تقرير مشروع مواضيع مختارة

عنوان التقرير: تطبيق SIM-Phshing في Tryhackme.

الاسم: محمد عبدالوارث النجري.

التاريخ: 2025/9/25.

البيئة التي تم استخدامها هي : tryhackme.

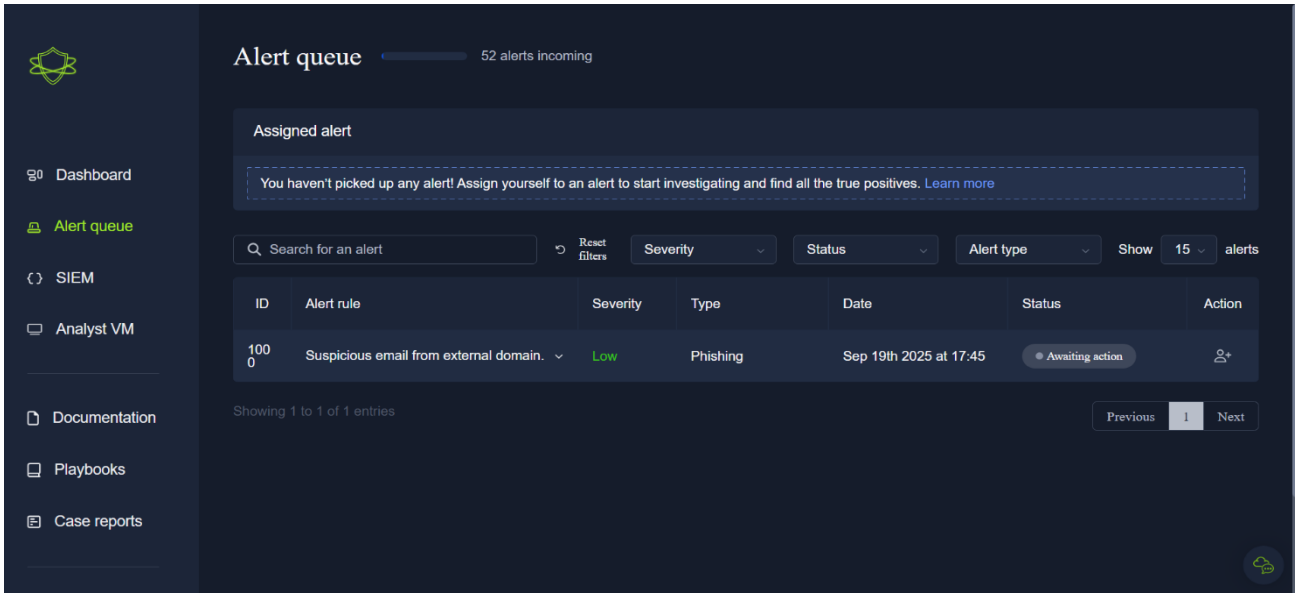
مستوى الوصول: حساب مستخدم عادي داخل ال lap.

الهدف من التقرير: يهدف الى تقييم أداء نظام الكشف عن التهديدات ضمن السيناريو المحدد خلال الفترة الزمنية.

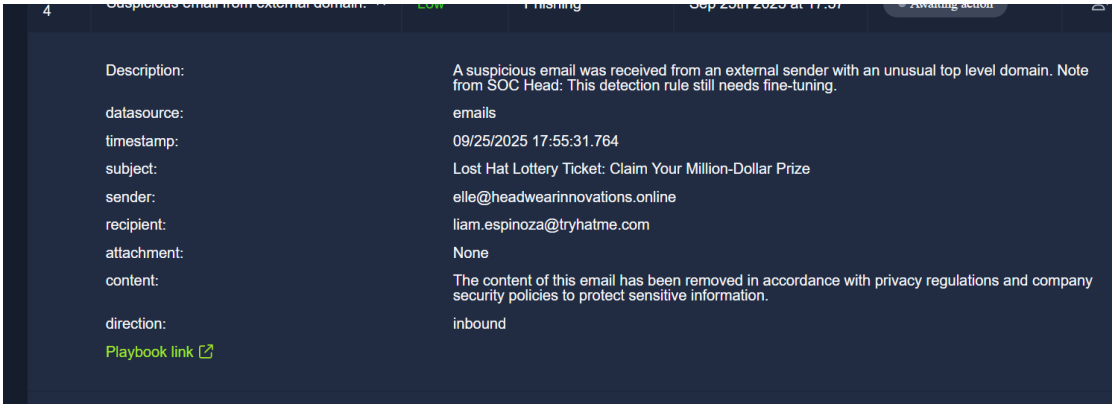
نطاق التقرير: يغطي هذا التقرير المؤشرات التالية الخاصة بسيناريو كشف محدد.

- عدد التنبيهات التي يريد منا النظام هي 53 تنبيه.

الخطوات التي تم اتباعها اثناء العمليات:

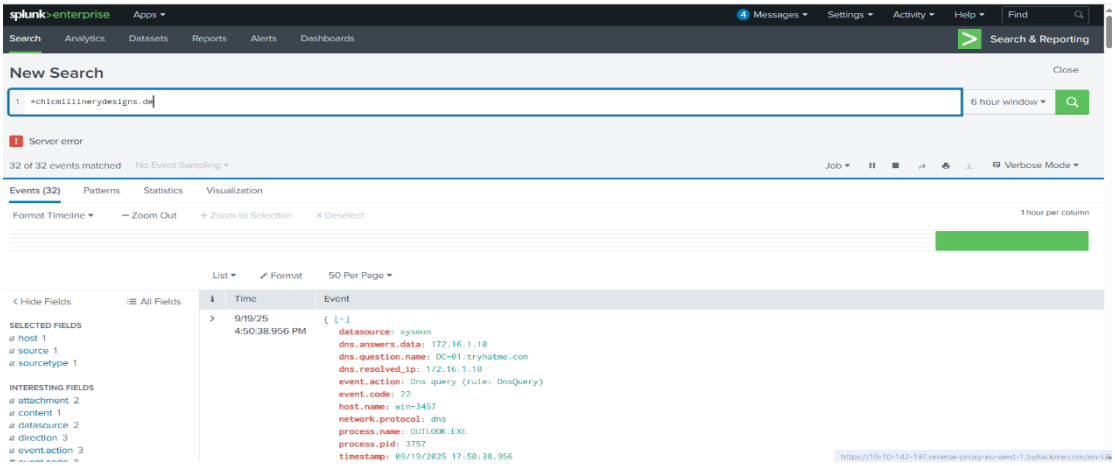


كما في الصورة يقوم نظام الSIM بإرسال تنبيه (alert) الى فريق الامن(SOC) فبالتالي يقوم الفريق بفحص التنبيه والتاكد منه اول خطوة هي عرض تفاصيل التهديد وماذا تعامل معه النظام SIM .

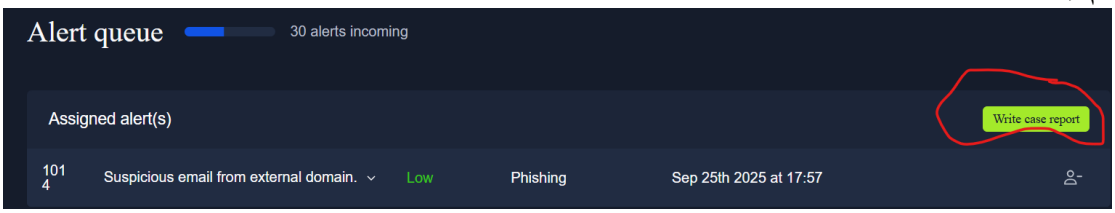


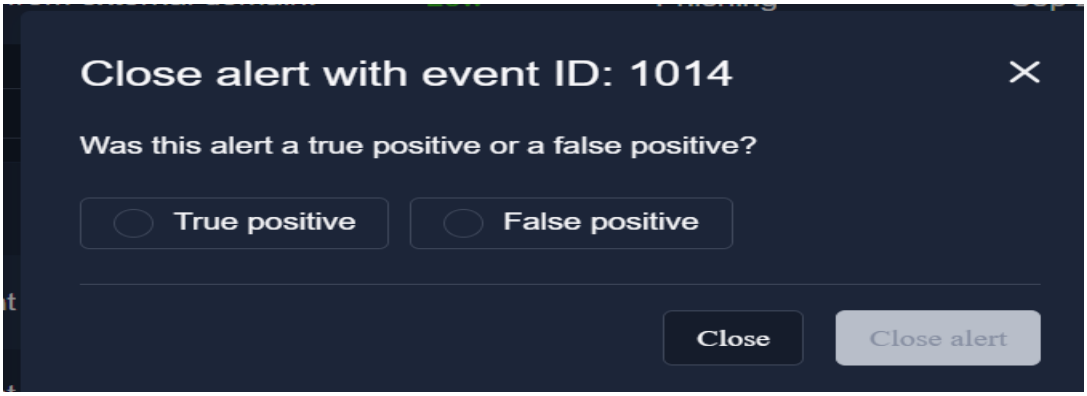
كما في الشكل تظهر معلومات التنبيه فهذا التهديد يحذر من doniam مشبوه
headwearinnovations.online وهو هذا النطاق أما الخطوة التالية وهي التأكد من إذا ما كان نطاق خبيث ام نطاق سليم وهي عملية عادية.

في المعرفة عن اذا ماكان تنبيه إيجابي او سلبي نستخدم أداة splunk التابع لنظام الSIM



في هذا النظام كماهو موضح يتم كتابة ال Domainفي محرك البحث للتاكد ما إذا كان سليم أم إحتيالية.

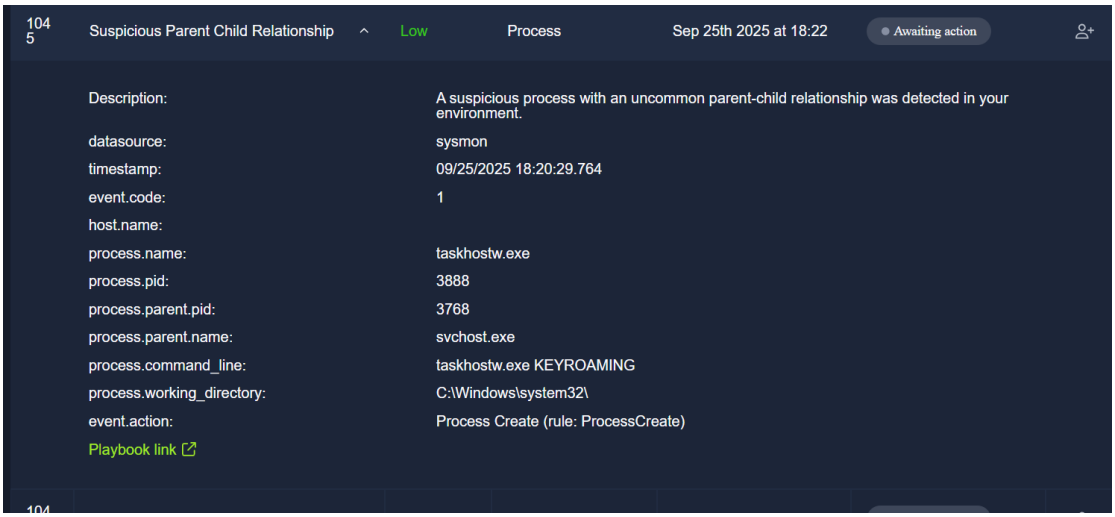




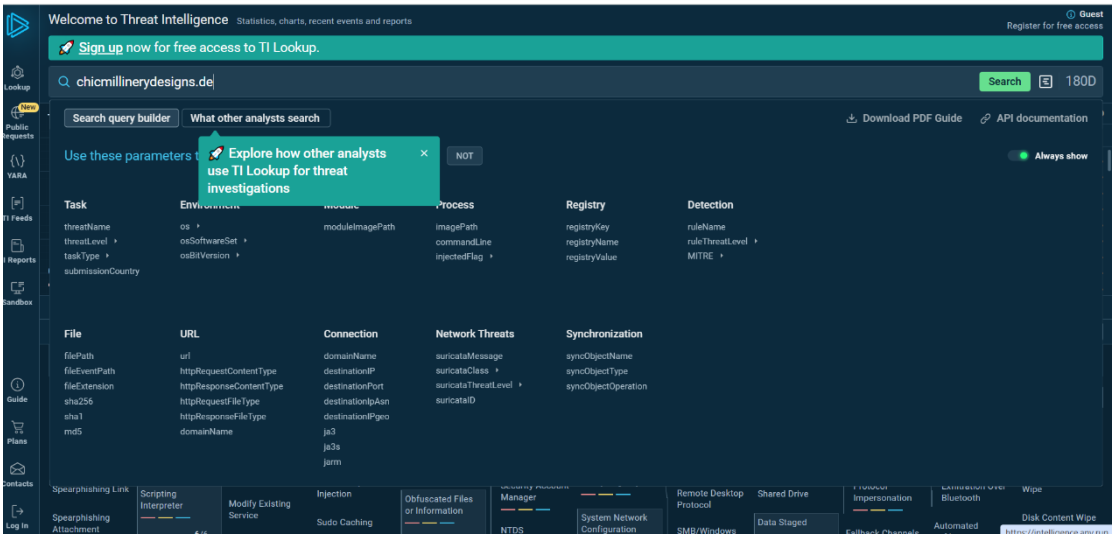
في هذا عند عمل التقرير هناك خيارين وهما :

- تنبيه سلبي: ومعناه ان العملية كانت طبيعية ولا تتظمن أي عملية مشبوهة.
- تنبيه إيجابي: ومعناه ان العملية تتظمن تهديد ومنها تختار هل تريد تصعيد الأمنية والامتيازات إذا تطلب الامر.

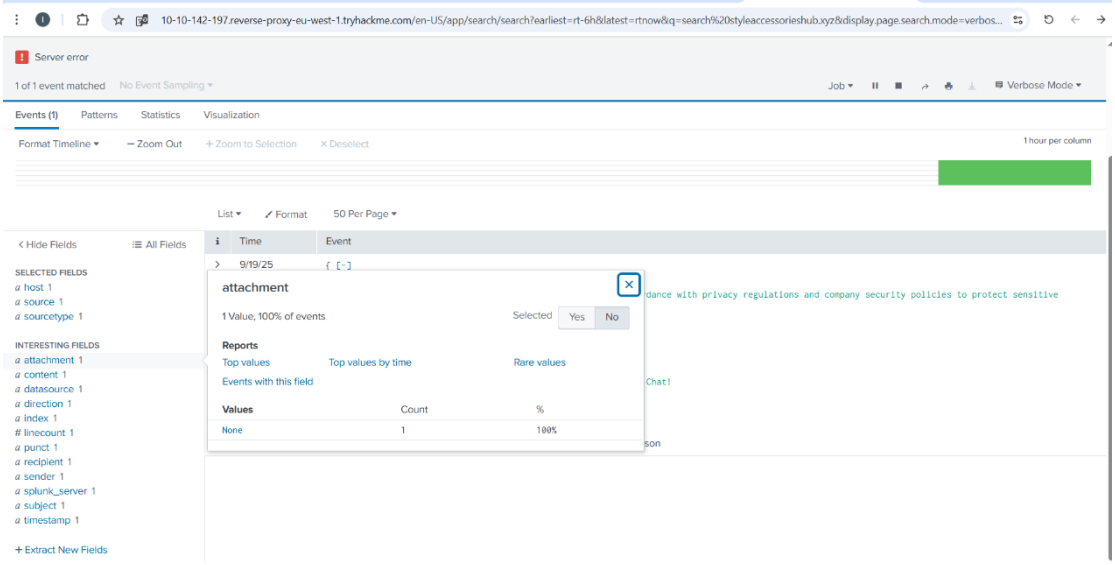
هذا هوه التقرير وفي الشكل كماهو موجود يقوم الموقع بتذكير اذا كان النظام يريد تصعيد الأمان والصلاحيات ام لا.



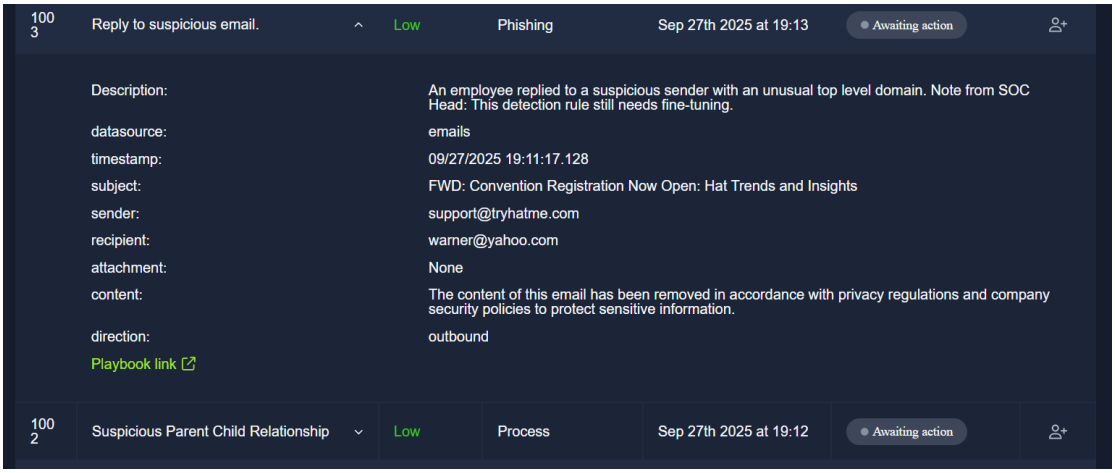
في هذا التنبيه كما في الشكل يظهر عملية تم تنفيذها من احد الأجهزة في الشركة وتم معرفتها انها خبيثة من قبل النظام ، فبالتالي نريد التأكد من هذه العملية.



يتم الدخول الى موقع viriuse total وإدخال العملية ف بالتالي يتم معرفة ما إذا كانت خبيثة ام سليمة. فبالتالي كانت سليمة وتم عمل تقرير ان التنبيه كان من نوع سلبي.

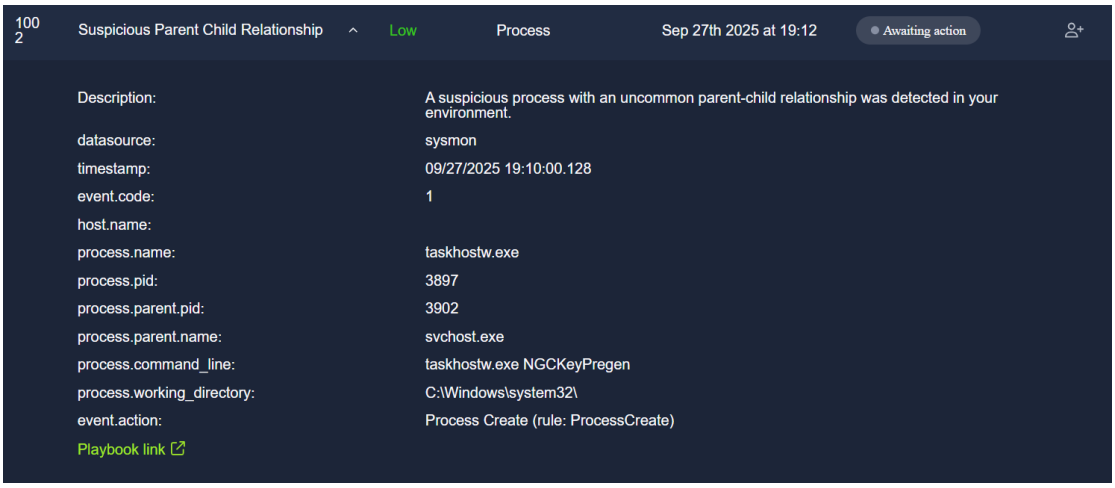


وكذلك من خلال ال splunk عبر البحث برقم العملية التي تظهر من معلومات التنبيه والتي هي 3888 فيتم معرفة ما إذا كانت عملية عادية او خبيثة.



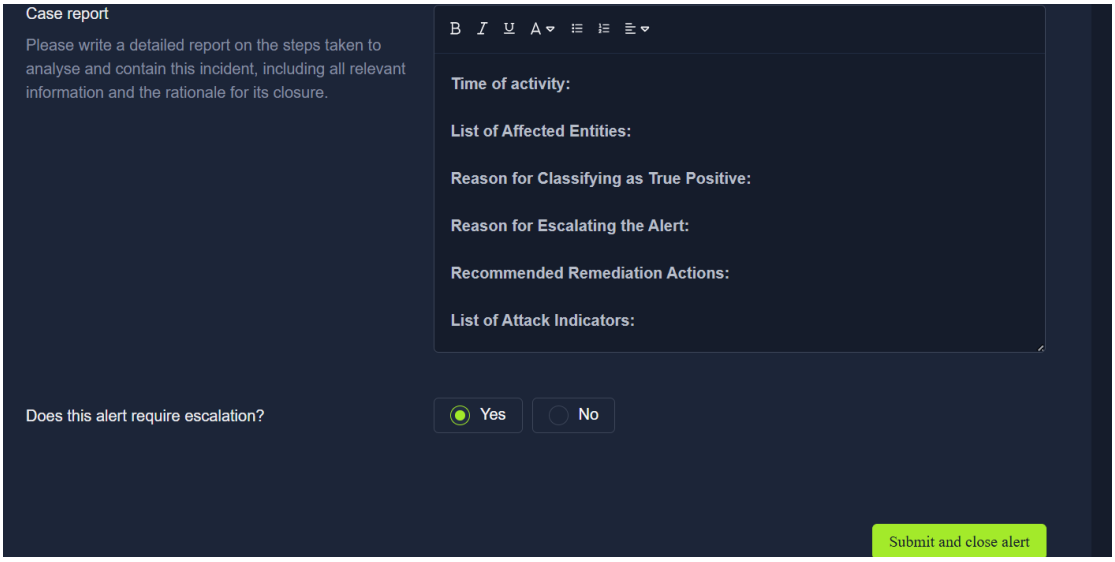
في هذ التنبيه يظهر ان هناك رد من الموظف على رسالة من مكان مريب ف اول شي قمنا به هو التأكد من مرسل الرسالة وهل ال dominname ليس ضار او انتحالي .

عنوان Domain هو tryhatme.com وهو من التي تم إثبات انها انتحالية وغير موثوقة في أداة ولذالك يحتاج ان نقوم بتصعيد الأمان وتقييد صلاحيات هذا المستخدم وفقا للسياسات والقوانين.



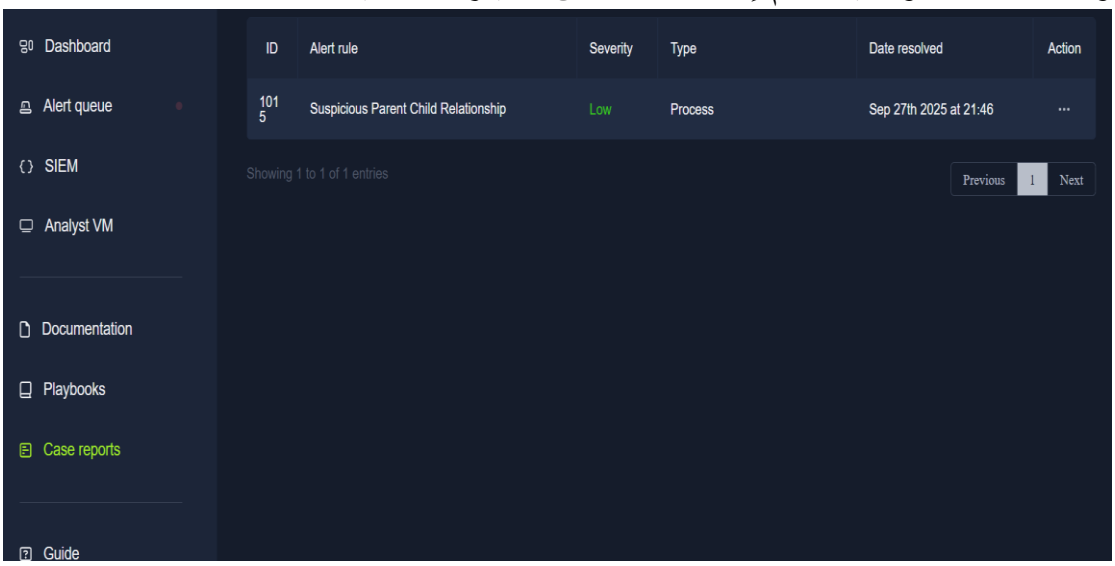
في هذا التنبيه الذي يعد الثاني يظهر ان هناك عملية يعتقد انها محاولة منح صلاحيات مخالفة لسياسات الشركة ولم يقم النظام باي شي حيال هذه العملية.

C:\Windows\servicing\TrustedInstaller.exe هذا الامر هو تعزيز صلاحيات تثبيت وحذف على النظام وهي صلاحيات عليا لا يمتلكها حتى الAdminstrator نفسه.



تم عمل تقرير ورفعه الى المسؤلين على الشركة وكذالك تم تقييد ك هذا العمليات على المستخدمين لانها تمثل تهديد لامن المعلومات الخاص بالشركة. حيث تم تصنيفه تنبيه من النوع الإيجابي لانها عملية خطيرة .

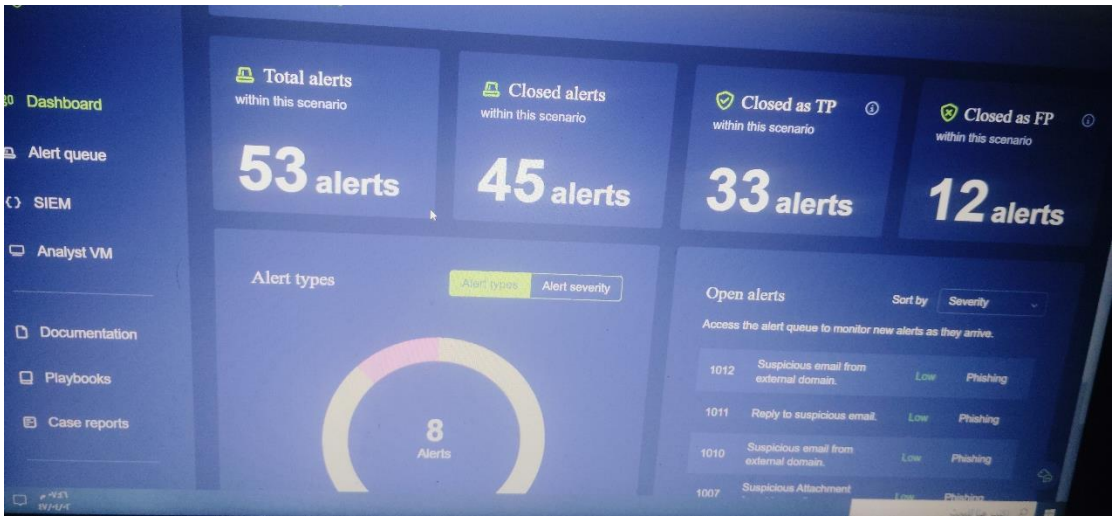
وكذلك تمت التوصية لعدم إعطاء اشخاص امتيازات عالية .



في هذا الصندوق يظهر به التنبيهات التي تم التعامل معها منها السلبية وكذالك الإيجابية ووجودها مهم من اجل اثناء المسائلة من قبل الحكومة او حتى من قبل المسؤلين على الشركة ومهم مدير لشركة ومسؤول الامن السيبراني فيها للاطلاع على الإنجازات التي تم التعامل معها .

i	Time	Event
>	9/19/25 5:44:24.104 PM	{ [-] attachment: None content: The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information. datasource: emails direction: outbound recipient: best@modernmillinerygroup.online sender: liam.espinoza@tryhatme.com subject: Grow Your Hat Business Overnight with this Secret Formula timestamp: 09/19/2025 18:44:24.104 } Show as raw text host = 10.10.204.97:8989 source = eventcollector sourcetype = _json
>	9/19/25 5:44:10.104 PM	{ [-] attachment: None content: The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information. datasource: emails direction: outbound recipient: molina@modishmillinery.com sender: miguel.odonnell@tryhatme.com subject: RE: RE: Upcoming Trade Show Attendance: Meet our Hat Experts timestamp: 09/19/2025 18:44:10.104 } Show as raw text host = 10.10.204.97:8989 source = eventcollector sourcetype = _json

هنا في الSIM يظهر ان هذا الdomain احتيالي وعدد من المنتحلين الذي استخدموا هذا النظام.



بعد التعامل مع التنبيهات وإعلاق الغرفة تم إنجاز 45 تنبيه والتعامل معها بشكل فعال وكذلك مها 33 كانت تنبيهات إيجابية ومنها ما تطلب رفع التصعيد ورفع الامتيازات،

أيضا 12 تنبيه كان من النوع السلبي حيث كانت أنشطة طبيعية واستغرق من الوقت 113 دقيقة للتعامل مع كل التنبيهات.