Endpoint Security- Talking Notes

## Slide 1:

Endpoints are where the war begins. Not in data centres or boardrooms, but in the quiet hum of laptops, phones, and forgotten servers. Each device a soldier. Each login a potential betrayal.

Good morning. Today, I want to take you inside that front line, where detection, investigation, and neutralization aren’t buzzwords, but survival tactics.

## Slide 2:

Curiosity? No. That’s for the onlookers. What pulled me in was necessity – because to defend a system, you must first understand the poetry of its collapse.

## Slide 3:

I chose the Endpoint Security module for one simple truth: this is where it begins. From a phishing email to a malicious remote tool, attackers seldom blast the front gate, they walk through a cracked window, someone’s laptop.

TryHackMe gave me the luxury of learning the hard way: no textbooks, no safety nets. Just me, a machine, and the threat I had to find, analyse, and clean out. That’s the kind of education that teaches you to spot not only the attack, but the thinking behind it.

## Slide 4:

In this line of work, information isn’t just power, its currency, traded in secrets and split-second decisions. And the right tool at the right time? That’s how you stay one step ahead of chaos.

My goal was simple: detect, investigate, and neutralize malicious activity. To think like a defender, to anticipate the attack before it breathes. For that, I assembled my toolkit.

## Slide 5:

TCPView: to monitor open network connections. The "Who's talking? and Why?"

Process Explorer: For parent-child relationships.

Sysmon and OSQuery: to dig deeper, system telemetry, behavioural insights, logs from the abyss.

Each tool played its part. Each one whispered a fragment of truth.

## Slide 6:

The exercise began when windows detected a suspicious process. I compared all running processes against baseline system behaviour and quickly realised. One doesn't belong. Beacon.exe

## Slide 7:

It was communicating over port 4444. A port often used by reverse shells and remote access tools.

## Slide 8:

I followed the IP trail, and it revealed more bad news.

## Slide 9:

Beacon.exe was remote accessing four different devices. It wasn’t just a compromise; it was a foothold for lateral movement. And that's when I understood what this task was about: threat detection, built on knowledge, tools, and timing.

## Slide 10:

You don't need explosions to stop a breach. Just certainty. A line of code. A log entry. A finger on the trigger.

## Slide 11:

I isolated the process, verified the threat, and restored system integrity.

## Slide 12:

For the first time, I didn't just read about threat response. I performed it. Not in a textbook. Not in a lecture. But in an environment where my decisions mattered. That's the power of TryHackMe, guided labs that simulate the world I'll one day defend.

## Slide 13:

This project changed the way I think about Cybersecurity. I no longer see Malware as just code. I see it as behaviour, a deviation from the norm, a puzzle that needs to be solved.

## Slide 14:

It taught me how to investigate, how to communicate my findings, and how to think like someone sitting in a real Security Operations Centre.

Because this isn't just a project. It's the first chapter of a career.

## Slide 15:

Sometimes The smallest anomalies reveal the biggest truths. And in that quiet space between normal and abnormal? That's where defenders live.

Thank you.

## References:

TryHackMe

Adobe Stock Photographs