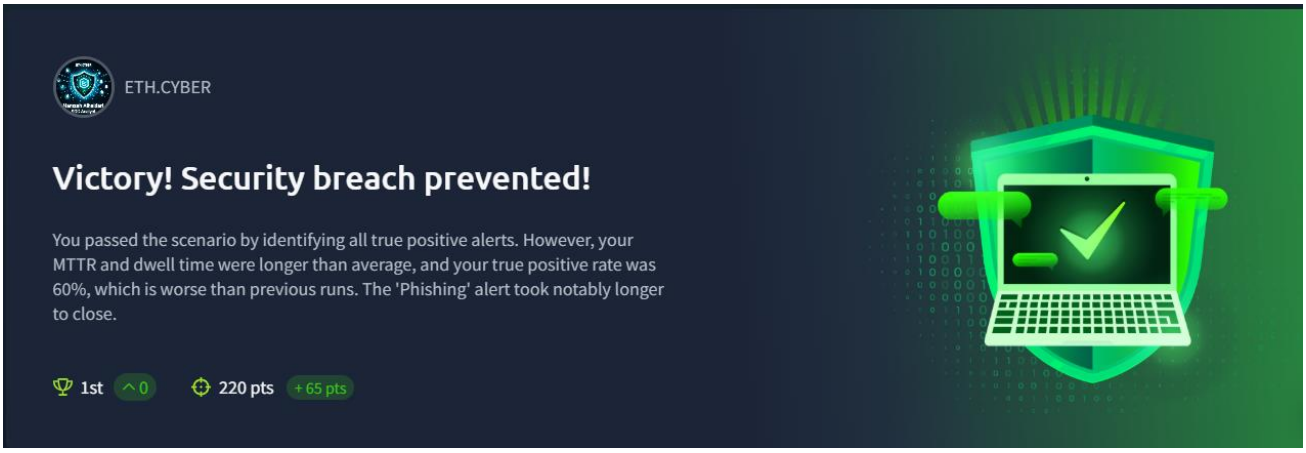
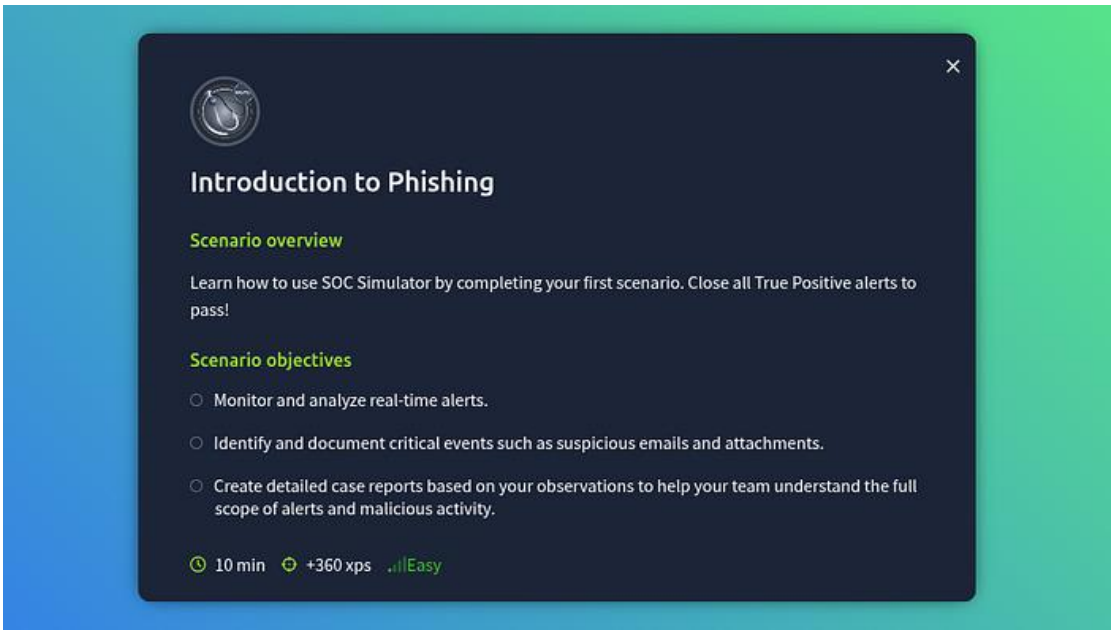
Introduction to Phishing

By:Eng:Hamzah Ali Alhaidari





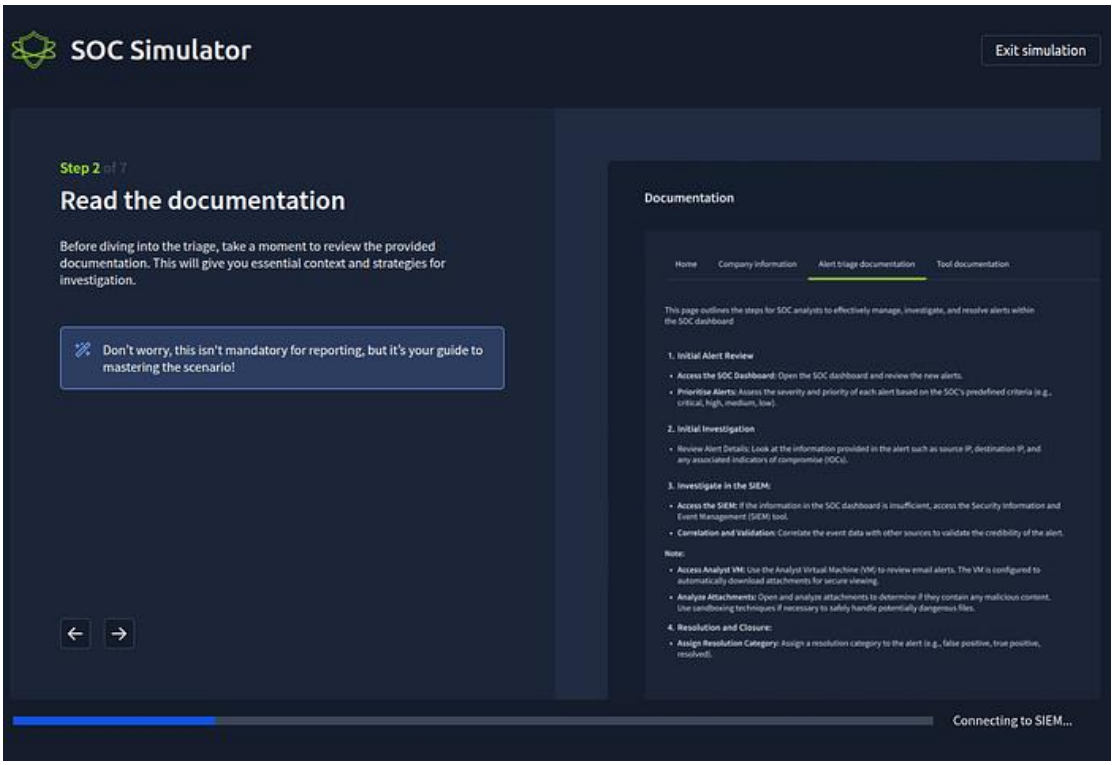
Introduction to Phishing

In this post I am going to talk about my experience with the TryHackMe SOC Simulator, so it's not going to be a walk through but more of an overview of what it is and how it works.

The one we are going to be looking at today is the "Introduction to Phishing" simulation (free!).

Let's boot up the simulation! Note that I am using **Splunk** in this task, **Elastic** is also available.

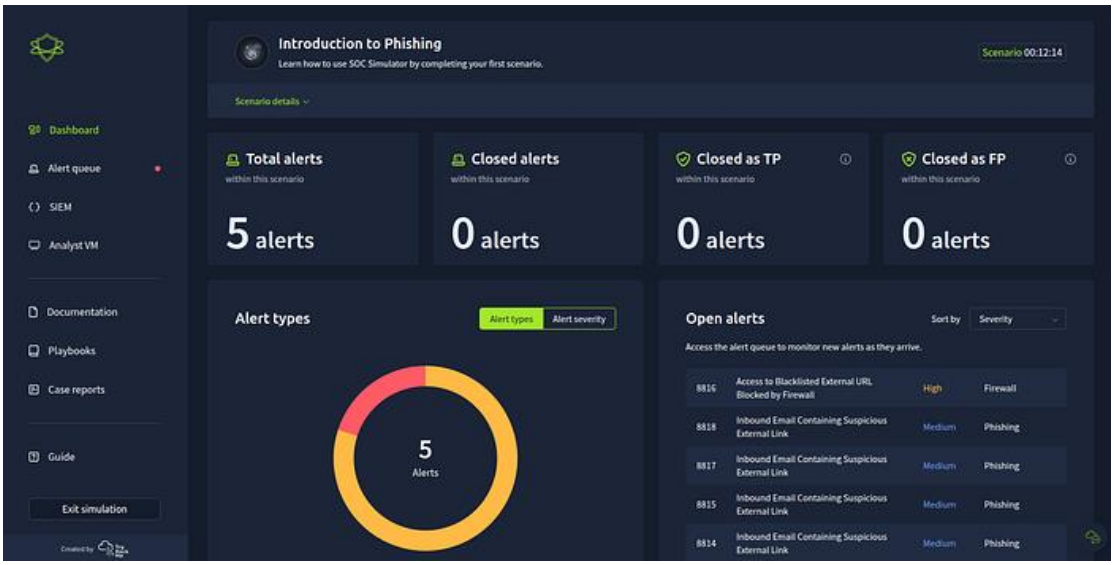
Press enter or click to view image in full size



Loading up the simulation.

This is how it looks upon entering the simulator:

Press enter or click to view image in full size



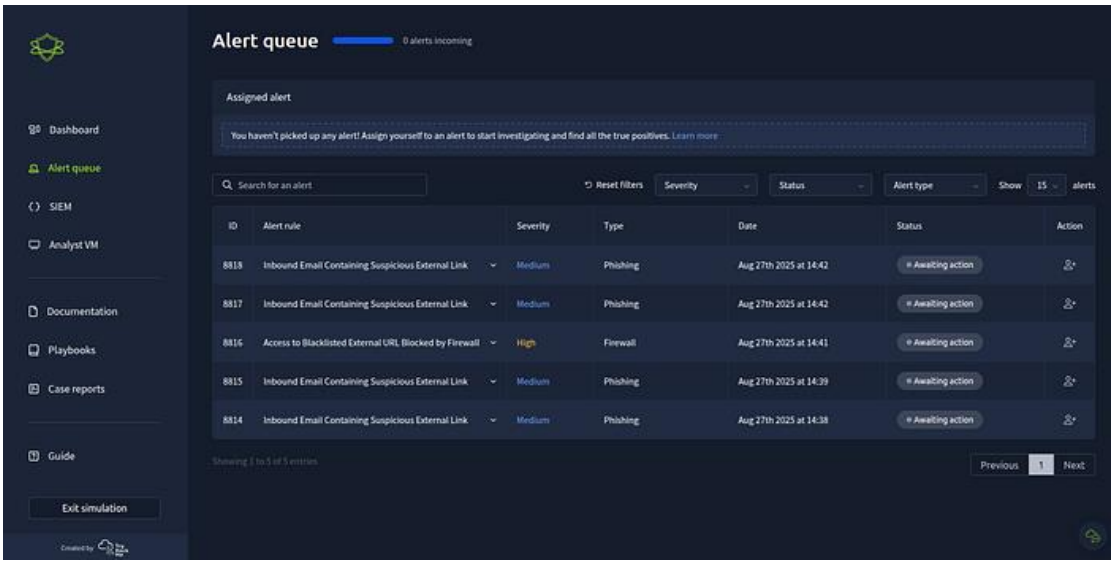
Dashboard view

We can see we have an overview of the dashboard. Sections include **Total alerts**, **Closed alerts**, **Closed as TP**, **Closed as FP** and section sorting out **Alert types** and **Open alerts**.

A useful overview of what is going on.

The **Alert queue** section:

Press enter or click to view image in full size

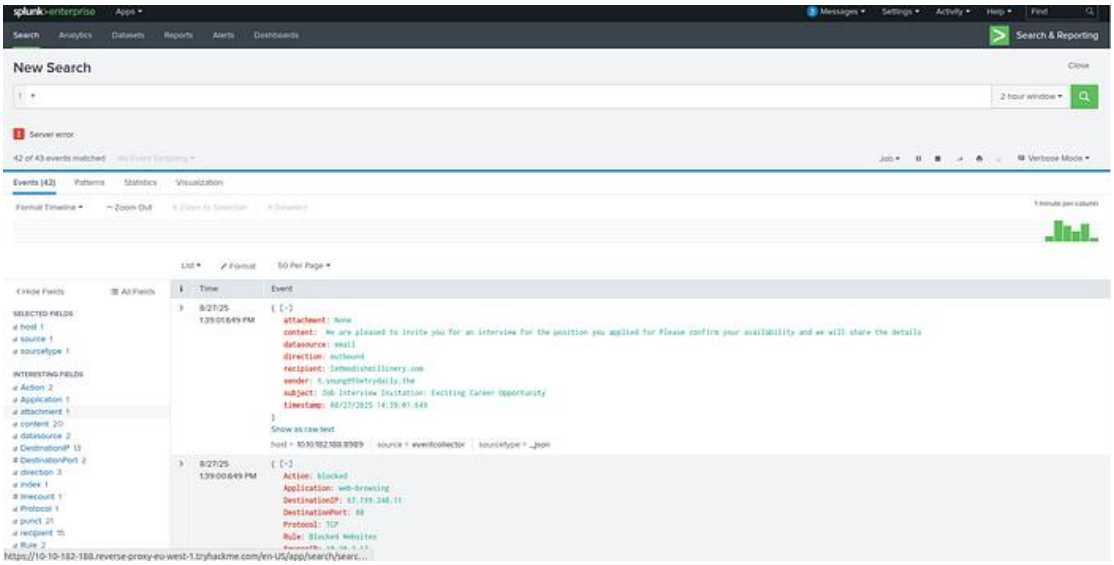


Alert queue view

We can see various details **ID** and **Severity**, along with others here in a nice concise list. Along with **Action** where you click to begin investigating that alert.

Below is a look at **Splunk** after clicking the **SIEM** (Security Information and Event Management) link.

Press enter or click to view image in full size

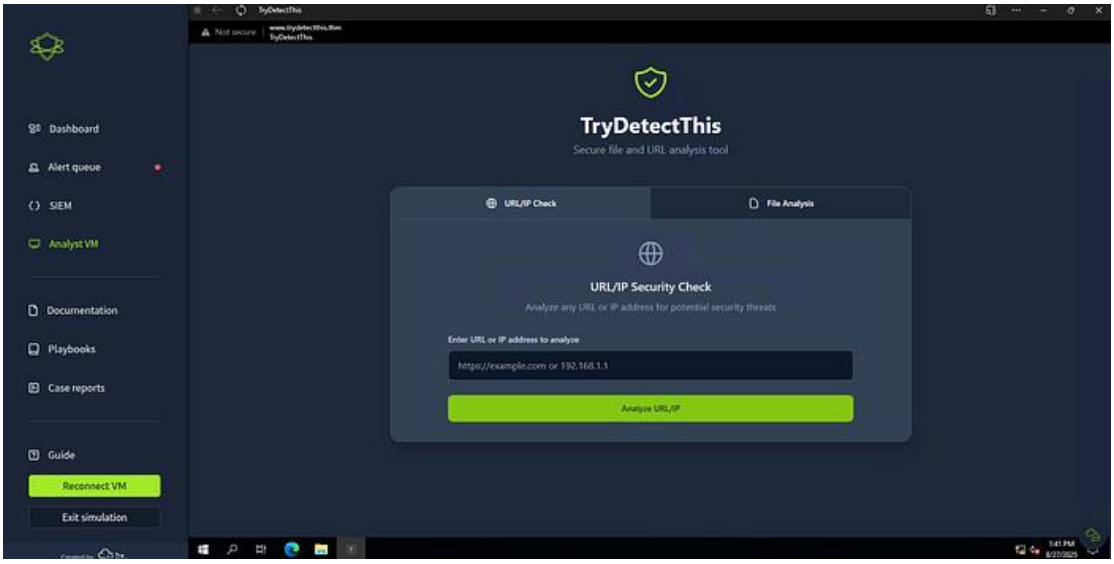


SIEM view (splunk)

I first learned about **Elastic**, but the more and more I use **Splunk**, the more I like it. It's very robust and filtering can be super streamlined. You can see by default it uses a wildcard to have everything included.

Clicking on the **Analyst VM** will bring you to a Windows VM:

Press enter or click to view image in full size

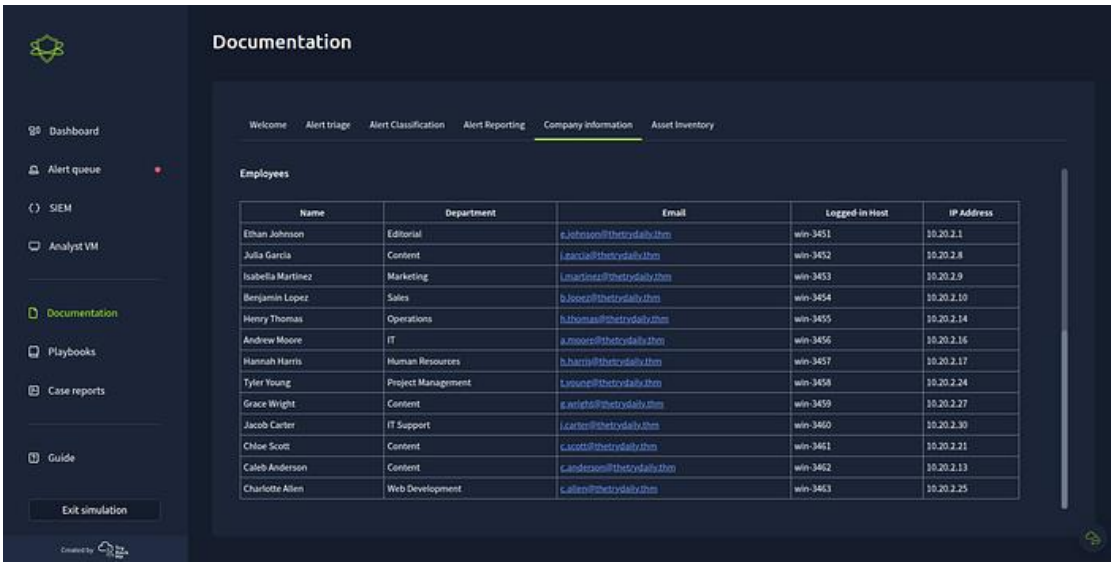


Analyst VM view

There was a folder on the desktop with some attachments in it that I didn't end up using — might be for another exercise, not sure. The screenshot shows what a shortcut on the desktop brings us to. Some kind of scanning tool/site that we can put files, URL's and IP's into.

Below we see Documentation, there's a fair bit of it, but very useful. With **Company Information** being a particular hot spot.

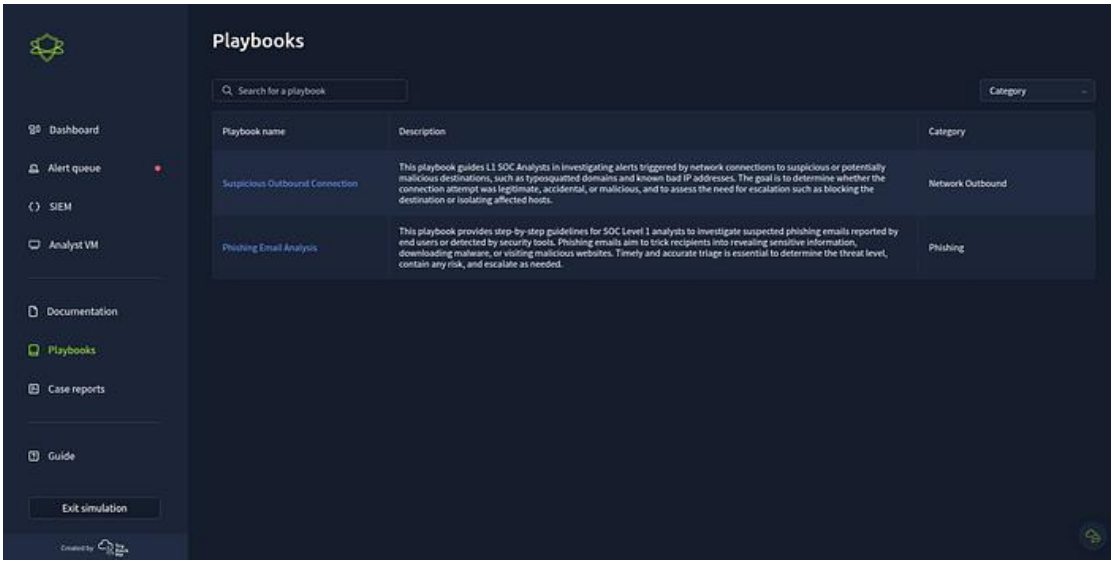
Press enter or click to view image in full size



Documentation view

We have a section for **Playbooks** which I read through before beginning the tasks.

Press enter or click to view image in full size

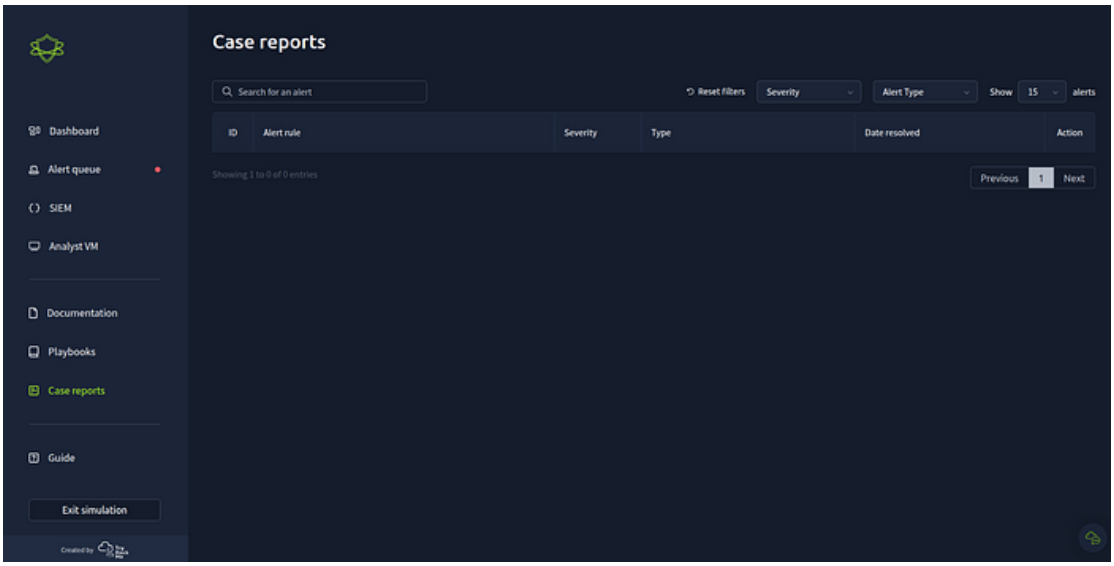


Playbooks view

Clicking there will bring you to different nodes that you can click on for further information. I had a weird issue where when I clicked on a node, it wouldn't let me go "back". There wasn't a way to close it or go back to I would have to refresh.

Case reports below allows us to navigate to the cases we have submitted.

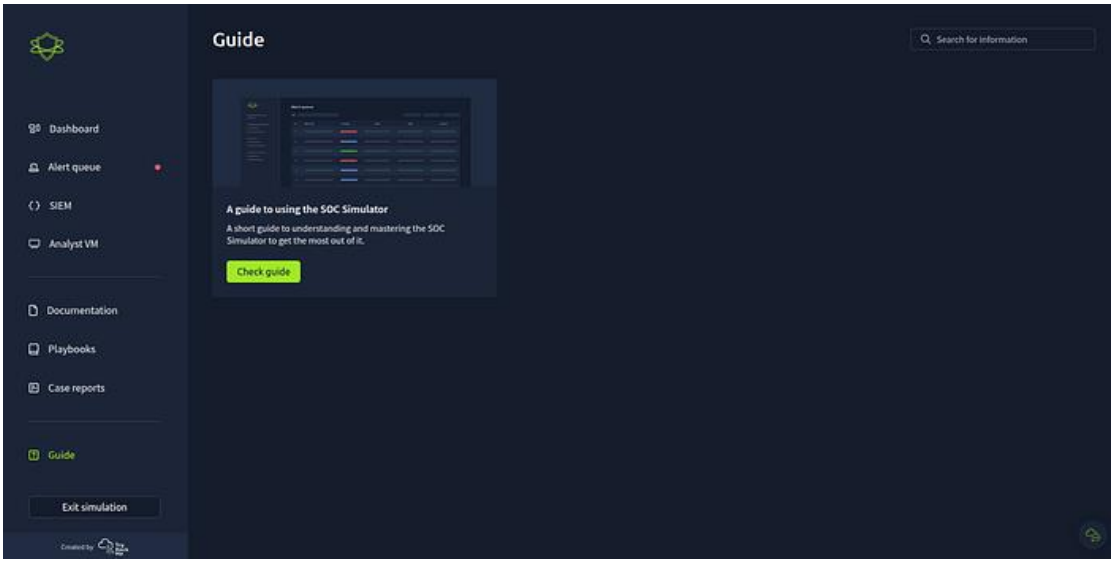
Press enter or click to view image in full size



Case reports view

Finally there is a **Guide** which looks to be the same guide that we see while everything loads upon launching the simulation.

Press enter or click to view image in full size



Guide view

I would make sure you read everything and download all this information to your head first as this will make working through the tasks a lot easier.

What we want to do is head to the **Alert Queue** where we will see our **alerts**. We're looking for True Positives so upon reflection, it would make sense to start with the alerts that have the highest **severity** although I found that looking deeper into the lesser threatening ones really helped build a picture of what actually happened but that might be a waste of time? I certainly took my time!

Once we get the information needed within the alert we can use that information to find out more about the target or victim of the attack. This is where the **Documentation** comes into play.

We can take notes of possible **IOC** (Indicators of Compromise), **IP**'s, **URL**'s and such. Or just paste it into some kind of notepad see we can easily get this information into the **SIEM**.

From there we can start digging, perhaps using the timestamp might be a good start to get the exact alert? Perhaps looking up the email, host name, IP address or anything else noted down. We need to use what we know and continue from there.

Finding suspicious **URL**'s, **IP**'s and **Files** could be than scanned or analysed on the **Analyst VM**.

Once we have a good picture in our minds of what has happened we can then **Write case report**.

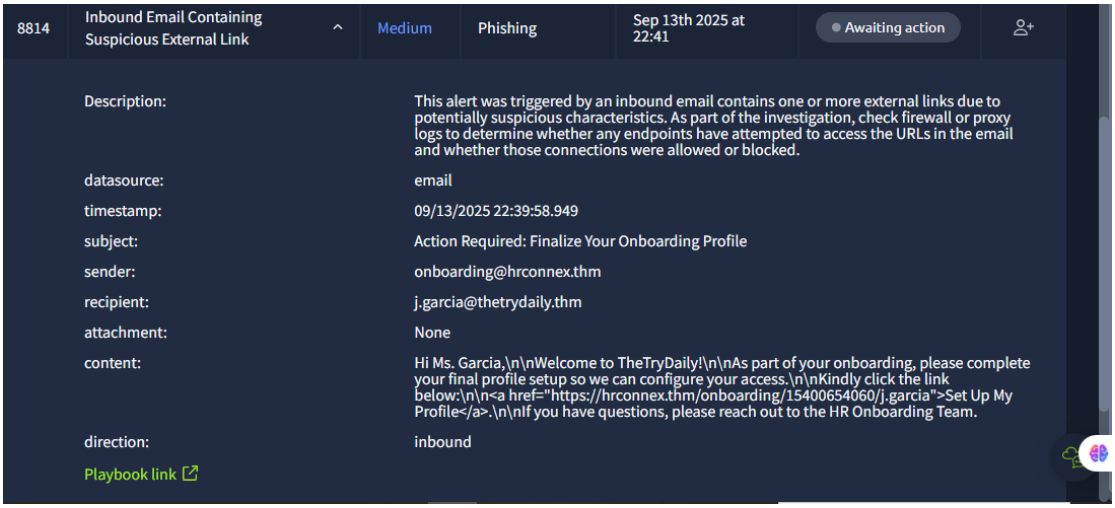
Here we need to decide if this event was a **True Positive** or **False Positive**.

A **True Positive** being an event that's happened and is malicious that may or may not need escalation.

A **False Positive** being an event that's tripped up or alerts the **SIEM** or other tools by accident or because of some strange behaviour either from someone innocent or faulty hardware/software as an example.

TryHackMe have better examples and explanations, just how I think of it.

We can pick which one we think it is and write a little report. There are some useful headers in there already for us but I felt like it was missing one. A header about what it all means. As is, with all the details taken onboard, what does it mean: Was there damages? Was there an actual breach? Is this something to be concerned about?



To analyze the suspicious email, the alert contained the following information:

• **Title**: Inbound Email Containing Suspicious External Link

• **Category**: Phishing

• **Date and Time**: Sep 13th 2025 at 22:41

• **Description**: This alert was triggered by an inbound email containing one or more external

links due to potential investigation, check firewall or proxy logs to determine whether any

endpoints have attempted to those connections were allowed or blocked.

• **Datasource**: email

• **Timestamp**: 09/13/2025 22:39:58.949

• **Subject**: Action Required: Finalize Your Onboarding Profile

• **Sender**: onboarding@hrconnex.thm

• **Recipient**: j.garcia@thetrulythm

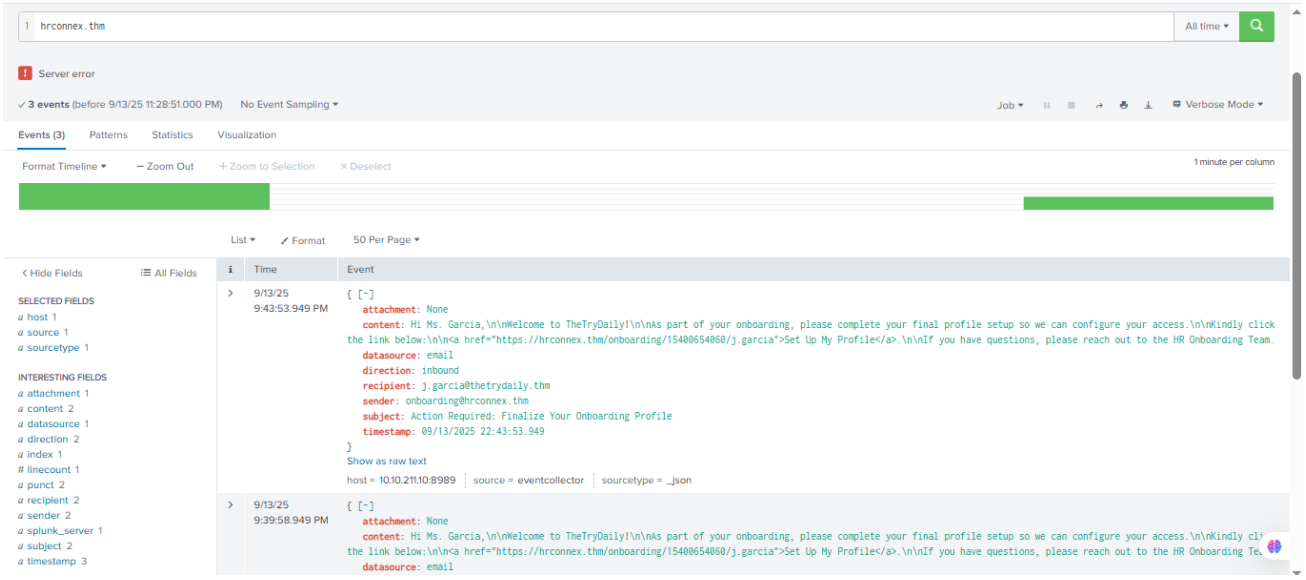
• **Attachment**: None

• **Content**: Hi Ms. Garcia,\n\nWelcome to TheTryDaily!\n\nAs part of your onboarding, please complete your final profile setup so we can configure your access.\n\nKindly click the link below:\n\nSet Up My Profile.\n\nIf you have questions, please reach out to the HR Onboarding Team.

The email, sent to j.garcia@thetrydaily.thm on Sep 13th 2025 at 22:41 CEST, is an onboarding notification titled "Action Required: Finalize Your Onboarding Profile." The title uses urgency in the title by stating “Action Required”, encouraging the user to engage now. It comes from onboarding@hrconnex.thm, seemingly the HR Onboarding Team, and asks Ms. Garcia to complete her profile via a link (https://hrconnex.thm/onboarding/15400654060/j.garcia) for TheTryDaily. It offers support via the same email. The sender domain and destination domain aligns up with each other by both domains using the “.thm” extension. The alert flags it as potential phishing despite matching domains because it contains URL to an external source

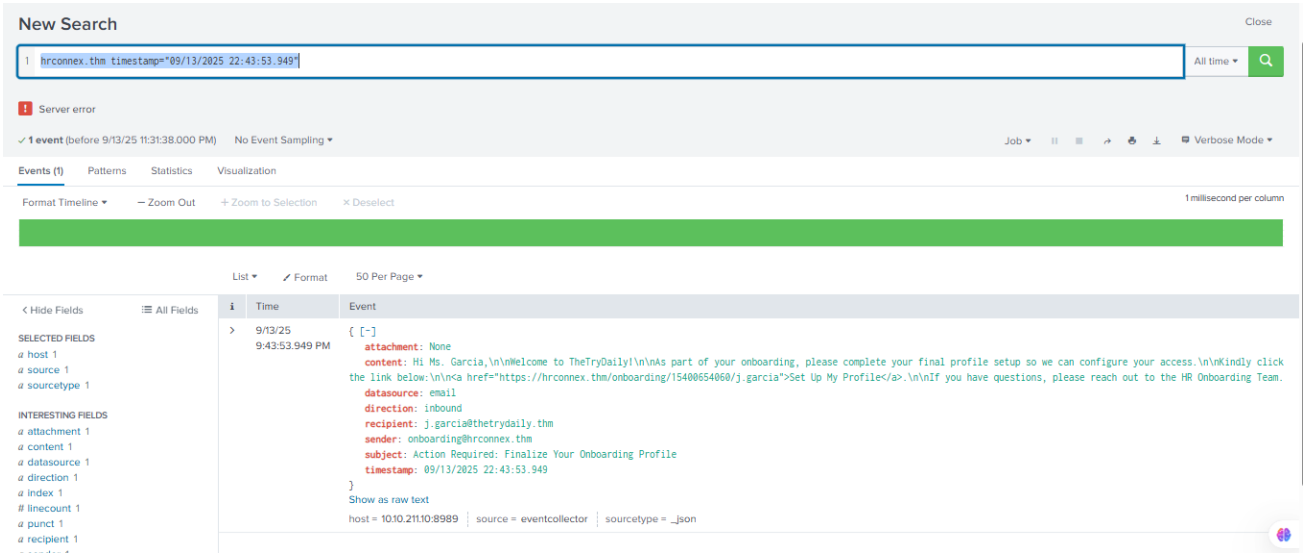
Take ownership of the alert by selecting ”Action” and set alert to ”Assigned alerts” for the analyst to work on. Assigned alerts can contain multiple alerts.

From the information in the assigned alert, copy the senders email domain and search in Splunk SIEM to look for the specific event. Open the SIEM section and move to Splunk. The result for the search of the email address domain, brings up 3 recorded events.

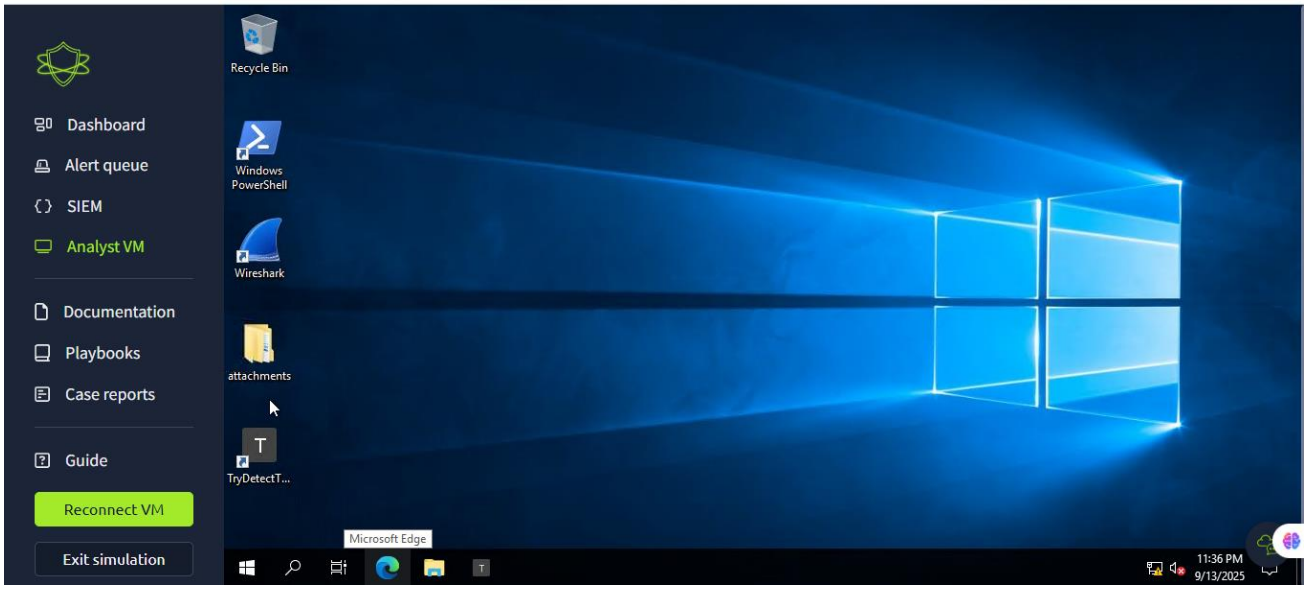


To narrow down the search to find the specific event we are looking for, add in unique information to the search query related to the specific email we are looking for. I noted down the timestamp earlier, include the timestamp in the query with the following search:

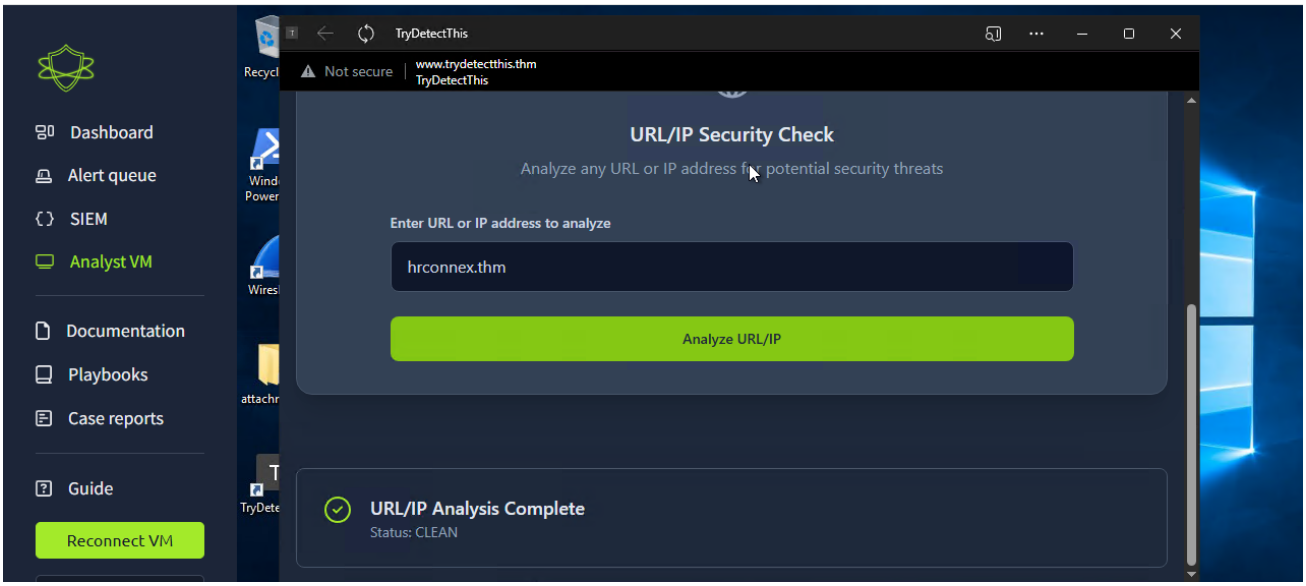
hrconnex.thm timestamp="09/13/2025 22:43:53.949"

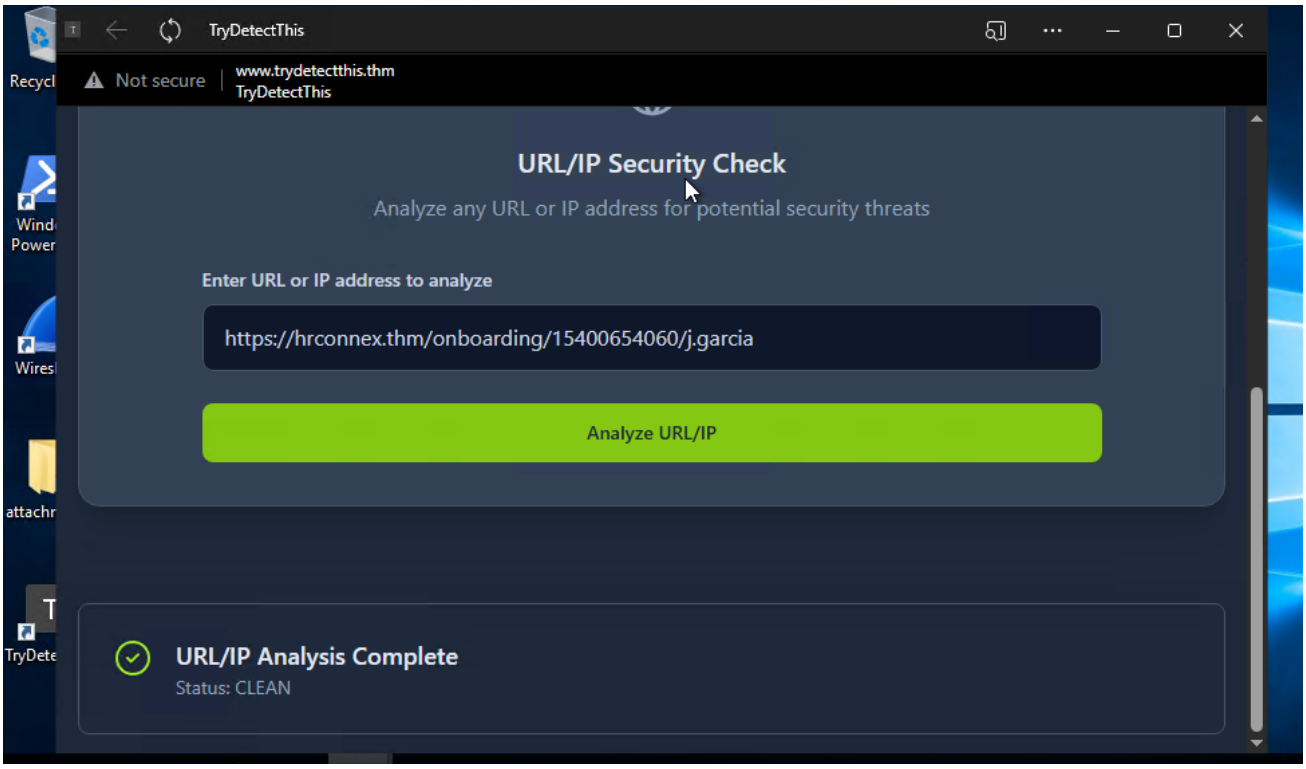


1 event found, this is the one specific to the alert we are looking at. The log contains the sender's domain and the external URL listed in the main content that triggered the alert



Inside the Analyst VM workstation, open the ”TryDetectThis” application to look up the listed domain reputation and external URL function. TryDetectThis tool is for threat intel research.





The domain of the sender and external URL came up CLEAN Analysis, meaning the domain and URL is seemingly safe. This points to the possibility that this might be a false positive.

Case report ID 8814

Incident classification

False positive

10 /10 points

Time of Activity:

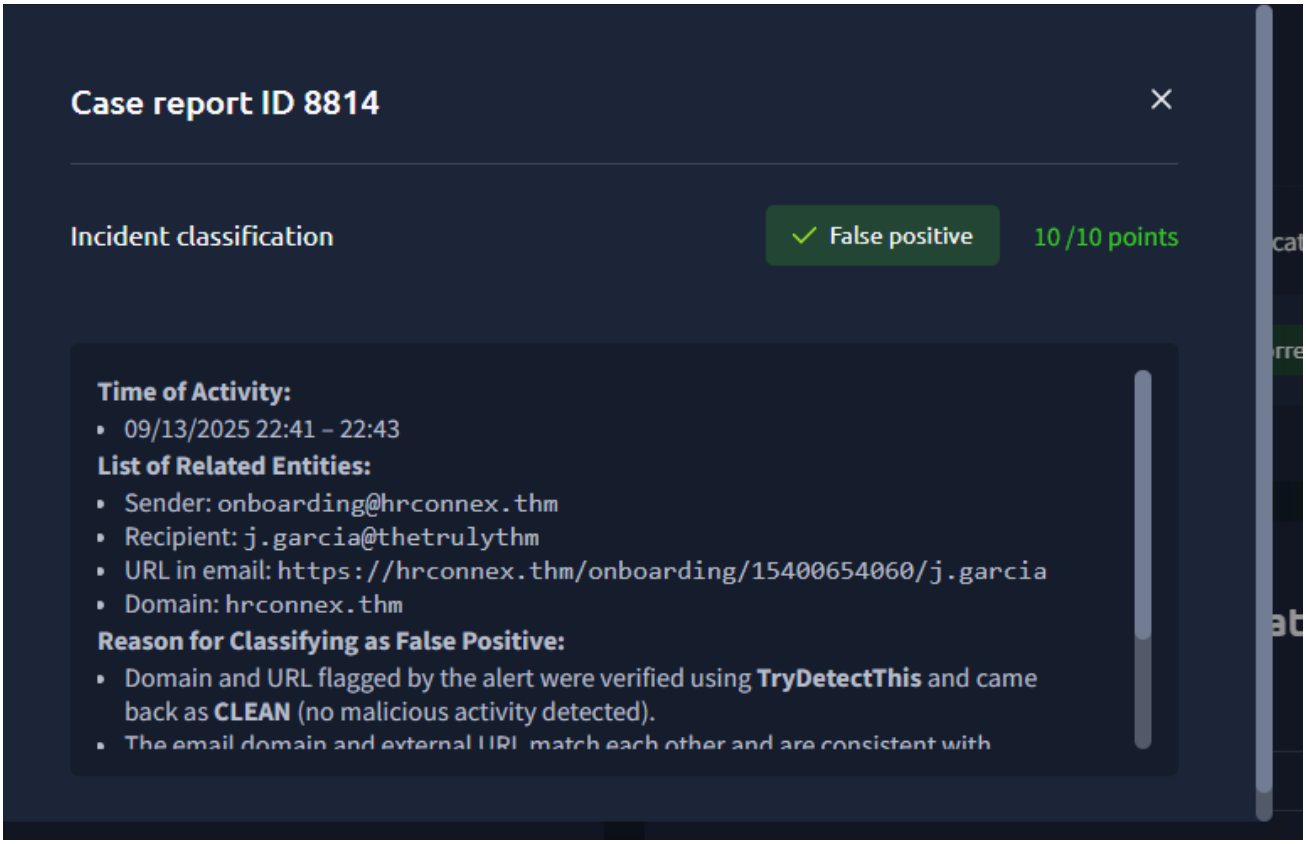
- 09/13/2025 22:41 – 22:43

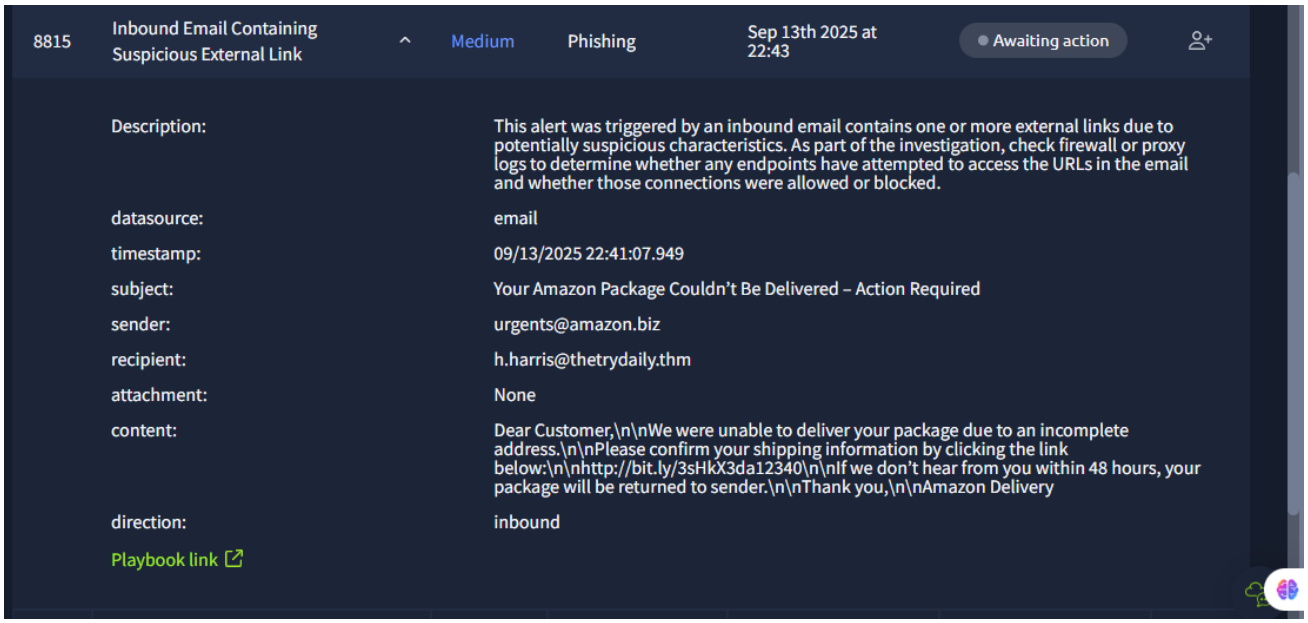
List of Related Entities:

- Sender: onboarding@hrconnex.thm
- Recipient: j.garcia@thetrulythm
- URL in email: https://hrconnex.thm/onboarding/15400654060/j.garcia
- Domain: hrconnex.thm

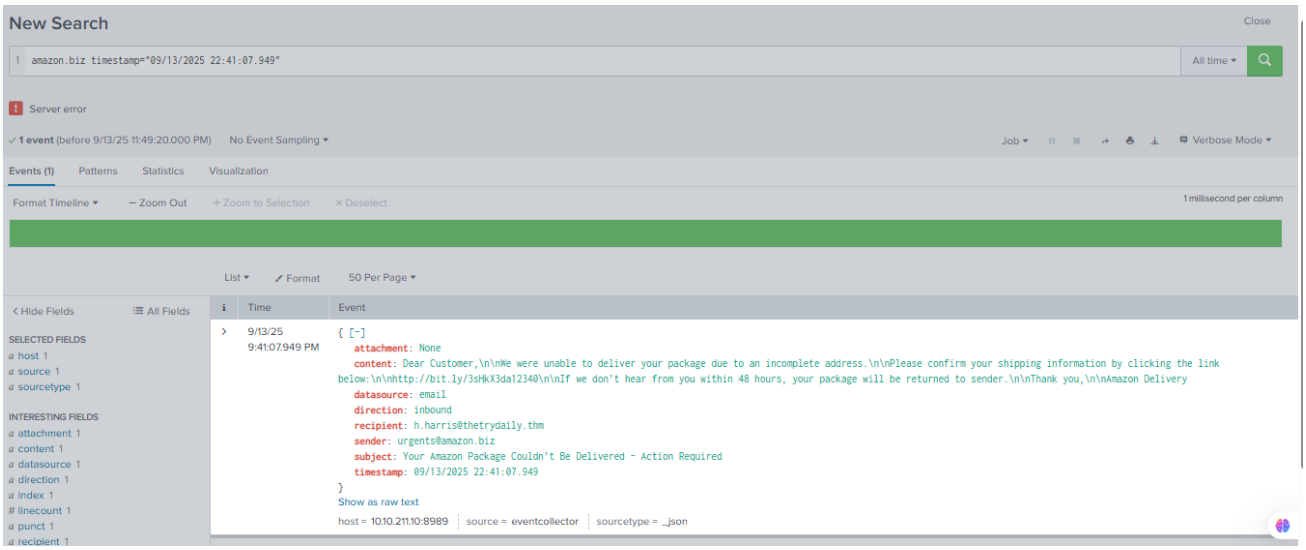
Reason for Classifying as False Positive:

- Domain and URL flagged by the alert were verified using **TryDetectThis** and came back as **CLEAN** (no malicious activity detected).
- The email domain and external URL match each other and are consistent with legitimate company onboarding.
- No indicators of compromise (IOC) or suspicious activity were found in SIEM logs beyond this email.





Lookup the specific alert on Splunk using unique information within the email such as domain and timestamp for the alert. Search up in Splunk:



Found the specific event on Splunk.

• **Description**: This alert was triggered by an inbound email containing one or more external links due to potentially suspicious characteristics. As part of the investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email and whether those connections were allowed or blocked.

• **Timestamp**: 09/13/2025 22:41:07.949

• **Subject**: Your Amazon Package Couldn't Be Delivered – Action Required

• **Sender**: urgents@amazon.biz

• **Recipient**: h.harris@thetrydaily.thm

• **Attachment**: None (No attachment)

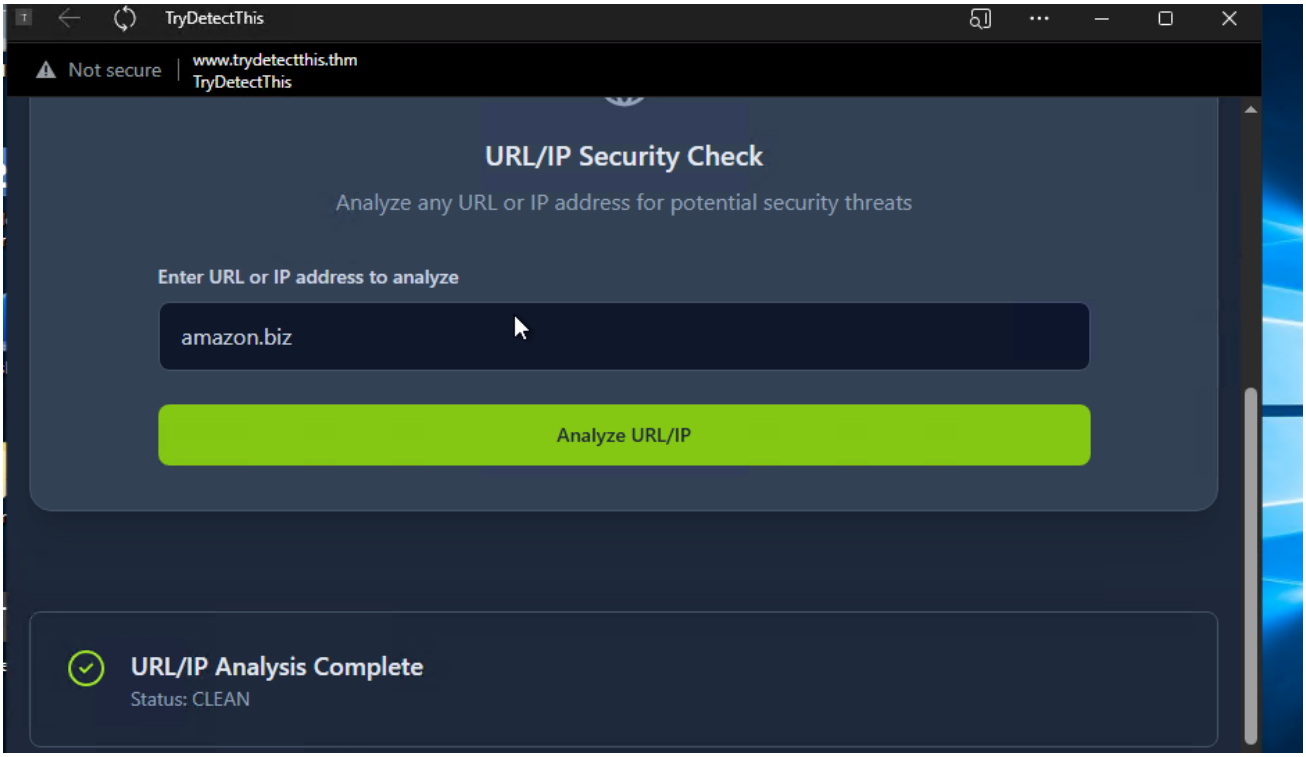
• **Content**: Dear Customer,\n\nWe were unable to deliver your package due to an incomplete address.\n\nPlease confirm your shipping information by clicking the link below:\n\nhttp://bit.ly/3sHkX3da12340\n\nIf we don't hear from you within 48 hours, your package will be returned to sender.\n\nThank you,\n\nAmazon Delivery

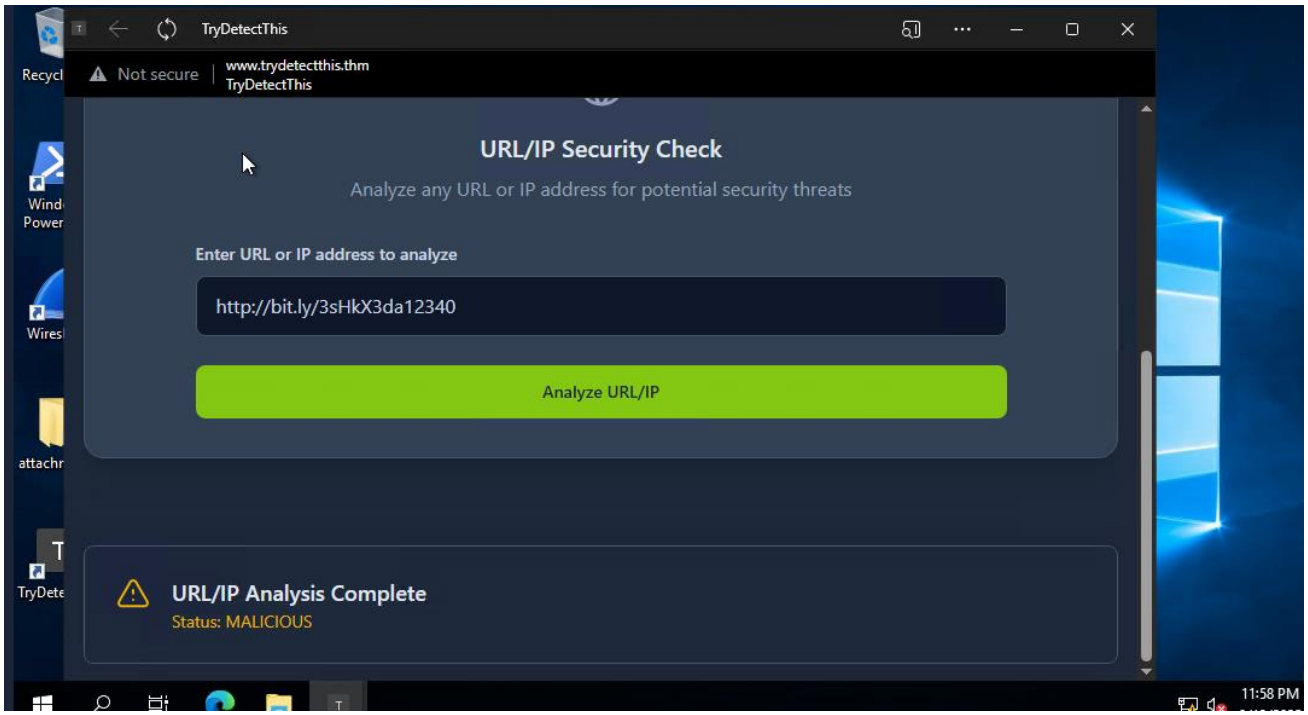
• **Direction**: Inbound

This email seems to be coming from Amazon at domain "amazon.biz" sent to the user h.harris at our organisation "TheTryDaily". The .biz extension seems a little suspicious. Subject says package could not be delivered and uses urgency to request action. The main content asks the viewer to clicking the link below listed as a bit.ly URL. Bitly is a common URL shortener, used by many phishers to mask

or hide a potential malicious link. The URL is highly suspicious, as Amazon most likely wouldn't use Bitly instead of a trusted amazon domain. The email also uses urgency by stating action is required within 48 hours, a common tactic for phishing campaigns to encourage engagement.

Use the TryDetectThis application to lookup the sender domain and listed external URL.





The domain “amazon.biz” came up clean, but the external URL came up as malicious function. This points to the possibility of being a phishing email with a malicious link.

This email alert “8815” is a **True Positive**

Report

Time of Activity:

- 09/13/2025 22:41:07 – 22:43:00

List of Affected Entities:

- Sender: urgents@amazon.biz
- Recipient: h.harris@thetrydaily.thm
- URL in email: http://bit.ly/3sHkX3da12340
- Domain: amazon.biz
- Destination IP: (lookup in firewall logs if connection attempted)

Reason for Classifying as True Positive:

- Email contains a **malicious shortened URL** (bit.ly/3sHkX3da12340) confirmed by **TryDetectThis**.
- Use of urgency in subject (“Action Required within 48 hours”) aligns with **phishing tactics**.
- URL redirection via Bitly indicates attempt to mask malicious destination.
- The sender domain .biz is suspicious compared to legitimate Amazon domains, raising further concern.

Reason for Escalating the Alert:

- Confirmed **malicious URL** could compromise the user or network if clicked.
- Email targets internal user (h.harris@thetrydaily.thm) and is inbound.
- Escalation ensures proper investigation, endpoint checks, and preventive measures.

Recommended Remediation Actions:

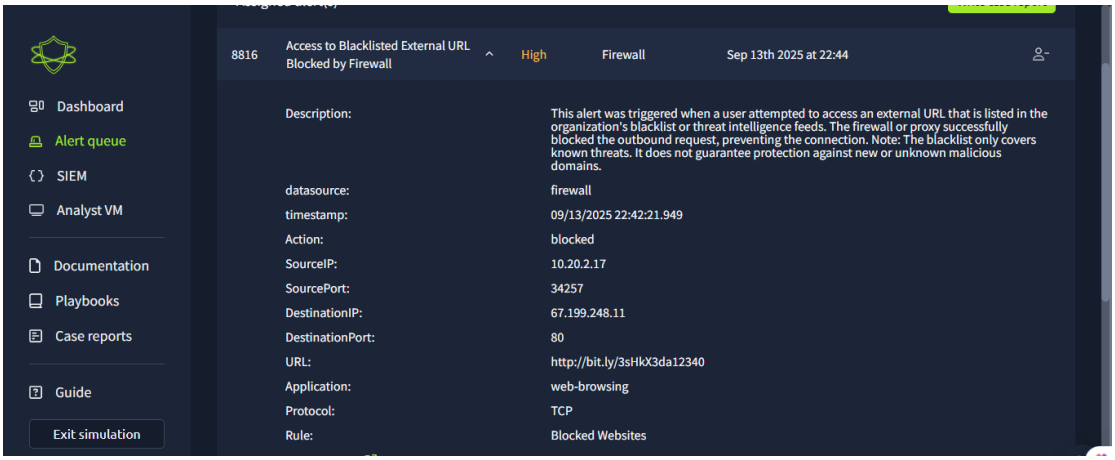
1. Isolate affected user endpoint (h.harris@thetrydaily.thm) if URL was clicked.
2. Block malicious URL (bit.ly/3sHkX3da12340) at firewall/proxy level.
3. Conduct **EDR/AV scan** on recipient endpoint to ensure no compromise.
4. Notify user about the phishing attempt and provide training on recognizing such emails.
5. Check email gateway and SIEM for other potential recipients of the same email.
6. Document incident in SOC incident tracker for future reference and threat intel sharing.

List of Attack Indicators:

- Subject line: "Your Amazon Package Couldn't Be Delivered – Action Required" (urgency tactic).
- Sender domain: amazon.biz (suspicious compared to legitimate amazon.com).
- Malicious URL: http://bit.ly/3sHkX3da12340 (confirmed by threat intel).
- Direction: Inbound email.
- Use of Bitly to mask malicious destination.

---

datasource=firewall SourceIP="10.20.2.17" SourcePort=34257



The next alert triggered is for ”Access to Blacklisted external URL blocked by firewall”. The alert is from the network firewall, the alert contains the following information:

• Title: Access to Blacklisted External URL Blocked by Firewall

• Description: This alert was triggered when a user attempted to access an external URL that is listed in the organization’s blacklist or threat intelligence feeds. The firewall successfully blocked the outbound request, preventing the connection. Note: The blacklist only covers known or known malicious domains; it does not provide protection against new or unknown malicious domains.

• Timestamp: 09/13/2025 22:42:21.949

• Action: Blocked

• Source IP: 10.20.2.17

• Source Port: 54217

• Destination IP: 67.199.248.11

• Destination Port: 80

• URL: http://bit.ly/3HxkdA2340

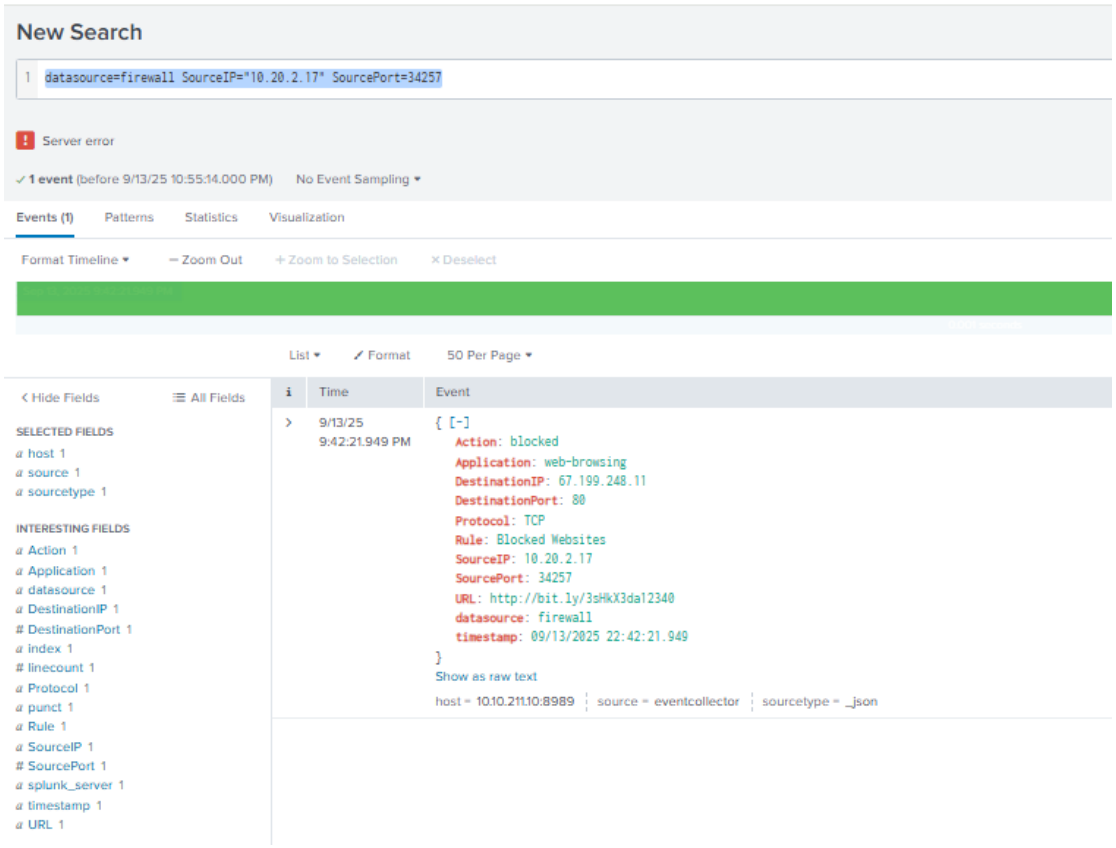
• Application: web browsing

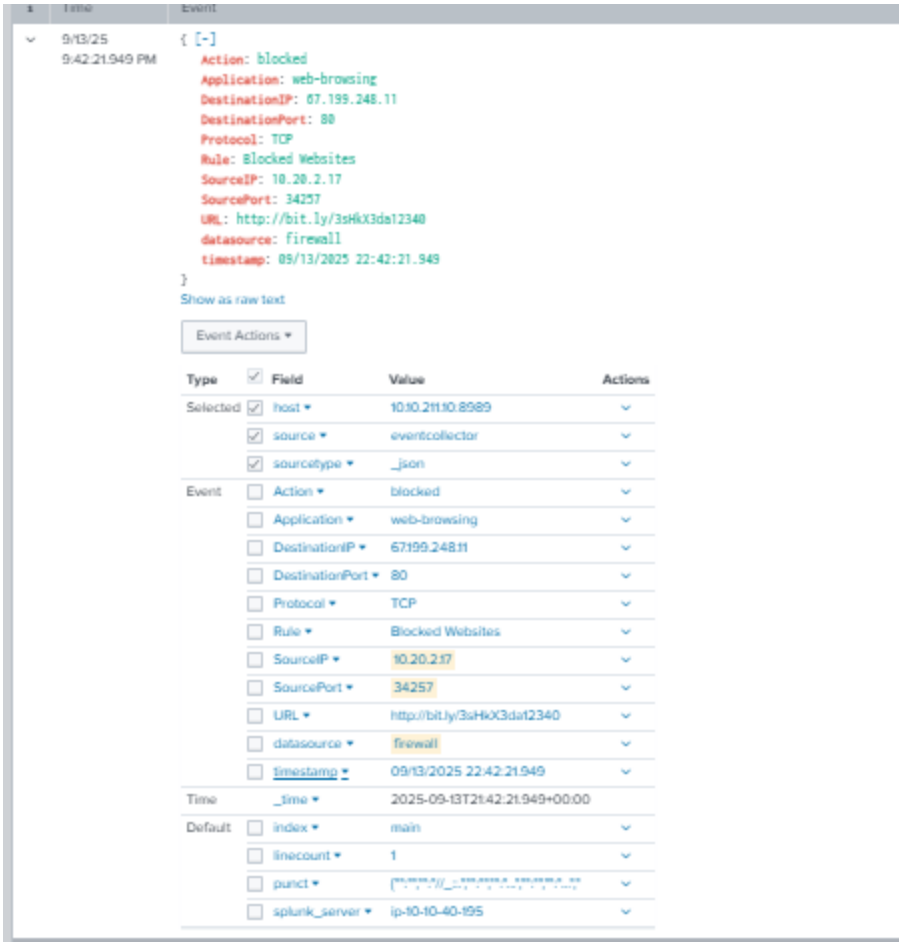
• Rule: Blocked Websites

This alert tells us that a user within our network has attempted to visit an external URL that was listed in our organizations blacklist of domains. These domains will be automatically blocked if

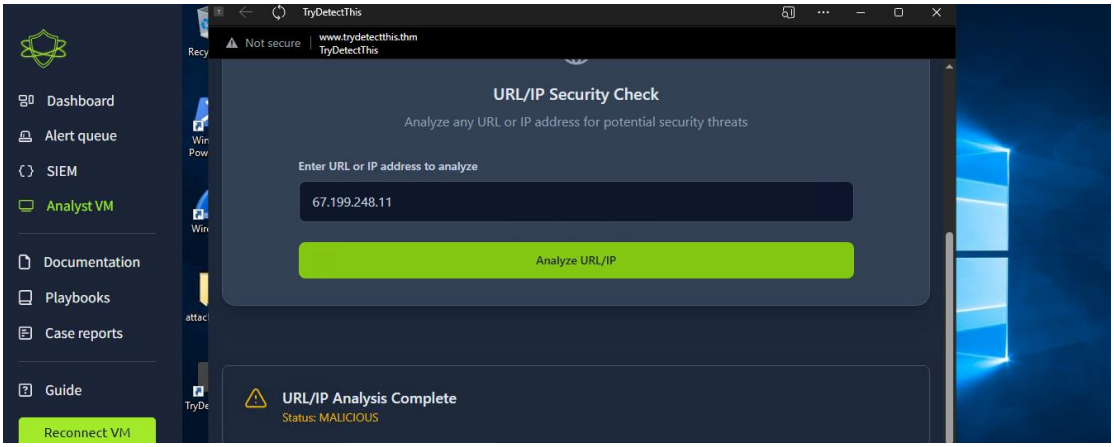
visited by our users. The firewall successfully blocked the outbound request. It states that the IP 10.20.2.17 using port 54217 had tried to visit IP 67.199.248.11 at port 80 at URL http://bit.ly/3HxkdA2340. The domain “bit.ly” was a part of our organization’s blacklist of domains, likely because it is a URL shortener often used to hide actual malicious domains.

Add the alert to assigned alerts with the 2 other emails we previously covered





In the Splunk log for the specific firewall alert, we see the matching information in the log. The URL contains a blacklisted domain, was blocked for that reason. The Destination IP hosting the web service on port 80 should be further investigated through threat intel.



The destination IP was flagged as Malicious.

Report

Time of Activity:
09/13/2025 22:42:21.949

List of Affected Entities:

- Source IP: 10.20.2.17
- Source Port: 54217
- Destination IP: 67.199.248.11
- Destination Port: 80
- URL: http://bit.ly/3HxkdA2340 (bit.ly – blacklisted domain)
- Application: Web browsing
- User: Device linked to employee at IP 10.20.2.17 (needs confirmation from asset management)

Reason for Classifying as True Positive:

- The accessed link contained a **known blacklisted domain** (bit.ly).
- Threat Intelligence confirmed that the **destination IP 67.199.248.11** is malicious.
- The activity is consistent with malicious behavior involving **URL shorteners masking phishing/malware sites**.

Reason for Escalating the Alert:

- Although the firewall successfully blocked the connection, the **attempt itself indicates user engagement with a phishing/malicious link**.
- Escalation is required to investigate the affected user (possible phishing victim).
- Monitoring is necessary to ensure there was no **parallel attempt through another device or network path**.

Recommended Remediation Actions:

1. Identify and notify the user at Source IP (10.20.2.17). Confirm whether they intentionally clicked the link.
2. Perform a forensic check on the device for other suspicious activity.
3. Continue monitoring network logs for repeated attempts to reach the same domain/IP.
4. Block/alert on URL shortener domains (bit.ly and similar).
5. Provide user awareness training on avoiding shortened/masked URLs.
6. Confirm no data exfiltration attempts were made (review proxy/firewall logs).

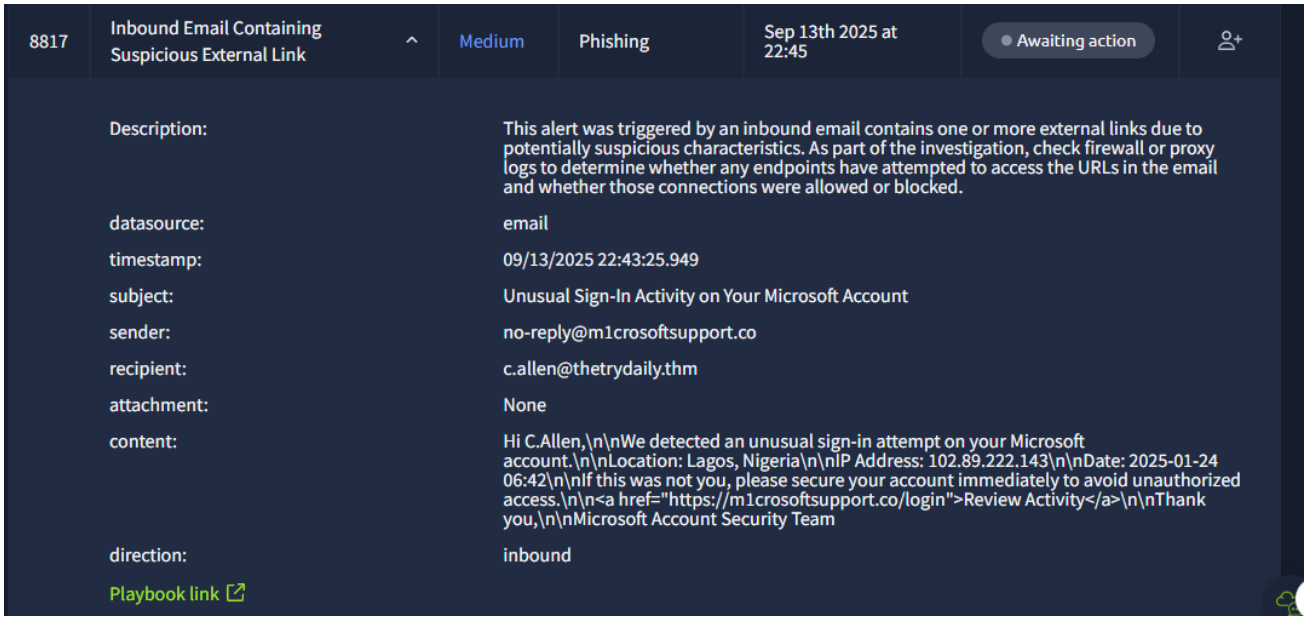
List of Attack Indicators (IOCs):

- Suspicious URL: http://bit.ly/3HxkdA2340
- Source IP: 10.20.2.17

Destination IP: 67.199.248.11 •

Protocol/Port: TCP 80 (HTTP) •

Domain: bit.ly (blacklisted) •



The next email alert contains the following information:

• **Alert ID**: 8817

• **Title**: Inbound Email Containing Suspicious External Link

• **Category**: Phishing

• **Description**: This alert was triggered by an inbound email containing one or more external links due to potential investigation, check firewall or proxy logs to determine whether any endpoints have attempted to those connections were allowed or blocked.

• **Datasource**: email

timestamp: 09/13/2025 22:43:25.949

subject: Unusual Sign-In Activity on Your Microsoft Account

sender: no-reply@m1crosoftsupport.co

recipient: c.allen@thetrydaily.thm

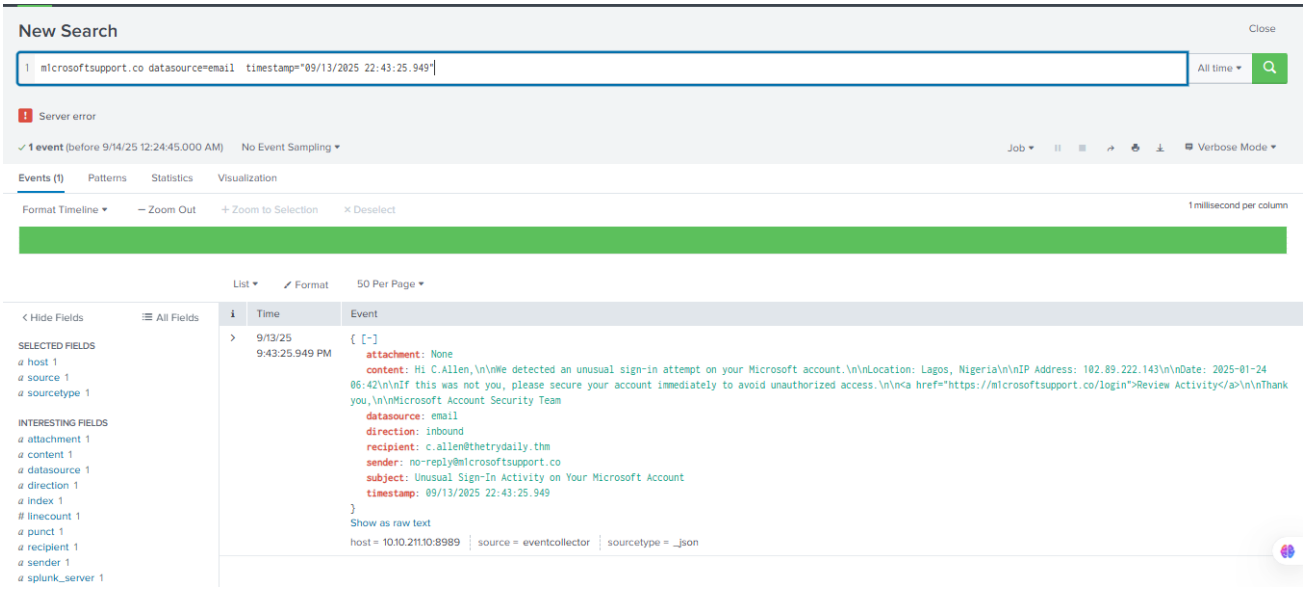
attachment: None

content: Hi C.Allen,\n\nWe detected an unusual sign-in attempt on your Microsoft account.\n\nLocation: Lagos, Nigeria\n\nIP Address: 102.89.222.143\n\nDate: 2025-01-24 06:42\n\nIf this was not you, please secure your account immediately to avoid unauthorized access.\n\nReview Activity\n\nThank you,\n\nMicrosoft Account Security Team

This email claims to be from Microsoft (no-reply@m1crosoftsupport.co) about an unusual sign-in from Lagos (IP: 102.89.222.143) on Sep 13th 2025 at 22:45. The senders domain contains a “1” number in the domain as in “m1crosoftsupport.co”, highly suspicious. The link (https://microsoftsupport.co/login) is also suspicious, likely leading to a malicious site. Sent to c.allen@thetruly.thm with no attachments.

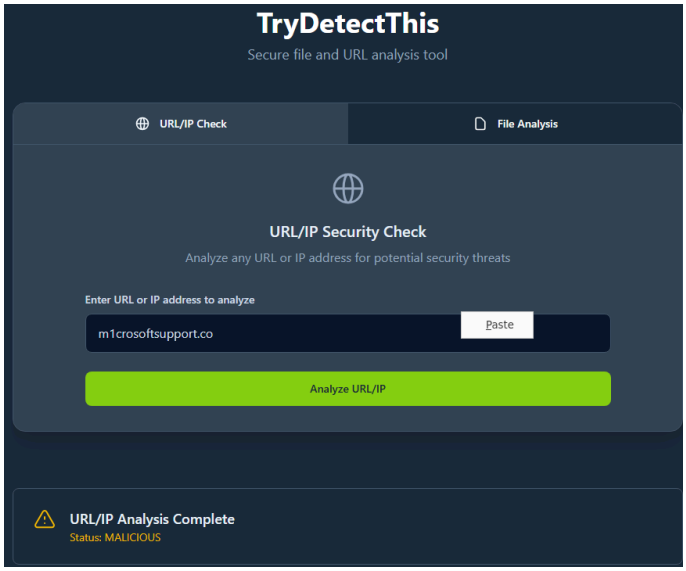
First impressions, this looks like a phishing email. Let's investigate further through Splunk log and threat intelligence.

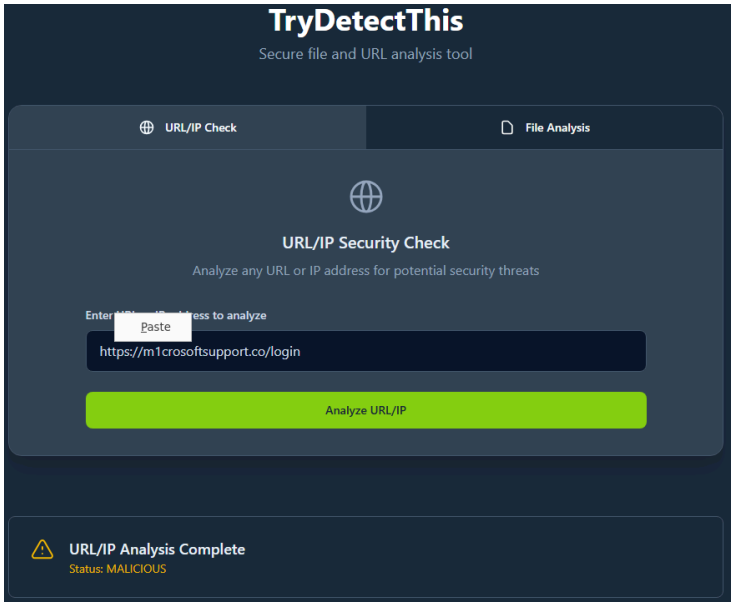
Search: m1crosoftsupport.co datasource=email timestamp="09/13/2025 22:43:25.949"



This splunk search narrowed it down to the specific event.

The log contains the email information provided. Using the stated information, do threat intelligence research on the senders domain “m1crosoftsupport.co” and listed URL in the main content.





Both the senders domain at “m1crosoftsupport.co” and the listed URL under the same domain were flagged as malicious. We can determine that this email alert is a malicious phishing email and is therefore a true positive alert.

The email alert “8817” is a **True Positive**

Report

Time of Activity:
09/13/2025 22:43:25.949

List of Affected Entities:

- Sender: no-reply@m1crosoftsupport.co
- Recipient: c.allen@thetrydaily.thm
- Subject: Unusual Sign-In Activity on Your Microsoft Account
- Attachment: None
- Suspicious URL: https://m1crosoftsupport.co/login
- IP (claimed in email content): 102.89.222.143

Reason for Classifying as True Positive:

- The sender’s domain (m1crosoftsupport.co) is a typosquatted version of Microsoft.
- Threat intelligence flagged both the sender domain and embedded URL as malicious.
- The email uses urgency and scare tactics (unusual sign-in alert) which are common phishing techniques.
- The URL redirects to a fake Microsoft login page designed for credential harvesting.

Reason for Escalating the Alert:

- This is a targeted phishing attempt against an internal user.
- Clicking the link could lead to credential theft and unauthorized access.
- Presence of typosquatting indicates a broader phishing campaign.

Recommended Remediation Actions:

1. Block the domain m1crosoftsupport.co and related IPs.
2. Notify the recipient (c.allen) and ensure they did not click the link.
3. Search email logs for other messages from the same sender.
4. Update email filters to detect typosquatted domains.
5. Monitor authentication logs for suspicious login attempts.
6. Reinforce phishing awareness training for users.

List of Attack Indicators:

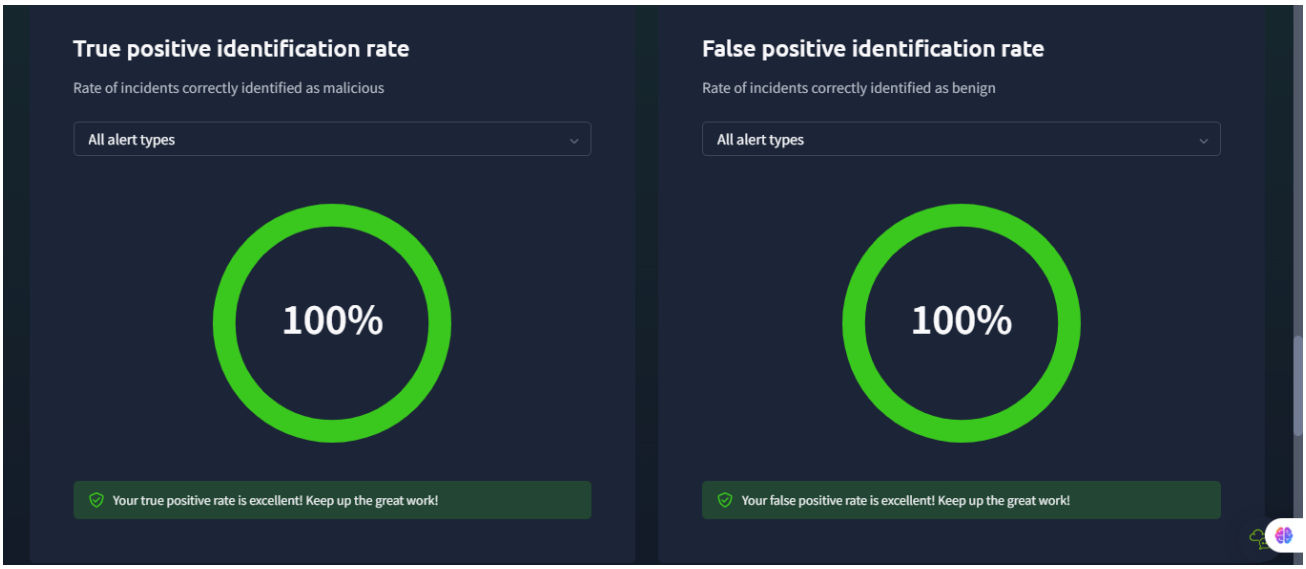
- Malicious Domain: m1crosoftsupport.co
- Malicious URL: https://m1crosoftsupport.co/login
- Sender Email: no-reply@m1crosoftsupport.co
- IP in message lure: 102.89.222.143

ETH.CYBER

Victory! Security breach prevented!

You passed the scenario by identifying all true positive alerts. However, your MTTR and dwell time were longer than average, and your true positive rate was 60%, which is worse than previous runs. The 'Phishing' alert took notably longer to close.

1st ^ 0 220 pts + 65 pts



True positives

Assess your accuracy on the alerts you marked as true positives.

Overall analysis POWERED BY AI

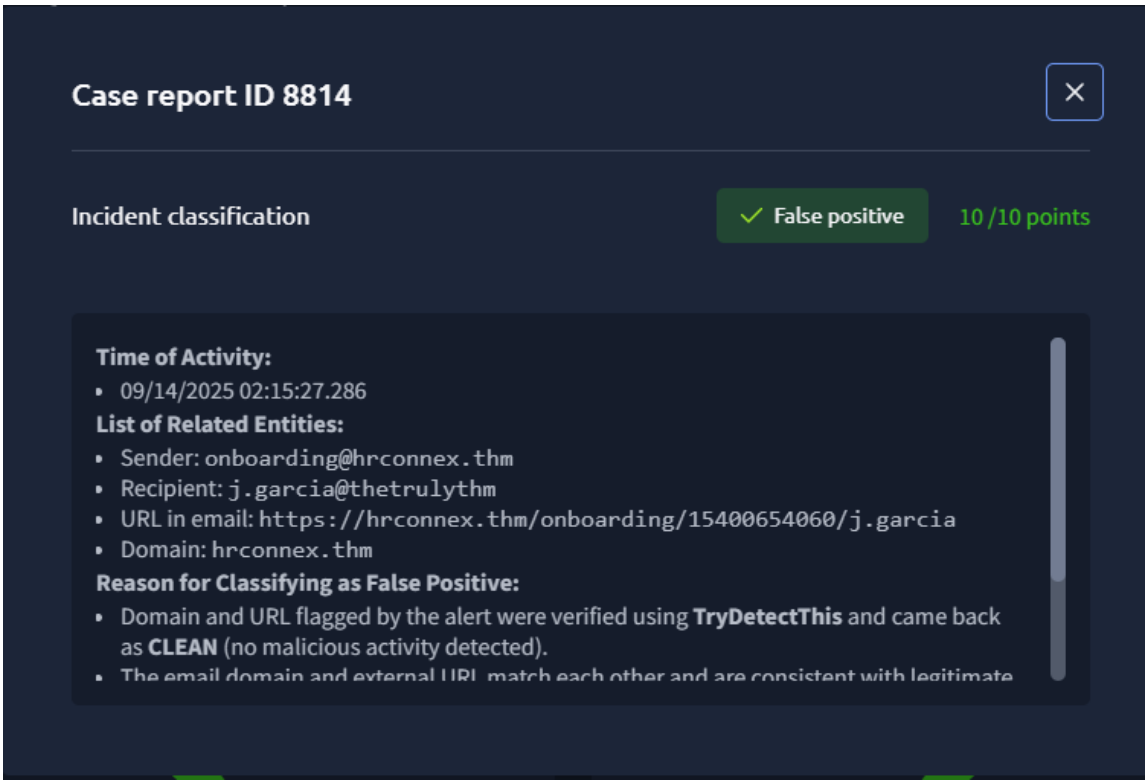
Your reports provide a comprehensive overview of the incidents, effectively covering the essential details such as the entities involved, the nature of the threat, and the actions taken. However, there is room for improvement in consistently addressing the 'When' aspect across all reports, as the timing of events is crucial for understanding the sequence and urgency of the incidents. Additionally, while the 'Why' is generally well-covered, ensuring that the rationale for classifying alerts as true positives is clear and concise will enhance the clarity of your reports. Keep up the good work and continue to refine these areas for even more effective reporting.

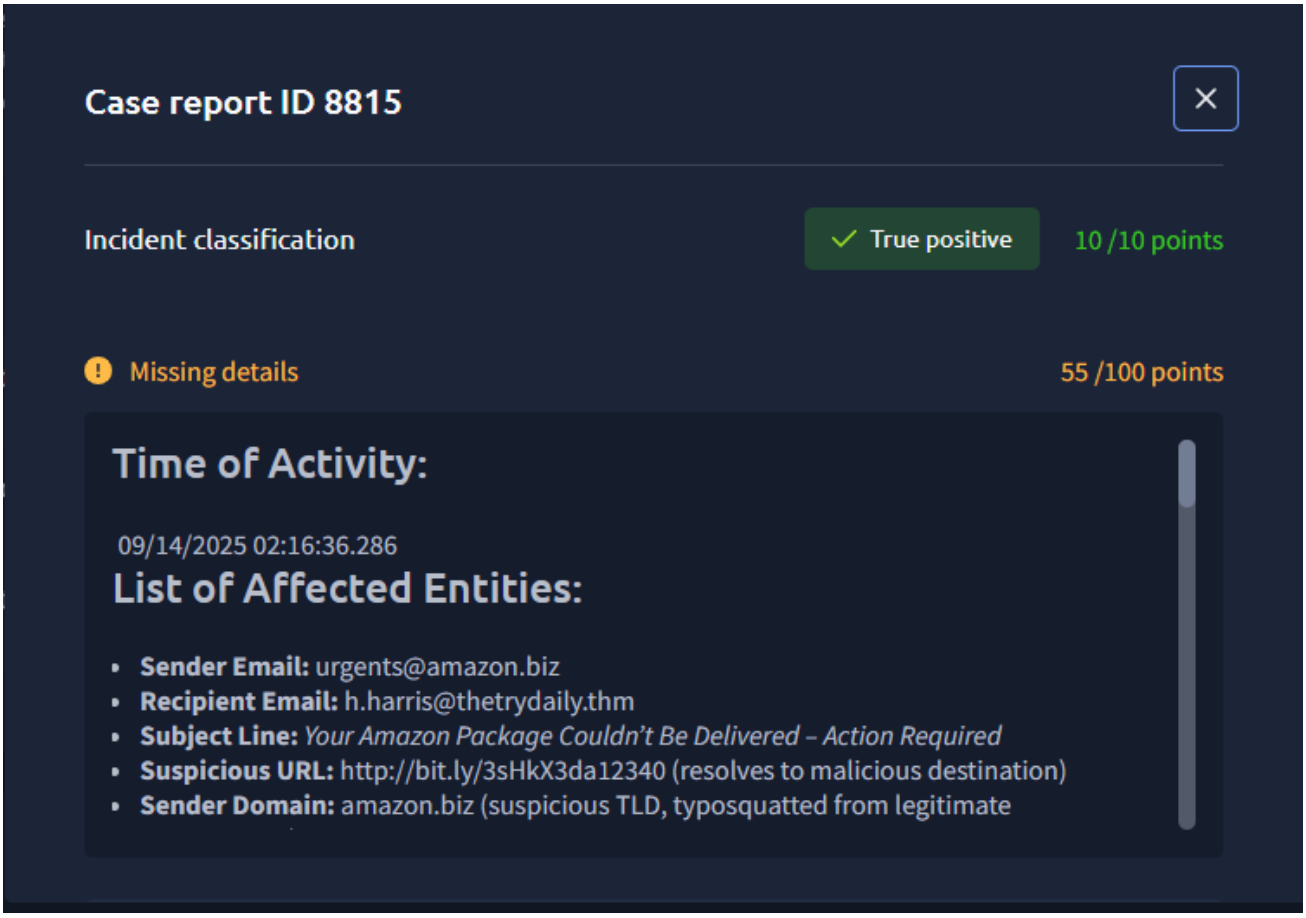
ID	Alert rule	Severity	Type	Time to resolve	Classification	Action
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	3.47 minutes	Correct	View analysis
8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	1.22 minutes	Correct	View analysis
8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	1.05 minutes	Correct	View analysis

False positives

Assess your accuracy on the alerts you marked as false positives.

ID	Alert rule	Severity	Type	Time to resolve	Classification	Action
8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	2.12 minutes	Correct	View


Case report ID 8814
Incident classification
False positive
10 /10 points
Time of Activity:
09/14/2025 02:15:27.286
List of Related Entities:
Sender: onboarding@hrconnex.thm
Recipient: j.garcia@thetrulythm
URL in email: https://hrconnex.thm/onboarding/15400654060/j.garcia
Domain: hrconnex.thm
Reason for Classifying as False Positive:
Domain and URL flagged by the alert were verified using TryDetectThis and came back as CLEAN (no malicious activity detected).


Case report ID 8815
Incident classification
True positive
10 /10 points
Missing details
55 /100 points
Time of Activity:
09/14/2025 02:16:36.286
List of Affected Entities:
Sender Email: urgents@amazon.biz
Recipient Email: h.harris@thetrydaily.thm
Subject Line: Your Amazon Package Couldn't Be Delivered – Action Required
Suspicious URL: http://bit.ly/3sHkX3da12340 (resolves to malicious destination)
Sender Domain: amazon.biz (suspicious TLD, typosquatted from legitimate

Case report ID 8816

Incident classification — ✓ True positive — 10 /10 points

Missing details — 70 /100 points

09/14/2025 02:17:50.286

List of Affected Entities:

- **User / Endpoint:** John Doe's workstation (associated with 10.20.2.17)
- **Source IP:** 10.20.2.17
- **Source Port:** 54217
- **Destination IP:** 67.199.248.11
- **Destination Port:** 80
- **URL Accessed:** http://bit.ly/3HxkdA2340
- **Application:** Web browsing

Reason for Classifying as True Positive:

- The URL accessed contains a **domain listed on the organization's internal blocklist**

Case report ID 8817

Incident classification — ✓ True positive — 10 /10 points

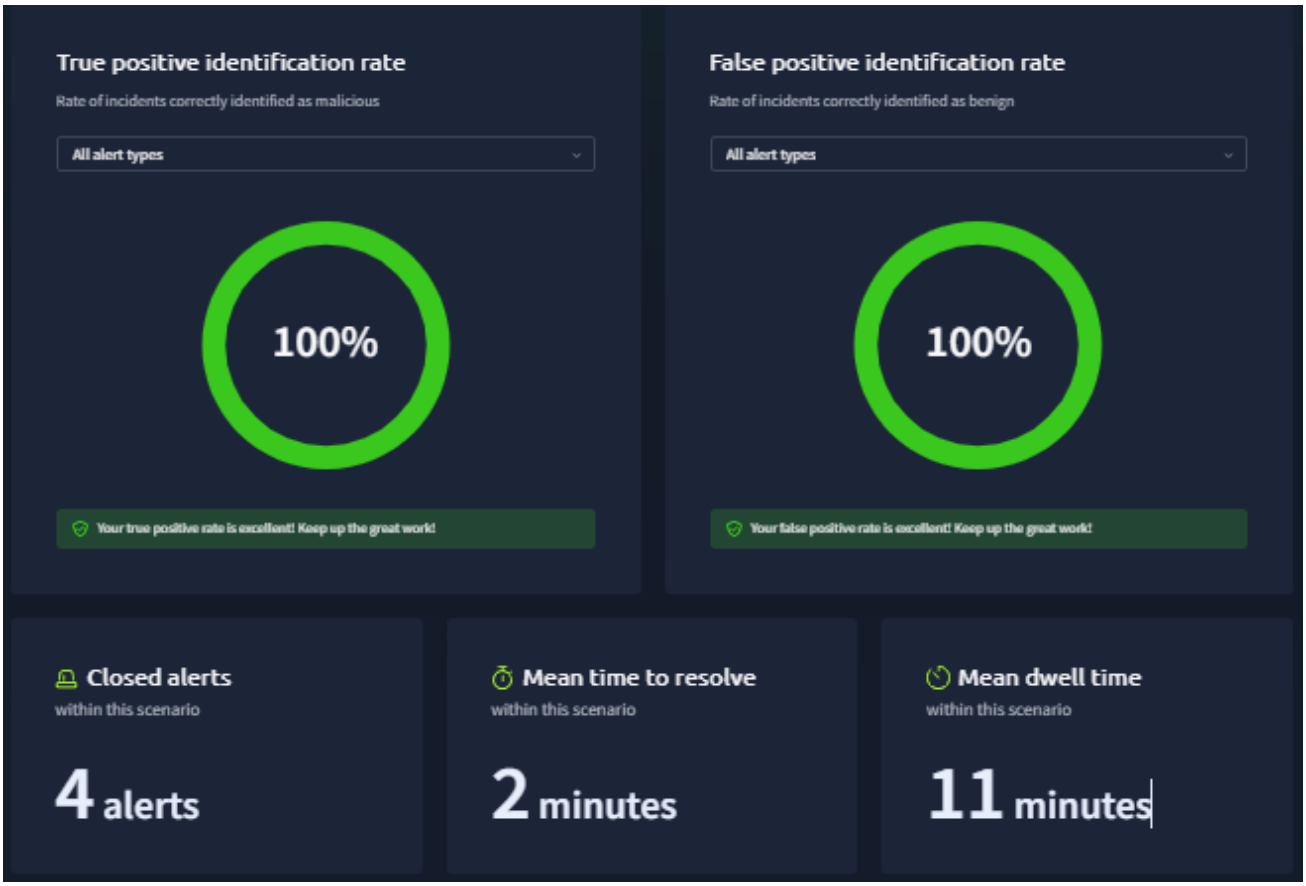
Missing details — 45 /100 points

Time of Activity:

09/14/2025 02:18:54.286

List of Affected Entities:

- **Sender Email:** no-reply@m1crosoftsupport.co
- **Recipient Email:** c.allen@thetrydaily.thm
- **Subject:** *Unusual Sign-In Activity on Your Microsoft Account*
- **Attachment:** None
- **Suspicious URL:** https://m1crosoftsupport.co/login
- **IP (claimed in email content):** 102.89.222.143
- **Internal Affected Host:** Mailbox of c.allen
- **Destination (Phishing Domain Hosting):** 102.89.222.143



https://tryhackme.com/soc-sim/summary/68c616b3aa468a7609a9be48

https://tryhackme.com/soc-sim/public-summary/c0b2d6e5df4b6fbd0391aa4861a2f462ae9b89f3e02f83f32b230ace99a415332b50198e9145262ed6f69dc902cf3f2d

anther

TryHackMe | Cyber Security Training

Phishing Unfolding — TryHackMe — SOC Simulator — Overview | by Forrest Caffray | Sep, 2025 | Medium