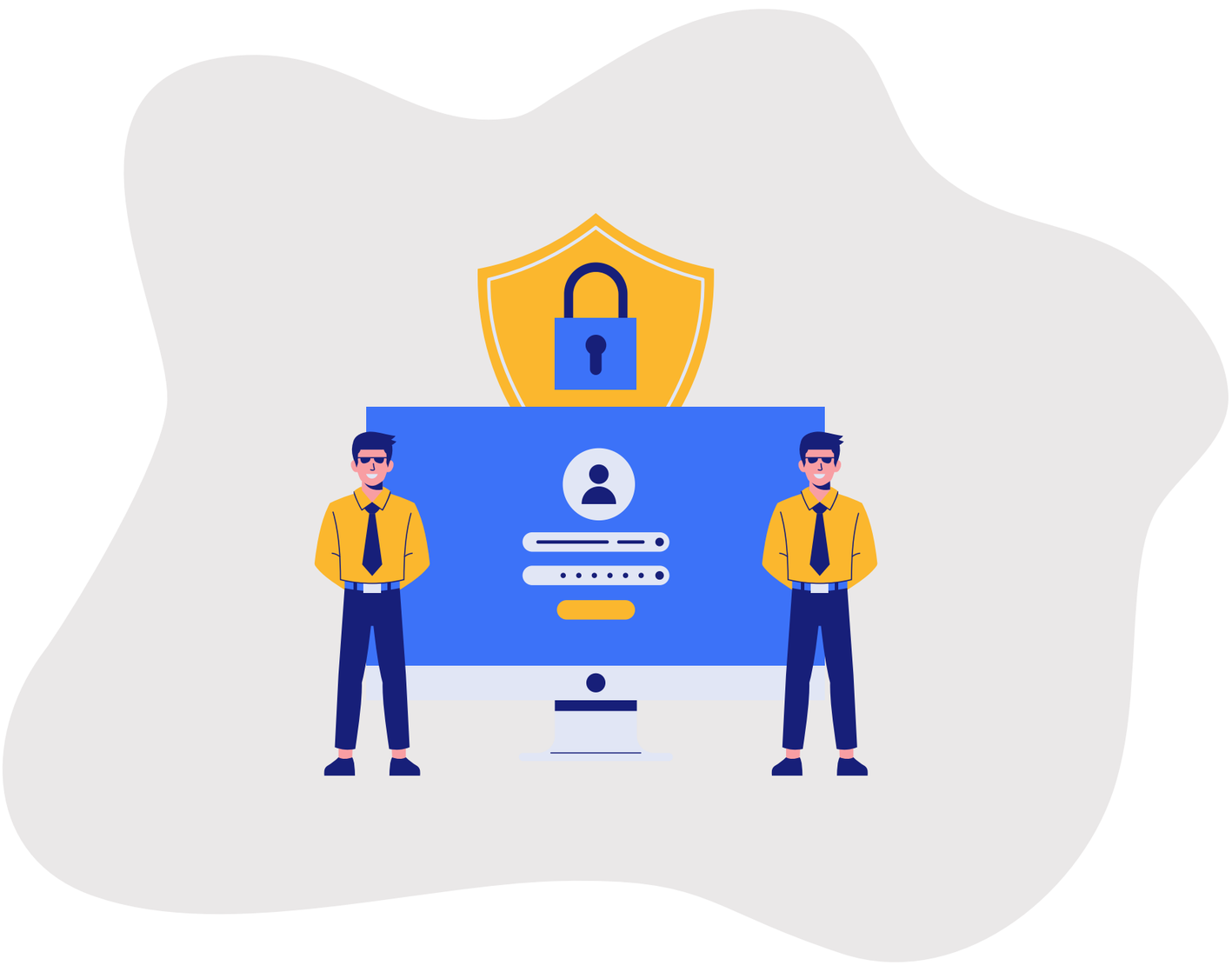
يحمي هذا الأخصائي **أنظمة التحكم الصناعي (ICS) والبنية التحتية الحيوية من الهجمات الإلكترونية**، مما يضمن استمرارية العمل وسلامة المعدات والمنشآت الصناعية من الأعطال أو الاختراقات.

المسارات التّعليمية لدخول مجال الأمن السيبراني الصناعي

- **بكالوريوس في هندسة الحاسوب، الأمن السيبراني، أو الهندسة الصناعية.**
- **شهادات متخصصة مثل: GICSP ،ICS-CERT، أو CompTIA Security+.**

الفروع الدّراسية التي تسمح بالالتحاق بالمجال

- العلمي، الصناعي، التكنولوجي.



المواد الدّراسية الأساسيّة لأخصائي الأمن السيبراني الصناعي

- شبكات الحاسوب.
- أنظمة التحكم الصناعية SCADA.
- بروتوكولات الأمن السيبراني.
- تحليل المخاطر والهجمات.
- أنظمة التشغيل والتحديثات.

لمن هذه المهنة؟

- لمن يهتم بالأمن الرقمي والبنية التحتية.
- لمن يملك تفكير تحليلي وتقني.
- لمن يستطيع العمل تحت الضغط وفي حالات الطوارئ.

مجالات العمل بعد التّخرّج

- مصانع الطاقة والكهرباء.
- شركات البتروكيماويات.
- المنشآت العسكرية والأمنية.
- شركات الصناعات الثقيلة.
- الموانئ والمطارات.

أخصائي الأمن السيبراني الصناعي (Industrial Cybersecurity Specialist)

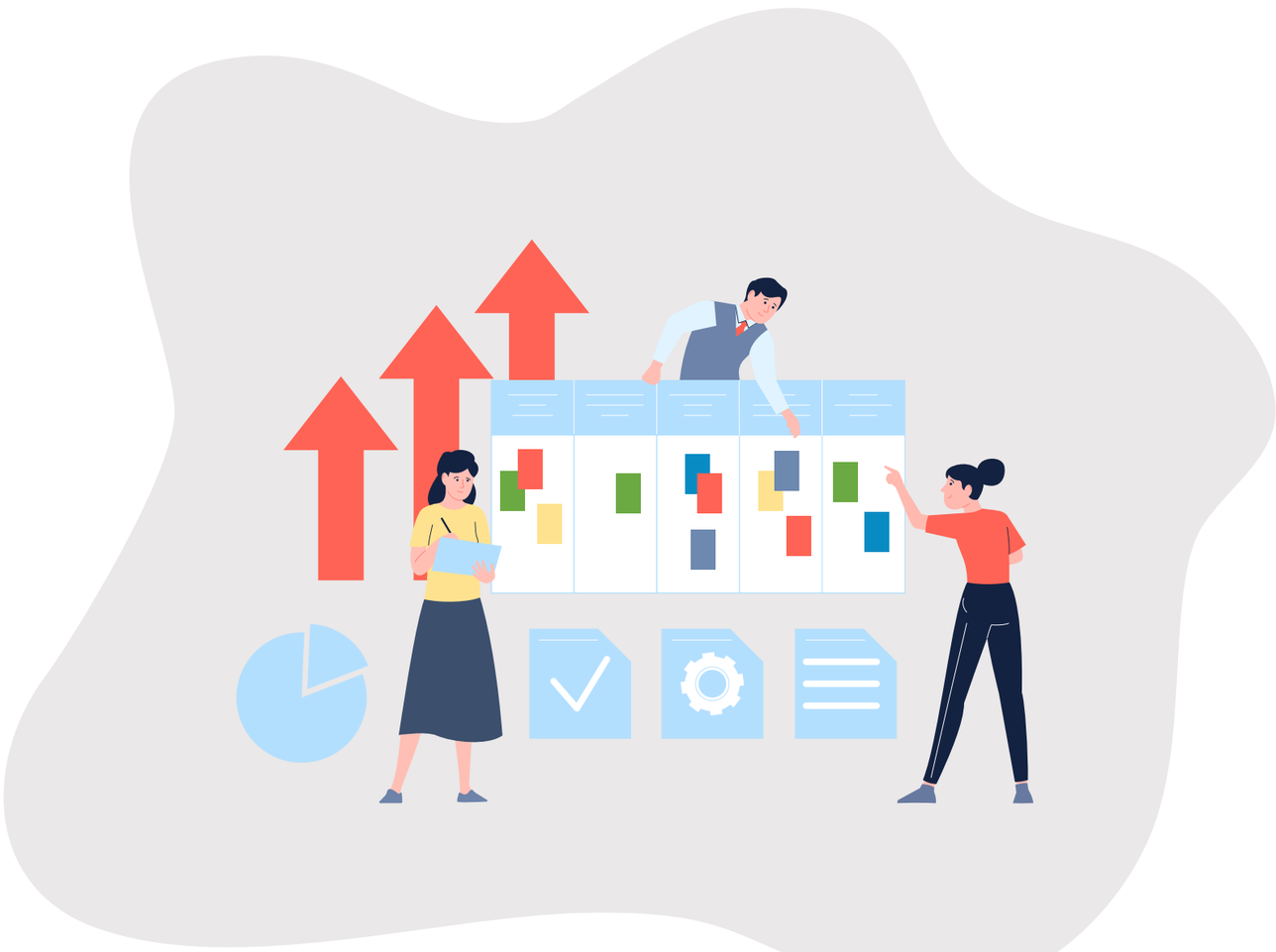
تحويل التفاصيل الصغيرة لنجاح كبير

المهارات المطلوبة للتميّز كأخصائي أمن سيبراني صناعي

- فهم أنظمة SCADA وPLC.
- تحليل سلوك البرمجيات الخبيثة.
- إعداد تقارير فنية دقيقة.
- التعاون مع فرق متعددة التخصصات.

المهام اليومية وطبيعة العمل

- تحليل وتقييم الثغرات الأمنية في أنظمة التحكم.
- مراقبة الشبكات الصناعية والكشف عن التهديدات.
- تطبيق وتحديث سياسات الحماية.
- إجراء اختبارات اختراق للأنظمة الصناعية.



سيناريوهات العمل

- أخصائي أمن معلومات في محطة كهرباء.
- محلل تهديدات في مصنع دوائي.
- مستشار أمن صناعي لدى شركة بترول.

أبرز المعتقدات الخاطئة عن أخصائي الأمن السيبراني الصناعي

المعتقد الخاطئ	المعتقد الصحيح
فقط للتفتيش	الجودة تتضمن تحسين العمليات والتدريب
وظيفة بيروقراطية	هي دور استراتيجي داخل المؤسسة