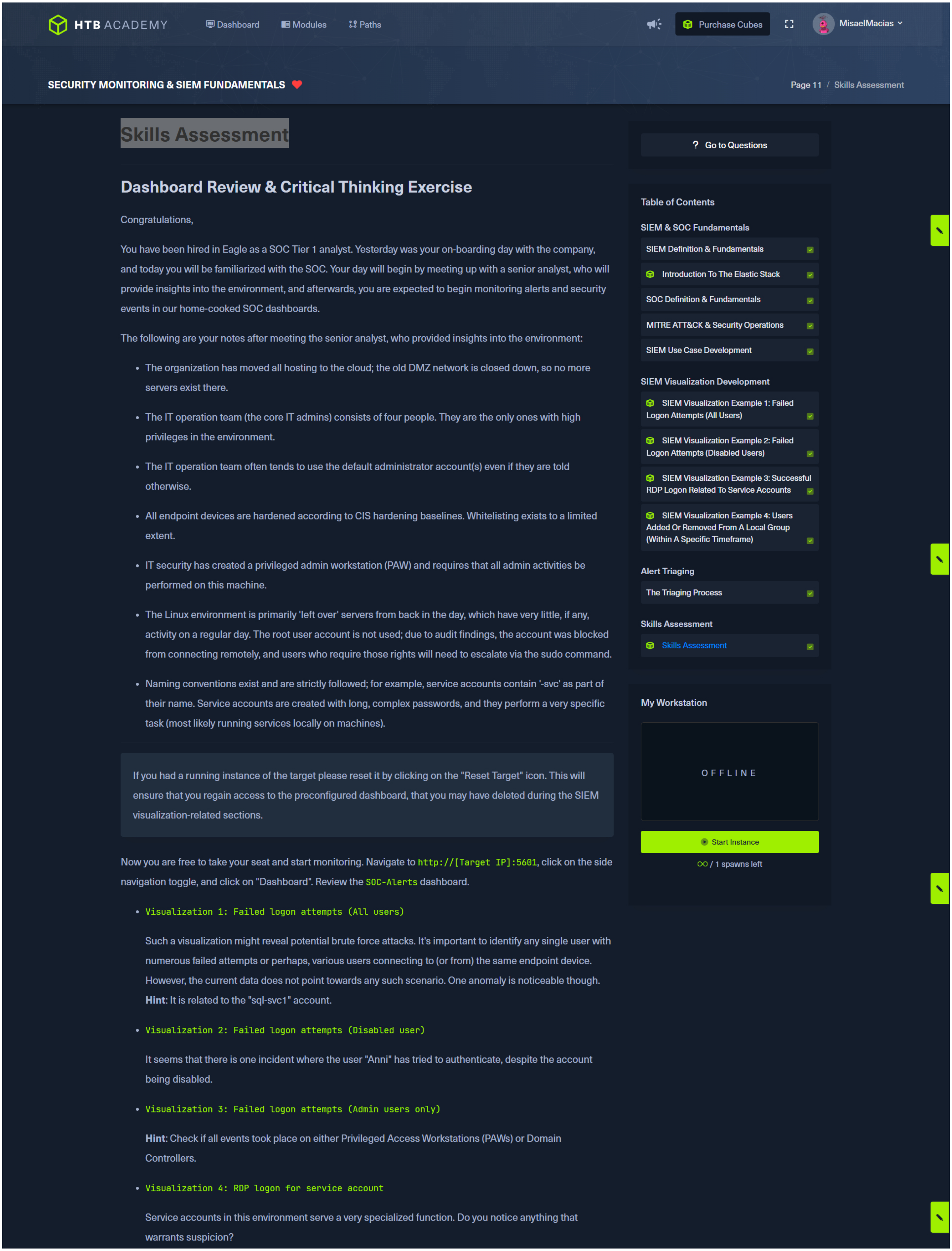


Skills Assessment

Dashboard Review & Critical Thinking Exercise

Congratulations,

You have been hired in Eagle as a SOC Tier 1 analyst. Yesterday was your on-boarding day with the company, and today you will be familiarized with the SOC. Your day will begin by meeting up with a senior analyst, who will provide insights into the environment, and afterwards, you are expected to begin monitoring alerts and security events in our home-cooked SOC dashboards.

The following are your notes after meeting the senior analyst, who provided insights into the environment:

- The organization has moved all hosting to the cloud; the old DMZ network is closed down, so no more servers exist there.
- The IT operation team (the core IT admins) consists of four people. They are the only ones with high privileges in the environment.
- The IT operation team often tends to use the default administrator account(s) even if they are told otherwise.
- All endpoint devices are hardened according to CIS hardening baselines. Whitelisting exists to a limited extent.
- IT security has created a privileged admin workstation (PAW) and requires that all admin activities be performed on this machine.
- The Linux environment is primarily 'left over' servers from back in the day, which have very little, if any, activity on a regular day. The root user account is not used; due to audit findings, the account was blocked from connecting remotely, and users who require those rights will need to escalate via the sudo command.
- Naming conventions exist and are strictly followed; for example, service accounts contain '-svc' as part of their name. Service accounts are created with long, complex passwords, and they perform a very specific task (most likely running services locally on machines).

> If you had a running instance of the target please reset it by clicking on the "Reset Target" icon. This will ensure that you regain access to the preconfigured dashboard, that you may have deleted during the SIEM visualization-related sections.

Now you are free to take your seat and start monitoring. Navigate to `http://[Target IP]:5601`, click on the side navigation toggle, and click on "Dashboard". Review the `SOC-Alerts` dashboard.

- `Visualization 1: Failed logon attempts (All users)`

  Such a visualization might reveal potential brute force attacks. It's important to identify any single user with numerous failed attempts or perhaps, various users connecting to (or from) the same endpoint device. However, the current data does not point towards any such scenario. One anomaly is noticeable though. **Hint**: It is related to the "sql-svc1" account.

- `Visualization 2: Failed logon attempts (Disabled user)`

  It seems that there is one incident where the user "Anni" has tried to authenticate, despite the account being disabled.

- `Visualization 3: Failed logon attempts (Admin users only)`

  Hint: Check if all events took place on either Privileged Access Workstations (PAWs) or Domain Controllers.

- `Visualization 4: RDP logon for service account`

  Service accounts in this environment serve a very specialized function. Do you notice anything that warrants suspicion?

? Go to Questions

Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

- `Visualization 5: User added or removed from a local group`

  An administrator has incorporated an individual (who is only represented by the SID value) into the "Administrators" group. Should you escalate to a Tier 2/3 analyst or consult with the IT Operations department first?

- `Visualization 6: Admin logon not from PAW`

  Administrators should exclusively utilize PAWs for server remote connections. Should you escalate to a Tier 2/3 analyst or consult with the IT Operations department first?

- `Visualization 7: SSH Logins`

  Be reminded that the root user account is not typically in use.

Go through the questions below and enter your answers.

Please allow 3-5 minutes for Kibana to become available after spawning the target of the questions below.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 Medium Load ▾

PROTOCOL

● UDP 1337 ○ TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 160ms ▾

ⓘ Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

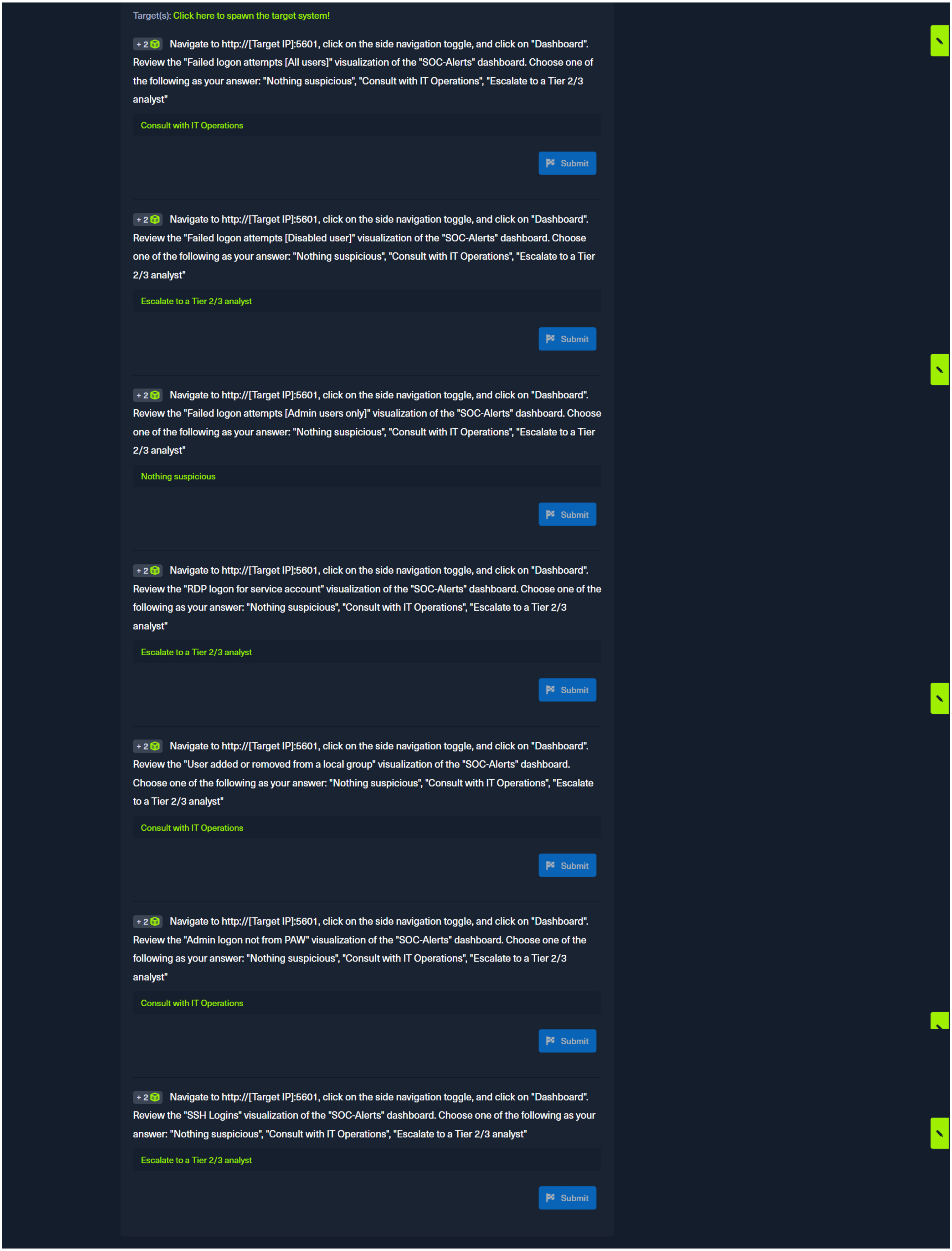
Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File



Target(s): Click here to spawn the target system!

+ 2 Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "Failed logon attempts [All users]" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Consult with IT Operations

+ 2 Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "Failed logon attempts [Disabled user]" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Escalate to a Tier 2/3 analyst

+ 2 Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "Failed logon attempts [Admin users only]" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Nothing suspicious

+ 2 Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "RDP logon for service account" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Escalate to a Tier 2/3 analyst

+ 2 Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "User added or removed from a local group" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Consult with IT Operations

+ 2 Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "Admin logon not from PAW" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Consult with IT Operations

+ 2 Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "SSH Logins" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Escalate to a Tier 2/3 analyst

Previous
Finish
Powered by HACKTHEBOX