LOCKNETWORKS.

استشارات أمن المعلومات · الرياض

شريك أعمالك في الأمن السيبراني.

استشارات أمن المعلومات للشركات بمختلف أحجامها، من أمن الشبكات واختبار الاختراق إلى الانتقال إلى السحابة.



```
secops@lock-networks ~

$ assess   --attack-surface        [ ok ]
$ plan     --tailored              [ ok ]
$ deploy   --controls              [ ok ]
$ monitor  --continuous            ● live
$ respond  --incidents             ○ standby
$ support  --ongoing               ○ standby
$
```

RUH · 24.7136°N 46.6753°E



الملف التعريفي · 2026

فن الشبكات

LOCKNETWORKS.

ABOUT — 01

من نحن

الشبكة المحكمة (Lock Networks) شركة استشارات في أمن المعلومات، يديرها فريق من أصحاب الخبرة في أمن الشبكات والدفاع السيبراني. نقدّم استشارات أمنية تقنية آنية للشركات بمختلف أحجامها وأنواعها، مستندين إلى سنوات من الخبرة والكفاءة.

نتخصص في أمن المعلومات وإدارة مخاطر تقنية المعلومات، وهدفنا أن تتبع مؤسستك أفضل الممارسات للحدّ من المخاطر بأقل تكلفة ممكنة.

9

مجالات خدمية

7

مجالات تقنية نغطيها

60+

حل ومنتج يدعمها خبراؤنا

VISION — 02

الرؤية والرسالة والقيم



رؤيتنا

أن نكون الشريك الأول المعترف به عالميًا في استشارات أمن المعلومات، وأن نضع معيارًا للتميز والابتكار.

نطمح إلى بيئة رقمية أكثر أمانًا تزدهر فيها المؤسسات بثقة.



رسالتنا

تمكين المؤسسات من حماية أصولها الرقمية وبناء فضاء سيبراني آمن، من خلال خدمات استشارية متميزة في أمن المعلومات.

نعمل على فهم التهديدات السيبرانية المتطورة وتوقّعها والحدّ منها، مما يمكّن عملاءنا من الابتكار والنمو بثقة.

قيمنا

التميّز

نسعى إلى نتائج استثنائية ونطوّر مهاراتنا باستمرار لنبقى في طليعة أمن المعلومات.

الإبداع

نشجّع التفكير خارج المألوف لمواجهة تحديات الأمن المعقدة.

الموثوقية

ثبات والتزام بالمواعيد، ليثق بنا العملاء في احتياجاتهم الأمنية الحرجة.

الالتزام

نكرّس جهدنا لنجاح عملائنا وأمنهم، بدعم وإرشاد مستمرين طوال فترة العمل.

النزاهة

أمانة وشفافية وسرية في كل تعاملاتنا.

LOCKNETWORKS.

WHY US — 03

لماذا الشبكة المحكمة

ما يميّزنا.

01
الخبرة
فريق من أصحاب الخبرة في أمن الشبكات والدفاع السيبراني.

02
التخصص
نركّز على أمن المعلومات وإدارة مخاطر تقنية المعلومات، فتأتي الحلول مناسبة للمخاطر.

03
استشارات آنية
نصائح محدّثة وذات صلة مع تغيّر مشهد التهديدات.

04
كفاءة التكلفة
حلول فعّالة تقلل المخاطر بأقل تكلفة.

05
التركيز على العميل
نبدأ من متطلباتك ونفصّل خدماتنا بما يناسب أعمالك.

06
الابتكار
نستخدم تقنيات حديثة لبناء حلول تسبق التهديدات الناشئة.

07
الأمن الاستباقي
نساعدك على اكتشاف الثغرات وتوقّع التهديدات ومنع الاختراقات قبل وقوعها.

08
النهج الشمولي
نجمع الجوانب التقنية وغير التقنية في مشهد الأمن بأكمله.

09
شراكات طويلة الأمد
دعم وإرشاد مستمران لضمان أمنك ونجاحك على المدى الطويل.

10
الريادة الفكرية
نسهم في مجتمع الأمن السيبراني بالأبحاث والتعاون مع القطاع.

```
secops@lock-networks ~

$ assess  --attack-surface          [ ok ]
$ plan    --tailored                [ ok ]
$ deploy  --controls                [ ok ]
$ monitor --continuous              ● live
$ respond --incidents               ○ standby
$ support --ongoing                 ○ standby
$ ▌
```

APPROACH — 04

منهجية العمل

نهج شامل واستباقي لأمن المعلومات، في ست خطوات.

01

التقييم

نقيّم وضعك الأمني الحالي ونحدد الثغرات والمخاطر ومجالات التحسين.

02

التخطيط

بناءً على التقييم، نضع خطة أمنية مخصصة تناسب قطاعك وحجمك ومتطلباتك.

03

التنفيذ

ننفّذ الإجراءات الأمنية بحلول موثوقة وأفضل الممارسات، ومنها جدران الحماية والتشفير وضوابط الوصول وأنظمة كشف التسلل.

04

المراقبة

نُشئ مراقبة مستمرة لاكتشاف الحوادث الأمنية والاستجابة لها لحظة وقوعها، باستخدام أدوات استخبارات التهديدات.

05

الاستجابة للحوادث

عند وقوع حادث أمني نستجيب بسرعة لتقليل أثره واستعادة الأنظمة ومنع تكراره.

06

الدعم المستمر

نقدّم دعمًا وصيانة مستمرين لتبقى إجراءاتك الأمنية محدّثة وفعّالة أمام التهديدات المتطورة.

LOCKNETWORKS.

SERVICES · TECHNOLOGIES — 05-06

ما نقوم به

09 مجالات خدمية

07 مجالات تقنية نغطيها

01 الاستشارات الأمنية

02 أمن البنية التحتية للشبكات

03 إدارة الهوية والوصول

04 اختبار الاختراق

05 مراجعة الشيفرة المصدرية

06 الانتقال إلى السحابة

07 حماية البيانات

08 المراقبة الأمنية والاستجابة

09 الحوكمة والمخاطر والامتثال

SERVICES — 05

خدماتنا

تسعة مجالات تمتد من الاستشارات وأمن الشبكات إلى الهوية والاختبار والسحابة وحماية البيانات والمراقبة والامتثال.

01

الاستشارات الأمنية

تقييم المخاطر وتوصيات أمنية ودعم الاستجابة للحوادث.

02

أمن البنية التحتية للشبكات

جدران حماية وضبط وصول وبوابات وإدارة حركة البيانات لشبكتك.

03

إدارة الهوية والوصول

الهويات والمصادقة متعددة العوامل والدخول الموحد والتحكم في الوصول.

04

اختبار الاختراق

اختبار من منظور المهاجم لتطبيقات الويب والجوال والشبكات اللاسلكية وVoIP.

05

مراجعة الشيفرة المصدرية

مراجعة شيفرة التطبيقات على ثلاث مراحل: التحضير والتحليل والحلول.

06

الانتقال إلى السحابة

انتقال منظّم إلى Azure أو GCP أو Amazon، من التقييم حتى التدريب والدعم.

07

حماية البيانات

تصنيف البيانات والتشفير ومنع فقدانها ومراقبة قواعد البيانات.

08

المراقبة الأمنية والاستجابة

SIEM واكتشاف التهديدات على الأجهزة ومراقبة سلامة الملفات ودعم الاستجابة.

09

الحوكمة والمخاطر والامتثال

تقييم المخاطر وتحليل الفجوات والسياسات وفحوص الامتثال التقنية.

TECHNOLOGIES — 06

التقنيات التي نغطيها

الحلول والمنتجات التي يستطيع خبراؤنا دعمك فيها، حسب المجال.

08


أمن الشبكات

10


أمن الأنظمة

02


إدارة الهوية والوصول

02


أمن الويب والتطبيقات

01


أمن البيانات

01


إدارة السجلات وSIEM

04


إدارة الثغرات

60+

حل ومنتج يدعمها خبراؤنا

TECHNOLOGIES · 1/2 — 06

الحلول والمنتجات

الحلول والمنتجات التي يستطيع خبراؤنا دعمك فيها، حسب المجال.

01 أمن الشبكات

08

جدار الحماية من الجيل التالي (NGFW)	Fortinet · Cisco FTD · Palo Alto · pfSense
بوابة أمان الويب	Palo Alto · Cisco Umbrella · Zscaler
منع التسلل إلى الشبكة (IPS)	Trend Micro TippingPoint · Cisco FTD · Snort · McAfee
تصفية البريد الإلكتروني	Trend Micro · McAfee · Cisco ESA · Fortinet · Microsoft Defender for Office 365
SASE	Zscaler · Cloudflare · Cisco Umbrella · Microsoft
تصفية المحتوى وخادم الوكيل	McAfee · Forcepoint · Cisco WSA · Cisco Umbrella · Zscaler
أمن DNS	Zscaler · Cloudflare · Cisco Umbrella · Infoblox
موازنة الأحمال والتحكم في الوصول إلى الشبكة (NAC)	AVI · Fortinet FortiADC · F5 BIG-IP · Cisco ISE

02 أمن الأنظمة

10

اكتشاف التهديدات على الأجهزة الطرفية والاستجابة لها (EDR)	Trend Micro · Microsoft Defender · Cisco AMP · SentinelOne · CrowdStrike
مراقبة سلامة الملفات (FIM)	Qualys · Trend Micro · McAfee · OSSEC · Microsoft Defender for Cloud
التشفير	Trend Micro · Microsoft BitLocker · Thales · Symantec · McAfee
البنية التحتية للمفاتيح العامة (PKI)	Gemalto HSM · DigiCert · Microsoft · Fortanix HSM · Thales HSM · AppViewX CLM
منع فقدان البيانات (DLP)	McAfee · Forcepoint · Microsoft · Trend Micro
التحكم في التطبيقات	Cisco AMP · Trend Micro · McAfee
إدارة التحديثات	Intune · SCCM
جدار حماية التطبيقات والحماية من هجمات DDoS	Sucuri · Akamai · Imperva · Cloudflare · F5 Silverline
أمن الحاويات	Nessus · Twistlock (Palo Alto) · Qualys
وسيط أمان الوصول إلى السحابة (CASB)	Cisco Cloudlock · Microsoft · Forcepoint

الحلول والمنتجات

الحلول والمنتجات التي يستطيع خبراؤنا دعمك فيها، حسب المجال.

03 إدارة الهوية والوصول

02

المصادقة متعددة العوامل	Azure · Okta · Cisco Duo · Google Workspace
الدخول الموحد	Azure · Okta · Cisco Duo · Google Workspace

04 أمن الويب والتطبيقات

02

جدار حماية التطبيقات والحماية من هجمات DDoS	Akamai · F5 · Cloudflare · Azure · Sucuri · Fortinet FortiWeb · Barracuda · Imperva
مراقبة نشاط قواعد البيانات (DAM)	Imperva · Oracle · McAfee · Guardium

05 أمن البيانات

01

تصنيف البيانات واكتشافها وحمايتها	Microsoft Information Protection

06 إدارة السجلات وSIEM

01

SIEM	IBM · AlienVault · Microsoft Sentinel

07 إدارة الثغرات

04

فحص ثغرات البنية التحتية	Metasploit · Kali · Qualys · Nessus · Nmap
فحص ثغرات تطبيقات الويب	SQLMap · Nikto · Kali · Burp Suite · Netsparker · WebScarab · Metasploit · Acunetix
فحص امتثال البنية التحتية	Qualys · Nessus
فحص امتثال تطبيقات الويب	Qualys · Nessus

أخبرنا بما تحتاجه وسنعود إليك.

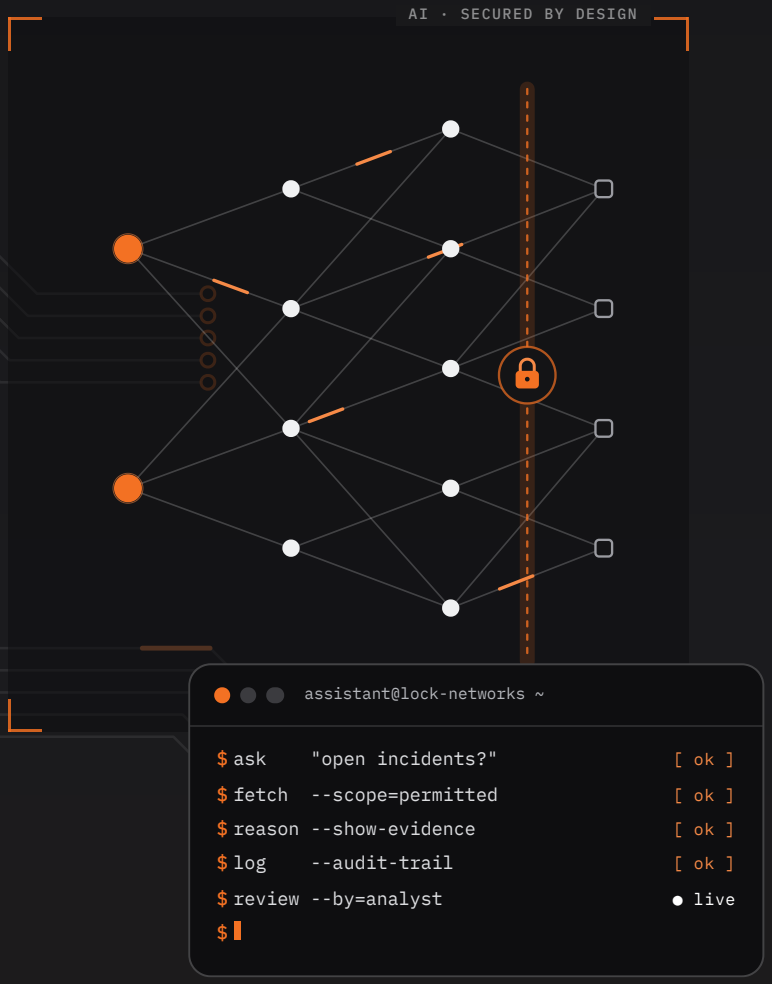
sales@locknetworks.sa
+966 54 394 3980

AI VISION · 1/2 — 07

ذكاء اصطناعي لأعمالك، والأمان مدمج فيه.

أصبح الذكاء الاصطناعي الطريق الذي يصل به الناس إلى بياناتهم وأنظمتهم والمعرفة الكامنة في مؤسستهم. إذا استُخدم جيدًا وفّر الوقت وحسّن القرارات، وإذا استُخدم دون ضوابط كشف المعلومات وبنى قراراته على إجابات لم يراجعها أحد.

رؤيتنا ذكاء اصطناعي آمن وخاضع للحوكمة ومرتبط بطريقة عمل مؤسستك الفعلية، يدعم حكم فريقك ويُبقي المسؤولية عليه.



كل إجابة يمكن تتبّعها،
وكل وصول مضبوط،
وكل قرار يبقى بيد إنسان.

AI VISION · 2/2 — 07

كيف نبني حلول الذكاء الاصطناعي

خمسة التزامات تقف خلف كل حل.

01

الأمان أولًا

نحمي بياناتك وهوياتك وعملياتك منذ أول قرار تصميمي، لا بإضافة الحماية في النهاية.

02

الإنسان يقود

يدعم الذكاء الاصطناعي خبراءك، ويراجع شخص مسؤول توصياته ويظل مسؤولًا عن النتيجة.

03

مصمَّم حول عملك

أنظمتك وإجراءات عملك وبيئة المخاطر لديك هي ما يشكّل الحل، والنموذج العام مجرد نقطة بداية.

04

حوكمة وقابلية للتدقيق

سياسات وسجلات وضوابط واضحة، لتعرف دائمًا ماذا فعل الذكاء الاصطناعي ولماذا.

05

تُقاس بالنتائج

قرارات أسرع وأمان أقوى وخدمة أفضل يمكن قياسها، لا تجربة تجريبية لا تصل إلى الإنتاج.

الثقة أولًا

قبل أن يلمس أي نظام ذكاء اصطناعي بياناتك، نحدد من يحق له الوصول إليها، وما الذي يُسجَّل، ومن يراجع المخرجات. وبذلك يبقى الذكاء الاصطناعي ضمن سياساتك والتزاماتك التنظيمية.

ضوابط الذكاء الاصطناعي المسؤول

- خصوصية البيانات
- التحكم في الوصول
- أطر الحوكمة
- سجلات التدقيق
- مراقبة استخدام الذكاء الاصطناعي
- صلاحيات حسب الإدارة
- خيارات داخل المنشأة وهجينة
- التبنّي المسؤول
- أمن المؤسسات

ما يمكن للذكاء الاصطناعي أن يقدّمه لمؤسستك

ستة مجالات نساعدك فيها على توظيف الذكاء الاصطناعي عمليًا.

01

المعرفة المؤسسية

مكان واحد تسأل فيه عن سياسات مؤسستك ووثائقها التقنية وقراراتها السابقة، بدل البحث في أنظمة متفرقة.

مساعد المعرفة · دعم الوثائق · ملخصات الاجتماعات · الاستفسار عن السياسات

02

دعم القرار

بيانات من مصادر متعددة تتحول إلى رؤى قابلة للتفسير، وكل استنتاج يمكن تتبّعه إلى الأدلة التي بُني عليها، فيقرر القادة بسرعة وثقة أكبر.

تحليل مصادر متعددة · نتائج قابلة للتفسير · قابلية التتبّع

03

عمليات الأمن

عون لمحللي مركز عمليات الأمن (SOC) في فرز التنبيهات وجمع الأدلة واقتراح خطوات الاستجابة، ليقل الوقت الضائع في الضجيج ويزيد المخصص للتهديدات الحقيقية.

فرز التنبيهات · تحليل المخاطر · إرشاد التحقيق · توصيات المعالجة · ترتيب الثغرات بحسب الأولوية

04

تجربة العملاء والموظفين

مساعدون يفهمون السياق ويجيبون بدقة: خدمة أسرع للعملاء، وإجابات أسرع للموظفين.

خدمة ذكية · استجابة أسرع · وصول مخصّص إلى المعرفة

05

عمليات تقنية المعلومات

أتمتة التحليلات الروتينية وتلخيص الحوادث، ليتفرغ المهندسون للأعمال التي لا يقوم بها غيرهم.

مساعدة أدلة التشغيل · ملخصات الحوادث · البحث في المعرفة التشغيلية

06

الحوكمة والامتثال

السياسات وتقييمات المخاطر ونتائج التدقيق ومتطلبات الامتثال تُشرح بلغة واضحة وتُربط بالإجراءات التي تتطلبها.

مراجعة الأدلة · ربط الضوابط بالمتطلبات · ملخصات الاستثناءات · فهم السياسات

هل تتساءل أين يناسبك الذكاء الاصطناعي؟

أخبرنا أين يضيع أكثر وقت فريقك. نبدأ من هدف العمل، ونتحقق من الجاهزية، ونجرّب على مسار عمل واحد، ثم ننشر حيث يجب أن تبقى بياناتك: داخل المنشأة أو بشكل هجين أو في سحابة آمنة.

sales@locknetworks.sa

+966 54 394 3980

CONTACT — 09

تواصل معنا

أخبرنا بما تحتاجه وسنعود إليك.

فن الشبكات

sales@locknetworks.sa

+966 54 394 3980

locknetworks.sa

الرياض، المملكة العربية السعودية

المقر المسجّل: HDB Hotel Aqeeq، 4135 طريق الملك فهد الفرعي، الرياض، المملكة العربية السعودية



© 2026 الشبكة المحكمة (Lock Networks). جميع الحقوق محفوظة.