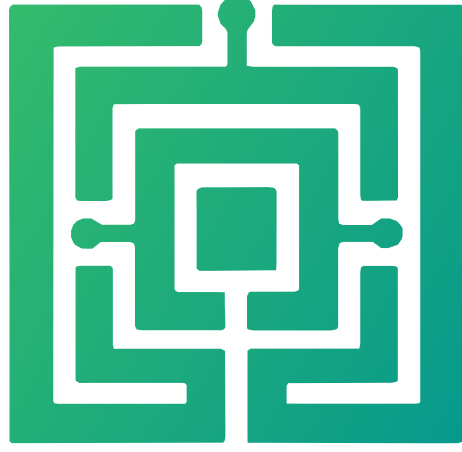


التقنية · الدفاع السيبراني · التجارة



TORAIZON

بروشور الأمن السيبراني ومركز العمليات الأمنية

الأمن الهجومي والدفاعي والمُدار — بالتفصيل

الأمن السيبراني • مركز العمليات الأمنية المُدار

أمن مُدار ومُثبت

أمن يُبنى ويُشغّل ويُثبت بفريق واحد.

01

الأمن السيبراني

هجوم ودفاع تحت سقف واحد. اختبار اختراق، فرق حمراء، تدقيق امتثال، إدارة هوية، أمن سحابي واستجابة للحوادث — كل ما يقف بين عملك وبين اختراق محتمل.

- ◆ تقييم الثغرات واختبار الاختراق
- ◆ الفريق الأحمر ومحاكاة الخصم
- ◆ التدقيق الأمني والامتثال
- ◆ كشف واستجابة نقاط النهاية (EDR/XDR)
- ◆ إدارة الهوية والوصول
- ◆ أمن السحابة وإدارة وضعية الأمان السحابي
- ◆ أمن التطبيقات وواجهات البرمجة
- ◆ منع تسرب البيانات والتشفير
- ◆ الاستجابة للحوادث والتحقيق الجنائي الرقمي
- ◆ التوعية الأمنية ومحاكاة التصيد

02

مركز العمليات الأمنية المُدار

مراقبة تهديدات على مدار الساعة مدعومة بالكامل بمنظومتنا الأمنية الخاصة. بلا أدوات من أطراف ثالثة. تحكم كامل. أقصى قدر من الاستخبارات. متوسط زمن الفرز: 4.2 دقيقة.

- ◆ كشف واستجابة مُدارة على مدار الساعة
- ◆ نشر وإدارة نظام إدارة معلومات وأحداث الأمان
- ◆ صيد التهديدات واستخبارات التهديدات
- ◆ إدارة عمليات EDR/XDR المُدارة
- ◆ إدارة السجلات والربط بينها
- ◆ التنسيق الأمني والأتمتة والاستجابة (SOAR)
- ◆ إدارة جدران الحماية وأنظمة الكشف/المنع المُدارة
- ◆ برنامج إدارة الثغرات
- ◆ خطط تصعيد الحوادث والاستجابة
- ◆ تقارير الوضعية الأمنية الشهرية

الأطر التي نتوافق معها — جاهزون للامتثال

NIST CSF

GDPR

HIPAA

PCI-DSS

SOC 2

ISO 27001

NCA ECC

SAMA CSF

الأمن السيبراني

هجوم ودفاع تحت سقف واحد. اختبار اختراق، فرق حمراء، تدقيق امتثال، إدارة هوية، أمن سحابي واستجابة للحوادث — كل ما يقف بين عملك وبين اختراق محتمل.

01

تقييم الثغرات واختبار الاختراق

اختبارات اختراق للويب والشبكة والسحابة والجوال تكشف الثغرات قبل المهاجمين.

02

الفريق الأحمر ومحاكاة الخصم

محاكاة خصم شاملة تختبر الأفراد والعمليات والتقنية معًا.

03

التدقيق الأمني والامتثال

تحليل فجوات ودعم اعتماد لـ ISO 27001 و SOC 2 و PCI-DSS والضوابط الأساسية للأمن السيبراني وغيرها.

04

كشف واستجابة نقاط النهاية (EDR/XDR)

رؤية فورية لنقاط النهاية واحتواء آلي ضد البرمجيات الخبيثة الحديثة.

05

إدارة الهوية والوصول

صلاحيات وفق مبدأ الحد الأدنى، مصادقة متعددة العوامل وحوكمة هوية عبر كل تطبيق.

06

أمن السحابة وإدارة وضعية الأمان السحابي

إدارة وضعية مستمرة عبر AWS و Azure و GCP والبيئات الهجينة.

07

أمن التطبيقات وواجهات البرمجة

دورة حياة تطوير آمنة، مراجعة كود وتحصين واجهات برمجية ضمن خط الإنتاج لديك.

08

منع تسرب البيانات والتشفير

ضوابط قائمة على السياسات تمنع خروج البيانات الحساسة من بيئتك.

09

الاستجابة للحوادث والتحقيق الجنائي الرقمي

احتواء سريع وتحقيق في السبب الجذري وحفظ أدلة موثقة سلسلة الحياة.

10

التوعية الأمنية ومحاكاة التصيد

تدريب مستمر للموظفين وحملات تصيد محاكاة تقلل المخاطر بشكل قابل للقياس.

عملية التنفيذ — من النطاق إلى المعالجة

01

تحديد النطاق

تحديد الأنظمة المستهدفة وقواعد الاشتباك وأهداف الامتثال.

02

الاختبار

اختبار يدوي وآلي وفق النطاق المتفق عليه.

03

التحقق

التحقق اليدوي من كل نتيجة لاستبعاد الإيجابيات الكاذبة.

04

التقرير

ملخص تنفيذي مع إرشادات معالجة تقنية.

05

إعادة الاختبار

إعادة اختبار مجانية للتأكد من إغلاق كل إصلاح للثغرة.

يقوم مهندسو الامتثال لدينا بربط كل ضابط بدليله — فيصبح تدقيقك القادم إجراءً شكليًا، لا أزمة طارئة.

مركز العمليات الأمنية

مراقبة تهديدات على مدار الساعة مدعومة بالكامل بمنظومتنا الأمنية الخاصة. بلا أدوات من أطراف ثالثة. تحكم كامل. أقصى قدر من الاستخبارات. متوسط زمن الفرز: 4.2 دقيقة.

02	نشر وإدارة نظام إدارة معلومات وأحداث الأمن ربط سجلات مركزي وتنبيهات مُهيأة لبيئتك.
01	كشف واستجابة مُدارة على مدار الساعة مراقبة مستمرة بإشراف بشري عبر كل بيئتك.
04	إدارة عمليات EDR/XDR المُدارة إدارة كاملة لدورة حياة أدوات كشف نقاط النهاية والكشف الموسّع.
03	صيد التهديدات واستخبارات التهديدات عمليات صيد استباقية قائمة على الفرضيات ومدعومة بمصادر استخبارات تجارية وشبكة الإنترنت المظلم.
06	التنسيق الأمني والأتمتة والاستجابة (SOAR) أتمتة قائمة على خطط تشغيل تحليل التنبيهات الروتينية خلال ثوانٍ.
05	إدارة السجلات والربط بينها سجلات موحدة ومحفوظ بها عبر نقاط النهاية والشبكة والهوية والسحابة.
08	برنامج إدارة الثغرات فحص مستمر وترتيب أولويات وتتبع معالجة.
07	إدارة جدران الحماية وأنظمة الكشف/المنع المُدارة ضبط القواعد والتحديث والمراقبة على مدار الساعة لدفاعات المحيط.
10	تقارير الوضعية الأمنية الشهرية تقارير جاهزة للإدارة التنفيذية عن اتجاهات المخاطر والحوادث وتغطية الضوابط.
09	خطط تصعيد الحوادث والاستجابة خطط تشغيل جاهزة ومُختبرة تقلل زمن الاستجابة عند الحاجة.

دورة حياة الكشف – من الإشارة إلى الاستجابة

05	04	03	02	01
الصيد والتحسين	الاستجابة	الفرز	الكشف	الجمع
عمليات صيد بعد الحادث؛ ضبط القواعد؛ تحديث خطط التشغيل؛ تغذية الدروس المستفادة في الكشف.	احتواء وعزل وتوثيق أدلة – بإشراف بشري وفق خطط تشغيل.	محللو المستوى الأول يتحققون من التنبيهات؛ SOAR يحل الروتيني منها تلقائيًا.	نماذج تعلم آلي وقواعد سلوكية ومطابقة مؤشرات اختراق عبر منظومة بيانات موحدة.	بيانات نقاط النهاية والشبكة والهوية والسحابة والتطبيقات – موحدة ومؤثرة.

منظومة توريزون – منظومتنا الخاصة

كل أداة في مركزنا الأمني مبنية ومملوكة من توريزون. لا عوائق ترخيص من موردين. لا بيانات تخرج من بيئتك دون إذن.

TZ-DLP

Data Loss Prevention

TZ-MDR

Managed Detection & Response

TZ-XDR

Extended Detection & Response

TZ-EDR

Endpoint Detection & Response

TZ-NDR

Network Detection & Response

TZ-SOAR

Orchestration & Automation

TZ-SIEM

Security Info & Event Mgmt

TZ-RMM

Remote Monitoring & Mgmt

مستويات التعاقد – اختر وضعيتك

من الإدارة المشتركة إلى التعهيد الكامل – نتوسع مع فريقك.

SOVEREIGN

محلي / منظم

مركز أمني معزول ومقيّد بالولاية القضائية للجهات الحكومية والدفاعية والمالية والقطاعات المنظمة.

- ◆ كل ما في المستوى المتميز
- ◆ خيار محلي / معزول بالكامل
- ◆ ضوابط سيادة البيانات
- ◆ محللون مصرّح لهم (مقيّدون باتفاقية سرية)
- ◆ احتفاظ وولاية قضائية مخصصة
- ◆ خيار اتفاقية استجابة حرجة أقل من ساعة

ELITE

الأكثر توازنًا

كشف واستجابة شاملان مع صيد استباقي للتهديدات وفريق محللين مخصص.

- ◆ كل ما في المستوى الأساسي
- ◆ صيد تهديدات + توافق مع إطار MITRE
- ◆ خطط أتمتة SOAR
- ◆ احتفاظ 365 يومًا
- ◆ فريق محللين مخصص
- ◆ اتفاقية استجابة حرجة أقل من 4 ساعات

CORE

أساسي

للمؤسسات النامية التي تحتاج مراقبة احترافية دون مركز أمني داخلي.

- ◆ مراقبة نقاط نهاية وشبكة على مدار الساعة
- ◆ نظام SIEM مع احتفاظ 90 يومًا
- ◆ تقرير تهديدات شهري
- ◆ دعم عبر البريد والتذاكر
- ◆ خطط تشغيل قياسية للحوادث

التقنية · الدفاع السيبراني · التجارة

لنبدأ معًا

اطلب عرضًا أو عرضًا توضيحيًا أو سعرًا — نرد خلال 48 ساعة.

+91 98951 99521

واتساب / هاتف

info@toraizon.net

البريد الإلكتروني

infotrade@toraizon.com.sa

استفسارات التجارة

www.toraizon.com.sa

الموقع

مبنى 6845، حي السلي، الرياض، المملكة العربية السعودية

العنوان