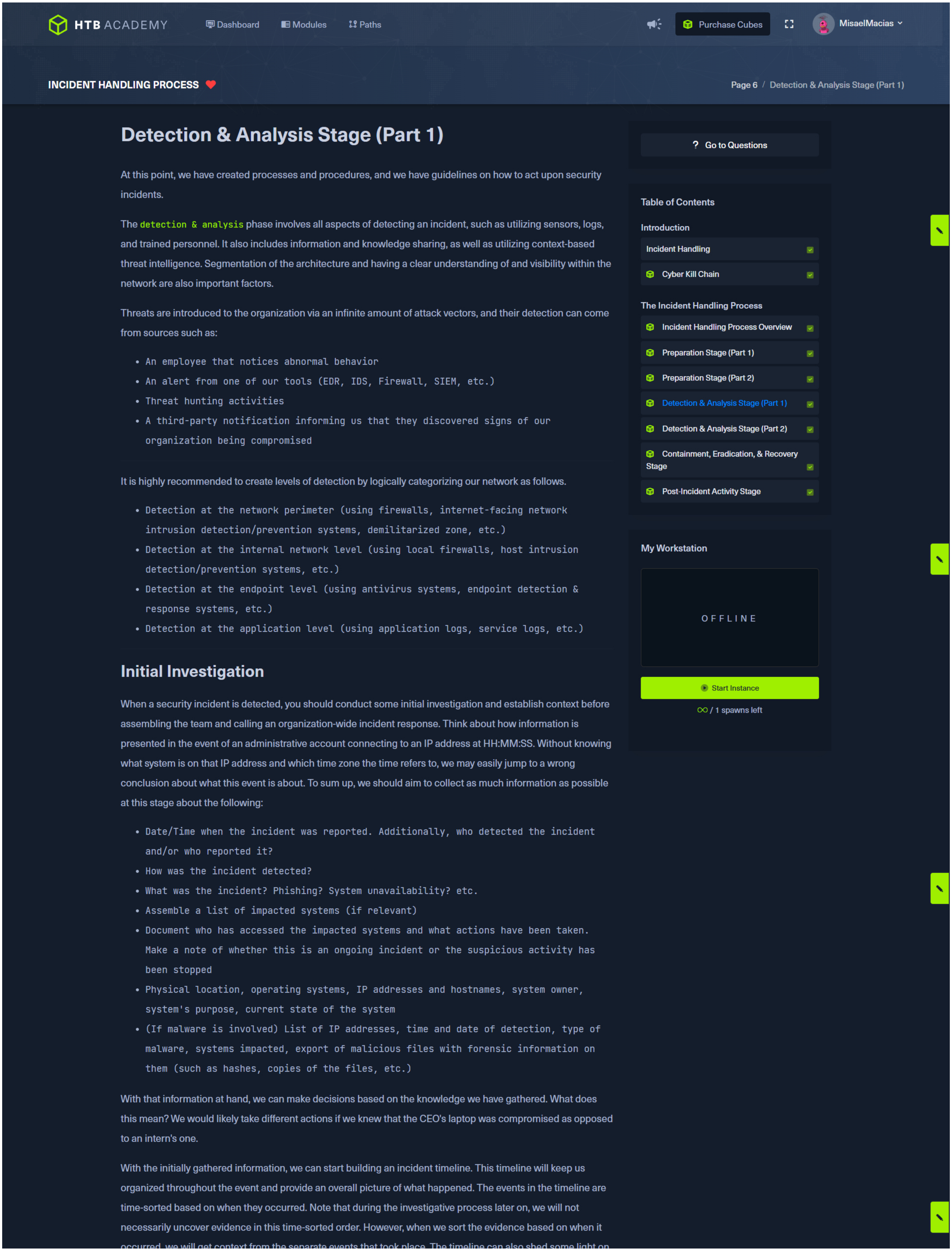

Detection & Analysis Stage (Part 1)

At this point, we have created processes and procedures, and we have guidelines on how to act upon security incidents.

The `detection & analysis` phase involves all aspects of detecting an incident, such as utilizing sensors, logs, and trained personnel. It also includes information and knowledge sharing, as well as utilizing context-based threat intelligence. Segmentation of the architecture and having a clear understanding of and visibility within the network are also important factors.

Threats are introduced to the organization via an infinite amount of attack vectors, and their detection can come from sources such as:

- `An employee that notices abnormal behavior`
- `An alert from one of our tools (EDR, IDS, Firewall, SIEM, etc.)`
- `Threat hunting activities`
- `A third-party notification informing us that they discovered signs of our organization being compromised`

It is highly recommended to create levels of detection by logically categorizing our network as follows.

- `Detection at the network perimeter (using firewalls, internet-facing network intrusion detection/prevention systems, demilitarized zone, etc.)`
- `Detection at the internal network level (using local firewalls, host intrusion detection/prevention systems, etc.)`
- `Detection at the endpoint level (using antivirus systems, endpoint detection & response systems, etc.)`
- `Detection at the application level (using application logs, service logs, etc.)`

Initial Investigation

When a security incident is detected, you should conduct some initial investigation and establish context before assembling the team and calling an organization-wide incident response. Think about how information is presented in the event of an administrative account connecting to an IP address at HH:MM:SS. Without knowing what system is on that IP address and which time zone the time refers to, we may easily jump to a wrong conclusion about what this event is about. To sum up, we should aim to collect as much information as possible at this stage about the following:

- `Date/Time when the incident was reported. Additionally, who detected the incident and/or who reported it?`
- `How was the incident detected?`
- `What was the incident? Phishing? System unavailability? etc.`
- `Assemble a list of impacted systems (if relevant)`
- `Document who has accessed the impacted systems and what actions have been taken. Make a note of whether this is an ongoing incident or the suspicious activity has been stopped`
- `Physical location, operating systems, IP addresses and hostnames, system owner, system's purpose, current state of the system`
- `(If malware is involved) List of IP addresses, time and date of detection, type of malware, systems impacted, export of malicious files with forensic information on them (such as hashes, copies of the files, etc.)`

With that information at hand, we can make decisions based on the knowledge we have gathered. What does this mean? We would likely take different actions if we knew that the CEO's laptop was compromised as opposed to an intern's one.

With the initially gathered information, we can start building an incident timeline. This timeline will keep us organized throughout the event and provide an overall picture of what happened. The events in the timeline are time-sorted based on when they occurred. Note that during the investigative process later on, we will not necessarily uncover evidence in this time-sorted order. However, when we sort the evidence based on when it occurred, we will get context from the separate events that took place. The timeline can also shed some light on

Table of Contents

Introduction

The Incident Handling Process

My Workstation

OFFLINE

occurred, we will get context from the separate events that took place. The timeline can also shed some light on whether newly discovered evidence is part of the current incident. For example, imagine that what we thought was the initial payload of an attack was later discovered to be present on another device two weeks ago. We will encounter situations where the data we are looking at is extremely relevant and situations where the data is unrelated and we are looking in the wrong place. Overall, the timeline should contain the information described in the following columns:

Date	Time of the event	hostname	event description	data source

Let's take one event and populate the example table from above. It will look as follows:

Date	Time of the event	hostname	event description	data source
09/09/2021	13:31 CET	SQLServer01	Hacker tool 'Mimikatz' was detected	Antivirus Software

As you can infer, the timeline focuses primarily on attacker behavior, so activities that are recorded depict when the attack occurred, when a network connection was established to access a system, when files were downloaded, etc. It is important to ensure that you capture from where the activity was detected/discovered and the systems associated with it.

Incident Severity & Extent Questions

When handling a security incident, we should also try to answer the following questions to get an idea of the incident's severity and extent:

- `What is the exploitation impact?`
- `What are the exploitation requirements?`
- `Can any business-critical systems be affected by the incident?`
- `Are there any suggested remediation steps?`
- `How many systems have been impacted?`
- `Is the exploit being used in the wild?`
- `Does the exploit have any worm-like capabilities?`

The last two can possibly indicate the level of sophistication of an adversary.

As you can imagine, high-impact incidents will be handled promptly, and incidents with a high number of impacted systems will have to be escalated.

Incident Confidentiality & Communication

Incidents are very confidential topics and as such, all of the information gathered should be kept on a need-to-know basis, unless applicable laws or a management decision instruct us otherwise. There are multiple reasons for this. The adversary may be, for example, an employee of the company, or if a breach has occurred, the communication to internal and external parties should be handled by the appointed person in accordance with the legal department.

When an investigation is launched, we will set some expectations and goals. These often include the type of incident that occurred, the sources of evidence that we have available, and a rough estimation of how much time the team needs for the investigation. Also, based on the incident, we will set expectations on whether we will be able to uncover the adversary or not. Of course, a lot of the above may change as the investigation evolves and new leads are discovered. It is important to keep everyone involved and the management informed about any advancements and expectations.

○ Enable step-by-step solutions for all questions

Questions

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

+1 True or False: Can a third party vendor be a source of detecting a compromise?

True

Submit

← Previous Next → Mark Complete & Next