LogRhythm
The Security Intelligence Company

أنظمة الاستخبارات الأمنية المعلوماتية

قم بتحديث أنظمة الرصد والاستجابة للتهديدات الأمنية المعلوماتية

اكتشف التهديدات الأكثر خطورة

ستتمكن من رصد التهديدات الأمنية المتقدمة باستخدام قدرات تحليل البيانات وآليات التعلم الذاتي التي يتضمنها محرك الذكاء الاصطناعي في لوجريثم، حيث أن تقنيات مقارنة الأنشطة وتحليل التهديدات الأمنية قادرة علة إجراء حسابات دقيقة لتقييم المخاطر وتحديد أولوية معالجتها. ليتمكن فريق العمل لديك من التركيز على المواضيع الأكثر إلحاحًا وأهمية.

ضع حدًا للتهديدات الداخلية وسرقة حسابات المستخدمين

لا يمكنك إغلاق الحسابات المستخدمين التي يُساء استغلالها من قبل المخربين إلا إذا تمكّنت من رؤيتها أولًا. يقوم محرك تحليل سلوكيات المستخدمين بتسليط الضوء على التهديدات الداخلية والصلاحيات المسروقة لتتمكن من التعرف على الحسابات المارة والصلاحيات التي يُساء استغلالها ووقف التهديدات الناشئة من تلك الحسابات.

قم برصد أي شذوذ في الشبكة أو أجهزة المستخدمين

راقب أنشطة الشبكة وأجهزة المستخدمين لتتمكن من رصد الهجمات المحتملة مثل محاولات التصيد والثغرات الأمنية المستجدة. تقوم لوجريثم بتحديث أدوات رصد تهديدات الشبكة وأجهزة المستخدمين للتحقق من قدرتها على التعامل مع الخصوم السيبرانيين.

ابحث بدقة وفعالية

قم بالتحري وفق حاجتك وبدون ضوضاء. يعتمد نظامنا على تقنيات نسيج الذكاء الاصطناعي (MDI)، الذي يستمد بياناته من أكثر من ٧٥٠ مصدر مختلف، ويقوم آليًا بوضع تلك البيانات في السياق المناسب. كما يساعدك نظام لوجريثم على استغلال بيانات الأجهزة وسجلات الأنشطة والقيام باستخلاص وتصنيف المعلومات المجمّعة للتمكّن من رصد التهديدات الأمنية المتقدمة والاستجابة لها وتفادي أضرارها.

نسّق وبرمج آليات الاستجابة

قم بإخماد التهديدات بسرعة باستخدام أدوات التنسيق التعاوني للإجراءات التي قمنا بتضمينها في ميزة إدارة الحوادث الأمنية المعلوماتية، حيث يمكنك ضبط إعدادات التحقيق والتعافي لتستفيد من الوظائف مسبقة الإعداد المشمولة في إطار SmartResponse™ للاستجابة الآلية. كما يمكنك تقييم مستوى عملية الاستجابة من حيث الوقت اللازم لعمليتي الرصد والاستجابة، وبالتالي تحسين الإجراءات المعتمدة تدريجيًا.

قم بتبسيط آليات الالتزام بالمعايير

توفر لوجريثم أدوات مسبقة الإعداد للالتزام الآلي بعدة معايير وأطر تنظيمية مثل: ISO ٢٧٠٠١ وPCI-DSS وFISMA وHIPAA وSOX و NIST وغيرها.

قم برصد التهديدات الأمنية السيبرانية والاستجابة ها وإخمادها

يمكن أن تنشأ الهجمات من داخل المؤسسة أو خارجها. يمكن ستحتاج إلى منظور موحّد لجمع التهديدات المتربصة قبل أن تتمكن من إخماد تلك التهديدات ومنعها من أن تتحول إلى اختراقات أمنية. استخدم لوجريثم لرصد التهديدات الناشئة وإخمادها بسرعة.

تعرف على إمكانيات لوجريثم

يمكننا مساعدتك في رصد التهديدات الأمنية المعلوماتية والاستجابة لها وإخمادها قبل أن تسبب الضرر لأعمالك.
للتعرف على إمكانياتنا قم بزيارة الوصلة التالية: www.logrhythm.com/demo

SC MAGAZINE ★★★★★

Gartner
A 2016 LEADER
SIEM Magic Quadrant

Gartner
HIGHEST SCORE | ALL 3 USE CASES
2015 SIEM CRITICAL CAPABILITIES

VENDOR LANDSCAPE AWARD
CHAMPION

FROST & SULLIVAN
2015 Global SIEM
Enabling Technology Leadership Award

WWW.LOGRHYTHM.COM/DEMO

المدخلات

جمع البيانات في الوقت الحقيقي

توليد البيانات في الوقت الحقيقي

الرقابة على الشبكات

التسجيل الكامل للبيانات — التحليل المتعمق لحزم البيانات — حركة البيانات في الطبقة السابعة — تفحص حزم البيانات والتطبيقات

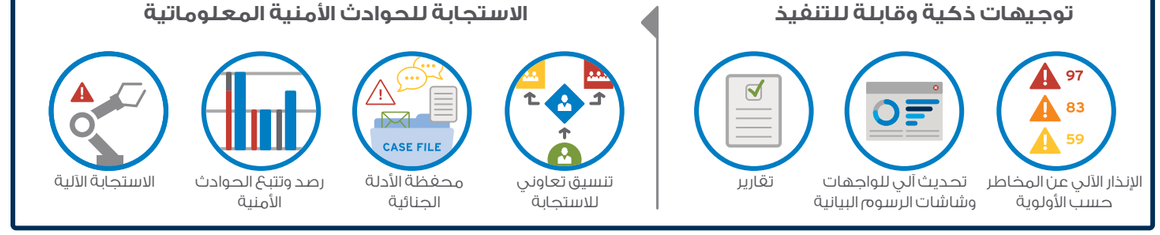
الرقابة على الأجهزة

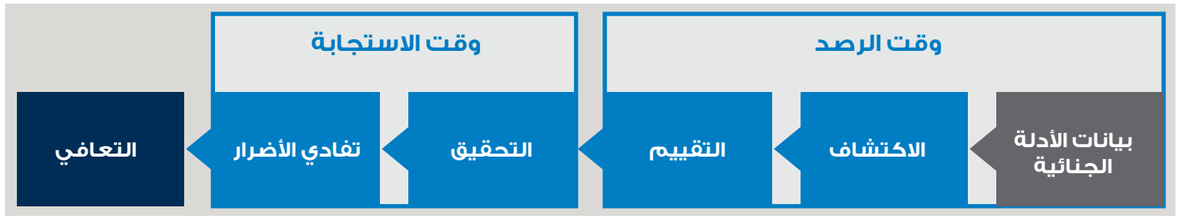
أنشطة المستخدمين — اتصالات الشبكة — أنشطة العمليات والخدمات — مصداقية سجل الملفات

أدوات التحليل

استخبارات وأبحاث مختبرات LogRhythm

المخرجات





قم بتوحيد آليات التحري والتحليل

قم بإتمام مهمتك

مهمتك هي أمن المعلومات، وهي مهمتنا أيضًا. قم بتمكين موظفيك عن طريق نظامنا المصمم لأغراض التحري والتحليل في الأنشطة المتعلقة بأمن المعلومات. وقم كذلك بتطبيق سيناريوهات الالتزام بمعايير أمن المعلومات بسرعة وكفاءة، وركز جهود موظفيك في حماية المؤسسة بدلًا من إنهاكهم في ضبط إعدادات الأنظمة الأمنية.

احصل على نطاق رؤية مركزي وموحّد

اجمع كافة الأدلة الجنائية المولدة في بيئة مؤسستك (مع أو بدون تركيب أدوات إضافية على الأجهزة)، وقم بالتخلص من مخازن تجميع البيانات، واحصل على نطاق رؤية مركزي مع نظام لوجريثم.

راقب الشبكة وأجهزة المستخدمين

قم بتغطية أي فجوات في بيانات الأدلة الجنائية عن طريق الرقابة على الشبكة وأجهزة المستخدمين. يوفر نظامنا مجسّات للرقابة على الشبكة والأجهزة للتأكد من الحصول على جميع تفاصيل الأدلة الجنائية التي تحتاجها لرصد وإخماد التهديدات الأمنية المتقدمة.

افهم بياناتك

فم بالتحري وفق حاجتك وبدون ضوضاء. يعتمد نظامنا على تقنيات نسيج الذكاء الاصطناعي (MDI)، الذي يستمد بياناته من أكثر من ٧٥٠ مصدر مختلف، ويقوم آليا بوضع تلك البيانات في السياق المناسب. كما يساعدك نظام لوجريثم على استغلال بيانات الأجهزة وسجلات الأنشطة والقيام باستخلاص وتصنيف المعلومات المجمعة للتمكن من رصد التهديدات الأمنية المتقدمة والاستجابة لها وتفادي أضرارها.

اعرف الوقت الحقيقي للحدث

لا تتجاهل أهمية التسلسل الزمني للهجمات. تقوم تقنية (TrueTime) بتسجيل الوقت الحقيقي لوقوع الأحداث، وهي تقنية مسجلة كبراءة اختراع باسم لوجريثم، وتوفر أدوات تصحيح الفوارق الزمنية بين الأجهزة المختلفة أو المناطق الجغرافية المتباعدة زمنيًا مع مراعاة أي تفاوت بين وقت قراءة البيانات ووقت تخزينها.

قم بدمج استخبارات التهديدات الأمنية بسلاسة

تتغير التهديدات الأمنية باستمرار، وتتغير معها أساليب ومسارات الهجوم أيضًا. يمكنك تخطي هذه العقبات باستخدام منهجيات تحليل السياق المكثف التي يوفرها مزودي الأدوات المتوافقة مع تقنيات (STIX/TAXI)، ومن البيانات المجمّعة عن طريق الأنظمة المفتوحة أو تلك المفتوحة تجاريًا، وكذلك من بيئات الإيهام (HONEYPOTS) المتوفرة لديك. استخدم جميع تلك المصادر لتقليل نسبة الاستنتاجات الخاطئة (FALSE POSITIVES) والتمكن من رصد التهديدات المتخفية، وتحديد أولويات الاستجابة للتحذيرات والمخاطر.

مختبرات لوجريثم تدعم فريق العمل لديك

مختبرات لوجريثم عبارة عن فريق أبحاث متخصص في مجالي أمن المعلومات والالتزام بالمعايير. يقوم فريق المختبرات بتطوير قواعد معالجة البيانات لأكثر من ٧٥٠ جهاز وتطبيق، وكذلك تطوير أدوات تحليلية لحمايتك من كافة أنواع الهجمات، بالإضافة إلى أدوات ضبط الالتزام المتوافقة مع ١٥ معيار وإطار عمل. يتضمّن فريق مختبرات لوجريثم مجموعة من الخبراء في مجالات رصد محاولات التسلل ومكافحة البرامج الضارة والاستجابة للحوادث الأمنية المعلوماتية والالتزام بالمعايير وغيرها من المواضيع الحيوية.

> **حلول لوجريثم للتحري والتحليل وفرت لنا مجالًا أوسع للرؤية وقدرة أكبر على الرقابة لنتمكن من تركيز جهودنا ووقتنا لمعالجة التحذيرات الأكثر إلحاحًا.**
>
> المصدر: ضابط أمن المعلومات في مؤسسة رائدة للبيع بالتجزئة