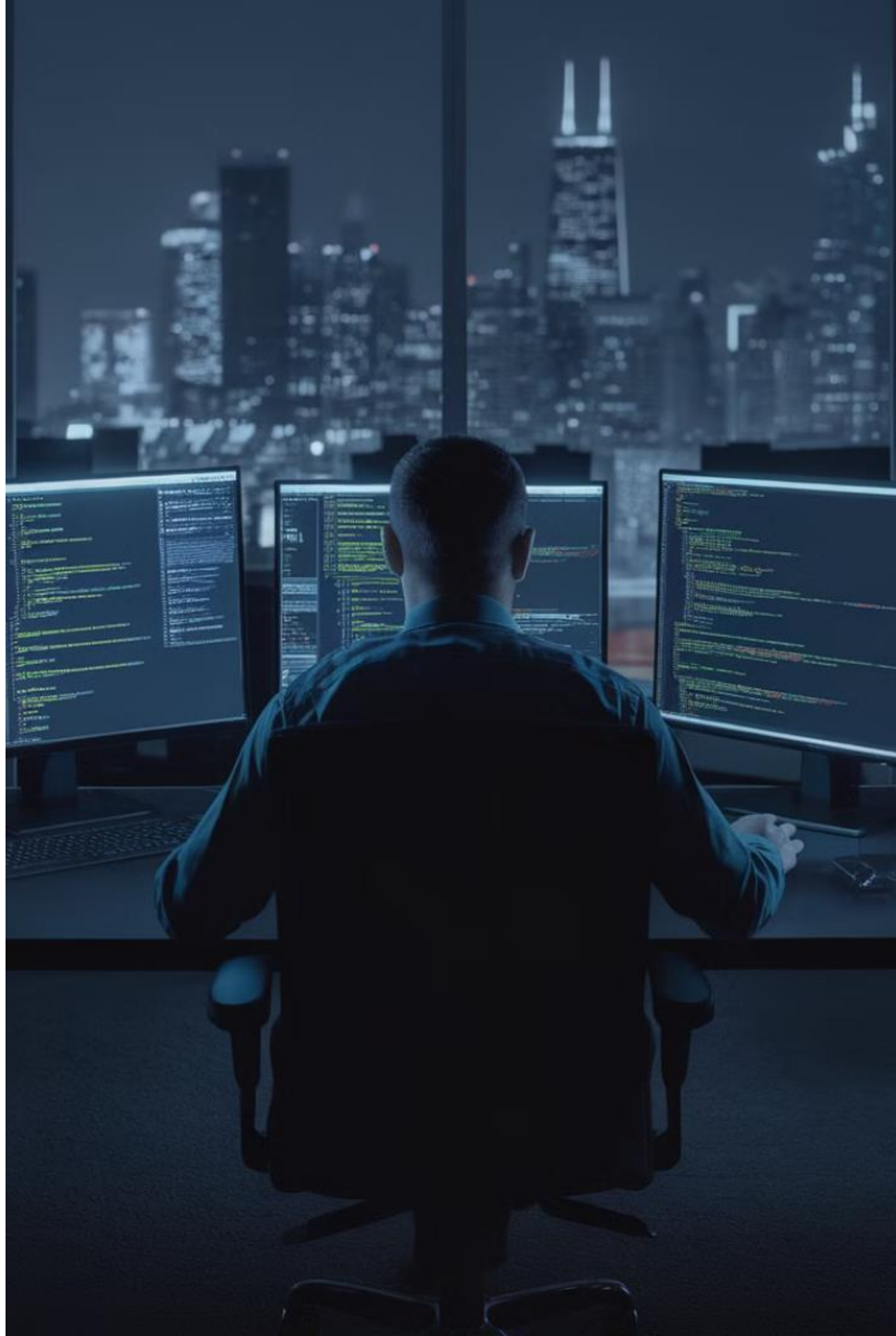
قواعد وضوابط الأمن السيبراني

تعرف على أهم القواعد والضوابط الأساسية للأمن السيبراني وكيفية تطبيقها لحماية نظامك وبياناتك.

Dr. Mohammed Alshahrani



تحديد الأدوار والمسؤوليات في المنظمة

الوعي الأمني

أهمية الوعي الأمني وتخصيص مهام محددة لكل مستوى من الموظفين لضمان حماية المعلومات.

تعيين المسؤوليات الأمنية

تحديد المسؤوليات الأمنية لجميع أفراد المنظمة، من فريق الأمن السيبراني إلى الموظفين العاديين.

سياسات الوصول وإدارة الحسابات

إدارة الحسابات الحساسة

أهمية إلغاء صلاحيات المستخدمين الذين لم يعودوا يعملون في المؤسسة.

إجراءات الوصول

تشمل الإجراءات المتعلقة بمنح وتقييد الوصول إلى الأنظمة والبيانات بناءً على مستوى الحاجة.

إدارة المخاطر السيبرانية

تحديد المخاطر السيبرانية

الكشف عن الثغرات

التعرف على نقاط الضعف والثغرات الأمنية في البيئة.

تحليل المخاطر

استخدام أدوات تحليل المخاطر للكشف عن الثغرات الأمنية.

التعرف على المخاطر

التعرف على المخاطر والتهديدات المحتملة للأمن السيبراني في بيئة العمل.

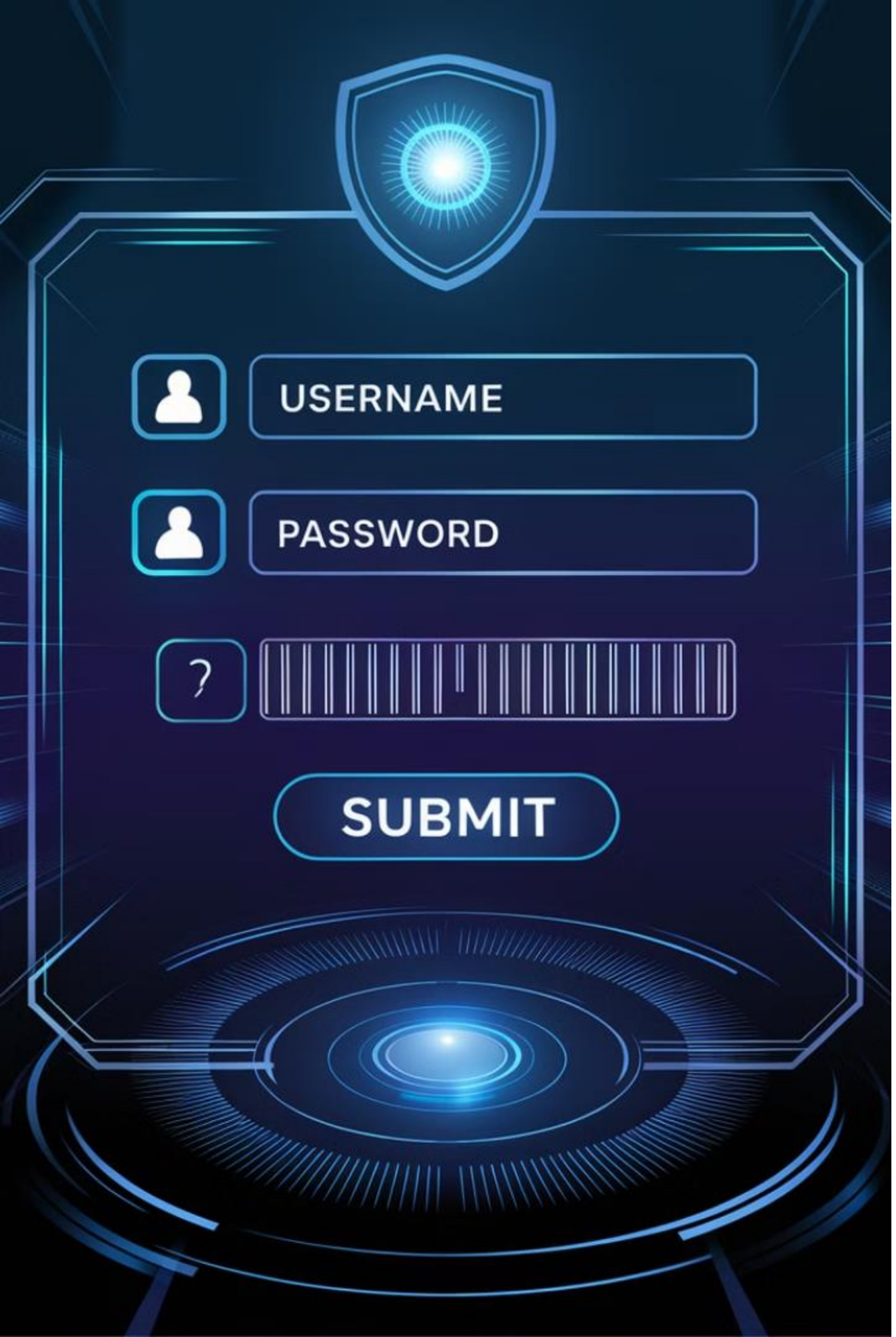
تقييم تأثير المخاطر واحتمال حدوثها

1 تحليل التأثير والخطر

تقييم مدى تأثير المخاطر في حال وقوعها واحتمالية حدوثها باستخدام نماذج مثل تحليل التأثير والخطر.

2 منهجيات التقييم

منهجيات تقييم المخاطر مثل Qualitativeو Quantitative.



ضوابط المصادقة

المصادقة الثنائية

تعزز المصادقة الثنائية الحماية عبر طبقتين من التحقق من الهوية.

كلمات المرور القوية

استخدام كلمات مرور قوية وآمنة يساعد في منع الوصول غير المصرح به.

رمز المرور المؤقت *(OTP)*

رمز المرور المؤقت يوفر طبقة إضافية من الأمان عند تسجيل الدخول.

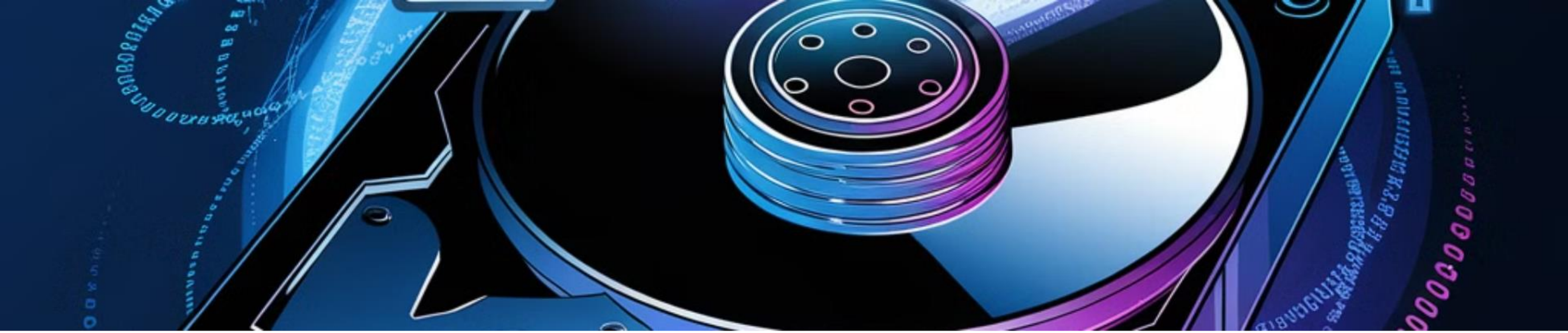
صلاحيات المستخدم وتقييد الوصول

مبدأ الحد الأدنى

تطبيق مبدأ "الحد الأدنى من الامتيازات "لضمان حصول كل مستخدم على الصلاحيات اللازمة فقط.

تقييد الصلاحيات

تقييد صلاحيات المستخدمين بناءً على الحاجة الفعلية لمهامهم أمر بالغ الأهمية.



تشفير البيانات

1

حماية البيانات الحساسة

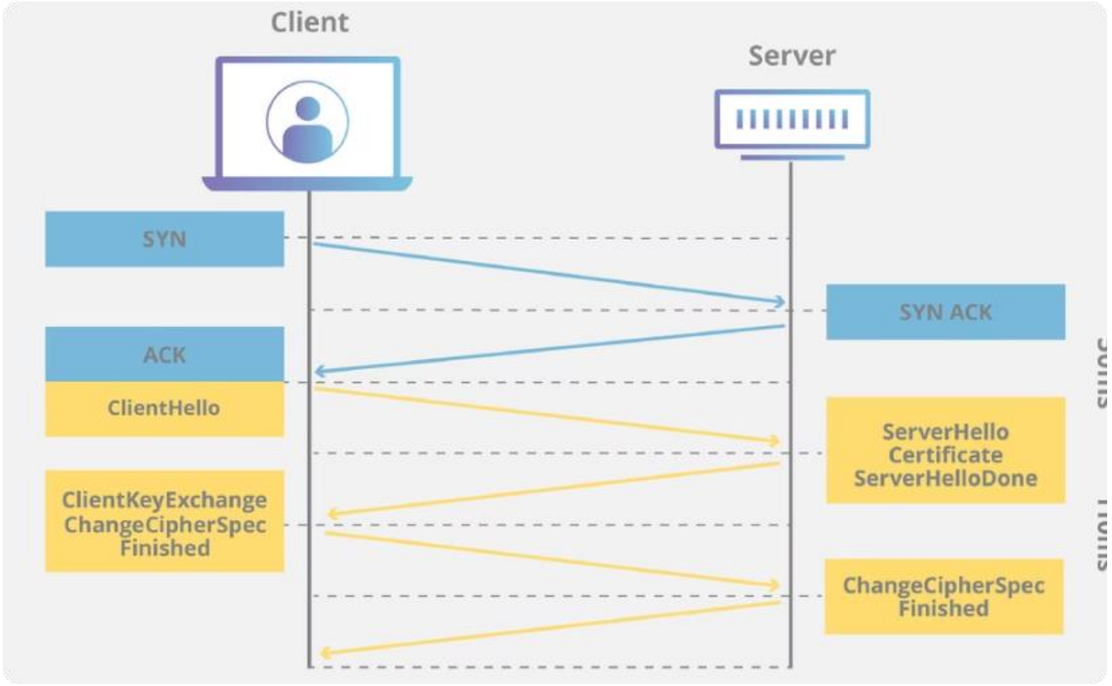
استخدام تقنيات التشفير لحماية البيانات الحساسة سواء في التخزين أو أثناء النقل.

2

أنواع التشفير

التشفير المتماثل والتشفير غير المتماثل هي من أنواع التشفير المستخدمة.

حماية البيانات أثناء النقل والتخزين



نقل آمن للبيانات

استخدام بروتوكولات آمنة مثل SSL/TLS لحماية البيانات أثناء النقل.

تشفير البيانات المخزنة

تأمين البيانات المخزنة باستخدام حلول تشفير الأقراص والنسخ الاحتياطي الآمن.

تأمين الشبكات

استخدام الجدران النارية وأنظمة كشف التسلل

الحماية المتكاملة

استخدام الجدران النارية وأنظمة كشف التسلل معًا يوفر حماية شاملة للشبكة.

أنظمة كشف التسلل *(IDS)*

تكتشف أنظمة كشف التسلل الأنشطة المشبوهة والتهديدات الأمنية داخل الشبكة.

الجدران النارية *(Firewalls)*

تقوم الجدران النارية بفلترة حركة المرور الشبكية وتحديد ما يُسمح بالدخول والخروج من الشبكة.

تأمين الشبكات

تقسيم الشبكات وتقنيات *VPN*

زيادة الأمان

تقسيم الشبكة وتقنيات VPNتعزز الأمن السيبراني.

تقنيات *VPN*

استخدام VPNلتأمين الاتصالات عن بعد وحماية البيانات.

تقسيم الشبكات

تقسيم الشبكة لزيادة الأمان وفصل الأنظمة الحرجة.

السياسيات الأمنية للمستخدمين

تدريب وتوعية الموظفين

أفضل الممارسات

توجيه الموظفين لاستخدام أفضل الممارسات عند التعامل مع البيانات الحساسة.

أهمية الوعي

رفع مستوى الوعي لدى الموظفين حول مخاطر الأمن السيبراني مثل هجمات التصيد الاحتيالي .(Phishing)

السياسيات الأمنية للمستخدمين

سياسات استخدام الأجهزة الشخصية *(BYOD)*

الحفاظ على الأمن

ضمان أمن البيانات والشبكة عند السماح باستخدام الأجهزة الشخصية في بيئة العمل.

قيود على الأجهزة

تطبيق قيود على الأجهزة الشخصية وتثبيت تطبيقات الحماية المناسبة لها.

التحكم في البيانات

وضع سياسات لضبط الوصول إلى البيانات من خلال الأجهزة الشخصية المستخدمة في بيئة العمل.

الحماية من البرمجيات الضارة

برامج مكافحة الفيروسات

الخط الأول للدفاع

برامج مكافحة الفيروسات هي خط الدفاع الأول ضد البرمجيات الضارة.

التحديث المنتظم

تحديث قواعد البيانات للبرامج بشكل دوري لمواكبة التهديدات الجديدة.

الحماية الشاملة

برامج مكافحة الفيروسات توفر حماية شاملة ضد البرمجيات الضارة.

الحماية من البرمجيات الضارة

استراتيجيات الدفاع ضد البرمجيات الخبيثة

1 تحليل البرمجيات المشبوهة

استخدام تقنيات متقدمة مثل Sandboxing لتحليل البرمجيات المشبوهة قبل السماح بتنفيذها.

2 الكشف عن البرمجيات الخبيثة

استخدام تقنيات التحليل السلوكي للكشف عن البرمجيات الخبيثة.

خطط الاستجابة للحوادث السيبرانية

تحليل الحوادث

وضع إجراءات لتحليل الحوادث السيبرانية والتعرف على أسبابها وآثارها.

احتواء الحوادث

تحديد الخطوات اللازمة لاحتواء الحوادث السيبرانية والحد من آثارها.

تحديد الحوادث

وضع خطط واضحة لتحديد الحوادث السيبرانية مثل هجمات DDoS أو الاختراقات.

إدارة الحوادث السيبرانية

الإبلاغ عن الحوادث وإجراءات الاحتواء

1 الإبلاغ الفوري

بروتوكولات الإبلاغ الفوري عن الحوادث السيبرانية وتحديد القنوات المناسبة لذلك.

2 إجراءات الاحتواء

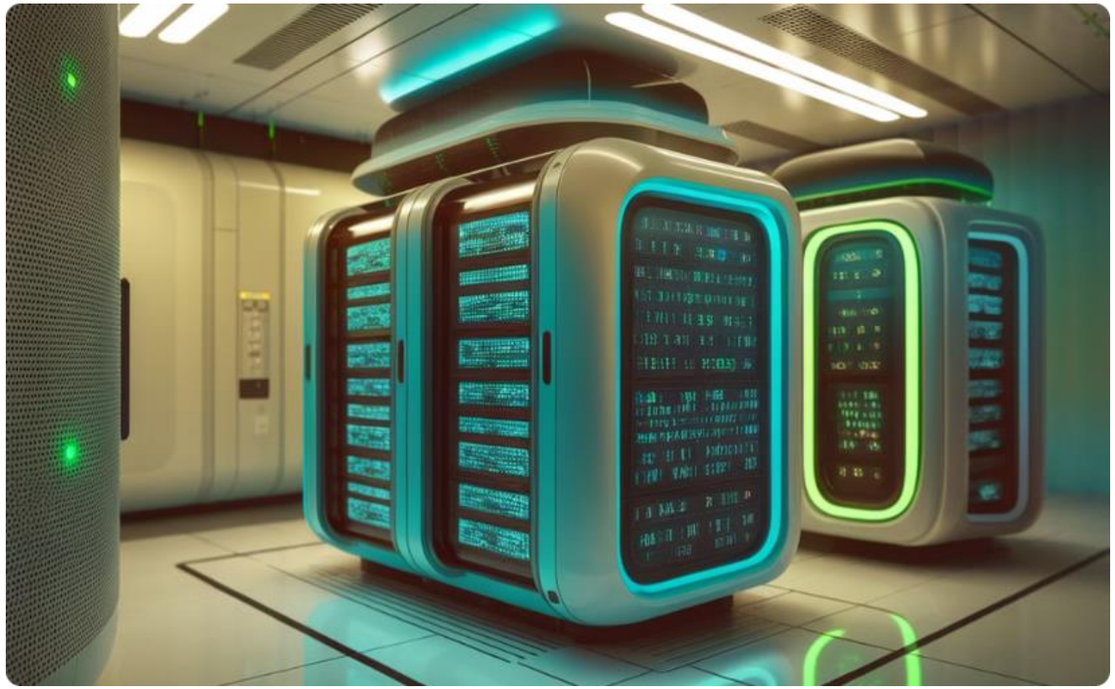
اتخاذ إجراءات احتواء الحادث لمنع انتشاره وتقليل الضرر الناتج.

النسخ الاحتياطي واستعادة البيانات

أهمية النسخ الاحتياطي المنتظم

تقنيات النسخ الاحتياطي

استخدام تقنيات مثل النسخ الاحتياطي الكامل والنسخ الاحتياطي التفاضلي لحماية البيانات.



النسخ الاحتياطي الدوري

ضمان استعادة البيانات في حالة الفقدان من خلال النسخ الاحتياطي الدوري للبيانات.

استراتيجيات استعادة البيانات في حالات الكوارث

الاستعادة عبر السحابة

استخدام الحلول السحابية لتأمين النسخ الاحتياطي والاستعادة السريعة للبيانات.

خطط الاستعادة السريعة

وضع خطط لاستعادة البيانات بسرعة في حالات الكوارث لضمان استمرارية العمل.

الامتثال للمعايير والتنظيمات

المعايير والتنظيمات الدولية

معايير دولية

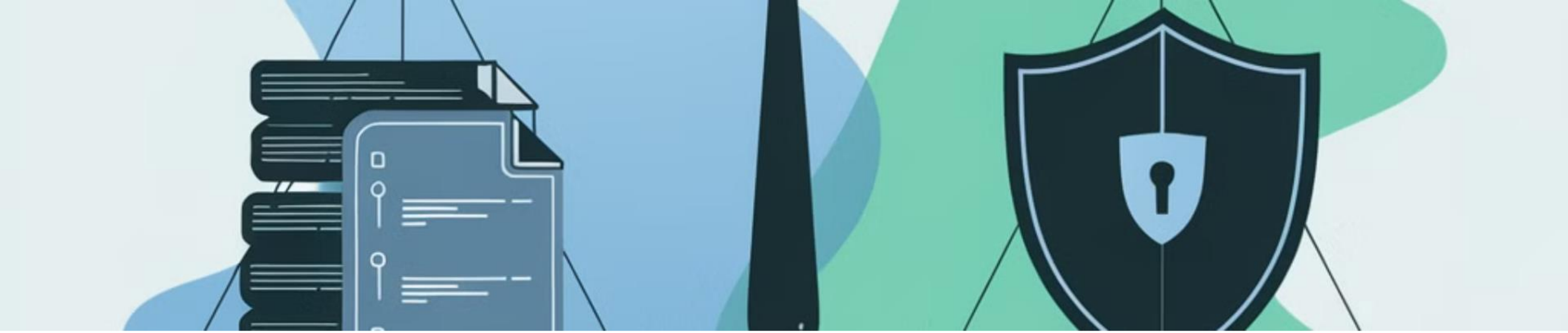
معايير مثل ISO 27001 وNIST تساعد في بناء أنظمة أمنية قوية.

تحسين السمعة

الامتثال لهذه المعايير يحسن سمعة المؤسسة ويقلل المخاطر.

تقليل المخاطر

الالتزام بالمعايير الدولية يساعد في تقليل المخاطر السيبرانية.



الامتثال للمعايير والتنظيمات

التوافق مع القوانين والتنظيمات

أهمية الالتزام

الامتثال للقوانين والتنظيمات يحمي الشركة من المخاطر القانونية والمالية.

عواقب عدم الامتثال

عدم الامتثال قد يؤدي إلى غرامات وعواقب قانونية خطيرة على الشركة.

الامتثال للقوانين

ضرورة الالتزام بالقوانين المحلية والدولية المتعلقة بحماية البيانات مثل اللائحة العامة لحماية البيانات (GDPR).

المراقبة والرصد

أدوات المراقبة المستمرة للشبكات

رصد الأنشطة غير العادية

أدوات المراقبة المستمرة تساعد في كشف الأنشطة غير الطبيعية والتحذيرات المبكرة.

إدارة معلومات الأمن

استخدام SIEMلرصد الأحداث الأمنية والاستجابة لها بشكل فعال.

التحليل والتقارير

تقديم لوحات معلومات وتقارير شاملة عن حالة الأمن السيبراني.

المراقبة والرصد

تحليل سجلات الأنشطة والتحذيرات

مراجعة السجلات الأمنية

تحليل السجلات الأمنية للكشف عن الأنماط المشبوهة قبل حدوث الهجمات.

الاحتفاظ بالسجلات

الاحتفاظ بالسجلات لمراجعتها وتحديد نقاط الضعف المحتملة.

اكتشاف التدخلات

استخدام تحليل السجلات لاكتشاف التدخلات المشبوهة قبل وقوع الهجمات.

اختبار الاختراق

تحديد الثغرات

اختبارات الاختراق تساعد في الكشف عن الثغرات الأمنية في النظام قبل أن يتم استغلالها.

هذه الاختبارات تعزز الأمن السيبراني للمنظمة وتحمي البيانات الحساسة.

أهمية الاختبارات الدورية

إجراء اختبارات الاختراق بشكل دوري لتحديد الثغرات الأمنية قبل استغلالها من قبل المهاجمين.

مواكبة التغيرات في البنية التحتية والتكنولوجيا من خلال الاختبارات الدورية.

تنفيذ التحليل الأمني الضعيف

1

استخدام أدوات التحليل

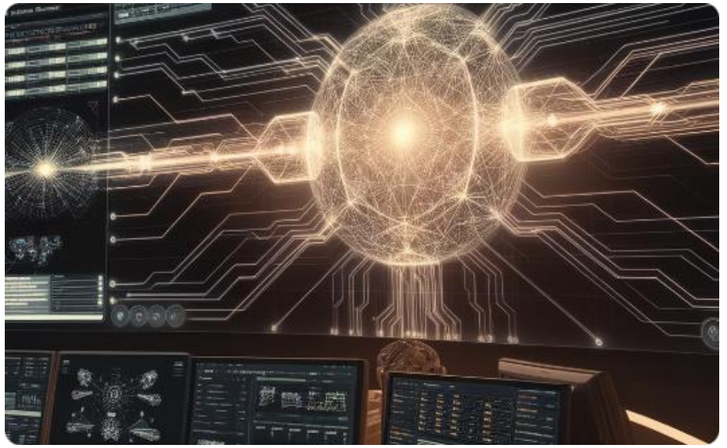
استخدام أدوات التحليل الأمني الضعيف لتحديد نقاط الضعف في الشبكة والأنظمة.

2

علاج نقاط الضعف

اتخاذ إجراءات لعلاج نقاط الضعف المكتشفة وتعزيز الأمن.

دور الذكاء الاصطناعي في الأمن السيبراني



تحليل البيانات

الذكاء الاصطناعي يمكن استخدامه لتحليل البيانات الكبيرة بسرعة وكفاءة لمواجهة التهديدات.

أمن الحوسبة السحابية

التوجهات المستقبلية تشمل تعزيز أمن الحوسبة السحابية والابتكارات في مجال الدفاع السيبراني.

كشف التهديدات

الذكاء الاصطناعي يساعد في الكشف السريع عن التهديدات السيبرانية من خلال تحليل البيانات الضخمة.