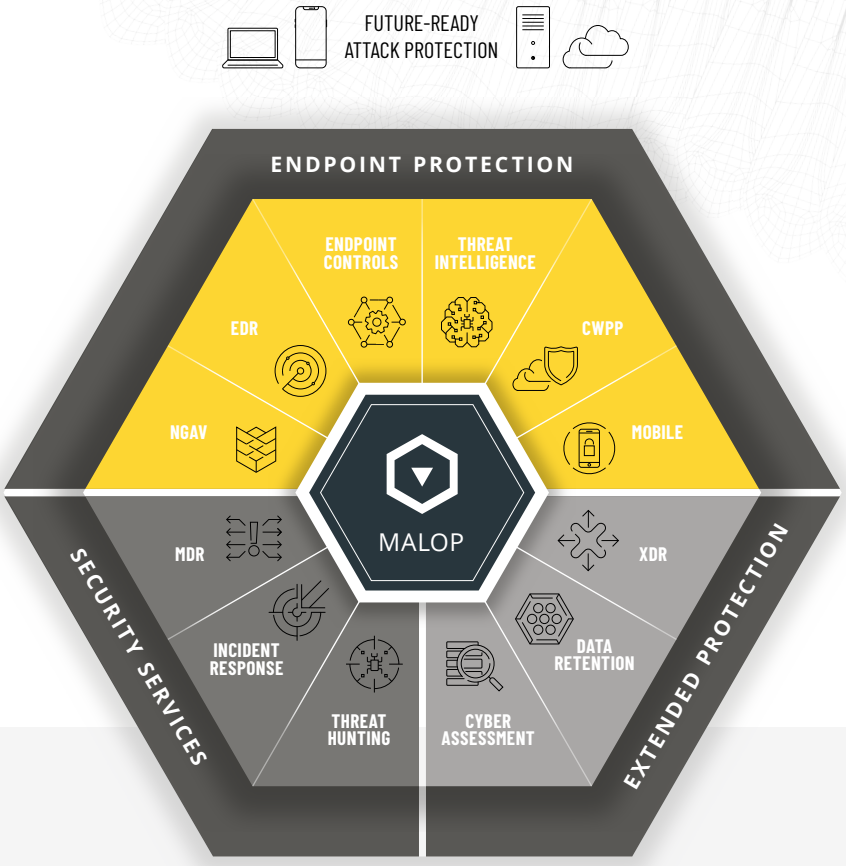
منصة "سايبريزون" الدفاعية

إدارة آمنة لنقاط النهاية



المزايا الرئيسية:

- فعالية مضمونة دون أي تأثير سلبي: خيارات سريعة ومرنة لنشر أدوات المنصة عبر السحابة وعلى أجهزة العملاء
- حماية متعددة الطبقات: الحماية الأفضل من برامج الفدية ومخاطر الطرف الثالث
- سياق سلس: آلية رصد توفر عرضاً مرئياً لمسار الهجوم بدلاً من التركيز على التنبيهات
- إصلاح مباشر: توفير الكثير من الوقت في عمليات التحقيق وإصلاح الضرر خلال دقائق بدلاً من ساعات

SUPPORTED SYSTEMS
WINDOWS MAC & IOS ANDROID LINUX

DEPLOYMENT OPTIONS
CLOUD FIRST HYBRID ON-PREM AIR-GAPPED

مصممة لتحقيق أهدافك الاستراتيجية

لعل أكثر ما يميز عصر تكنولوجيا المعلومات هو تعرضك المستمر للمخاطر والهجمات السيبرانية. وانطلاقاً من تفاعلها مع مستجدات هذا العصر، تدرك "سايبريزون" مدى حاجتك اليوم - أكثر من أي وقت مضى - الى شريك موثوق يمكن الاعتماد عليه. ولأن أغلب المهاجمين تلقوا تدريباً لدى جهات حكومية وعسكرية، فإننا في "سايبريزون" نعمل على قلب موازين القوى للتغلب عليهم عبر توظيف ألمع العقول والخبرات من الجهات الأمنية والعسكرية وخبراء أمن الشركات لتطوير ووضع أكثر طرق الحماية المتقدمة بين يديك.

حل متكامل

ترتكز استراتيجية عمل "سايبريزون" على توحيد الجهود مع فرق أمن المعلومات في مؤسسات العملاء لصد المهاجم وإبطال مفعوله. وتعمل منصة "سايبريزون" الدفاعية على حماية جميع نقاط النهاية في شبكة العميل باستخدام وحدة تحكم واحدة وفريق عمل متمرس يرصد ويعترض جميع العمليات الخبيثة وفق آلية خاصة ندعوها Malop (المصطلح مشتق اختصاراً من كلمتي Malicious Operation). وتوفر هذه الآلية عرضاً مرئياً لسياق الهجوم بالكامل، بعيداً عن الأسلوب التقليدي في إطلاق االإشعارات ولتنبيهات. ووحدها "سايبريزون" توفر معلومات يمكن استخدامها لاستباق تفكير المهاجم، وإصلاح الضرر بأسرع من وتيرة عملياته، بالإضافة إلى تقديم رؤى استباقية كفيلة بإنهاء أي هجوم آخر.

الأدوات التي يحتاجها فريقك

- **وضوح الرؤية لاستباق تفكير المهاجم**

تعمل منصة "سايبريزون" الدفاعية على تتبع مسار العمليات الخبيثة وإنهائها مع توفير عرض مرئي لسياق الهجوم كاملاً ابتداءً من السبب الجذري وانتهاءً بجميع المستخدمين والأجهزة المتضررة. وخلال ساعات قليلة فقط، يمكن نشر أدوات المنصة عبر الآلاف من نقاط النهاية لتوفير حماية فورية دون التأثير على تجربة المستخدم أو إنتاجيته.

- **السرعة لاستباق خطوات المهاجم**

تضمن المنصة تحليل الهجمات واستباق تحركات المهاجم مع صد التهديدات الناشئة في غضون دقائق وليس أيام. وتتيح آلية رصد العمليات الخبيثة (Malop) لفريق أمن المعلومات في مؤسستك رؤية مسار ونطاق الهجوم بالكامل من نقاط النهاية إلى جميع المستخدمين والأجهزة المتضررة، بالإضافة إلى جميع عمليات الاتصال الصادرة والواردة، والخط الزمني الكامل للهجوم. وسواء كان الهجوم عبارةً عن برمجية خبيثة عامة أو تهديداً يستهدف مؤسستك بالذات، ستتمكن حتماً من فهمه وإصلاحه بمنتهى الثقة.

- **الحزم في إنهاء الهجمات**

تتيح المنصة لفريق أمن المعلومات في مؤسستك إمكانية إصلاح الأضرار على امتداد الشبكة إما تلقائياً أو يدوياً بنقرة زر واحدة، وبالتالي إنهاء الهجمات دون الحاجة إلى إجراء تحليلات مطولة. ويمكن للمحللين تنفيذ مجموعة كاملة من عمليات الإصلاح ابتداءً من عزل الأجهزة المتضررة وإحباط إجراءات العمليات الخبيثة وانتهاءً بإزالة آليات استمرارها وتواجدها. ويتم ذلك كله عن طريق واجهة سهلة الاستخدام تعمل بطريقة التأشير والنقر. ويمكن تنفيذ محاور التحقيق وتعقب التهديدات بسهولة تامة دون الحاجة إلى تحريات معقدة، الأمر الذي يمكّن محللي المستويين الأول والثاني من إنجاز مهامهم بنفس الكفاءة التحليلية المطلوبة للمستوى الثالث.
باختصار، تجعل "سايبريزون" العميل على معرفة تامة بالتفاصيل الدقيقة للتهديد مع إيضاح مسار الهجوم بشكل أفضل، وفهم الارتباطات السياقية المطلوبة لبناء قدرات أمنية استباقية.

حول "سايبريزون"

"سايبريزون" هي المنصة الأبرز اليوم للحماية من الهجمات السيبرانية، وتوفر حماية استباقية تغطي شبكة العميل بالكامل ابتداءً من نقاط النهاية وصولاً إلى المشاريع وجميع الجوانب الأخرى. وتجمع منصّة "سايبريزون" الدفاعية أفضل حلول الكشف والاستجابة (الكشف والاستجابة في نقاط النهاية EDR والكشف والاستجابة الموسعة XDR) مع الجيل الأحدث من حلول مكافحة الفيروسات، والرصد الاستباقي للتهديدات بهدف توفير تحليل مفصّل لجميع عناصر العمليات الخبيثة. وبذلك يمكن للمدافعين إنهاء الهجمات السيبرانية من نقاط النهاية إلى جميع عمليات الشركة عن آخرها.

CYBEREASON.COM/DEMO