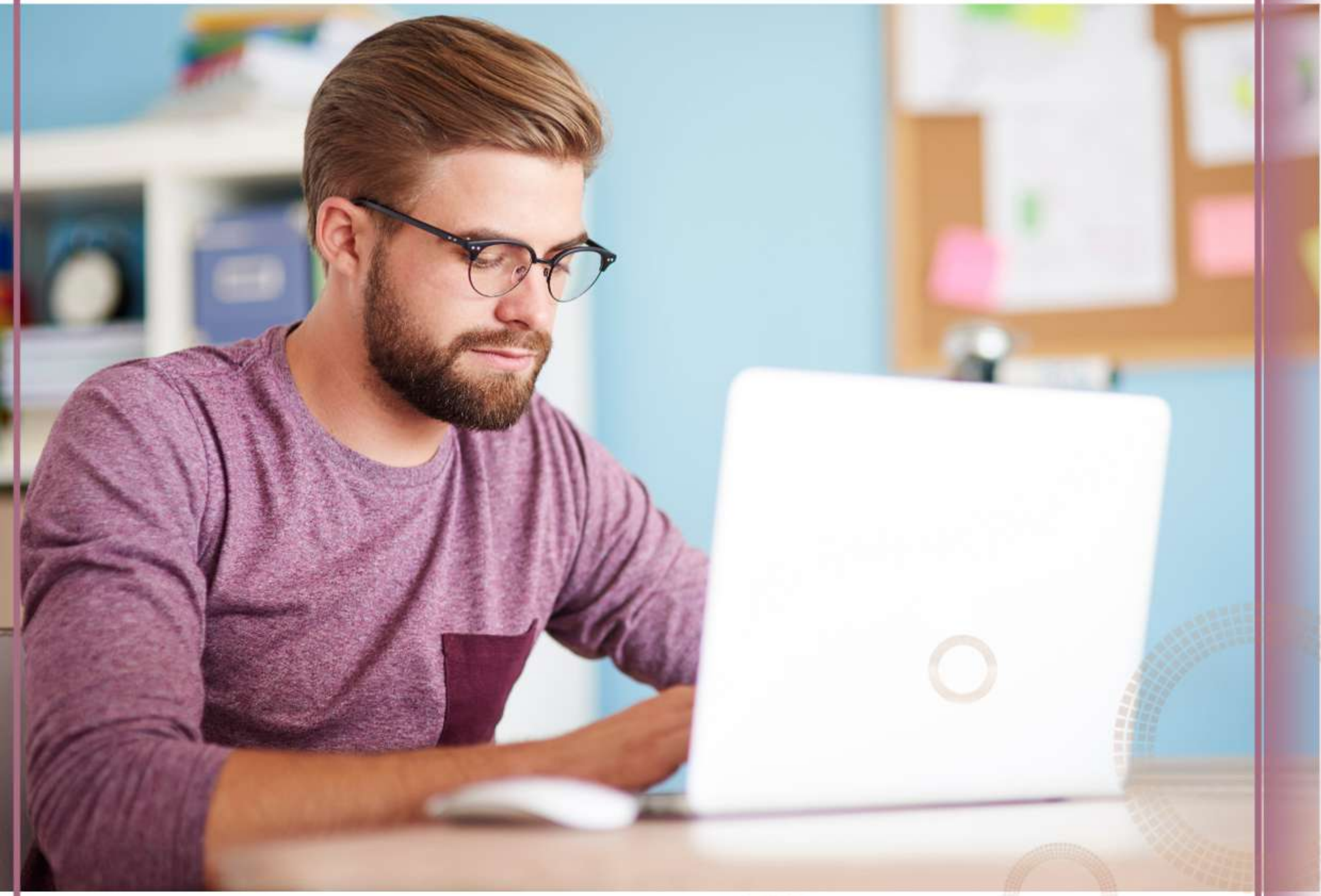
Kaspersky Anti Targeted Attack Platform Kaspersky Endpoint Detection and Response



Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1.Installing and Configure Central Node

- Install the operating system for Central Node
- Select the role, config the network, time, & access to the server

2.Configure Kaspersky Sandbox

- Configure the internet interface for virtual machine
- Setup up time synchronization
- Add the Virtual Machine Images

3.Connect the Central Node to the Sandbox

- Connect the Central Node to the Sandbox Server
- Active Central Node
- Create an Information security officer account

4.Connect Central Node to the Network Infrastructure (SPAN)

- Activate an additional network interface
- Enable traffic capture on the prepared network interface
- Traffic is being analyzed using the Dashboard in the Administrtr
- Check alerts in the security officer console to make sure

5.Connect the central Node to the Mail System using SMTP

- Configure the Central Node to receive Messages over SMTP
- Configure a rule that will copy messages
- Configure a mail route to the central Node
- Check mail traffic processg health frm the administratr console
- Check mail traffic prcessg health rom the secrty officr's console

6.Prevent Superfluous mail Processing

- Disable SMTP processing for the SPAN Sensor
- Connect sensor to proxy Server (ICAP)
- Enable the ICAP Sensor on the Central Node
- ICAP sensor health from the administrator's console
- ICAP Sensor health from the security officer's Console

7.Prevent Superfluous http traffic Processing

- Make sure that objects extractd frm http traffic are processed
- Exclude the proxy traffic from processing by IP address
- Extracted from http traffic are processed once
- Enable Kaspersky Endpoint Agent using the task change apps

9.Connect Kaspersky Endpoint Agent to the Central Node

- Create a policy for Kaspersky Endpoint agent
- Config connection to the Central node in the Kaspersky Endpt
- Check that Kaspersky Endpt Agent has connctd to central Node

10. Activate Kaspersky Endpoint Agent

- Add a key to the Kaspersky Security Center repository
- Add a key to the Kaspersky Security Center repository
- Kaspersky Endpoint Agent has installed the license

11. TAA subsystem Operates Properly

- Run the test title and process the alert
- Send an email message with a link to a malicious title
- Save and execute the malicious title on a user's computer

12. Demonstrate KATA operation result

- Consult the alerts
- Analyze the scanning results from the sandbox
- Find associated Alerts
- Process the alerts

13. Demonstrating analysis and response to a TAA alert

- Analyze IAA alerts
- Find the event that triggered the alert
- Analyze related events
- Isolate the compromised computer
- Get the suspicious title and scan it
- Find out what the malicious title was doing
- Consult the title scanning results
- Examine the code of the malicious script
- Delete dangerous title from the computer
- Verify that isolation and title access deny operate property
- Complete the incident investigation

14. Examine details of file execution in the sandbox

- Download and unzip the debug information
- Analyze the interpretable tiles related to the threat

15. Add third-party IDS rules

- Load snort community rules to KAIA
- Write a custom rule for suricata
- Upload your rule to KAIA
- Verify that KAIA applies the rule when scanning traffic

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474