



## 1. Launch simulator

The screenshot shows the SOC Simulator interface. At the top, there's a navigation bar with icons for 'Try Hack Me', 'Dashboard', 'Learn', 'Practice', 'Compete', and user stats ('191'). Below the navigation is a search bar and a progress/stats/leaderboard section. A central modal window titled 'Introduction to Phishing' is open. It contains a scenario overview, objectives (monitoring alerts, identifying critical events, creating case reports), and a timer (10 min). A yellow arrow points to the 'Start' button. The background shows other scenario cards like 'Phishing Unfolding' and 'APT2B: Execution'.

## 2. Choose exercise (Introduction to Phishing SOC Simulation)

This screenshot shows the 'Scenarios' tab of the SOC Simulator. It lists several scenarios: 'Phishing Unfolding', 'Introduction to Phishing' (which is highlighted with a yellow arrow on its 'Start' button), 'APT2B: Credential Access', and 'APT2B: Execution'. Each scenario card includes a thumbnail, duration, difficulty level, and a 'Start' button.

## 3. Choose SIEM tool (Splunk)

This screenshot shows a modal dialog titled 'Choose your SIEM tool'. It offers three options: 'Splunk' (selected, highlighted with a yellow arrow on its 'Start scenario' button), 'Elastic', and 'Sentinel'. Each option has a brief description. The background shows the same scenario cards as the previous screenshot.

4. Go to Alert Queue board
5. Assign yourself an alert (prioritize by Severity & Date/Time)

The screenshot shows the 'Alert queue' board with a dark theme. On the left is a sidebar with navigation links: Dashboard, Alert queue (which is selected and highlighted in yellow), SIEM, Analyst VM, Documentation, Playbooks, Case reports, and Guide. Below the sidebar is a 'Exit simulation' button. The main area has a header 'Alert queue' with a blue progress bar showing '0 alerts incoming'. Below the header is a section titled 'Assigned alert' with the message 'You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives.' A 'Learn more' link is present. A search bar and filter buttons for 'Severity', 'Status', 'Alert type', and 'Show 15 alerts' are at the top of the alert list. The alert list table has columns: ID, Alert rule, Severity, Type, Date, Status, and Action. Five alerts are listed:

ID	Alert rule	Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 18th 2026 at 14:01	Awaiting action	
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 18th 2026 at 14:00	Awaiting action	
8816	Access to Blacklisted External URL, Blocked by Firewall	High	Firewall	Jan 18th 2026 at 13:59	Awaiting action	
8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 18th 2026 at 13:58	Awaiting action	
8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 18th 2026 at 13:57	Awaiting action	

6. Click **Playbook** link for triaging guide

The screenshot shows the 'Alert queue' board with a dark theme. The sidebar and alert list are identical to the previous screenshot. In the center, a specific alert is detailed:

**Alert details:**

- 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 feed. The firewall or proxy successfully blocked the malicious 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: 01/18/2026 13:57:33.116
- Action: blocked
- SourceIP: 10.20.2.17
- SourcePort: 34297
- DestinationIP: 67.199.248.11
- DestinationPort: 80
- URL: http://bit.ly/3qHxK3d#12340
- Application: web-browsing
- Protocol: TCP
- Rule: Blocked Websites

**Playbook-link**

**Alert Triage Process**

STEP 2: Alert Triage Process

- Review the alert type and context: Is it related to a typosquatted domain, a known C2 server, a known malicious IP?
- For network monitoring: Review sensitive internal assets or external destinations known for malware/phishing.
- Look for clustering of similar alerts (multiple hits to the same domain or IP) or across multiple hosts.

The sidebar on the left shows the 'Alert Triage Process' steps: Assign Alert, Alert Triage Process (highlighted with a yellow box), Review Network Connection Details, Assess Reputation of Domain or IP, Correlate with Internal Activity, and Case Reporting.

- Take note of the IOCs (Indicators of Compromise) for investigation
- Click **SIEM** tab for investigation.

The screenshot shows the Splunk Alert queue interface. On the left sidebar, the 'SIEM' tab is selected, indicated by a yellow box and arrow labeled '2. click'. The main pane displays an alert titled 'Access to Blacklisted External URL Blocked by Firewall' with a 'High' priority. The alert details show a blocked connection from source IP 10.20.2.17 to destination port 80 (http://bit.ly/SinkXida12340). A yellow box highlights the 'DestinationPort' field, and another yellow arrow labeled '1. copy' points to the value '80'. Below the alert details is a search bar and a table of alerts.

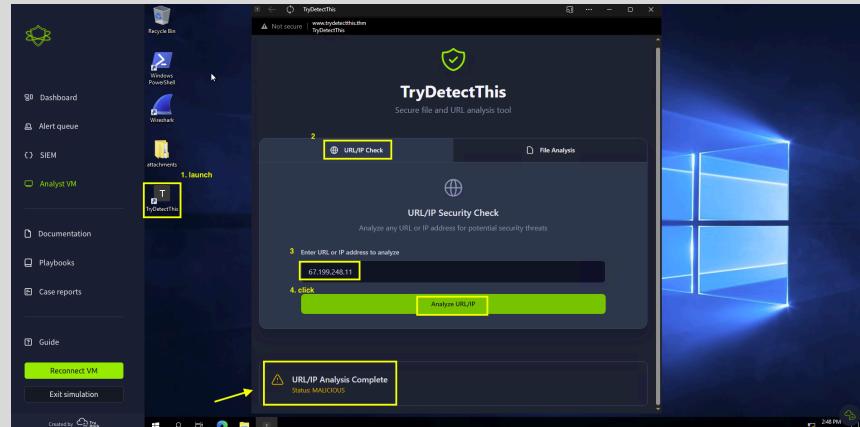
- Search/Investigate using SIEM (Splunk) for additional information

The screenshot shows the Splunk search interface with a search query 'destinationPort=80 OR host=87.199.244.11'. The results table shows one event matching the query. The event details pane displays a log entry with a yellow box highlighting the 'destinationPort' field set to '80'. Another yellow arrow labeled '2. copy' points to the value '80'. The log entry also includes other fields like 'host', 'index', 'source', and 'sourceType'.

- Click Analyst VM to investigate if files, IPs, and/or URLs are malicious.

The screenshot shows the Splunk Alert queue interface. On the left sidebar, the 'Analyst VM' tab is selected, indicated by a yellow box and arrow labeled '2. click'. The main pane displays an alert titled 'Access to Blacklisted External URL Blocked by Firewall' with a 'High' priority. The alert details show a blocked connection from source IP 10.20.2.17 to destination port 80 (http://bit.ly/SinkXida12340). A yellow box highlights the 'DestinationPort' field, and another yellow arrow labeled '1. copy' points to the value '80'. Below the alert details is a search bar and a table of alerts.

11. Launch TryDetectThis tool (THM Investigation Tool) > enter suspicious IP or URL to investigate.



12. Use other available tools (ex. VirusTotal) if needed to investigate

The screenshot shows the VirusTotal website with a step-by-step guide:

1. go to virustotal.com
2. select URL
3. paste URL from SIEM  
http://bit.ly/2mHKXdu2240
4. click Search

The analysis results page shows the following information:

- 4/97 security vendors flagged this URL as malicious
- http://bit.ly/2mHKXdu2240
- bitly
- bit.ly
- external resources
- malicious

Below the summary, there is a table of security vendor analysis results:

Security vendor	Analysis
CBDF	Malicious
Phishing Database	Phishing
Absin	Clean
ADMIN/SLabs	Clean
Ajenti/Ult	Clean
Arrests Against 419	Clean
BitDefender	Clean
BlueVil	Clean
Chong Lai Duo	Clean
CNC Threat Intelligence	Clean
Gabli	Clean
GridinSoft	Phishing
PresidentSec	Malicious
Acrosis	Clean
AllJobs (MONITORAPP)	Clean
Anti-VNL	Clean
benkow.cc	Clean
Blocklist	Clean
Certego	Clean
CMS Army	Clean
Criminal IP	Clean
Defender	Clean

13. Click **Write case report**: Specify if alert is True Positive or False Positive.

The screenshot shows the Alert queue interface. An alert for event ID 8816 is listed, detailing a blocked external URL by the Firewall. A modal window titled "Close alert with event ID: 8816" is open, asking "Was this alert a true positive or a false positive?" with "True positive" selected. At the bottom right of the modal, there is a button labeled "Write case report".

14. Write a thorough **incident report** : clearly document **who was affected, what happened, when and where it occurred, why it's significant, and how it was detected and remediated**, using concise, factual language that can be understood by both technical and non-technical stakeholders.

The screenshot shows the Incident report interface. It displays a detailed report for an inbound email containing a suspicious URL. The report includes sections for "Incident classification" (with "True positive" selected) and "Reason for Escalating the Alert" (which states the alert was escalated because it indicates a user-initiated attempt to access a known malicious URL).

15. If an event needs to be escalated, specify the reason, select **Yes** radio button, then click **Submit and close alert**.

The screenshot shows the Incident report interface. It displays a detailed report for an inbound email containing a suspicious URL. The report includes sections for "Incident classification" (with "True positive" selected), "Reason for Escalating the Alert" (which states the alert was escalated because it indicates a user-initiated attempt to access a known malicious URL), and "Does this alert require escalation?" (with "Yes" selected). At the bottom right, there is a button labeled "Submit and close alert".

16. Assign yourself another **alert** (prioritize by Severity & Date/Time) and **repeat the whole investigation and triaging process.**

**Alert queue** 0 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](#)

ID	Alert rule	Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:39	Awaiting action	<a href="#">Details</a>
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:39	Awaiting action	<a href="#">Details</a>
8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:36	Awaiting action	<a href="#">Details</a>
8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	Jan 21st 2026 at 13:38	Closed	<a href="#">Details</a>
8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:35	Closed	<a href="#">Details</a>

Created by [View profile](#)

**Alert queue** 0 alerts incoming

Assigned alert(s)

8814 Inbound Email Containing Suspicious External Link Medium Phishing Jan 21st 2026 at 13:35 [Write case 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: 01/21/2026 13:34:47.943 subject: Action Required: Finalize Your Onboarding Profile onboarding@incometech.com recipient: j.garcia@incometech.thm attachment: None content: Hi Ms. Garcia, [in]Welcome to TheTryDaily! [in]As part of your onboarding, please complete your final profile setup so we can configure your access. [in]Kindly click the link below: [in]<http://incometech.onboarding/15400654060/j.garcia> "Set Up My Profile". [in]If you have questions, please reach out to the IT Onboarding Team instead.

direction: inbound

[Playbook link](#)

**Phishing Email Analysis**

This playbook provides step-by-step guidelines for SOC Level 1 analysts to investigate suspected phishing emails reported by end users or detected by security tools. Phishing downloading malware, or visiting malicious websites. Timely and accurate triage is essential to determine the threat level, contain any risk, and escalate as needed.

Step 1: Assign Alert

Step 2: Alert Triage Process

Step 3: Analyze Email Artifacts

Email Analysis Tasks

- 3.1 Check Sender Reputation
- 3.2 Review Attachments

Step 4: Investigate Related

**STEP 2 Alert Triage Process**

- Familiarize yourself with the fields included in the alert. Review the phishing alert from your email security gateway (SEG), SIEM, or user report. Note available fields such as sender, subject, recipient, message ID, and delivery time.
- Identify the time at which the email was received. Review the timestamp field or header to determine when the message was delivered to the recipient's inbox. This helps in scope related activities.
- Identify the specific user associated with the alert. Determine which user or mailbox received the email. Note whether the user is a standard employee, VIP, or part of a sensitive business unit.
- Identify the user associated with the activity. Look up the recipient in internal directory tools to determine their department, title, and whether they are active or privileged. Review the "To" or "Recipient" field.
- Determine the malicious element in the email. Check whether the threat is a suspicious link, attachment, spoofed sender, or impersonation attempt.

**Alert queue** 0 alerts incoming

Assigned alert(s)

8814 Inbound Email Containing Suspicious External Link Medium Phishing Jan 21st 2026 at 13:35 [Write case 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: 01/21/2026 13:34:47.943 subject: Action Required: Finalize Your Onboarding Profile onboarding@incometech.com recipient: j.garcia@incometech.thm attachment: None content: Hi Ms. Garcia, [in]Welcome to TheTryDaily! [in]As part of your onboarding, please complete your final profile setup so we can configure your access. [in]Kindly click the link below: [in]<http://incometech.onboarding/15400654060/j.garcia> "Set Up My Profile". [in]If you have questions, please reach out to the IT Onboarding Team instead.

direction: inbound

[Playbook link](#) 1 copy

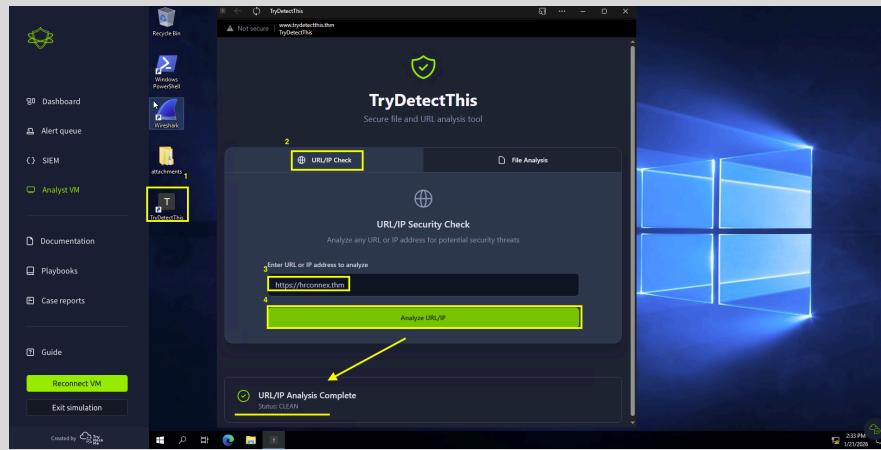
**Alert queue** 0 alerts incoming

Assigned alert

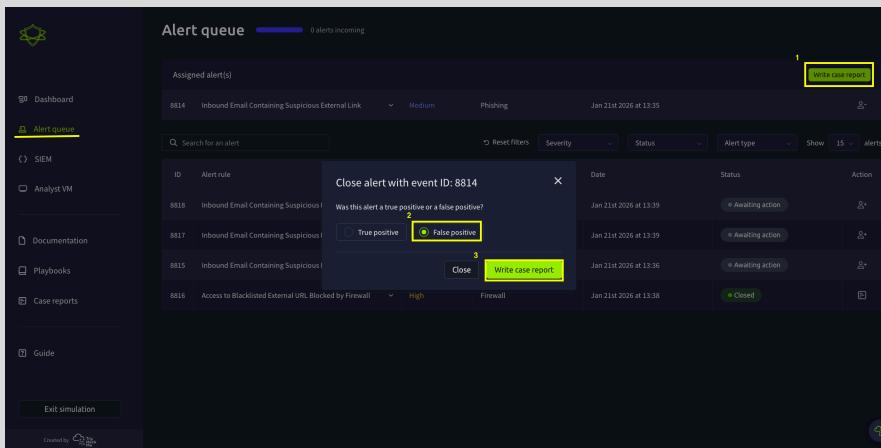
You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. [Learn more](#)

ID	Alert rule	Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:39	Awaiting action	<a href="#">Details</a>
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:39	Awaiting action	<a href="#">Details</a>

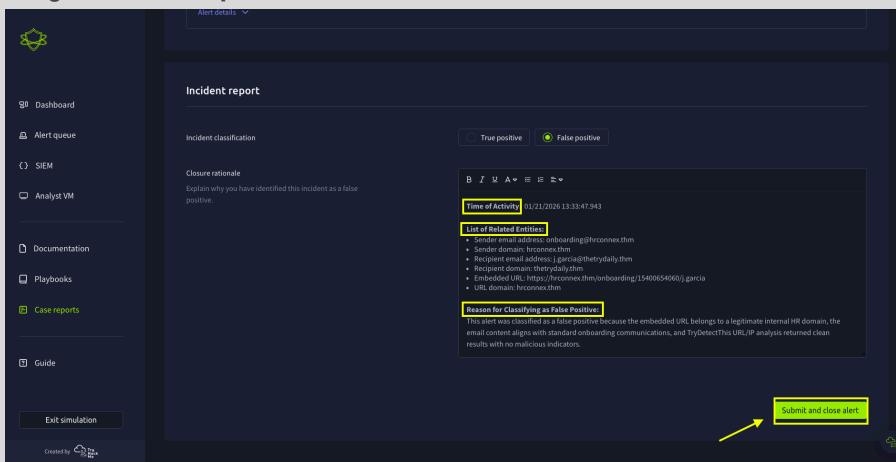
Created by [View profile](#)



17. Click **Write case report**, then Check **False Positive** in this case.



18. Write a thorough incident report, then click **Submit and close alert**



19. On to the **next alert** (prioritize by Severity & Date/Time) and **repeat the previous process**.

The screenshot shows the 'Alert queue' interface with the following details:

ID	Alert rule	Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:39	Awaiting action	
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:39	Awaiting action	
8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:39	Awaiting action	
8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	Jan 21st 2026 at 13:38	Closed	
8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	Jan 21st 2026 at 13:35	Closed	

An arrow points to the 'click' button next to the fourth alert (ID 8816).