SOC Simulator Introduction to Phishing

Started up the tryhackme SOC simulator and waiting for the first alert to come in. This was my first time Running through this program so was not sure what to expect or how to process the actions as they came in.

Choose to use the Splunk Edition this round and setup my dashboard so I could see the SEIM Dashboard, the Splunk enterprise on another monitor and also setup the Analyst VM on another screen.

Phishing Email Playbook shows the following:

Step 1: Assign alert

Step2: Alert triaging process

Step 3: Analyze Email artifacts ( Check Sender Reputation and review attachments)

Step 4: investigate related alerts

Step 5: Case reporting

First alert came in as a Medium Severity for a phishing type

First action was to assign the ticket to my self and check the info on the alert:  
Description:

This alert was triggered by an inbound email contains 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.

datasource: email

timestamp: 09/03/2025 18:47:53.433

subject: Action Required: Finalize Your Onboarding Profile

sender: onboarding@hrconnex.thm

recipient: j.garcia@thetrydaily.thm

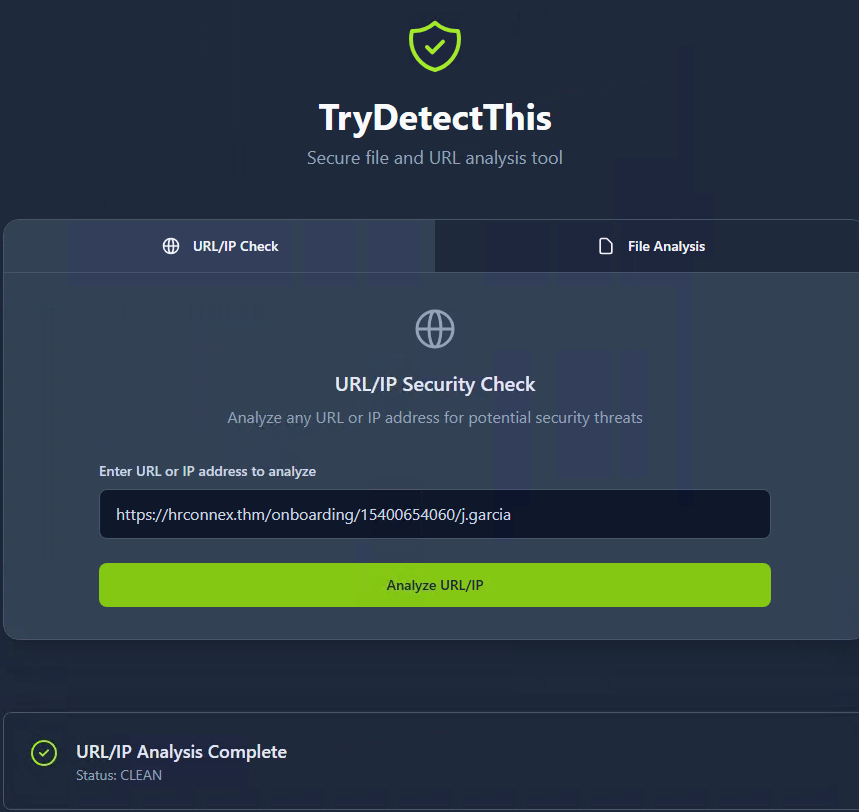
attachment: None

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\n<a href="https://hrconnex.thm/onboarding/15400654060/j.garcia">Set Up My Profile</a>.\n\nIf you have questions, please reach out to the HR Onboarding Team.

direction: inbound

So first off we notice it is an inbound email with no attachments. Ran the Https link through the trydetectthis on the Analyst Vm. This came back as clean.



After checking that I navigated over to the Splunk and did a search for anything with the Link from the email. Found two events located in splunk and pulled the ip address which was also ran through the trydetectthis which also came back clean.

So From what we can see from the Playbook and available information this looks to be a false positive Alert and we went to write up the case as following.

Who: Email from [Onboarding@hrconnex.thm](mailto:Onboarding@hrconnex.thm) Was flagged

What: Email with external link

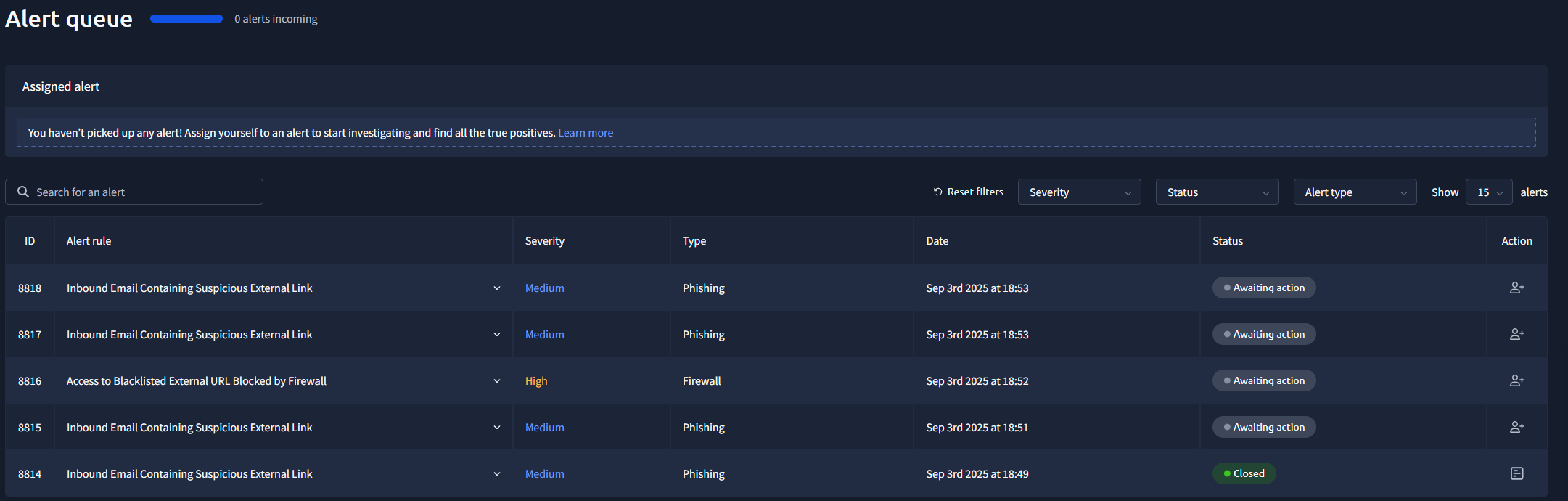
When: 09/03/2025 18:47:53.433

Where: J.garcia@thetrydaily.thm

Why: Onboarding request

Reason for classifying as false positive: Email and Ip address came back clean and did not see any other issues found to cause this to be flagged as malicious

Once submitted we see several Alerts in the dashboard so we of course pick the High severity as this should be the order they are picked from when showing in SIEM.



So The High severity Alert is due to access to a 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 or proxy successfully blocked the outbound request, preventing the connection. Note: The blacklist only covers known threats. It does not guarantee protection against new or unknown malicious domains.

datasource: firewall

timestamp: 09/03/2025 18:50:16.433

Action: blocked

SourceIP: 10.20.2.17

SourcePort: 34257

DestinationIP: 67.199.248.11

DestinationPort: 80

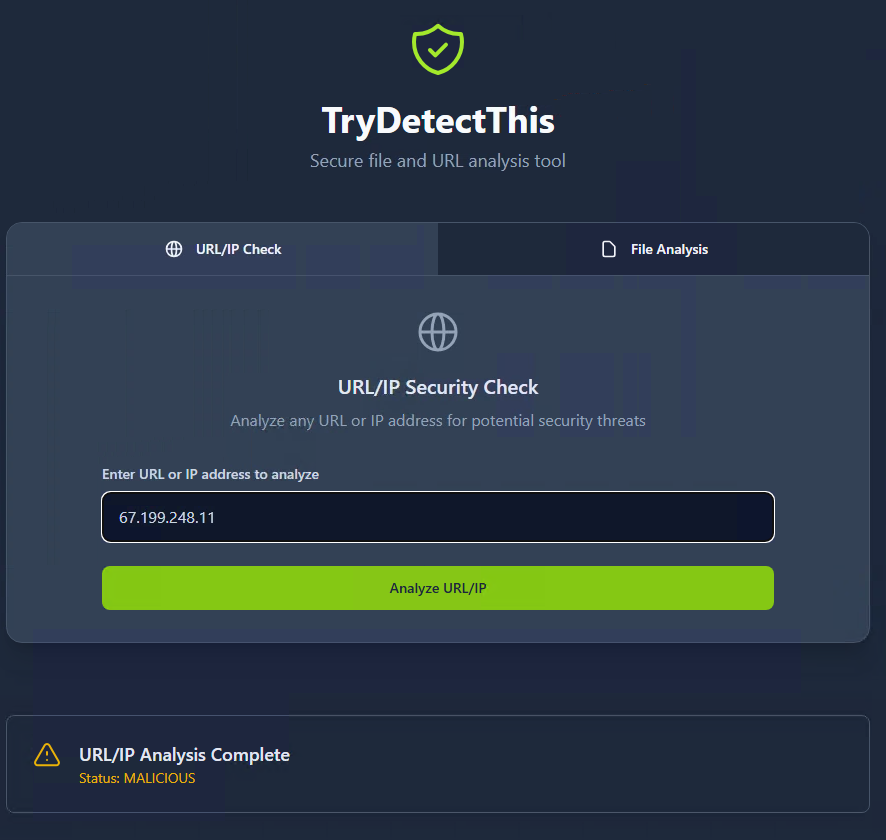
URL: http://bit.ly/3sHkX3da12340

Application: web-browsing

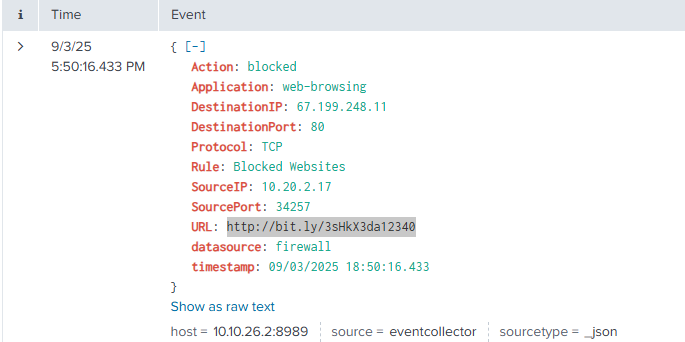
Protocol: TCP

Rule: Blocked Websites

So first thing I did was head over to the Anaylst Vm and put in the destination IP which was of course flagged as Malicious



I also put in the Source IP in Splunk and found two event alerts for the users ip address. Looks like there was a Rule: Blocked website used for the URL: <http://bit.ly/3sHkX3da12340>. The rule is in the firewall and was blocked successfully at the same timestamp as the alert in SIEM



So once we found all the information I double checked with the playbook and it states to follow the following:

Step 1: Assign alert

Step 2: Alert triagin Process

Step 3: Review network connections details

Step 4: Assess reputation of domain or ip

Step 5: Correlate with internal activity

Step 5 Case reporting.

I felt at this point I felt like we had enough information to note that this was properly blocked by the firewall ruie in place and the suer was not able to access the website. When starting the case report we set this as a true positive as the site is malicious and user tried to access a not allowed website.The write up looks like this:

**Time of activity:** 09/03/2025 18:50:16:443

**List of Affected Entities:** User IP 10.20.2.17

**Reason for Classifying as True Positive:** Website IP And URL both flagged as Malicious Reputation

**Reason for Escalating the Alert:** No Escalation was marked since the Site was properly blocked by the firewall rule.

**Recommended Remediation Actions:** User may need to be spoken to and informed that this site is a malicious site and to avoid this kinda thing in the future.

**List of Attack Indicators:** Web Site URL

Case was submitted successfully and we moved onto our next Alert which is a medium Phishing alert. Since all the remaining alerts are all medium per standard I grabbed the oldest alert first and assigned it to me. Information about the Alert is:

Description: This alert was triggered by an inbound email contains 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.

datasource: email

timestamp: 09/03/2025 18:49:02.433

subject: Your Amazon Package Couldn’t Be Delivered – Action Required

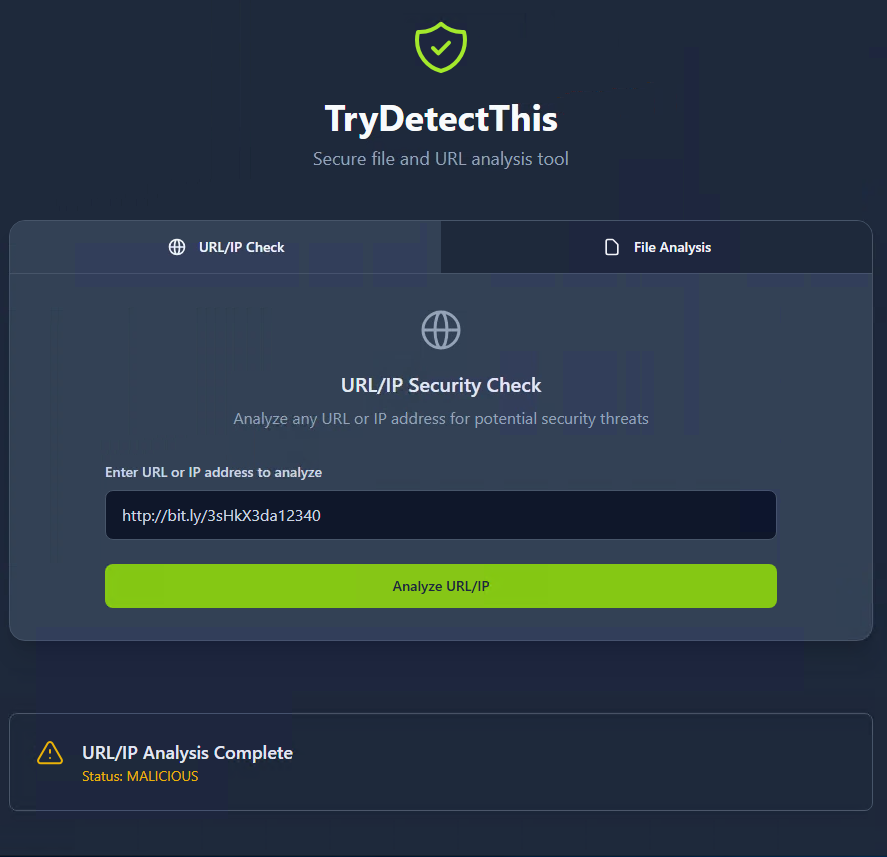
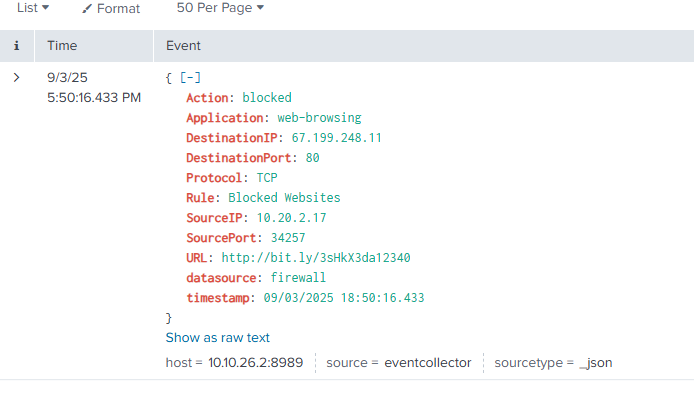
sender: urgents@amazon.biz

recipient: h.harris@thetrydaily.thm

attachment: None

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 is also an Inbound email that contains external Links. Checked the Playbook again and it follows the same rule pattern as our first case. So I went ahead and grabbed the URL from the Email and put it in the TryDetectThis To check its status. The link nhttp://bit.ly/3sHkX3da12340 Comes back as a malicious Address.  So with that information and went over to Spunk and checked to see if any proxy rules or firewalls triggered with this. Splunk showed one event With this link and showed the action of being blocked. The firewall has a rule engaged which blocked the URL. The Attackers IP on the URL 67.199.248.11 which was attempted to be accessed by user on Ip 10.20.2.17. Timestamp was at 09/03/2025 18:50:16.433. 

With all this information we are ready to close the case as a True Positive.

**Time of activity:** 09/03/2025 18:49:02.433

**List of Affected Entities:** 10.20.2.17

**Reason for Classifying as True Positive:** URL attached in Email is a Malicious Website and was blocked by the firewall Rule.

**Reason for Escalating the Alert:** Was not escalated due to Firewall Rule blocking the email successfully and no other Event was attempted with this Event

**Recommended Remediation Actions:** Setting up a Rule to block the IP address 67.199.248.11 to help avoid future attacks from this address

**List of Attack Indicators:** Ip address 67.199.248.11 and URL <http://bit.ly/3sHkX3da12340>

Two Cases left showing so we of course pick the oldest and assign it to our self. The following is the report:

Description: This alert was triggered by an inbound email contains 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.

datasource: email

timestamp: 09/03/2025 18:51:20.433

subject: Unusual Sign-In Activity on Your Microsoft Account

sender: no-reply@m1crosoftsupport.co

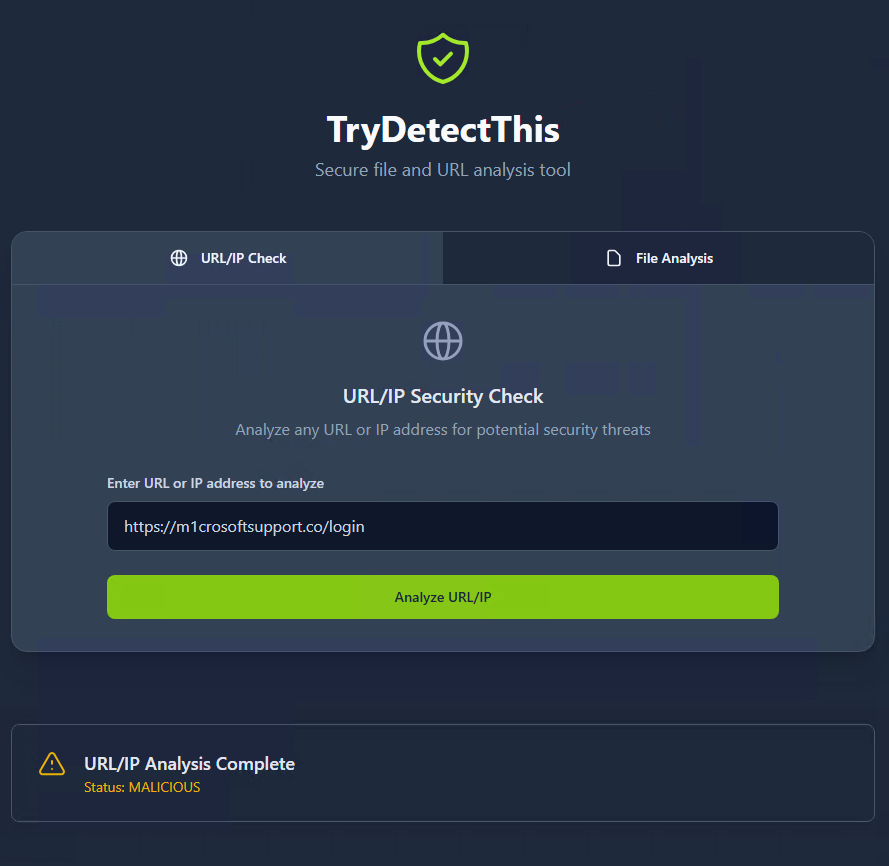
recipient: c.allen@thetrydaily.thm

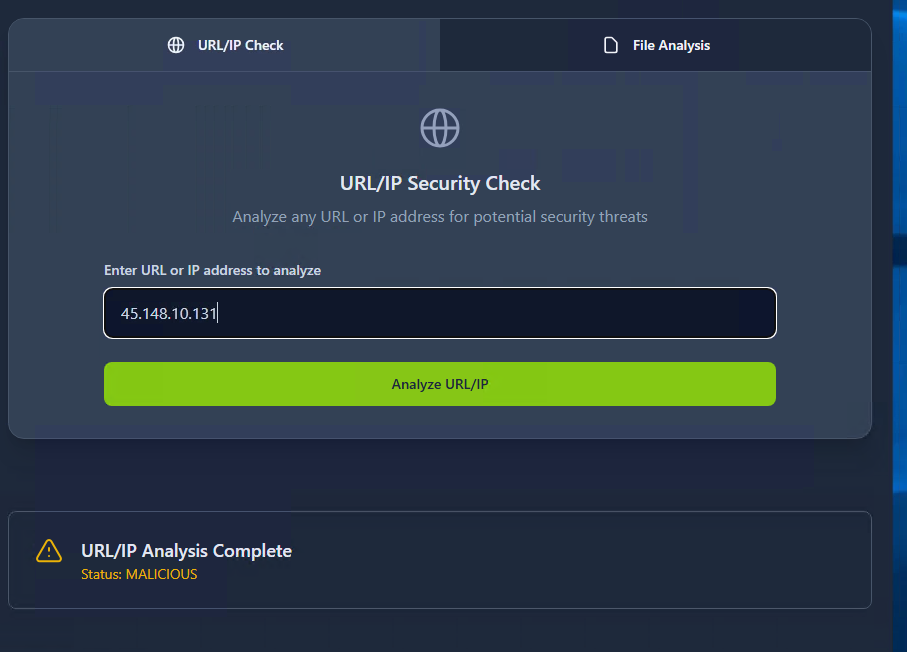
attachment: None

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\n<a href="https://m1crosoftsupport.co/login">Review Activity</a>\n\nThank you,\n\nMicrosoft Account Security Team

direction: inbound

This Alert came from a email containing External links from email at [no-reply@m1crosoftsupport.co](mailto:no-reply@m1crosoftsupport.co). First thing I did was pull the URL test that for its reputation.



Checked the proxy/firewall rules and pulled the IP address: 45.148.10.131 Which also came back as Malicious

This showed a Problem with the fire wall rules and it was allowed access by a allowed-internet rule. So this case is a True Positive and will need some steps to prevent this action from progressing in the future

**Time of activity:** 09/03/2025 18:51:20.433

**List of Affected Entities:** C.allen at email c.allen@thetrydaily.thm

**Reason for Classifying as True Positive:** The Email link and IP address of the sender both come back as malicious in the Trydetectthis security check.

**Reason for Escalating the Alert:** This malicious URL made it past the firewall due to an allowed internet access rule that is in place.

**Recommended Remediation Actions:** Ip address and URL need to be added to the denied list to prevent further attempts of making it into the system.

**List of Attack Indicators:** Sent email address as strange character where the “I” was replaced with the digit “1”. The email is a call to action to prompt action right away to get the user to provide their log in credentials

Last Case is also a Phishing Email with an medium alert. Looks like it was triggered by external link. Information is below about the alert:

Description: This alert was triggered by an inbound email contains 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.

datasource: email

timestamp: 09/03/2025 18:51:48.433

subject: Action Required: Finalize Your Onboarding Profile

sender: onboarding@hrconnex.thm

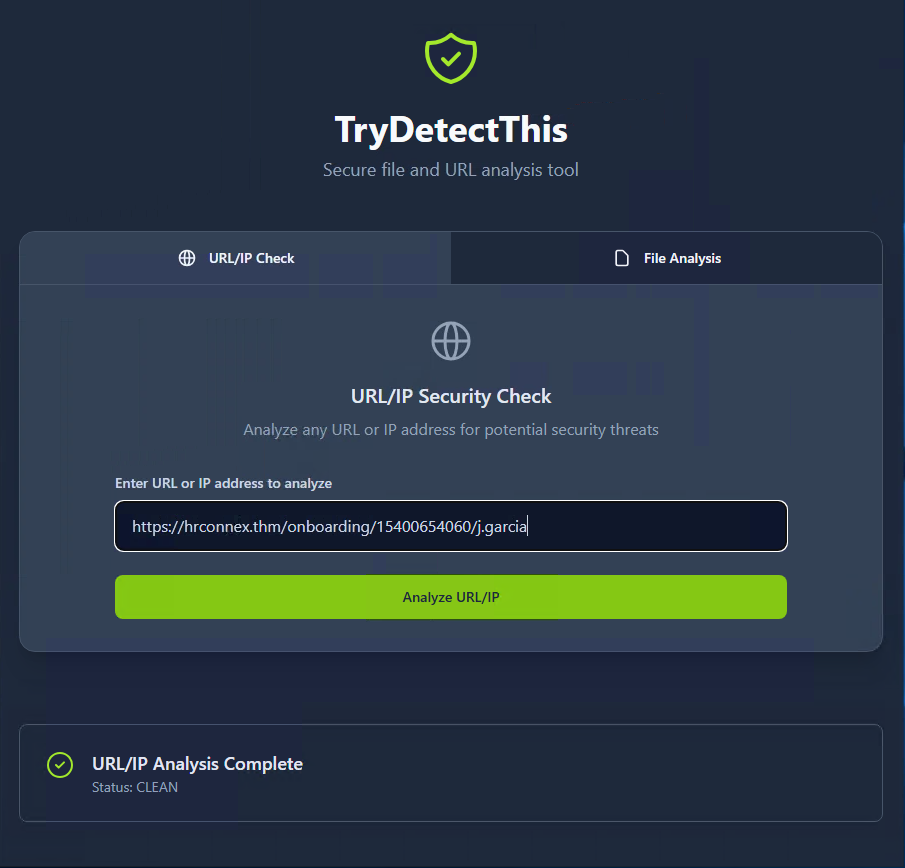
recipient: j.garcia@thetrydaily.thm

attachment: None

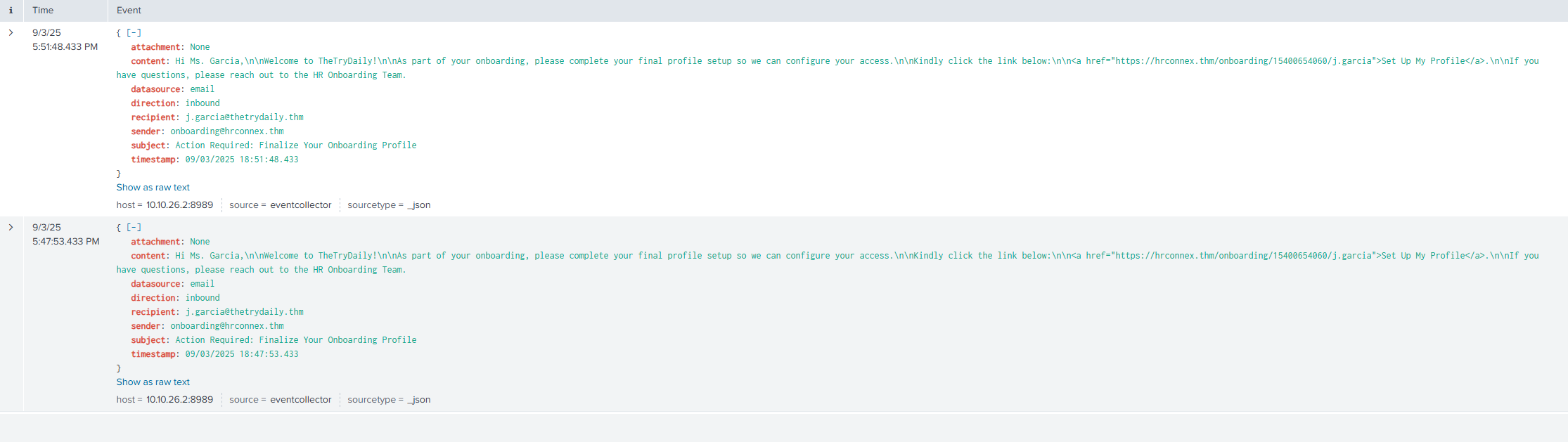
content: Hi Ms. Garcia,\n\nWelcome to TheTryDaily!\n\nAs part of your onboarding, please complete your final profile setup so we can configure your access.\n\nKindly click the link below:\n\n<a href="https://hrconnex.thm/onboarding/15400654060/j.garcia">Set Up My Profile</a>.\n\nIf you have questions, please reach out to the HR Onboarding Team.

direction: inbound

Playbook is the same as all the other phishing Email Alerts so we are pretty familiar now with the steps. So we pull the URL from the Email and send it over to the Trydetect this provided that the link was Safe and clean



Checked the proxy/firewall rules within splunk and found two events triggered



From what we can see the two events are identical and is showing a false positive report. Went ahead and set the case as closed as a false positive.:

Who: Email from Onboarding@hrconnex.thm to J.garcia@thetrydaily.thm

What: Email with external link

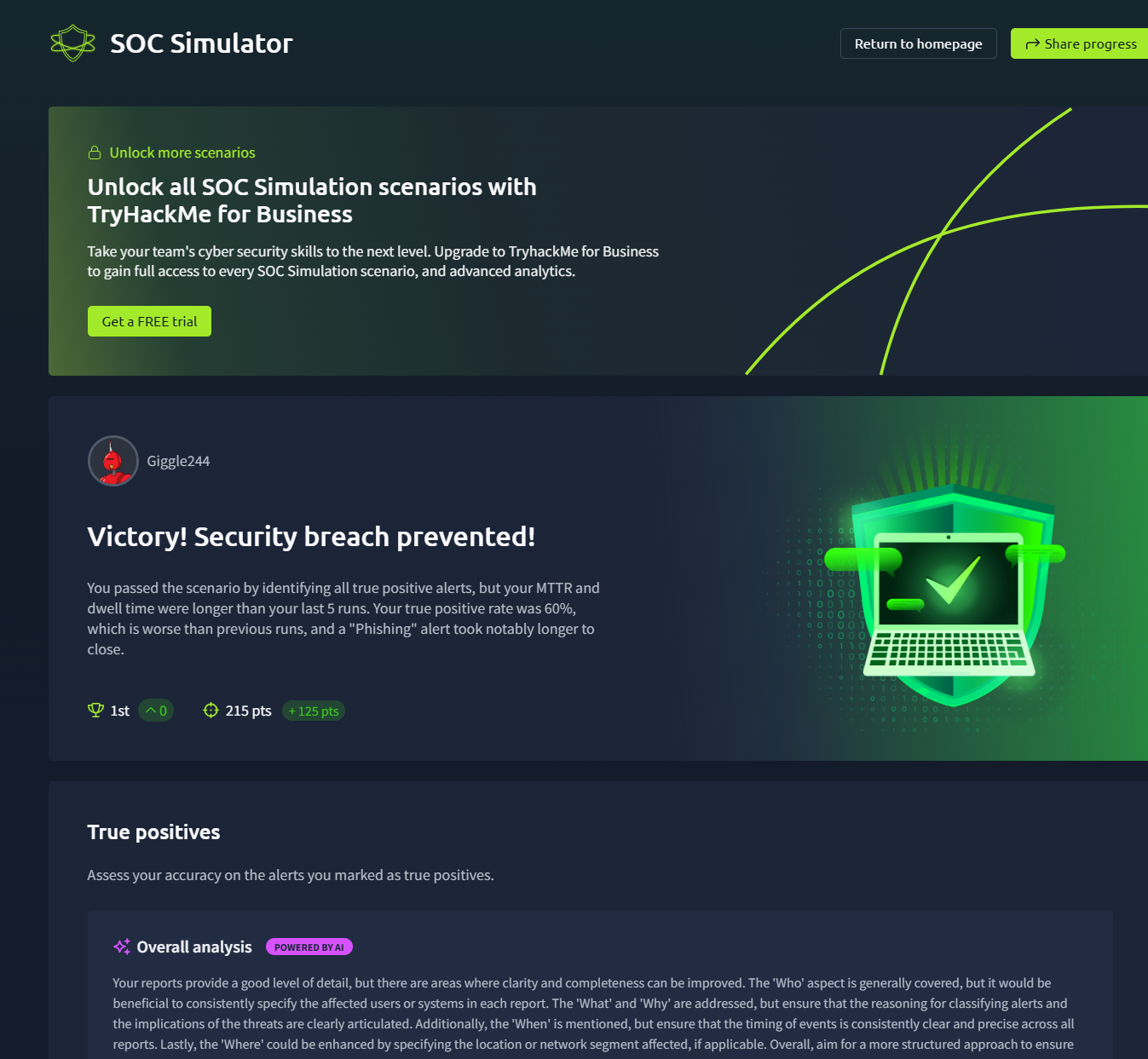
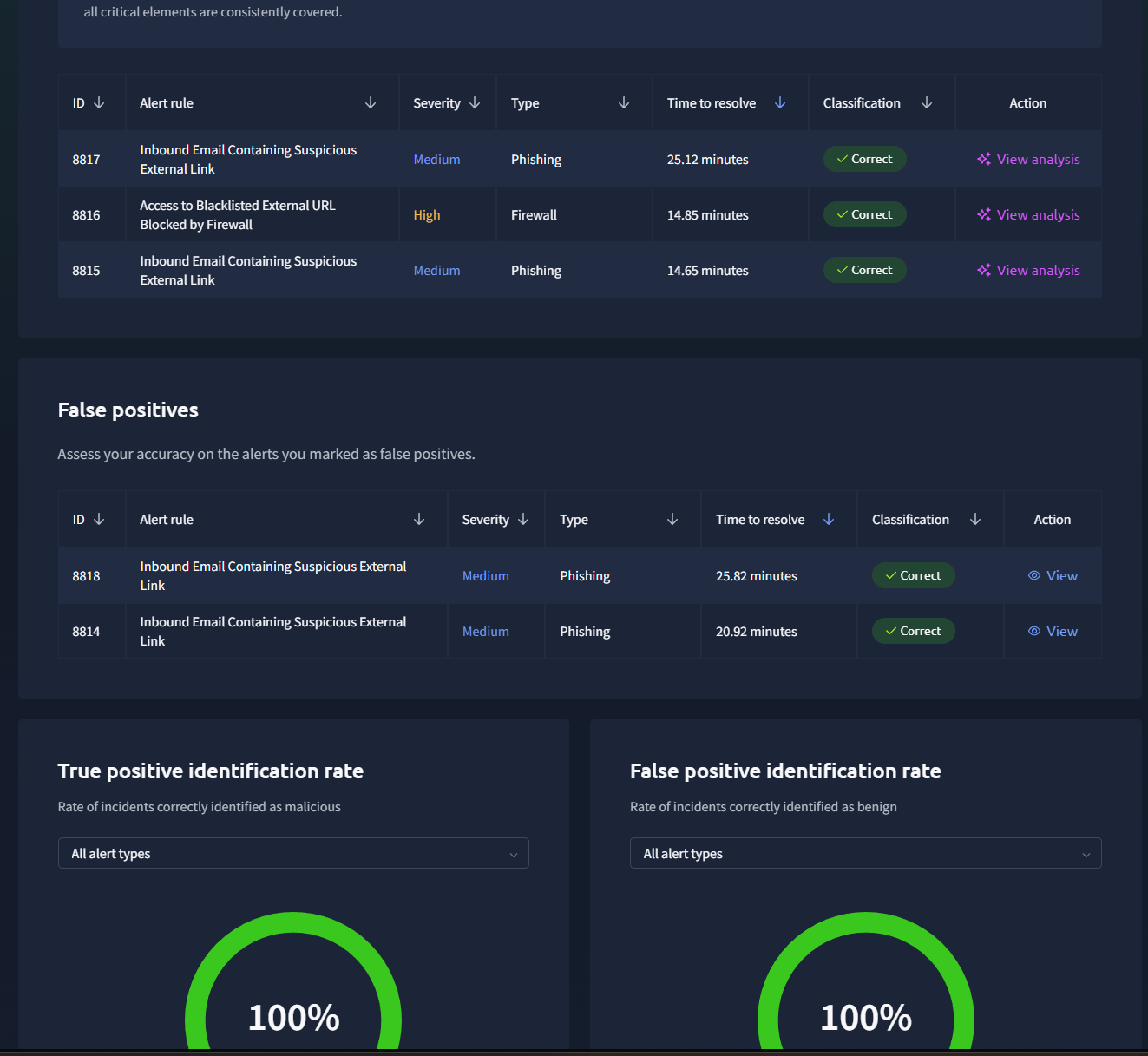
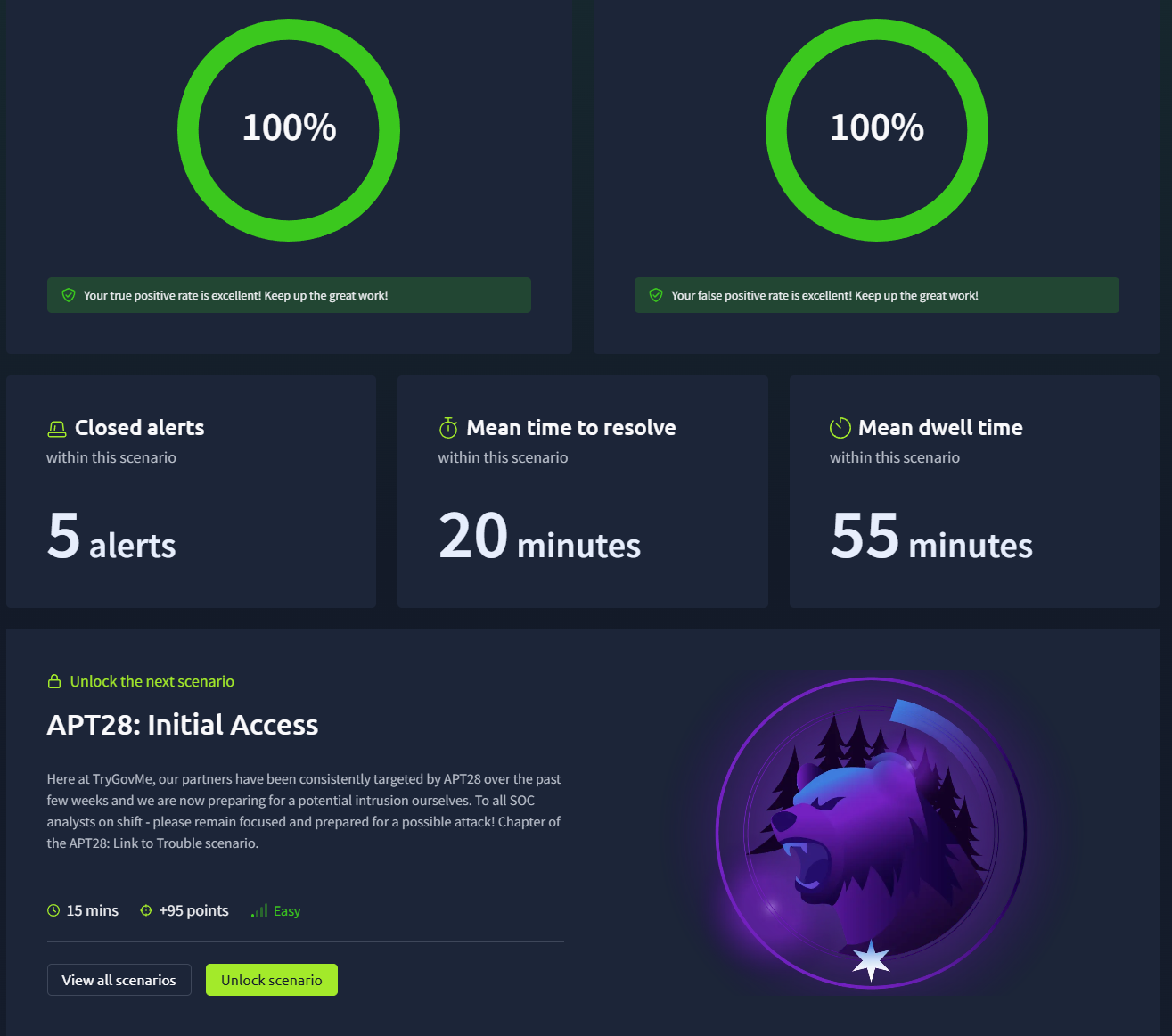
When: 09/03/2025 18:51:48.433

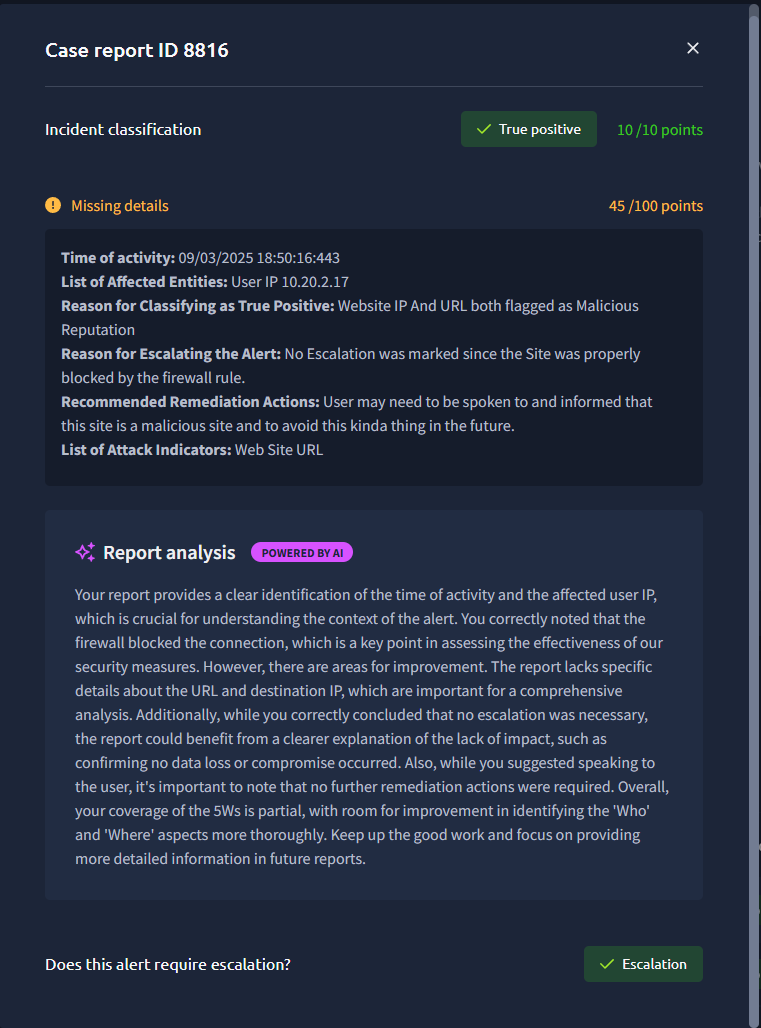
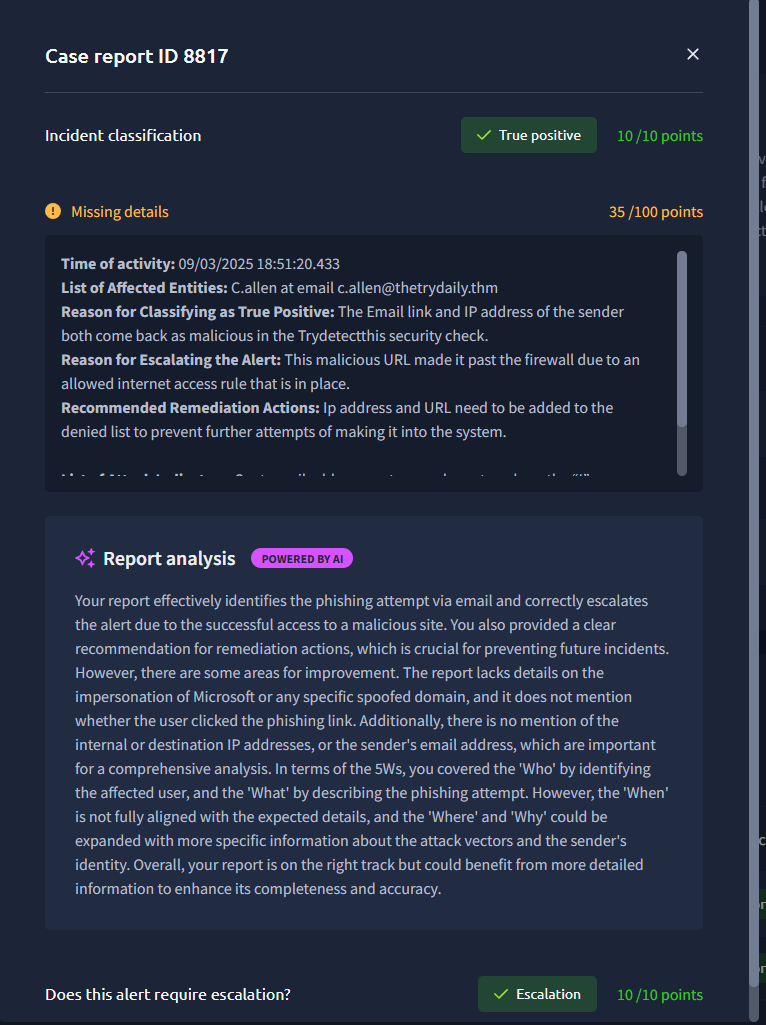
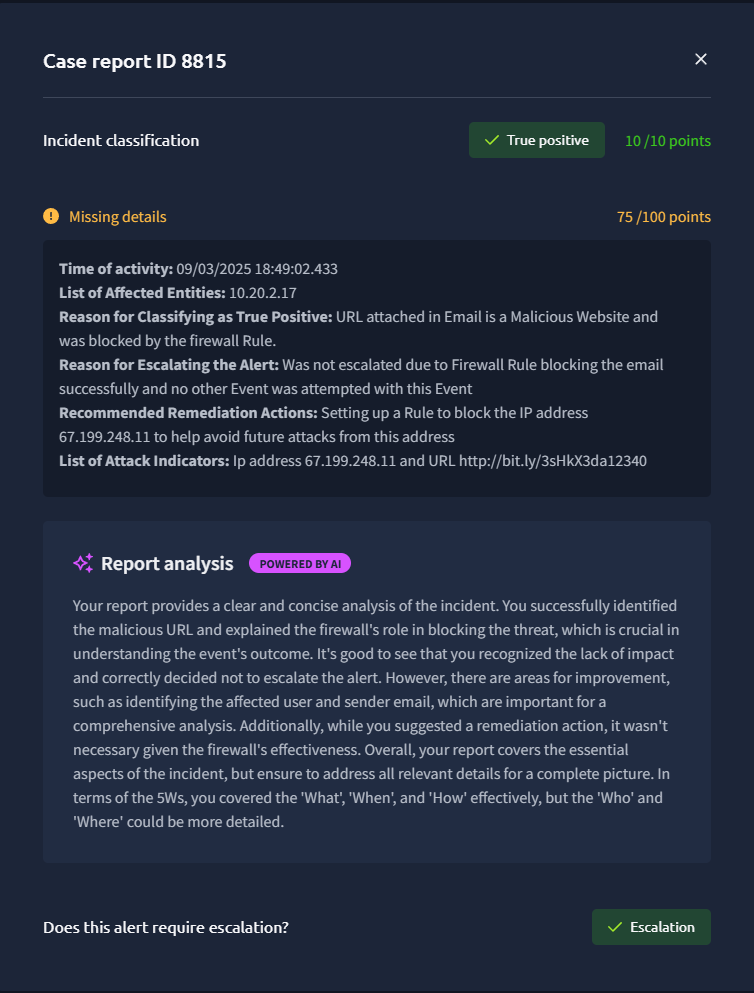
Where: J.garcia@thetrydaily.thm email box

Why: Onboarding request

Reason for classifying as false positive: Email and Ip address came back clean and did not see any other issues  found to cause this to be flagged as malicious

With All the cases closed We got the report of how well we did.

Wrap up of the experience with tryhackmes Soc Simulator. Over all my time was a lot longer than I would have normally taken due to me writing up this report while I was doing it and also trying to familiarize my self with the different provided resources like Splunk and the Anylast VM. As we can see we identified all the Event correctly which is great to see but obviously our score was not perfect which I kinda expected since I am currently not doing SOC Anaylst work every day. So my Descriptions when reporting true positives need a lot more work to meet up with what could or should be expected. I have provided a few screenshots of the advise given back to me for others who want to see what kind of feed back the position might require.   

Overall it looks like my weakness is not providing enough information about the incident like providing the desitnation and source Ip address to clearly identify the Incident even if no escualtion was needed. This will be something I will userly work on to improve my SOC Skills to better prepare me for when I find my self with a Job as a SOC Teir Anaylst.

Thank you for Checking out my report on the SOC Simualtion on TryHackMe and I highly recommend this to anyone who is interested or looking to increase their skills in the field.