
CZ SENTINEL
شاهد ما يراه المهاجمون
منصة استخبارات الانكشاف الرقمي وإدارة سطح الهجوم الخارجي
CYBERZONES
Innovation & Research Division

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

لماذا تحتاج المؤسسات إلى Sentinel؟

معظم الهجمات السيبرانية لا تبدأ باستغلال ثغرة مباشرة... بل تبدأ بمرحلة الاستطلاع (Reconnaissance).

- البحث عن أصول غير مُدارة أو منسية
- إعدادات مكشوفة دون قصد
- معلومات عامة قابلة للاستغلال
- آثار رقمية تكشف بنية المؤسسة التقنية

المشكلة أن كثيراً من المؤسسات لا تدرك حجم انكشافها العلني إلا بعد استغلاله.

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

ما هي منصة Sentinel فعلياً؟

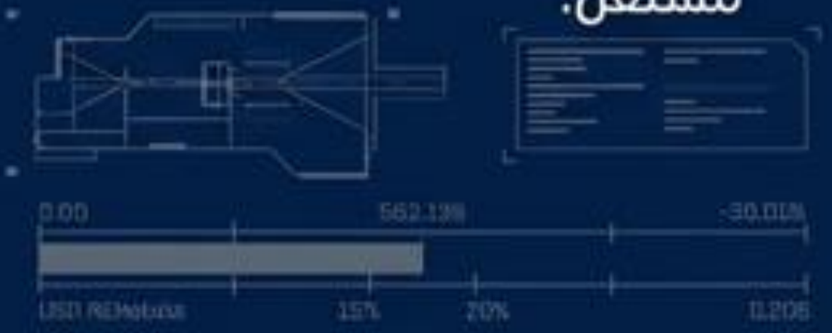
Sentinel ليست أداة فحص اختراق تقليدية، وليست ماسح ثغرات داخلي.

هي منصة استخبارات تعرّض رقمي، تركز على ما ظهر للعلن وتحوّله إلى رؤية مخاطر قابلة للإدارة.

تركز على فهم وتحليل سطح الهجوم الخارجي من منظور المهاجم.

1. اكتشاف سطح الهجوم الخارجي
(External Attack Surface Discovery)

- تحديد النطاقات والأصول المرتبطة بالمؤسسة.
- تحليل الخدمات الظاهرة للعامة.
- كشف الأصول التي قد لا تكون ضمن الحوكمة الرسمية (Shadow IT).
- إظهار البنية الرقمية من منظور خارجي مستقل.



CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

2. مراقبة الانكشاف المستمر
(Continuous Exposure Monitoring)

تحليل الفروق (Delta Intelligence) **بين الفترات الزمنية.**

- متابعة التغيرات في الوجود الرقمي.
- رصد ظهور أصول جديدة غير معتمدة.
- اكتشاف تغيرات قد تزيد مستوى المخاطر.

ماذا تغير؟

الأصول الجديدة، الانكشافات الانكشافات الحديثة، التغير في مستوى المخاطر.

CYBER ZONES
CZ SENTINEL

3. تحويل البيانات المفتوحة إلى استخبارات سياقية (OSINT-Driven Risk Intelligence)

بيانات مفتوحة
(Open Data)

تحليل البيانات المتاحة علناً
وربطها بسياق المخاطر.

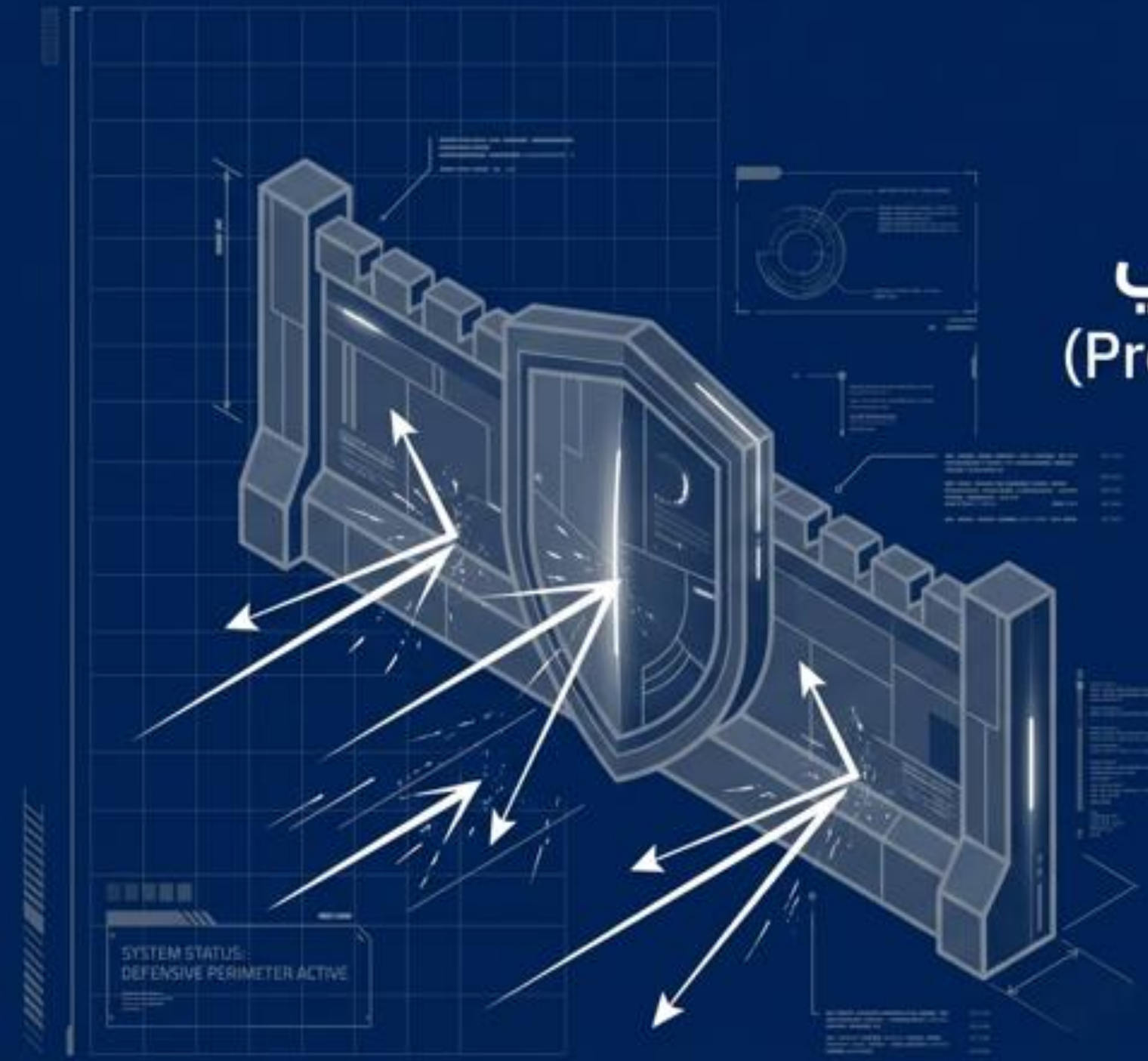
تحليل البيانات
(Data Analysis)

تصنيف مستوى الانكشاف.
(Exposure Classification)

دعم اتخاذ القرار الأمني بناءً
على رؤية خارجية مستقلة.

استخبارات سياقية
(Contextual Intelligence)

CYBER ZONES
SENTINEL
SEE WHAT ADVERSARIES SEE



4. دعم الأمن الاستباقي
(Preventive Security Posture)

- معالجة الانكشاف قبل استغلاله.
- تقليل احتمالية أن تصبح هدفاً سهلًا.
- تحسين إدارة الأصول الرقمية غير المرئية داخلياً.

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

آلية العمل: من الجمع إلى التحليل

مثال: في حال ظهور نطاق فرعي جديد غير مُدار مرتبط بالمؤسسة، يقوم Sentinel باكتشافه، مقارنته بالنتائج السابقة، وتسجيله كتغيّر جديد قد يمثل نقطة انكشاف محتملة قبل أن يتم استغلاله.

كيف تختلف Sentinel عن أدوات الأمن التقليدية؟

Sentinel	أدوات تقليدية
تركز على المخاطر الخارجية	تركيز داخلي على الشبكة
لا تحتاج وصول داخلي	تحتاج وصول للنظام
تكتشف الانكشاف والسياق	تكتشف ثغرات تقنية مباشرة
تعالج مرحلة ما قبل الهجوم	تعمل بعد الاختراق غالباً
رؤية من منظور المهاجم: أساسية في التصميم	رؤية من منظور المهاجم: محدودة

Sentinel لا تستبدل أدوات الأمن التقليدية، بل تكملها من خلال سد فجوة الرؤية الخارجية.

تطوير داخلي مبني على الخبرة

منصة استخبارات مبنية على خبرات استشارية
وعملية في تحليل التعرض المؤسسي.

سيادة البيانات والعمل كنظام محلي

(On-Premise)

توليد تقارير احترافية قابلة للمشاركة على مستوى الإدارة العليا.

لا يعتمد على بيانات طرف ثالث جاهزة فقط، بل يعيد تحليل الانكشاف في سياق المؤسسة نفسها.

يمنح المؤسسة تحكماً كاملاً كاملاً في بياناتها دون الاعتماد على منصات خارجية سحابية.

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

الخلاصة

- منصة استخبارات انكشاف رقمي وإدارة سطح الهجوم الخارجي.
- مطورة داخلياً بواسطة Cyber Zones ضمن مبادرات البحث والتطوير.
- تركز على مرحلة ما قبل الهجوم.
- تحول البيانات المفتوحة إلى رؤية مخاطر عملية.
- تمنح المؤسسة منظور المهاجم... قبل أن يبدأ الهجوم.

CYBER ZONES
CZ SENTINEL

ابدأ برؤية ما يراه المهاجمون

تدعو شركة سايبر زونز الشركات والأفراد المهتمين إلى تجربة المنصة.

https://cyber-zones.com/
Get in touch: info@cyber-zones.com

CYBER ZONES
DIGITAL ZONES CONSULTING