PORTFOLIO PROJECTS

SOC SIMULATOR

TANISH RATHORE

03/06/2025

Overview

01
Project Overview

02
Scenario Details

03
Objectives

04
Hands-On Analysis

05
Github Repository Structure

06
Conclusion

Project Overview

This project documents the Introduction to Phishing scenario in SOC Simulator (TryHackMe). The goal is to analyze real-time alerts, distinguish between true positives and false positives, and document findings in a case report to improve the security posture of the organization.

Scenario Details

The SOC team receives multiple alerts regarding potential phishing attempts. Analysts must:

- Monitor and analyze real-time alerts in the SOC Simulator dashboard.
- Identify and document critical events such as suspicious emails and attachments.
- Create a case report summarizing the incident and close confirmed true positives.

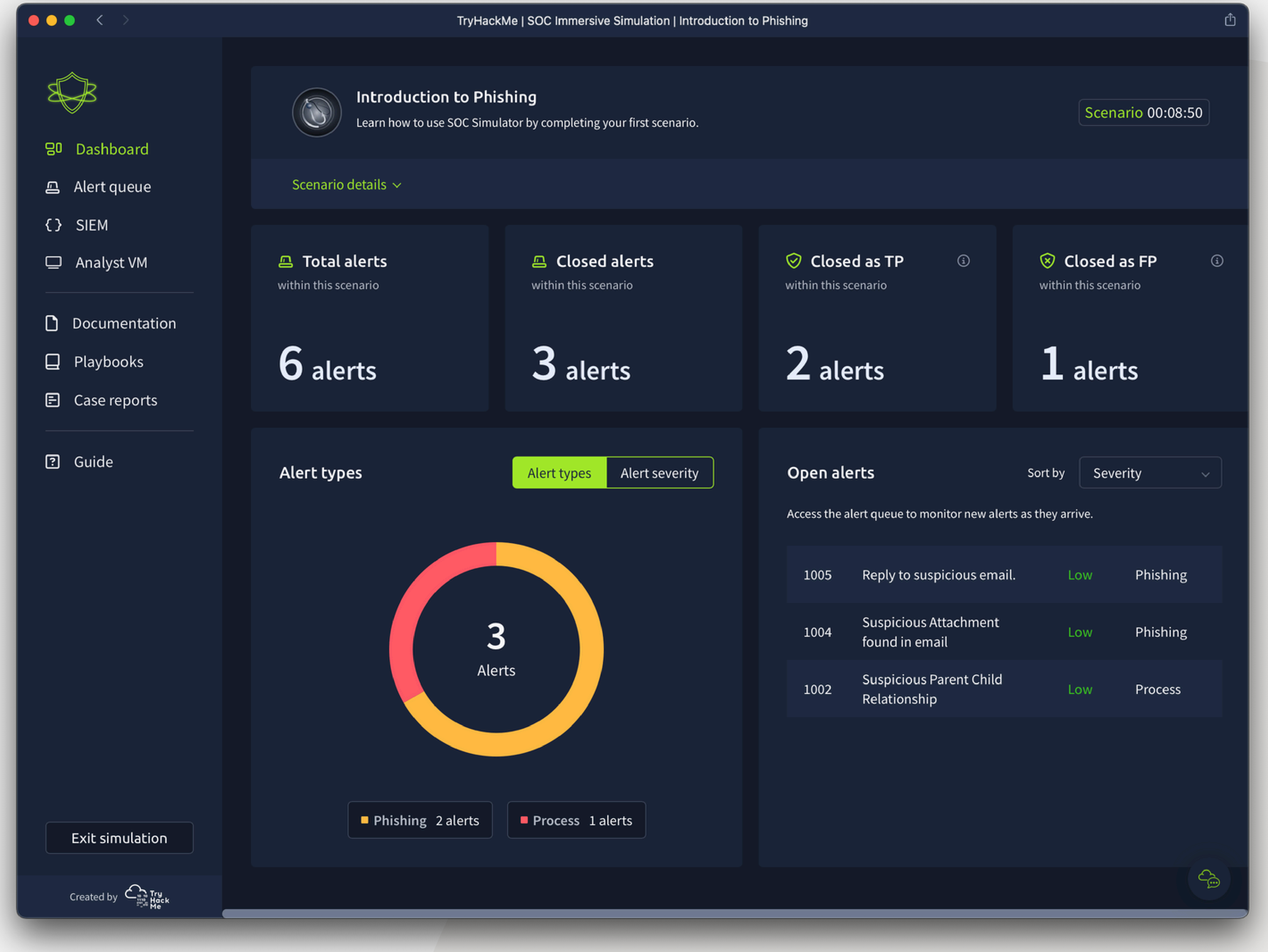
Scenario Objectives

- ✅ Monitor and analyze security alerts related to phishing.
- ✅ Identify malicious emails, attachments, and URLs.
- ✅ Report false positives and investigate true positives.
- ✅ Close cases with detailed documentation for SOC teams.

Hands-On Analysis

Step 1: Reviewing the SOC Simulator Dashboard

- Screenshot: Main Dashboard Overview
- Description: The dashboard provides a live feed of alerts generated by the system, categorized by severity.



TryHackMe | SOC Immersive Simulation | Introduction to Phishing

Introduction to Phishing

Learn how to use SOC Simulator by completing your first scenario.

Scenario 00:08:50

Scenario details

Total alerts	Closed alerts	Closed as TP	Closed as FP
within this scenario	within this scenario	within this scenario	within this scenario
6 alerts	3 alerts	2 alerts	1 alerts

Alert types

Open alerts — Sort by: Severity

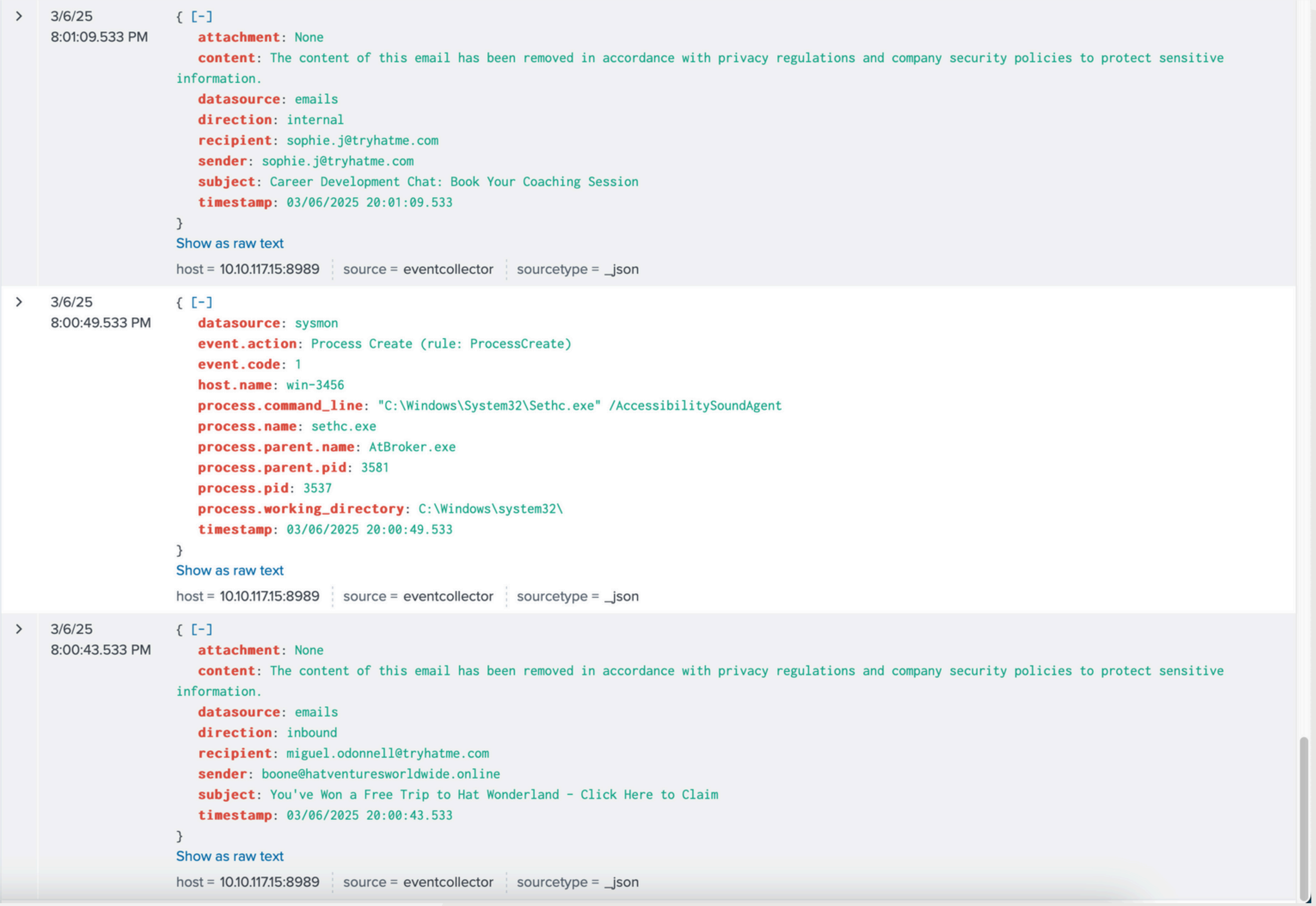
Access the alert queue to monitor new alerts as they arrive.

1005	Reply to suspicious email.	Low	Phishing
1004	Suspicious Attachment found in email	Low	Phishing
1002	Suspicious Parent Child Relationship	Low	Process

Hands-On Analysis

Step 2: Analyzing Alerts

- Screenshot: Alerts Panel in SIEM (Splunk)
- Description: We examine alerts related to phishing emails, attachment downloads, and credential harvesting attempts.
- Key Finding: Indicators such as suspicious sender domains, embedded malicious links, and abnormal attachment names help in identifying phishing attempts.

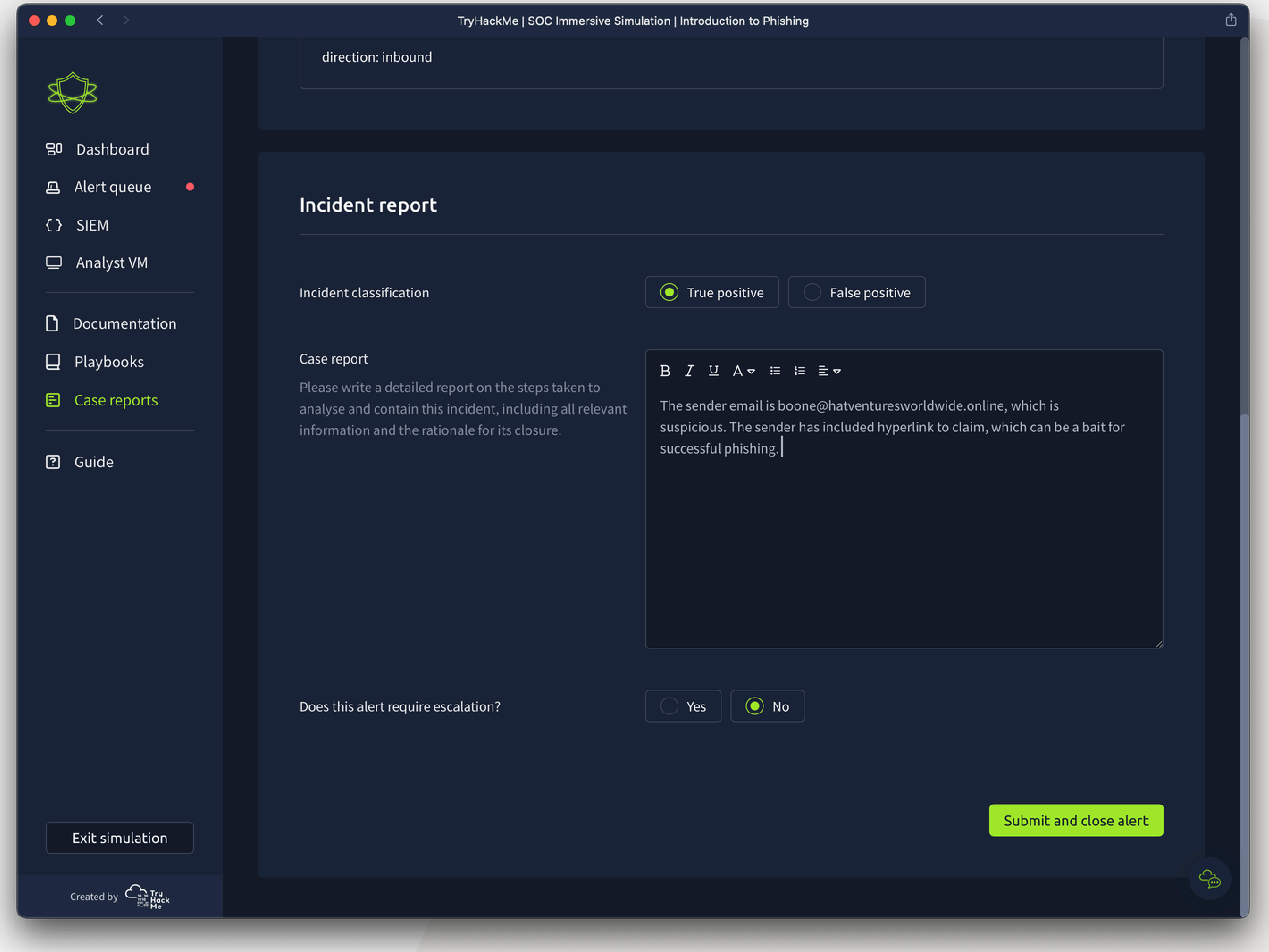


```
>  3/6/25           { [-]
   8:01:09.533 PM      attachment: None
                       content: The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive
                    information.
                       datasource: emails
                       direction: internal
                       recipient: sophie.j@tryhatme.com
                       sender: sophie.j@tryhatme.com
                       subject: Career Development Chat: Book Your Coaching Session
                       timestamp: 03/06/2025 20:01:09.533
                    }
                    Show as raw text
                    host = 10.10.117.15:8989   source = eventcollector   sourcetype = _json

>  3/6/25           { [-]
   8:00:49.533 PM      datasource: sysmon
                       event.action: Process Create (rule: ProcessCreate)
                       event.code: 1
                       host.name: win-3456
                       process.command_line: "C:\Windows\System32\Sethc.exe" /AccessibilitySoundAgent
                       process.name: sethc.exe
                       process.parent.name: AtBroker.exe
                       process.parent.pid: 3581
                       process.pid: 3537
                       process.working_directory: C:\Windows\system32\
                       timestamp: 03/06/2025 20:00:49.533
                    }
                    Show as raw text
                    host = 10.10.117.15:8989   source = eventcollector   sourcetype = _json

>  3/6/25           { [-]
   8:00:43.533 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: inbound
                       recipient: miguel.odonnell@tryhatme.com
                       sender: boone@hatventuresworldwide.online
                       subject: You've Won a Free Trip to Hat Wonderland - Click Here to Claim
                       timestamp: 03/06/2025 20:00:43.533
                    }
                    Show as raw text
                    host = 10.10.117.15:8989   source = eventcollector   sourcetype = _json
```

Hands-On Analysis

Step 3: Reporting False Positives & Investigating True Positives

- Screenshot: False Positive and True Positive Reporting Panel
- Description: We analyze email headers, attachment hashes, and user activity logs to differentiate between false and true positives.



direction: inbound

Incident report

Incident classification ● True positive ○ False positive

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.

The sender email is boone@hatventuresworldwide.online, which is suspicious. The sender has included hyperlink to claim, which can be a bait for successful phishing.

Does this alert require escalation? ○ Yes ● No

GitHub Repository Structure

📂 SOC-Simulator-Phishing/

│ ──── 📁 screenshots/ → Contains images of dashboards, alerts, and case reports.

│ ──── 📁 logs/ → Sample security logs related to phishing incidents.

│ ──── 📁 reports/ → Includes this presentation as a copy to review

│ ──── 📜 README.md → Project overview, objectives, and how to navigate the repository.

Conclusion

This project provides hands-on experience in monitoring phishing attacks within a SOC environment. By leveraging the SOC Simulator, we gained insights into real-world alert handling, SIEM log analysis, and case documentation—essential skills for a SOC Analyst (Tier 1) role.

PORTFOLIO PROJECTS

Thank you

BY TANISH RATHORE