IT SYSADMINS EGYPT

Transfer Your Knowledge

SIEM

SECURITY INFORMATION AND EVENT MANAGEMENT

HTTPS://ITSYSADMINS-EG.ORG

Table of Contents

ايه هو ال SIEM ؟ 3

مكونات ال SIEM 3

جمع اللوجات (Log Collection): 3

تخزين اللوجات (Log Storage): 3

تحليل الأحداث (Event Correlation): 4

تنبيه الأمان (Security Alerts): 4

تحليل الأحداث السابقة: (Forensic Analysis) 4

التقارير (Reporting): 4

إزاي الـ SIEM بيجمع اللوجات من أنظمة مختلفة ويوحد قراءتها: 5

1. استخدام الـ Agents: 5
2. الدعم للبروتوكولات الموحدة: 6
3. التحويل والتنسيق (Normalization): 6
4. تكامل API (APIs Integration) 6
5. مستودعات اللوجات المركزية (Centralized Log Repositories): 6

إزاي بيوحد البيانات ؟ 7

اضرار ال SIEM لو مفيش فريق عمل متخصص 7

كثرة التنبيهات (Too Many Alerts): 7

فهم اللوجات (Understanding Logs): 7

إدارة النظام (System Management): 7

طيب ايه الفريق اللي محتاجه او الإدارة اللي محتاجها أي مؤسسة عشان تديره ؟ 8

خلاصة القول <<<<<< 8

Hazem Mohamed

ايه هو ال SIEM ؟

SIEM (Security Information and Event Management)

هو نظام بيساعد الشركات على جمع وتحليل الـ(Logs)(اللوجات يا هندسة) اللي بتخرج من كل الأجهزة اللي في الشبكة، وده بيخليها تكتشف التهديدات والهجمات المحتملة وتتصرف بسرعة، هحاول اشرح الموضوع بطريقة مبسطه من وجهة نظري التي لا قيمه لها بردوا

مكونات ال SIEM

جمع اللوجات (Log Collection):

بيجمع اللوجات من كل أجهزة الشبكة زي السيرفرات، الراوترات، وأجهزة الكمبيوتر، وبيحطهم في مكان واحد

تخزين اللوجات (Log Storage):

بعد ما يجمع اللوجات، النظام بيخزنها لفترة محددة عشان تقدر ترجع لها في أي وقت تحتاجه. اللوجات دي ممكن تبقى مفيدة جدًا في تحقيقات أمنية لاحقة لو حصل هجوم أو تهديد معين

Hazem Mohamed

تحليل الأحداث (Event Correlation):

هنا بقى بييجي الجزء الذكي، مش بس بيجمع البيانات، كمان بيحللها بشكل آلي، بيحاول يربط بين الأحداث اللي حصلت في أكتر من جهاز أو مكان في الشبكة عشان يشوف إذا كان في تهديد أو هجوم بيحصل مثلًا، لو حد حاول يدخل على جهاز بشكل غير مشروع أكتر من مرة في وقت قصير، أو لو في بيانات غريبة بتتنقل في الشبكة، هيكشف السلوك ده بالصلاة علي النبي (عليه افضل الصلاة و السلام)

تنبيه الأمان (Security Alerts):

اكتشف حاجة مش طبيعية، زي محاولة اختراق أو نشاط مريب، هيبعت تنبيه فوري للفريق الأمني. التنبيه ده بيقولهم إن في لو مشكلة لازم ياخدوا بالهم منها ويتصرفوا بسرعة

تحليل الأحداث السابقة : (Forensic Analysis)

بيديك القدرة ترجع تشوف كل اللوجات اللي اتجمعت وقت الهجوم، وتعمل تحليل مفصل عشان لو حصل هجوم أو اختراق فعلي ده بيساعد الفرق الأمنية إنها تاخد دروس للمستقبل وتمنع تكرار الهجوم,تعرف إيه اللي حصل وإزاي الهجوم تم.

التقارير (Reporting):

بيطلع تقارير دورية عن كل اللي بيحصل في الشبكة، زي عدد المحاولات الغير شرعية للدخول أو أي نشاط مريب التقارير دي بتساعد الإدارة وفريق الأمن ياخدوا قرارات بناءً على البيانات الموجودة

Hazem Mohamed

دي المكونات الأساسية و كل منتج مصنع من شركه بيبقي ليه مميزاته زي مثلا ممكن تلاقي منتج SIEM بيتمتع بخاصيه قياس مدي توافق الأجهزة مع المعايير ممكن مثلا " File integrity Monitoring" وفي انظمه في ال نظام الـ SIEM مش بتشتغل بس على البيانات اللي بتجيله من داخل الشبكة، لكن كمان بيقدر يستعين بمعلومات خارجية عن الهجمات الإلكترونية اللي بتحصل حول العالم، ده بيساعده يربط بين البيانات اللي جاياله وبين التهديدات المعروفة في الوقت الحقيقي، فلو فيه هجوم جديد منتشر عالميا، الـ SIEM يقدر يكشفه بسرعة لو حصل في شبكتك، ويديلك تنبيه قبل ما التهديد ينتشر أو يسبب ضرر كبير وده اللي بيسمه "Threat Intelligence Feeds"،وده كله علي سبيل المثال و ليس الحصر .... نفتح قوس لحضراتكم واقفلوه في التعليقات بعد اذنكم....(.....)

نظام الـ SIEMبيجمع اللوجات من أنظمة وأجهزة مختلفة في الشبكة، وده بيتم باستخدام مجموعة من الأساليب اللي بتسمحله بدمج وقراءة البيانات بطريقة موحدة، حتى لو الأنظمة دي مختلفة في طريقة توليدها للبيانات. طيب إزاي ده بيحصل؟

إزاي الـ SIEM بيجمع اللوجات من أنظمة مختلفة ويوحد قراءتها:

1. استخدام الـAgents:

في بعض الأحيان، الـ SIEM بيستخدم برامج صغيرة اسمها "Agents" بتتثبت على الأنظمة المختلفة زي السيرفرات، أجهزة الكمبيوتر، أو حتى التطبيقات. الـ Agents دي بتكون مسؤولة عن جمع اللوجات بشكل مباشر من كل جهاز وترسلها للـ SIEM. الوظيفة الأساسية للـ Agents هي إنها توحد البيانات وتبعتها للنظام في شكل مفهوم ومناسب للتحليل.

Hazem Mohamed

2. الدعم للبروتوكولات الموحدة:

معظم أنظمة الـ SIEM بتدعم بروتوكولات قياسية زي Syslog أو SNMP اللي بتساعد في جمع البيانات من أجهزة الشبكة المختلفة (زي الروترات والسويتشات) بشكل موحد. الأنظمة المختلفة بتولد بياناتها وتبعتها للـ SIEM باستخدام البروتوكولات دي، والـ SIEM بيقدر يفهم اللوجات دي بسهولة.

3. التحويل والتنسيق:(Normalization)

لما اللوجات بتوصل للـSIEM ، بيتم تحويلها أو "تطبيعها(Normalization) "، يعني النظام بياخد اللوجات من مصادر متعددة وبأشكال مختلفة، ويحولها لشكل موحد بحيث يكون سهل تحليله. ده بيخلي الـ SIEM يقدر يتعامل مع البيانات بسهولة بغض النظر عن مصدرها أو نوع الجهاز اللي جاي منه.

4. تكامل:(APIs Integration) API

بعض أنظمة الـ SIEM بتستخدم API لربط الأنظمة المختلفة وجمع اللوجات بشكل مباشر. الـ API بيسمح للـ SIEM إنه يتواصل مع الأنظمة أو التطبيقات ويطلب منها البيانات أو يستقبلها بشكل مستمر ومنظم.

5. مستودعات اللوجات المركزية:(Centralized Log Repositories)

بعض الشركات بتستخدم مستودعات لوجات مركزية عشان تخزن كل اللوجات في مكان واحد قبل ما الـ SIEM ياخدها ويحليلها. النظام بياخد كل اللوجات من المستودع المركزي ده، وده بيسهل عملية التحليل لأنه بيتم في مكان واحد.

Hazem Mohamed

إزاي بيوحد البيانات؟

بعد ما اللوجات بتتجمع من الأنظمة المختلفة، مرحلة التطبيع (Normalization)هي اللي بتقوم بتوحيد البيانات. التطبيع هو عملية تحويل اللوجات اللي جاية من مصادر مختلفة لأشكال قياسية، يعني بيحط كل البيانات في قالب واحد بحيث يكون سهل فهمها. كل لوج بيتم تحليله حسب نوعه (زي هل هو لوج دخول، أو خطأ، أو محاولة اختراق)، وبعد كده يتوحدوا عشان الـ SIEM يقدر يربط بين الأحداث المختلفة.

بفضل العمليات دي، الـ SIEM بيقدر يتعامل مع أنظمة وأجهزة كتيرة جدًا ومتنوعة ويحلل البيانات بشكل دقيق، حتى لو الأجهزة دي بتولد أنواع مختلفة من اللوجات.

اضرار ال SIEM لو مفيش فريق عمل متخصص

وجود السيم لوحده من غير فريق متخصص ممكن يسبب مشاكل بدل ما يحلها، زي إيه؟

:(Too Many Alerts) كثرة التنبيهات

هتغرق في التنبيهات من غير ما تعرف تفرق بين اللي يستاهل و ايه واللي لا.. زحمه في ايميلك بس وصداع علي الفاضي.

:(Understanding Logs) فهم اللوجات

.اللوجات معقدة ومحتاجة تحليل دقيق، لو مفيش حد فاهم، ممكن تهديدات خطيرة تعدي من غير ما تاخد بالك

:(System Management) إدارة النظام

محتاج متابعة دورية وتظبيط عشان يشتغل بكفاءة. لو مفيش إدارة صحيحة، ممكن يبقى غير فعال

Hazem Mohamed

طيب ايه الفريق اللي محتاجه او الإدارة اللي محتاجها أي مؤسسة عشان تديره ؟

هو فريق :

SOC (Security Operations Center): ، ومحتاج الناس الحلوة دي :

(Security Analyst): محلل أمني

بيراقب التنبيهات وبيحلل اللوجات عشان يعرف إذا كانت التهديدات خطيرة ولا لأ

(Security Engineer): مهندس أمني

محتاج مسئول عن اعدادته و ادارته عشان يشتغل بكفاءة

(Incident Responder): خبير استجابة للحوادث

بيتدخل بسرعة لما يحصل هجوم أو تهديد عشان يحله قبل ما يتفاقم و الفأس تقع في الراس.

خلاصة القول >>>>>>

الSIEM

هو أداة قوية لتحسين الأمن في شركتك، لكن لازم يكون عندك فريق متخصص عشان تقدر تستفيد منه بشكل فعال.

Hazem Mohamed

لو معندكش الفريق ده، ممكن تبقى اللوجات والتنبيهات مصدر إزعاج بدل ما تكون مفيدة....

انا مش هذكر أسماء أي أدوات او منتجات لو ليك تجربة مع النظام ده أو أي تعليق، ياريت تشاركني تجربتك

👇

أراكم علي خير....

متنساش تتابع البودكاست و الدعاء>>>>>

https://music.youtube.com/playlist?list=PL8Sl8JhOhmTdlDwW_f738YIInZOuEYiN9&si=-D36sio03xcEb3aC

وتقدر تابعنا علي تليجرام : https://t.me/+NGqtypVPPIJjZDlk

وكمان عندنا موقع من ٢٠١٩ محدش بيفتحه ☺: https://itsyadmins-eg.info

Hazem Mohamed

شكرا انك فتحت الملف و قريته وصلت للنهاية ، لاتنسانا بالدعاء

تابعني علي لينكيدان :

https://music.youtube.com/playlist?list=PL8Sl8JhOhmTdlDwW_f738YIInZOuEYiN9&si=-D36sio03xcEb3aC

Hazem Mahmoud