

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:

Alert queue 52 alerts incoming

Assigned alert

You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. [Learn more](#)

Search for an alert Reset filters Severity Status Alert type Show 15 alerts

ID	Alert rule	Severity	Type	Date	Status	Action
1000	Suspicious email from external domain. ▾	Low	Phishing	Sep 19th 2025 at 17:45	Awaiting action	⚙️

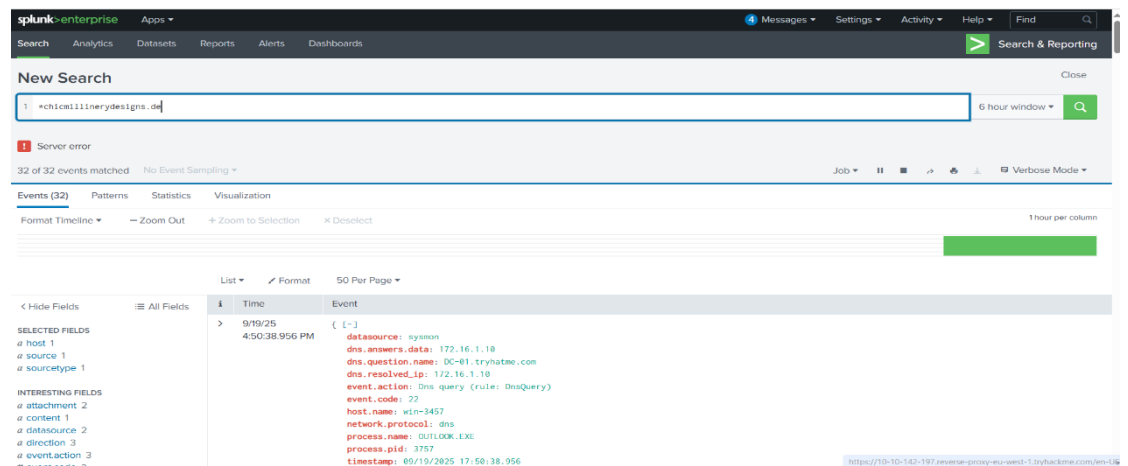
Showing 1 to 1 of 1 entries Previous 1 Next

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

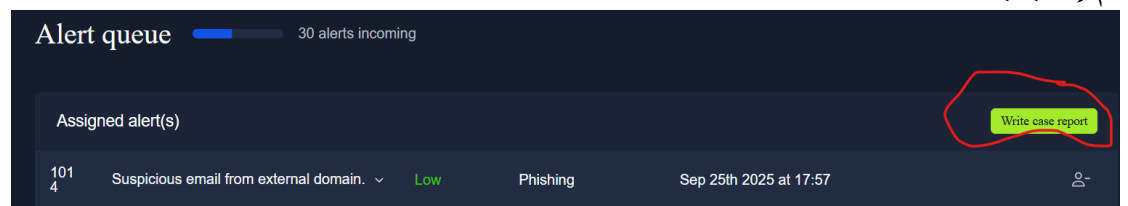
4	Suspicious Email from external domain.	Low	Phishing	Sep 25th 2025 at 17:57	Assigning action
Description:		A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.			
datasource:		emails			
timestamp:		09/25/2025 17:55:31.764			
subject:		Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize			
sender:		elle@headwearinnovations.online			
recipient:		liam.espinoza@tryhatme.com			
attachment:		None			
content:		The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.			
direction:		inbound			
Playbook link					

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 Domain في محرك البحث للتأكد ما إذا كان سليم
أم إحتيالية.



Close alert with event ID: 1014

Was this alert a true positive or a false positive?

☐ True positive ☐ False positive

Close Close alert

في هذا عند عمل التقرير هناك خيارين وهما :

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

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

Time of activity:

List of Affected Entities:

Reason for Classifying as True Positive:

Reason for Escalating the Alert:

Recommended Remediation Actions:

List of Attack Indicators:

Does this alert require escalation?

☒ Yes ☐ No

Submit and close alert

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

104
5 Suspicious Parent Child Relationship ^ Low Process Sep 25th 2025 at 18:22 ● Awaiting action

Description: A suspicious process with an uncommon parent-child relationship was detected in your environment.

datasource: sysmon

timestamp: 09/25/2025 18:20:29.764

event.code: 1

host.name:

process.name: taskhostw.exe

process.pid: 3888

process.parent.pid: 3768

process.parent.name: svchost.exe

process.command_line: taskhostw.exe KEYROAMING

process.working_directory: C:\Windows\system32\

event.action: Process Create (rule: ProcessCreate)

[Playbook link](#)

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.

100 3	Reply to suspicious email.	Low	Phishing	Sep 27th 2025 at 19:13	Awaiting action	⌵
Description:		An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:		emails				
timestamp:		09/27/2025 19:11:17.128				
subject:		FWD: Convention Registration Now Open: Hat Trends and Insights				
sender:		support@tryhatme.com				
recipient:		warner@yahoo.com				
attachment:		None				
content:		The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:		outbound				
Playbook link						
100 2	Suspicious Parent Child Relationship	Low	Process	Sep 27th 2025 at 19:12	Awaiting action	⌵

في هذا 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 .

sender: sophie.j@tryhatme.com

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

100 2	Suspicious Parent Child Relationship	Low	Process	Sep 27th 2025 at 19:12	Awaiting action	⌵
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		09/27/2025 19:10:00.128				
event.code:		1				
host.name:						
process.name:		taskhostw.exe				
process.pid:		3897				
process.parent.pid:		3902				
process.parent.name:		svchost.exe				
process.command_line:		taskhostw.exe NGCKeyPregen				
process.working_directory:		C:\Windows\system32\				
event.action:		Process Create (rule: ProcessCreate)				
Playbook link						

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

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

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

B I U A

Time of activity:

List of Affected Entities:

Reason for Classifying as True Positive:

Reason for Escalating the Alert:

Recommended Remediation Actions:

List of Attack Indicators:

Does this alert require escalation?

☒ Yes ☐ No

Submit and close alert

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

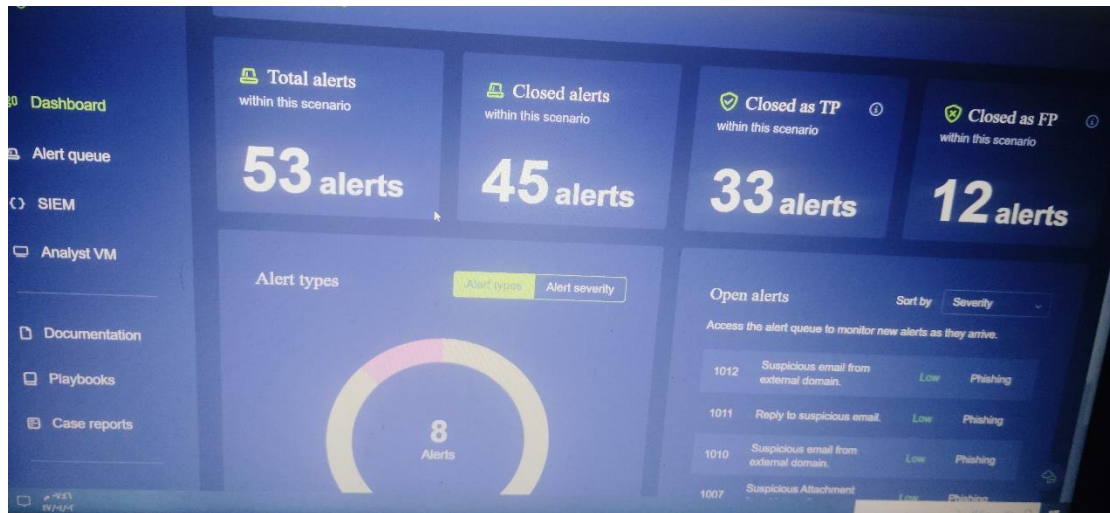
وكذلك تمت التوصية لعدم إعطاء اشخاص امتيازات عالية .

Dashboard	ID	Alert rule	Severity	Type	Date resolved	Action
Alert queue	1015	Suspicious Parent Child Relationship	Low	Process	Sep 27th 2025 at 21:46	...
SIEM	Showing 1 to 1 of 1 entries					
Analyst VM	Previous 1 Next					
Documentation						
Playbooks						
Case reports						
Guide						

في هذا الصندوق يظهر به التنبيهات التي تم التعامل معها منها السلبية وكذلك الإيجابية ووجودها مهم من اجل اثناء المسائلة من قبل الحكومة او حتى من قبل المسؤولين 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	<pre>[-] 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</pre>
>	9/19/25 5:44:10.104 PM	<pre>[-] 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</pre>

هنا في ال SIM يظهر ان هذا ال domain احتيالي وعدد من المنتحلين الذي استخدموا هذا النظام.



بعد التعامل مع التنبيهات وإغلاق الغرفة تم إنجاز 45 تنبيه والتعامل معها بشكل فعال وكذلك 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.

