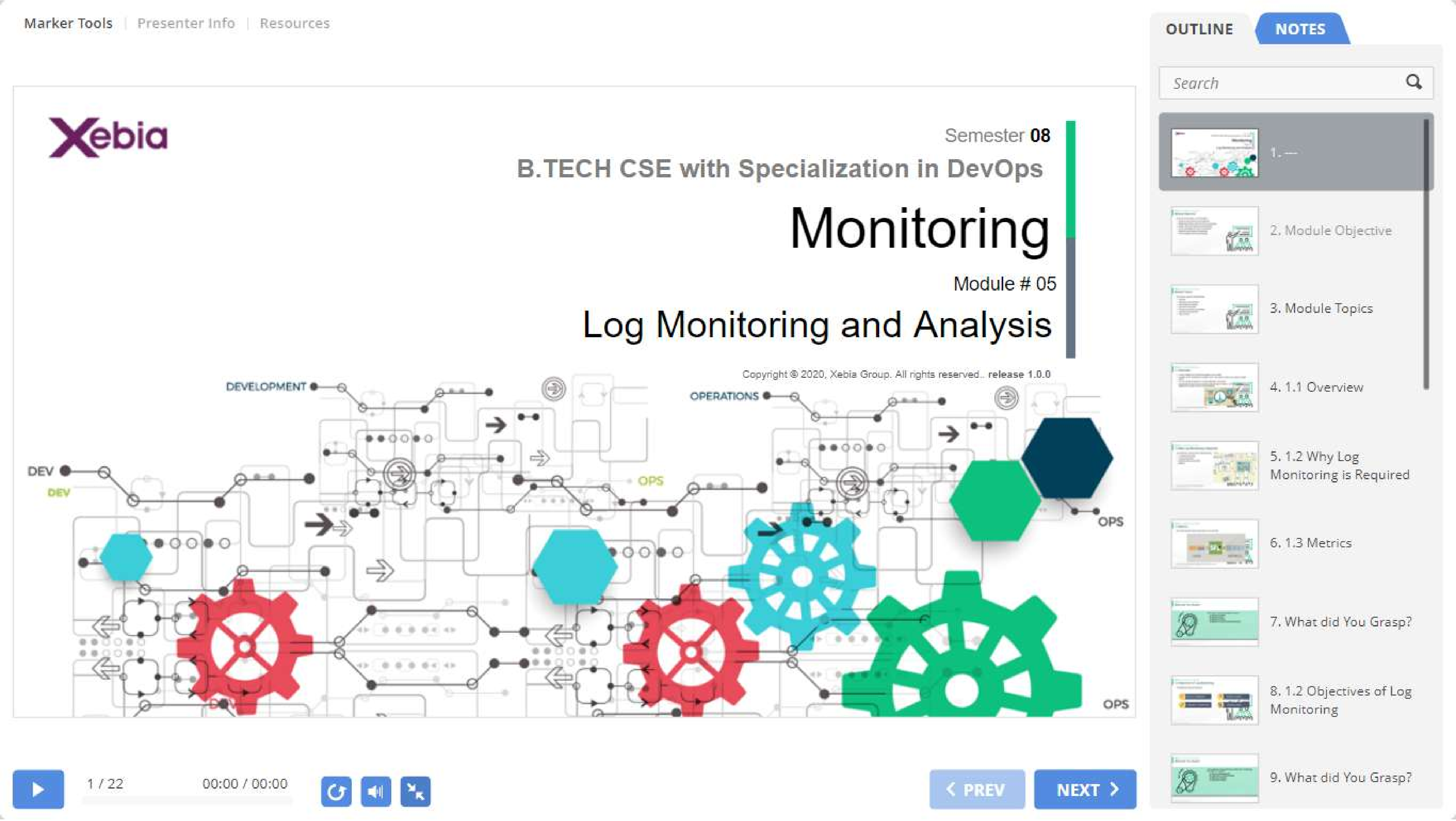


Xebia

Semester **08**

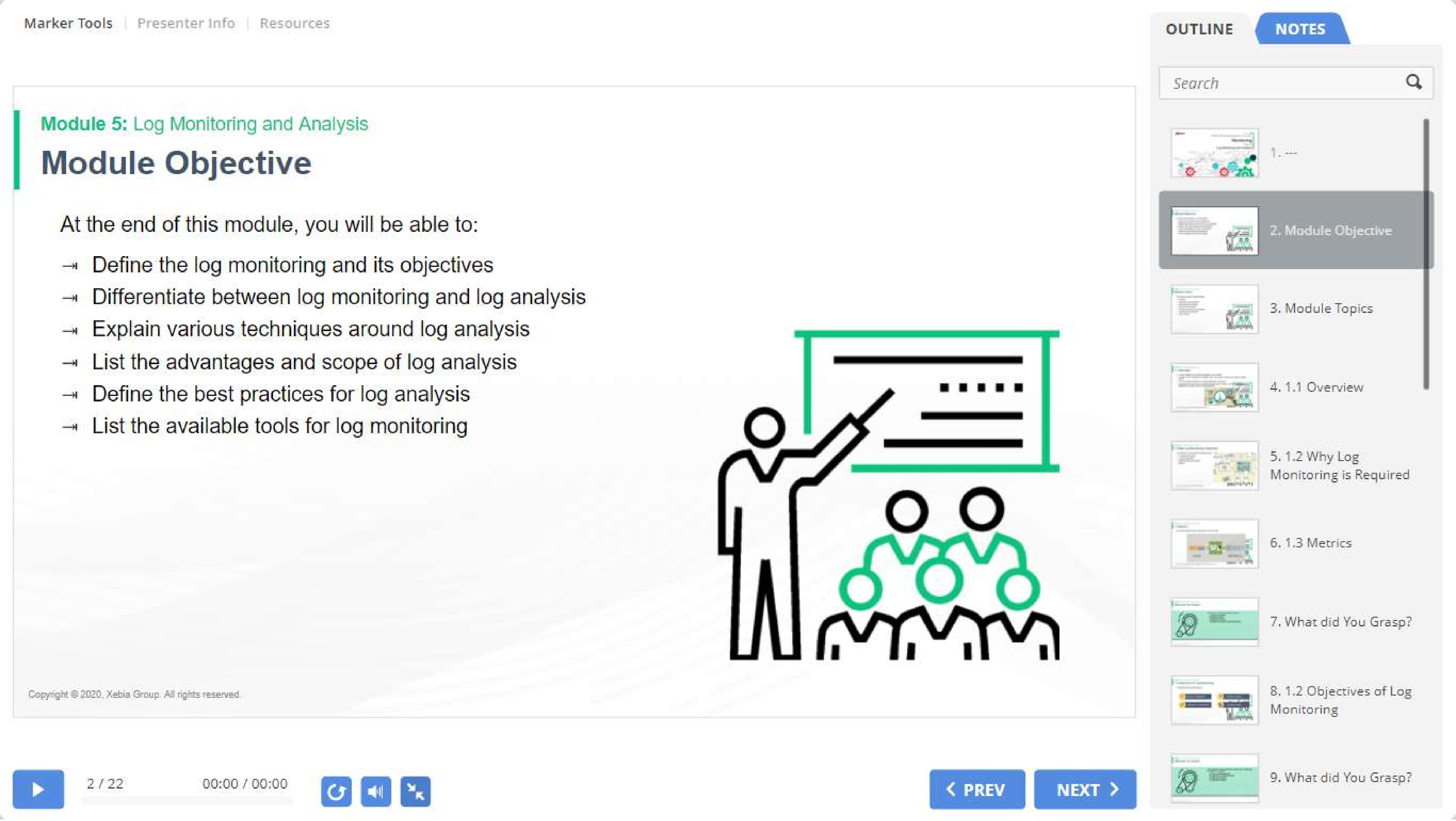
B.TECH CSE with Specialization in DevOps

Monitoring

Module # 05

Log Monitoring and Analysis

1. —
2. Module Objective
3. Module Topics
4. 1.1 Overview
5. 1.2 Why Log Monitoring is Required
6. 1.3 Metrics
7. What did You Grasp?
8. 1.2 Objectives of Log Monitoring
9. What did You Grasp?



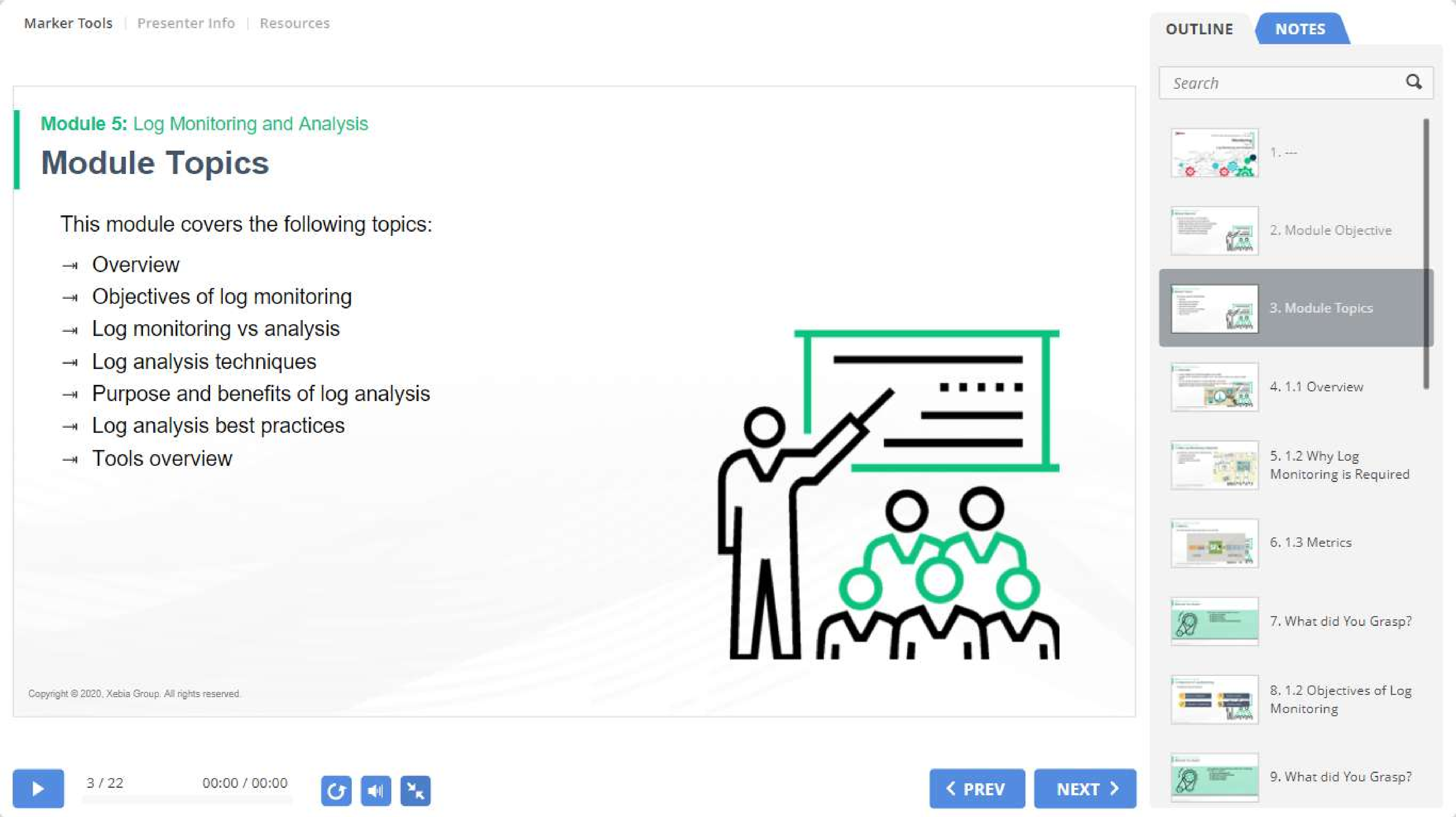
Module 5: Log Monitoring and Analysis

Module Objective

At the end of this module, you will be able to:

- Define the log monitoring and its objectives
- Differentiate between log monitoring and log analysis
- Explain various techniques around log analysis
- List the advantages and scope of log analysis
- Define the best practices for log analysis
- List the available tools for log monitoring

1. ---
2. Module Objective
3. Module Topics
4. 1.1 Overview
5. 1.2 Why Log Monitoring is Required
6. 1.3 Metrics
7. What did You Grasp?
8. 1.2 Objectives of Log Monitoring
9. What did You Grasp?

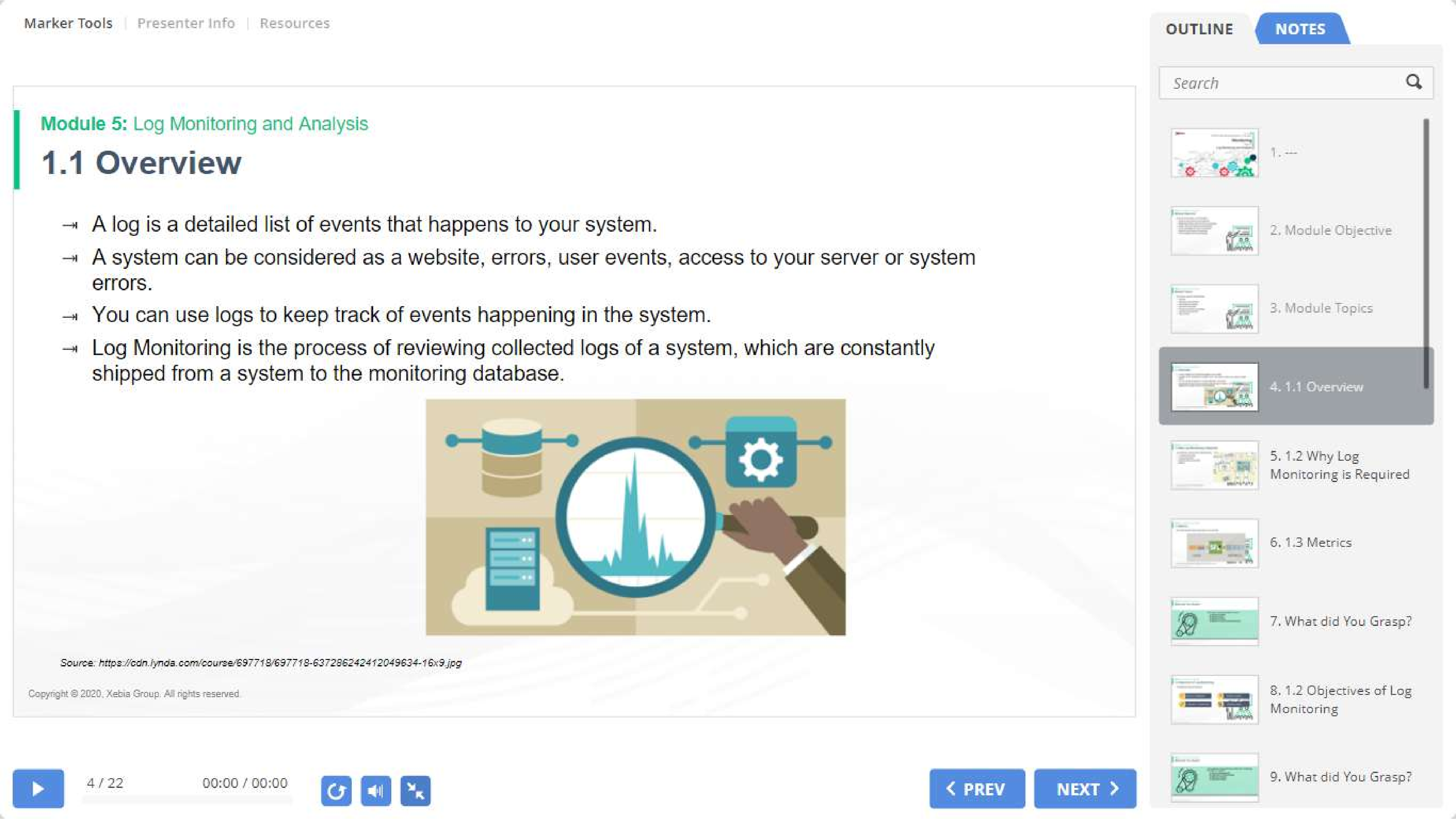


Module 5: Log Monitoring and Analysis

Module Topics

This module covers the following topics:

- Overview
- Objectives of log monitoring
- Log monitoring vs analysis
- Log analysis techniques
- Purpose and benefits of log analysis
- Log analysis best practices
- Tools overview



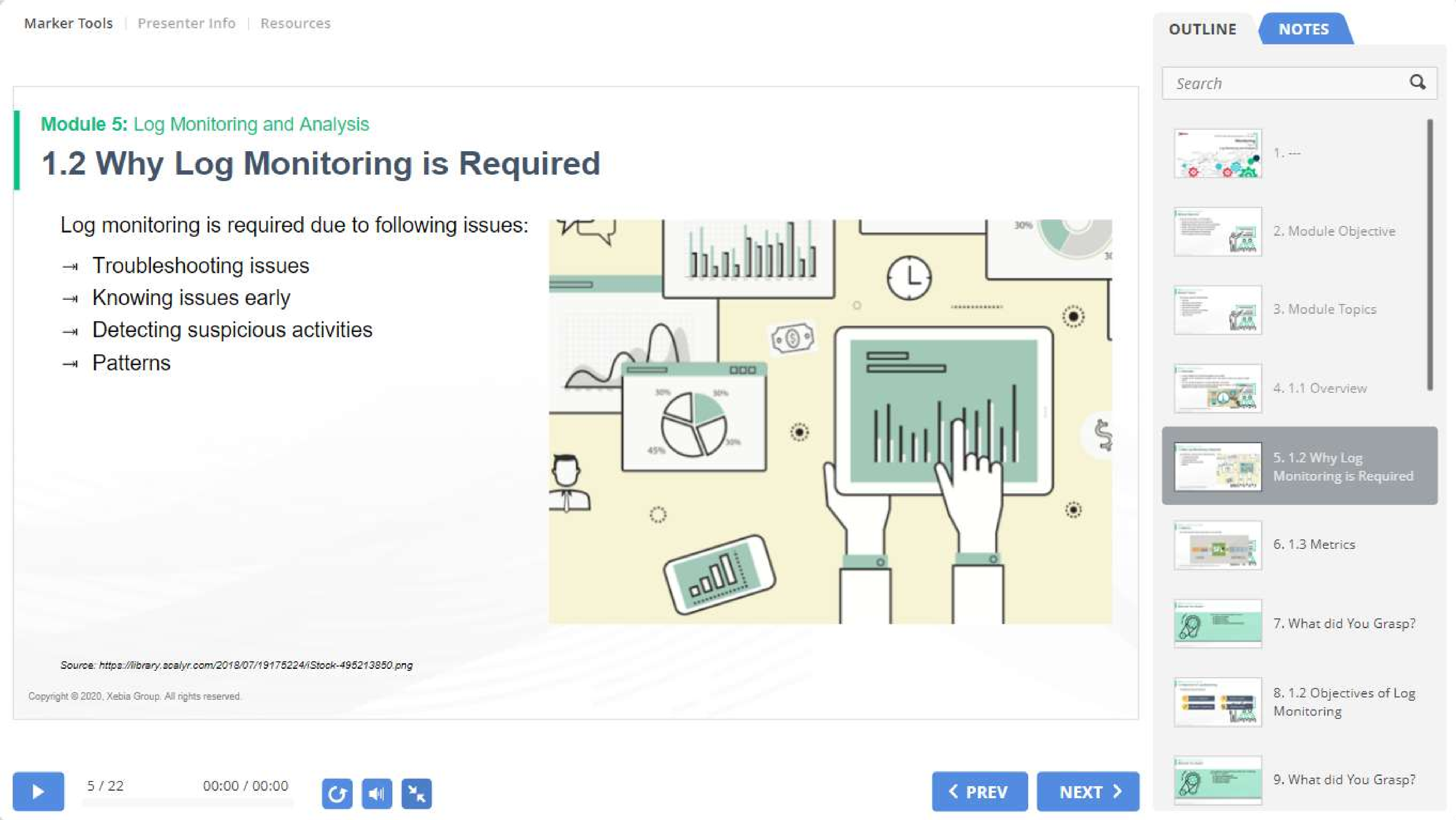
Module 5: Log Monitoring and Analysis

1.1 Overview

- A log is a detailed list of events that happens to your system.
- A system can be considered as a website, errors, user events, access to your server or system errors.
- You can use logs to keep track of events happening in the system.
- Log Monitoring is the process of reviewing collected logs of a system, which are constantly shipped from a system to the monitoring database.

Source: https://cdn.lynda.com/course/697718/697718-637286242412049634-16x9.jpg

1. ---
2. Module Objective
3. Module Topics
4. 1.1 Overview
5. 1.2 Why Log Monitoring is Required
6. 1.3 Metrics
7. What did You Grasp?
8. 1.2 Objectives of Log Monitoring
9. What did You Grasp?



Module 5: Log Monitoring and Analysis

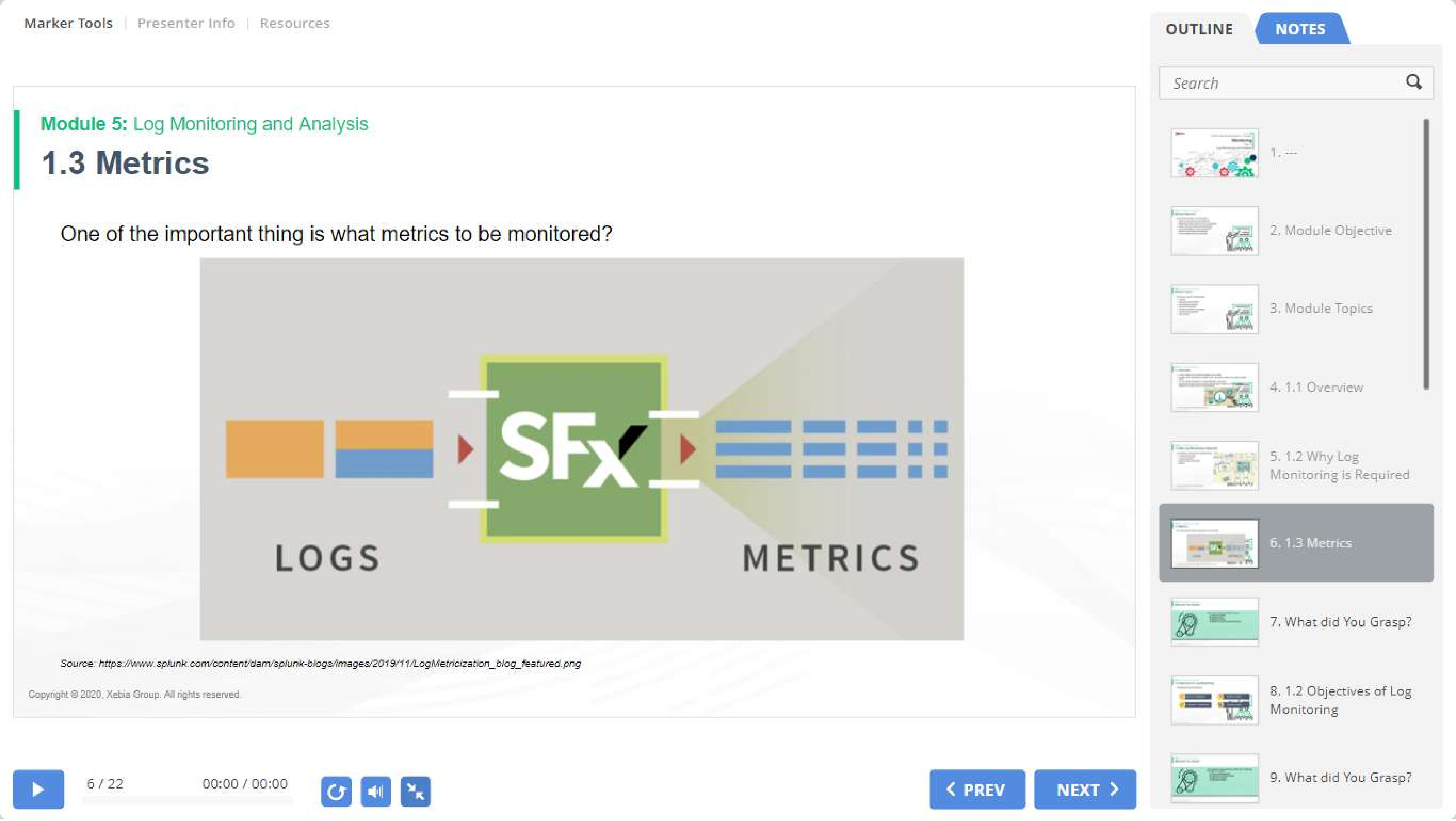
1.2 Why Log Monitoring is Required

Log monitoring is required due to following issues:

- Troubleshooting issues
- Knowing issues early
- Detecting suspicious activities
- Patterns

Source: https://library.scalyr.com/2018/07/19175224/iStock-495213850.png

1. ---
2. Module Objective
3. Module Topics
4. 1.1 Overview
5. 1.2 Why Log Monitoring is Required
6. 1.3 Metrics
7. What did You Grasp?
8. 1.2 Objectives of Log Monitoring
9. What did You Grasp?

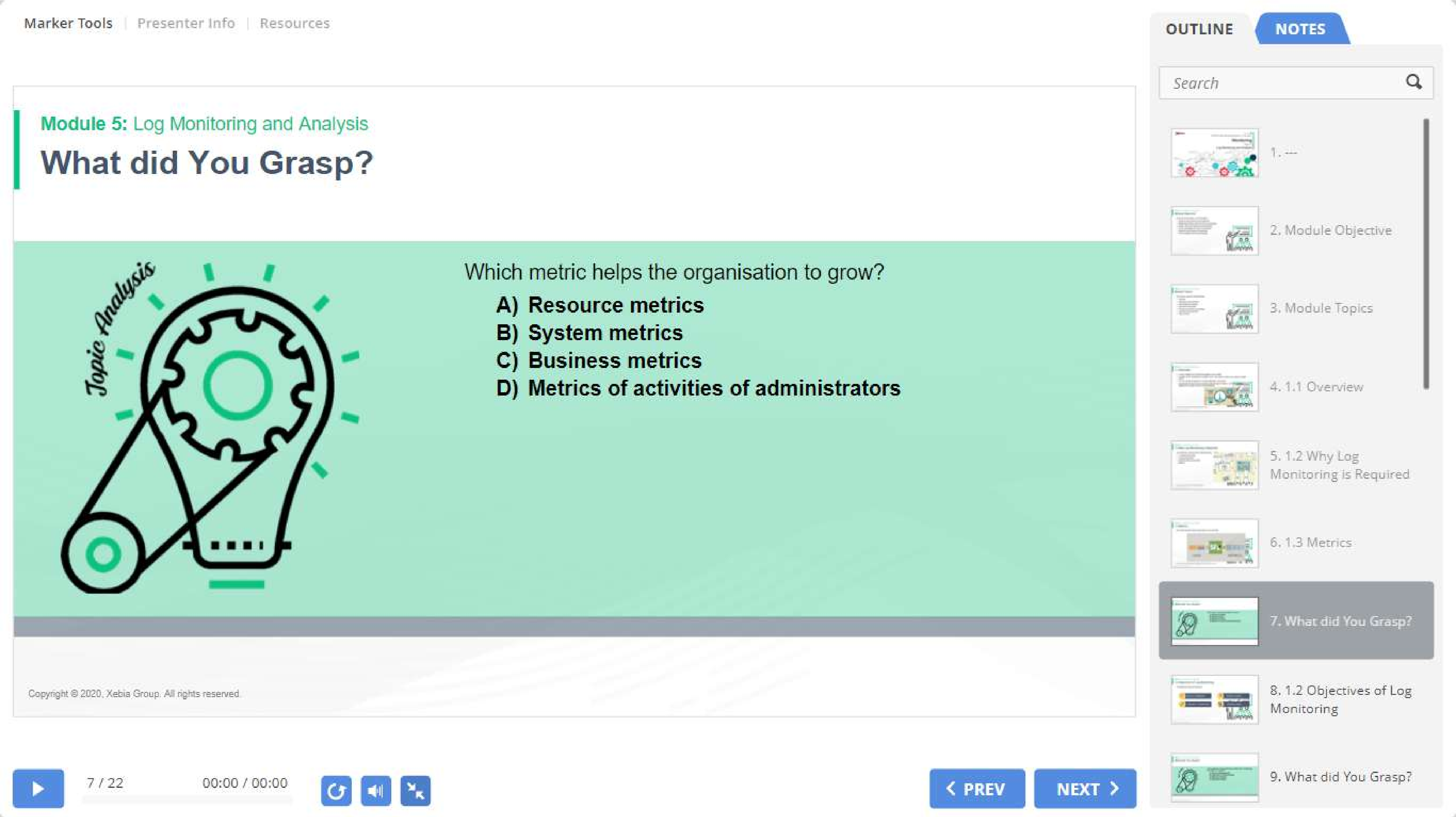


Module 5: Log Monitoring and Analysis

1.3 Metrics

One of the important thing is what metrics to be monitored?

Source: https://www.splunk.com/content/dam/splunk-blogs/images/2019/11/LogMetricization_blog_featured.png



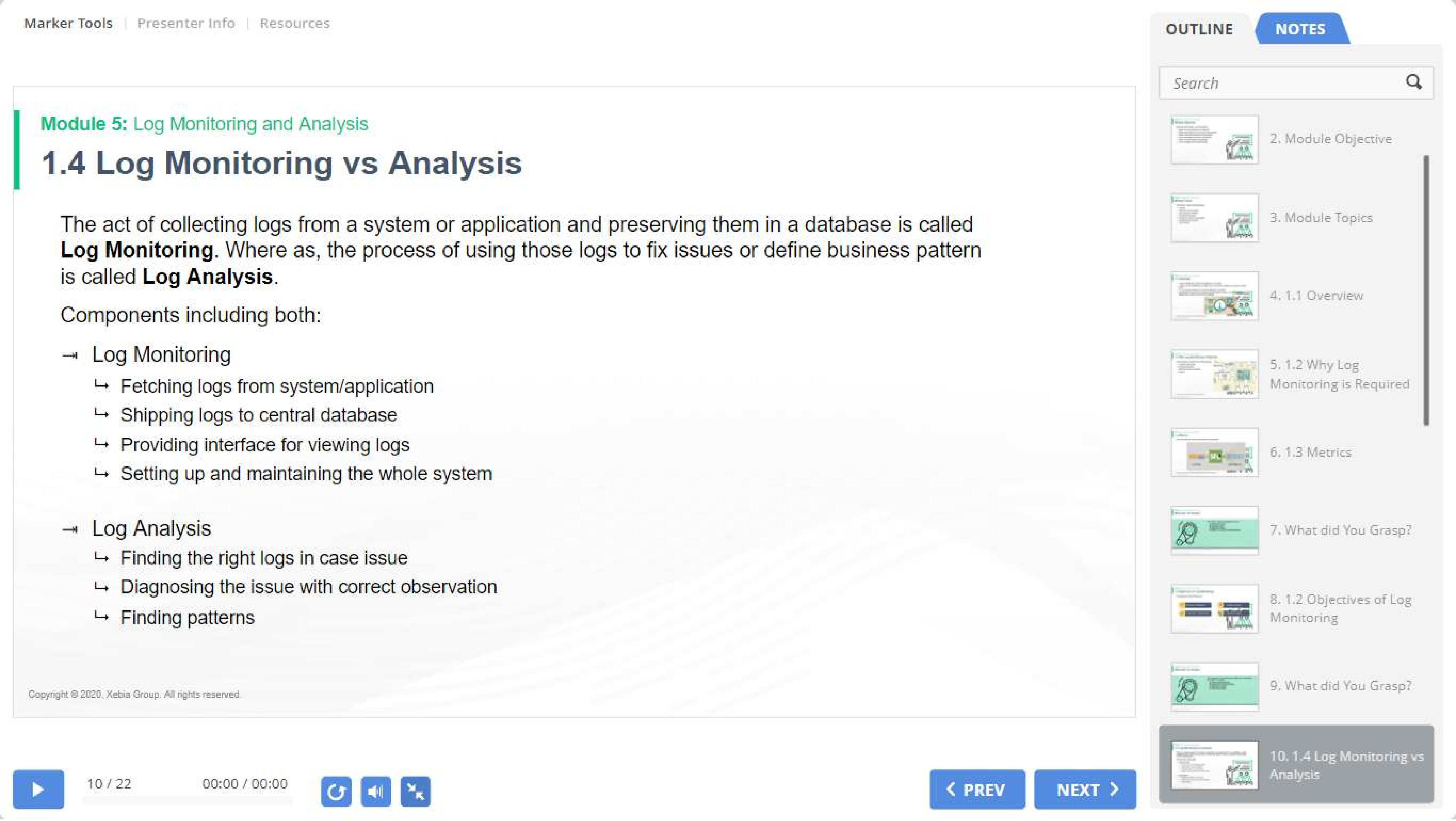
Module 5: Log Monitoring and Analysis

What did You Grasp?

Which metric helps the organisation to grow?

A) Resource metrics
B) System metrics
C) Business metrics
D) Metrics of activities of administrators

1. ---
2. Module Objective
3. Module Topics
4. 1.1 Overview
5. 1.2 Why Log Monitoring is Required
6. 1.3 Metrics
7. What did You Grasp?
8. 1.2 Objectives of Log Monitoring
9. What did You Grasp?



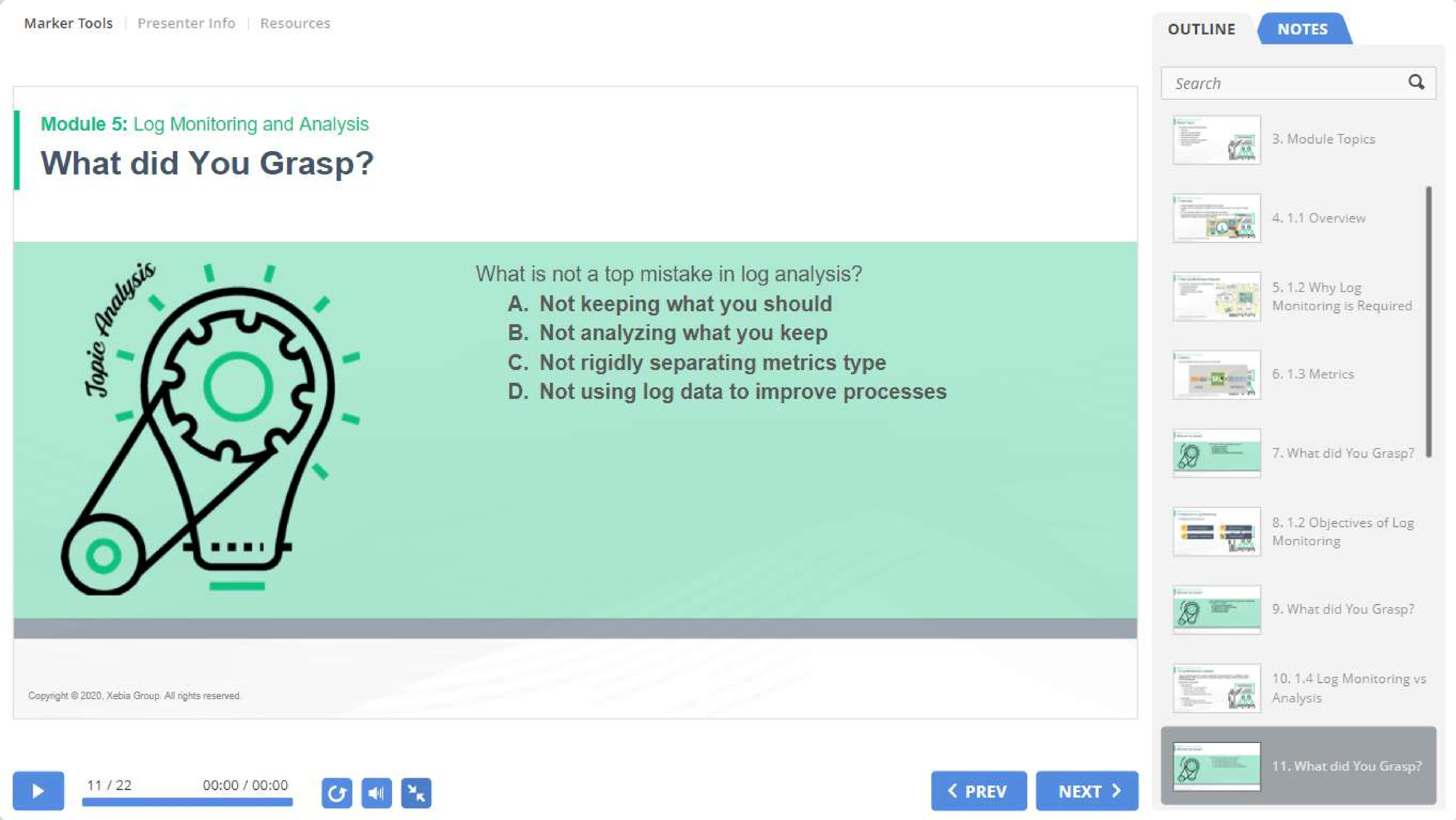
Module 5: Log Monitoring and Analysis

1.4 Log Monitoring vs Analysis

The act of collecting logs from a system or application and preserving them in a database is called **Log Monitoring**. Where as, the process of using those logs to fix issues or define business pattern is called **Log Analysis**.

Components including both:

- Log Monitoring
  - Fetching logs from system/application
  - Shipping logs to central database
  - Providing interface for viewing logs
  - Setting up and maintaining the whole system
- Log Analysis
  - Finding the right logs in case issue
  - Diagnosing the issue with correct observation
  - Finding patterns

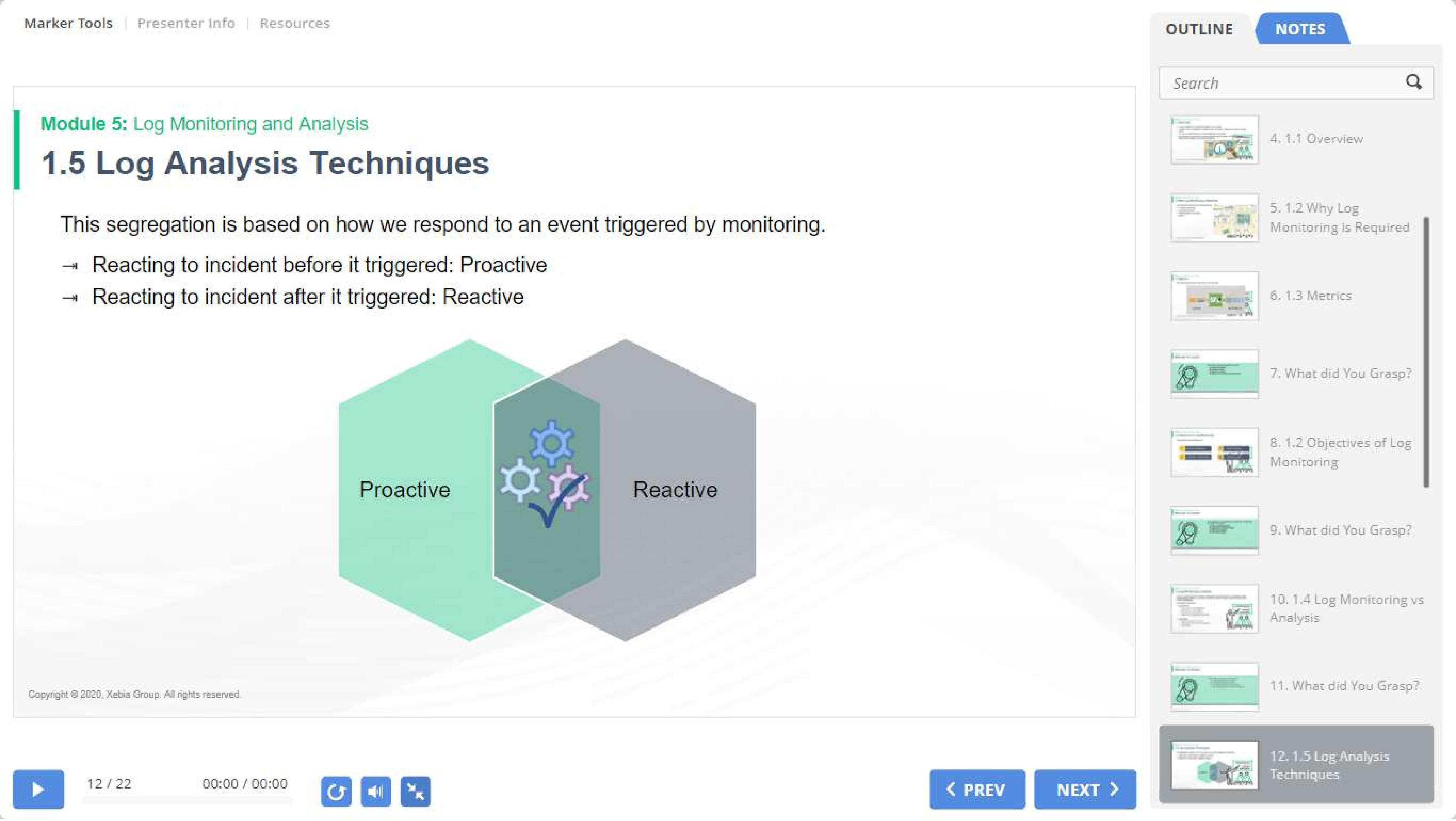


Module 5: Log Monitoring and Analysis

What did You Grasp?

What is not a top mistake in log analysis?

A. **Not keeping what you should**
B. **Not analyzing what you keep**
C. **Not rigidly separating metrics type**
D. **Not using log data to improve processes**



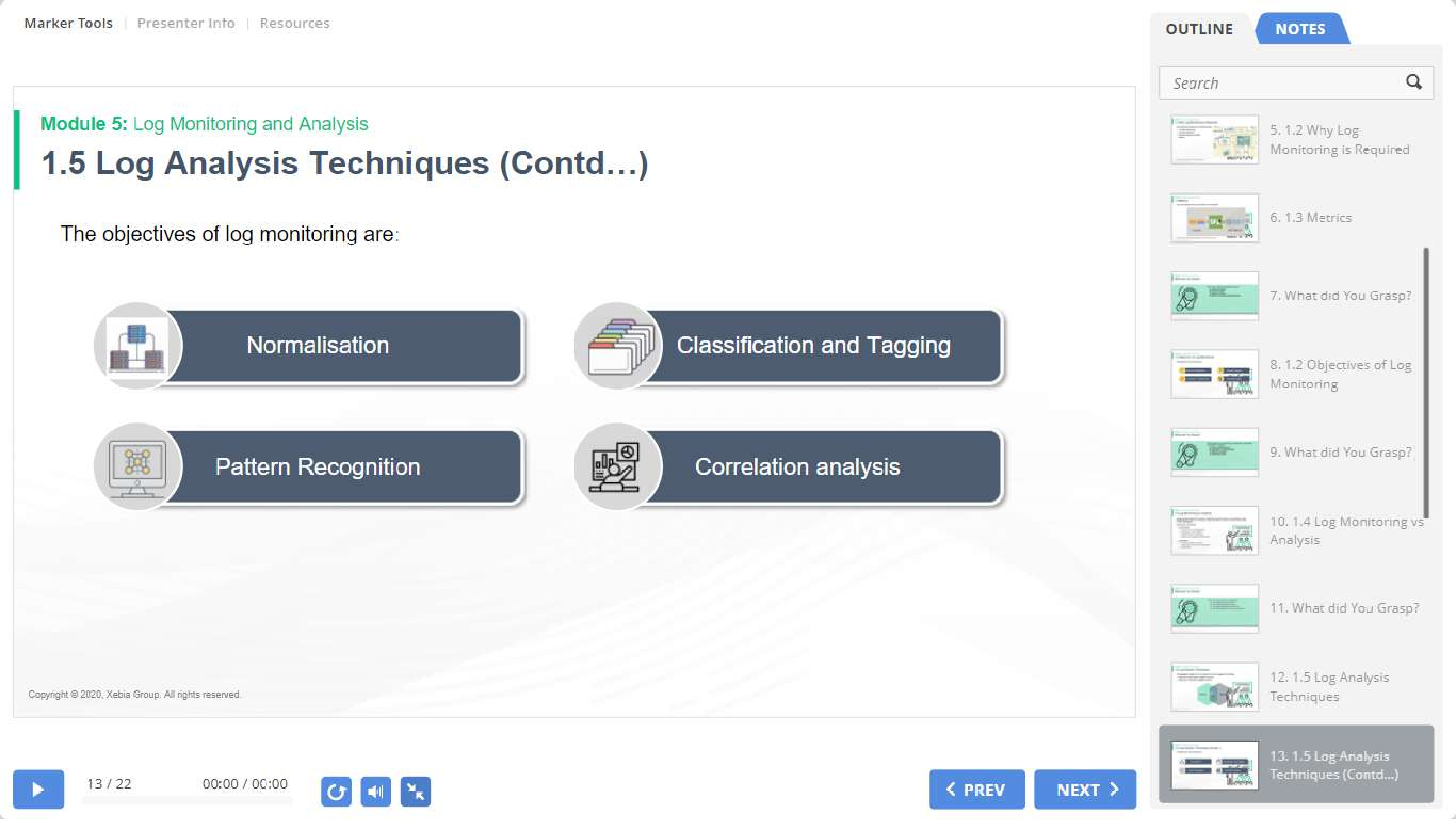
Module 5: Log Monitoring and Analysis

1.5 Log Analysis Techniques

This segregation is based on how we respond to an event triggered by monitoring.

- Reacting to incident before it triggered: Proactive
- Reacting to incident after it triggered: Reactive

4. 1.1 Overview
5. 1.2 Why Log Monitoring is Required
6. 1.3 Metrics
7. What did You Grasp?
8. 1.2 Objectives of Log Monitoring
9. What did You Grasp?
10. 1.4 Log Monitoring vs Analysis
11. What did You Grasp?
12. 1.5 Log Analysis Techniques



Module 5: Log Monitoring and Analysis

1.5 Log Analysis Techniques (Contd…)

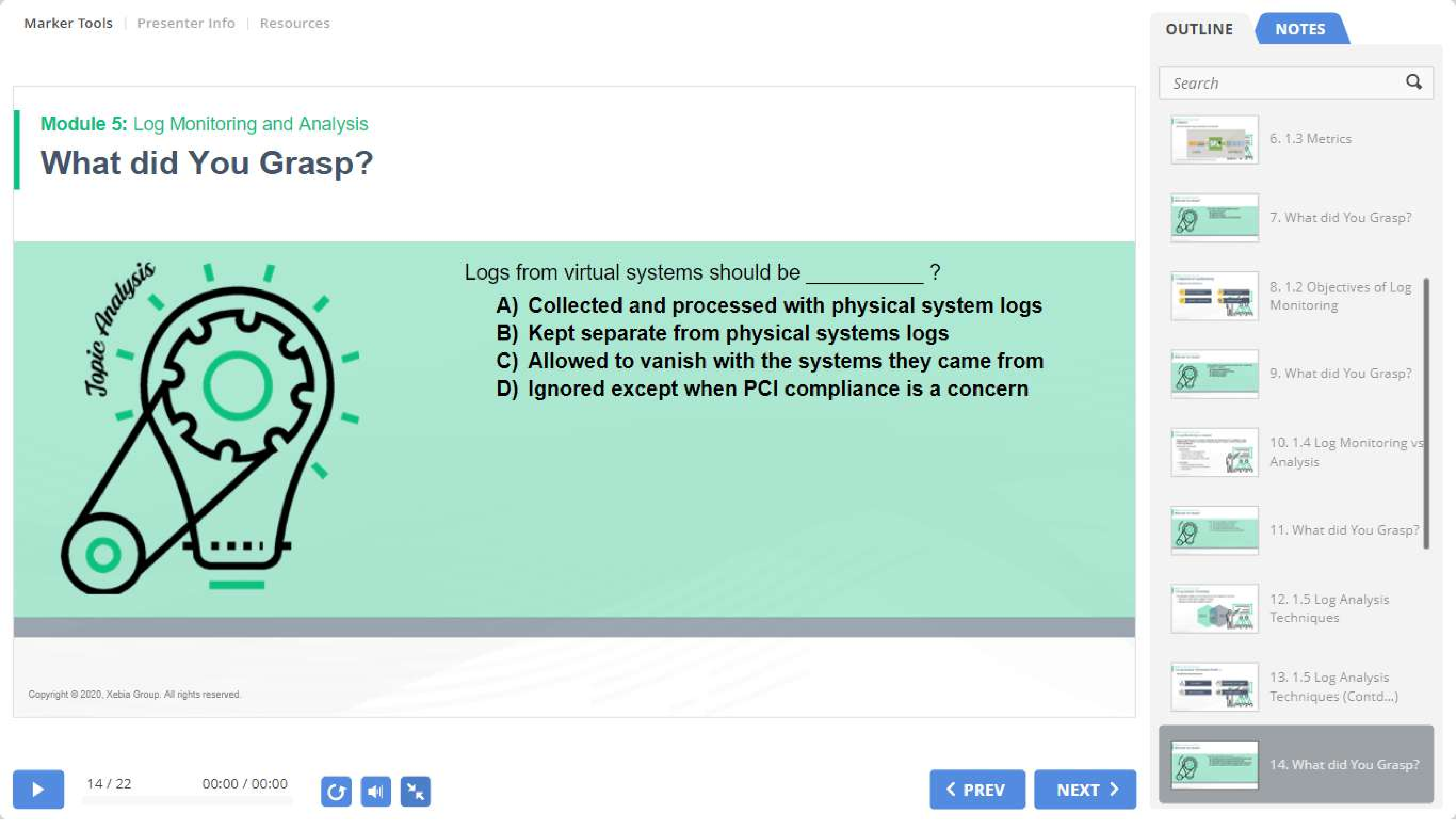
The objectives of log monitoring are:

- Normalisation
- Classification and Tagging
- Pattern Recognition
- Correlation analysis

5. 1.2 Why Log Monitoring is Required
6. 1.3 Metrics
7. What did You Grasp?
8. 1.2 Objectives of Log Monitoring
9. What did You Grasp?
10. 1.4 Log Monitoring vs Analysis
11. What did You Grasp?
12. 1.5 Log Analysis Techniques
13. 1.5 Log Analysis Techniques (Contd...)

13 / 22

00:00 / 00:00

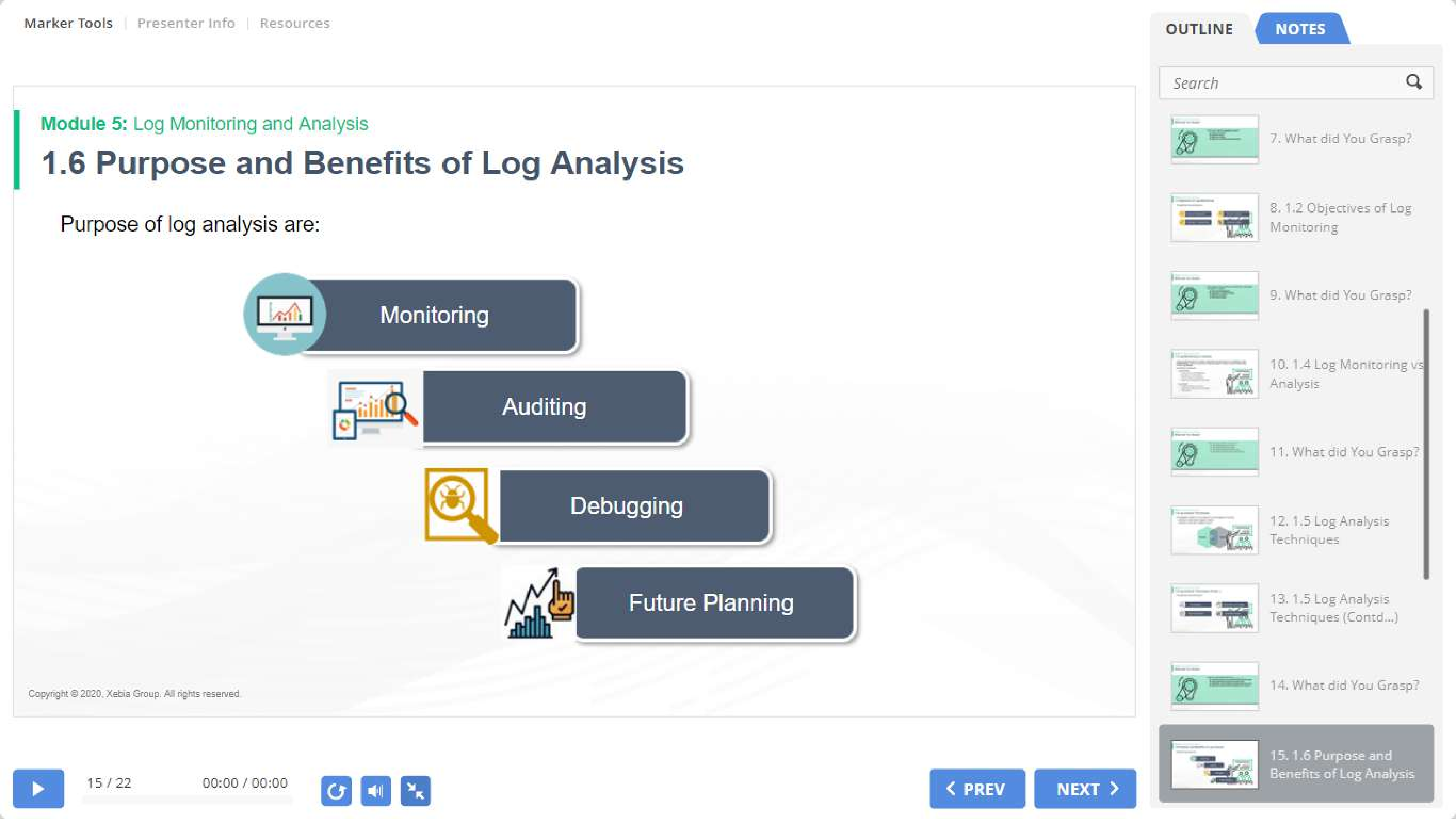


Module 5: Log Monitoring and Analysis

What did You Grasp?

Logs from virtual systems should be __________ ?

A) Collected and processed with physical system logs
B) Kept separate from physical systems logs
C) Allowed to vanish with the systems they came from
D) Ignored except when PCI compliance is a concern



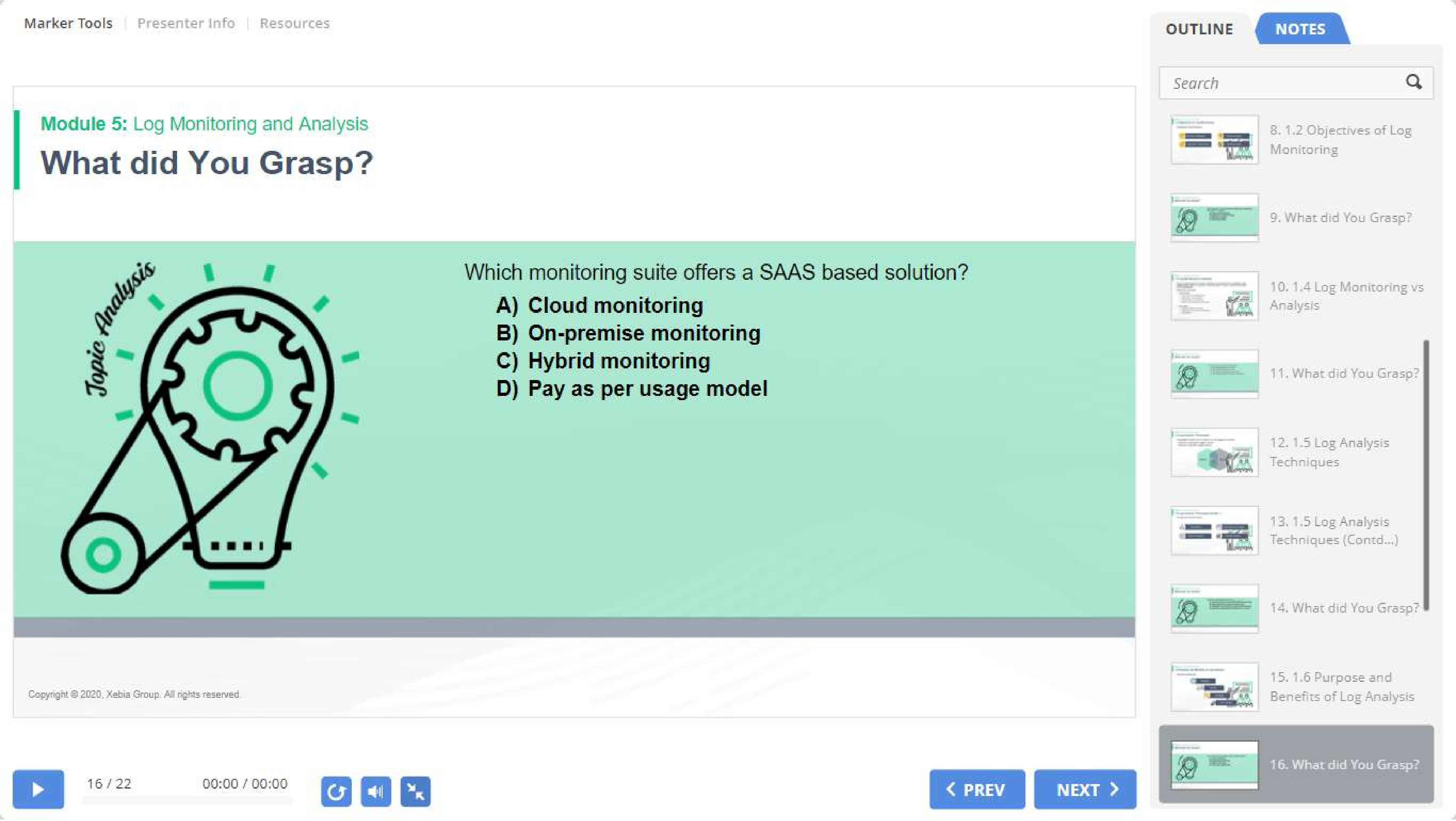
Module 5: Log Monitoring and Analysis

1.6 Purpose and Benefits of Log Analysis

Purpose of log analysis are:

- Monitoring
- Auditing
- Debugging
- Future Planning

7. What did You Grasp?
8. 1.2 Objectives of Log Monitoring
9. What did You Grasp?
10. 1.4 Log Monitoring vs Analysis
11. What did You Grasp?
12. 1.5 Log Analysis Techniques
13. 1.5 Log Analysis Techniques (Contd...)
14. What did You Grasp?
15. 1.6 Purpose and Benefits of Log Analysis



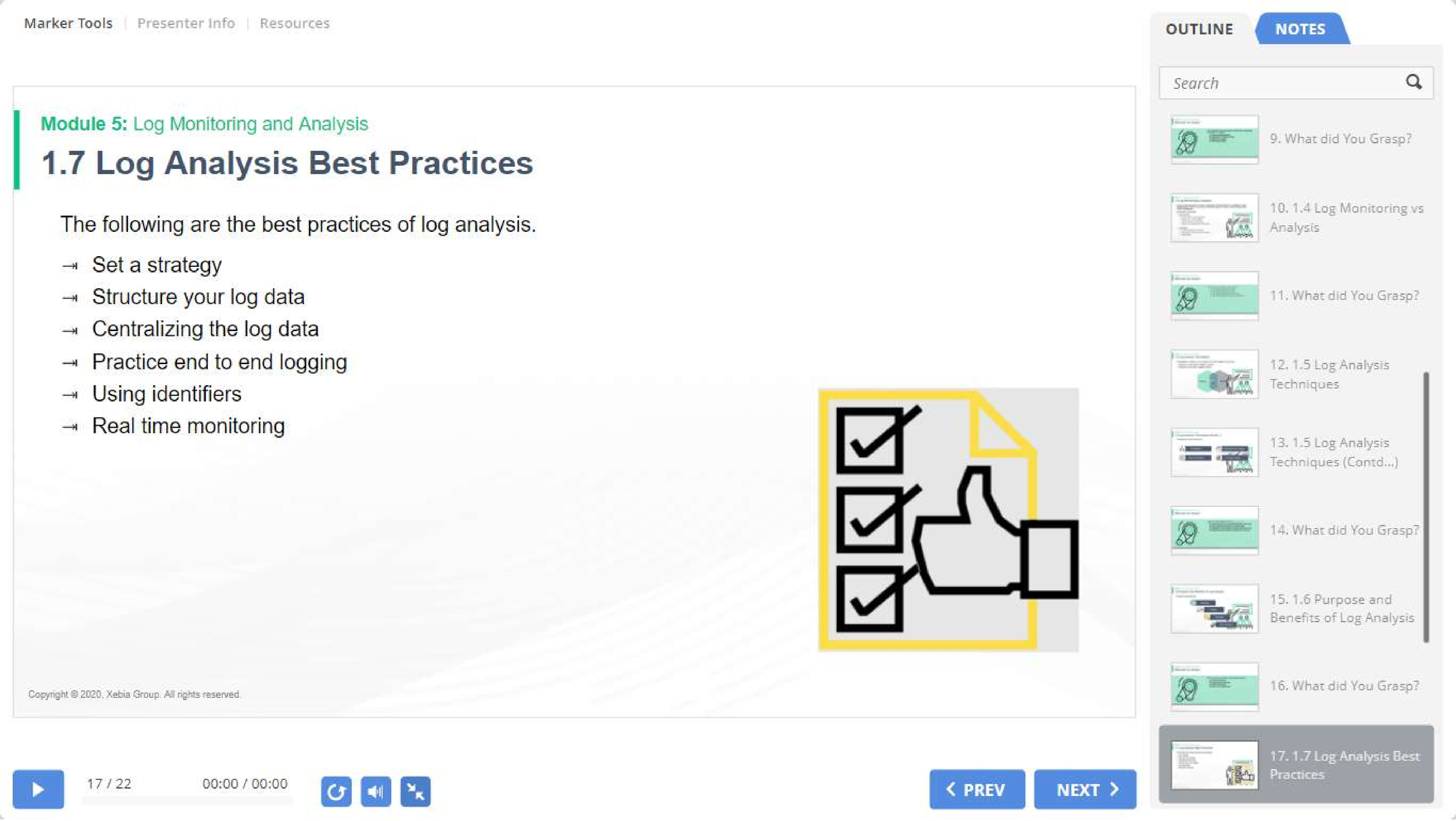
Module 5: Log Monitoring and Analysis

What did You Grasp?

Which monitoring suite offers a SAAS based solution?

A) Cloud monitoring
B) On-premise monitoring
C) Hybrid monitoring
D) Pay as per usage model

8. 1.2 Objectives of Log Monitoring
9. What did You Grasp?
10. 1.4 Log Monitoring vs Analysis
11. What did You Grasp?
12. 1.5 Log Analysis Techniques
13. 1.5 Log Analysis Techniques (Contd...)
14. What did You Grasp?
15. 1.6 Purpose and Benefits of Log Analysis
16. What did You Grasp?



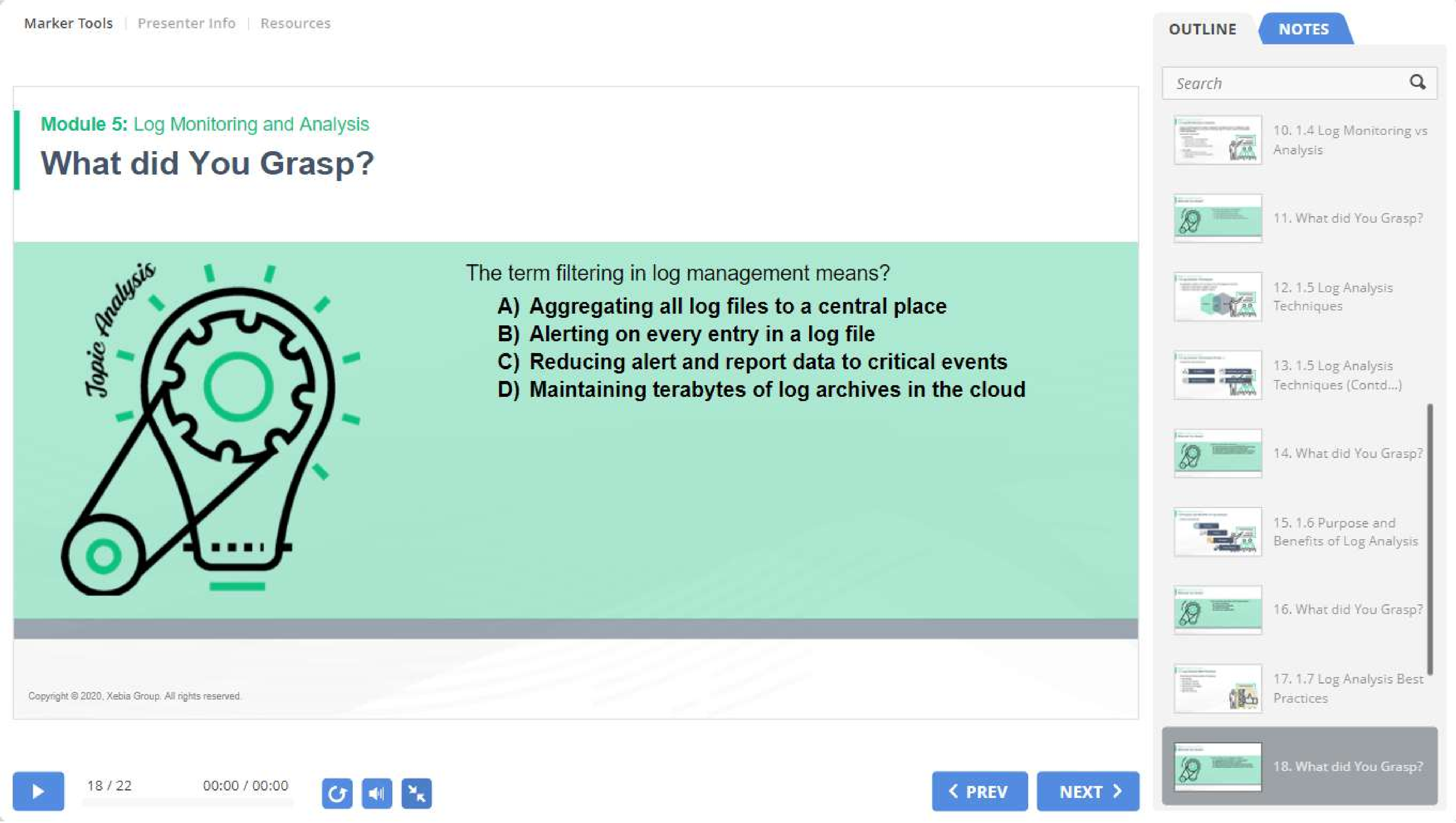
Marker Tools | Presenter Info | Resources
OUTLINE
NOTES
Search
9. What did You Grasp?
10. 1.4 Log Monitoring vs Analysis
11. What did You Grasp?
12. 1.5 Log Analysis Techniques
13. 1.5 Log Analysis Techniques (Contd...)
14. What did You Grasp?
15. 1.6 Purpose and Benefits of Log Analysis
16. What did You Grasp?
17. 1.7 Log Analysis Best Practices
17 / 22
00:00 / 00:00
PREV
NEXT

Module 5: Log Monitoring and Analysis

1.7 Log Analysis Best Practices

The following are the best practices of log analysis.

- Set a strategy
- Structure your log data
- Centralizing the log data
- Practice end to end logging
- Using identifiers
- Real time monitoring

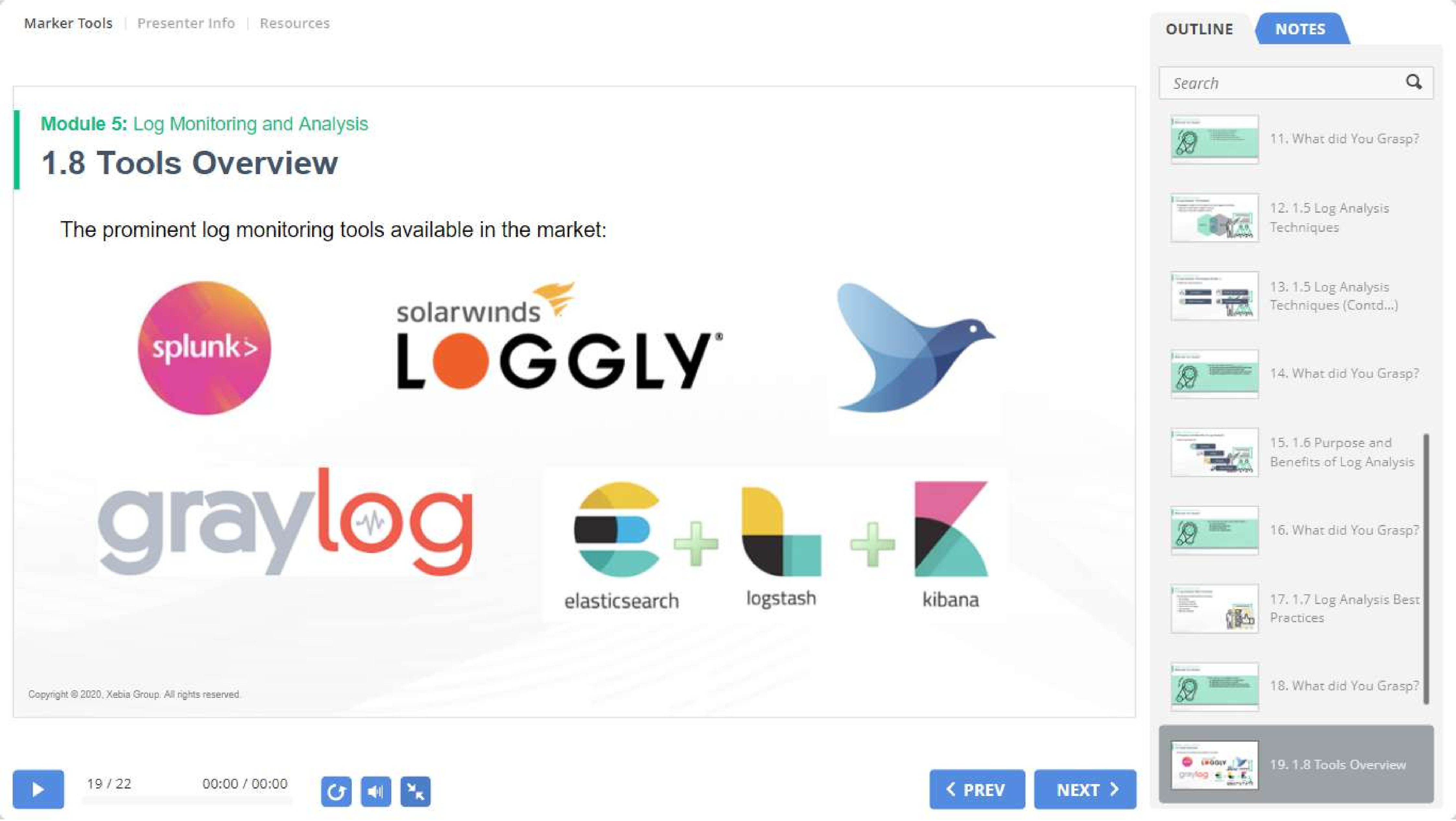


Module 5: Log Monitoring and Analysis

What did You Grasp?

The term filtering in log management means?

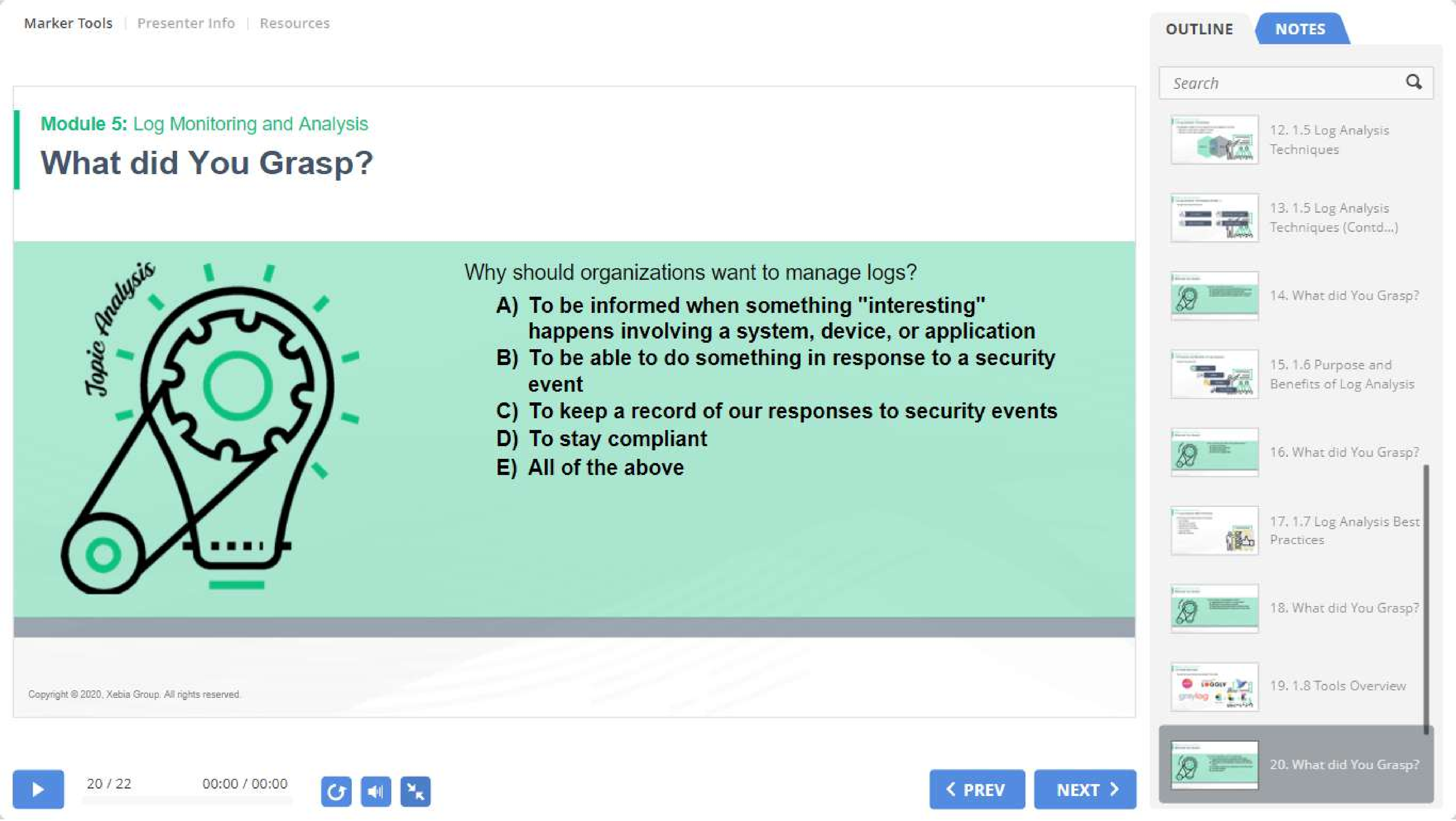
- **A) Aggregating all log files to a central place**
- **B) Alerting on every entry in a log file**
- **C) Reducing alert and report data to critical events**
- **D) Maintaining terabytes of log archives in the cloud**



Module 5: Log Monitoring and Analysis

1.8 Tools Overview

The prominent log monitoring tools available in the market:



Module 5: Log Monitoring and Analysis

What did You Grasp?

Why should organizations want to manage logs?

A) To be informed when something "interesting" happens involving a system, device, or application

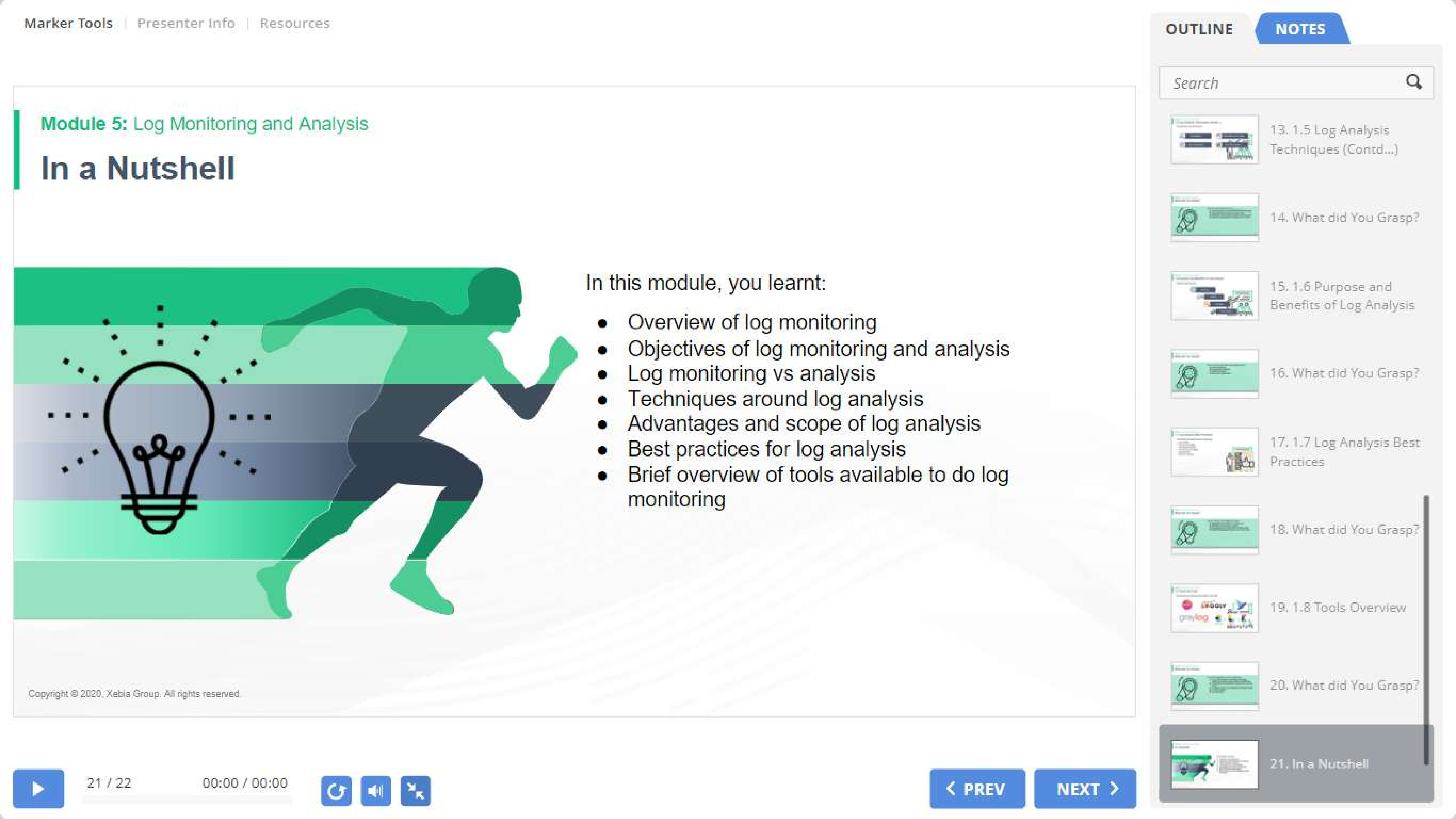
B) To be able to do something in response to a security event

C) To keep a record of our responses to security events

D) To stay compliant

E) All of the above

12. 1.5 Log Analysis Techniques
13. 1.5 Log Analysis Techniques (Contd...)
14. What did You Grasp?
15. 1.6 Purpose and Benefits of Log Analysis
16. What did You Grasp?
17. 1.7 Log Analysis Best Practices
18. What did You Grasp?
19. 1.8 Tools Overview
20. What did You Grasp?

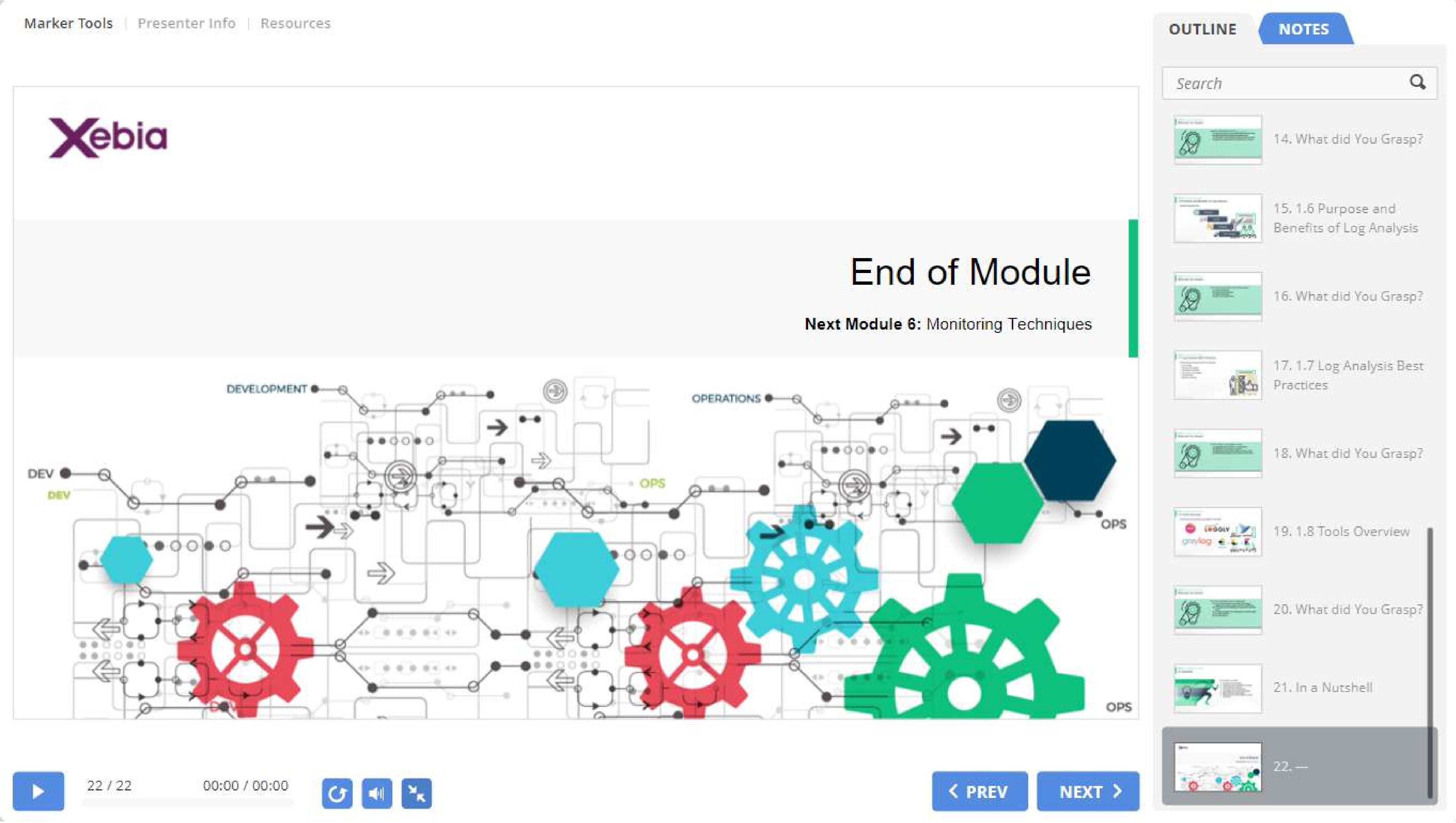


Module 5: Log Monitoring and Analysis

In a Nutshell

In this module, you learnt:

- Overview of log monitoring
- Objectives of log monitoring and analysis
- Log monitoring vs analysis
- Techniques around log analysis
- Advantages and scope of log analysis
- Best practices for log analysis
- Brief overview of tools available to do log monitoring



End of Module

Next Module 6: Monitoring Techniques

14. What did You Grasp?
15. 1.6 Purpose and Benefits of Log Analysis
16. What did You Grasp?
17. 1.7 Log Analysis Best Practices
18. What did You Grasp?
19. 1.8 Tools Overview
20. What did You Grasp?
21. In a Nutshell
22. —