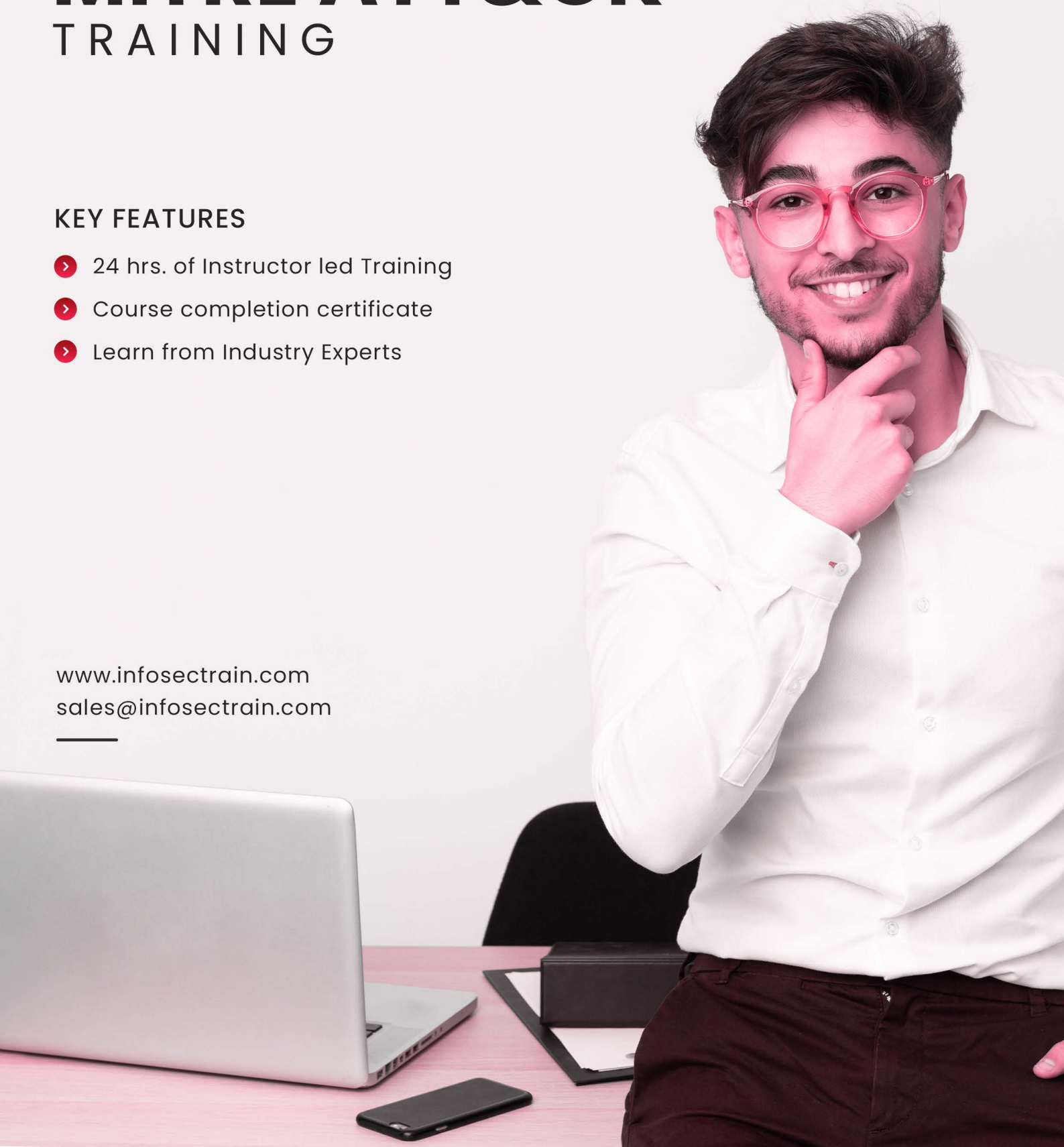
INFOSECTRAIN

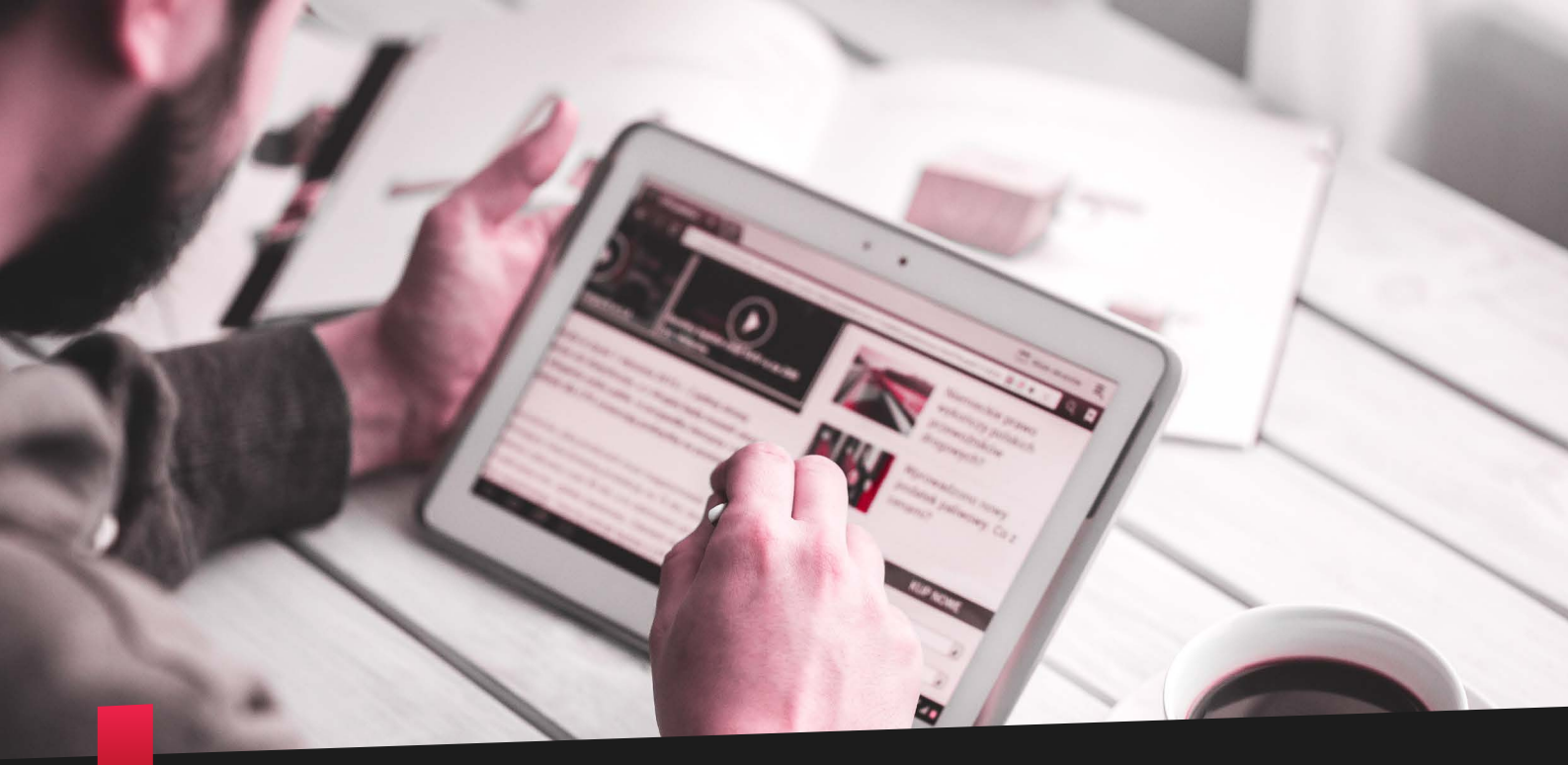
# MITRE ATT&CK
## TRAINING



### KEY FEATURES

- 24 hrs. of Instructor led Training
- Course completion certificate
- Learn from Industry Experts

www.infosectrain.com
sales@infosectrain.com



## Course Description

MITRE ATT&CK Framework Training at Infosec Train has been customized for the participants to provide the in-depth knowledge on the various adversary tactics and techniques to defend a network based on real-world observations of cyberattacks. These tactics and techniques are displayed in matrices that are arranged by attack stages like:

• Initial system access and advances to data theft or machine control

Our ATT&CK training includes expert guidance on various matrices:

• PRE-ATT&CK Matrix- techniques which are used for reconnaissance, target identification, and attack planning.

• Windows- techniques which are used to hack Windows.

• Linux: techniques which are used to hack all aspects of Linux.

• MacOS- techniques which are used to hack MacOS.

## The key features of the training are:

Online/onsite training by the experts of the domain.

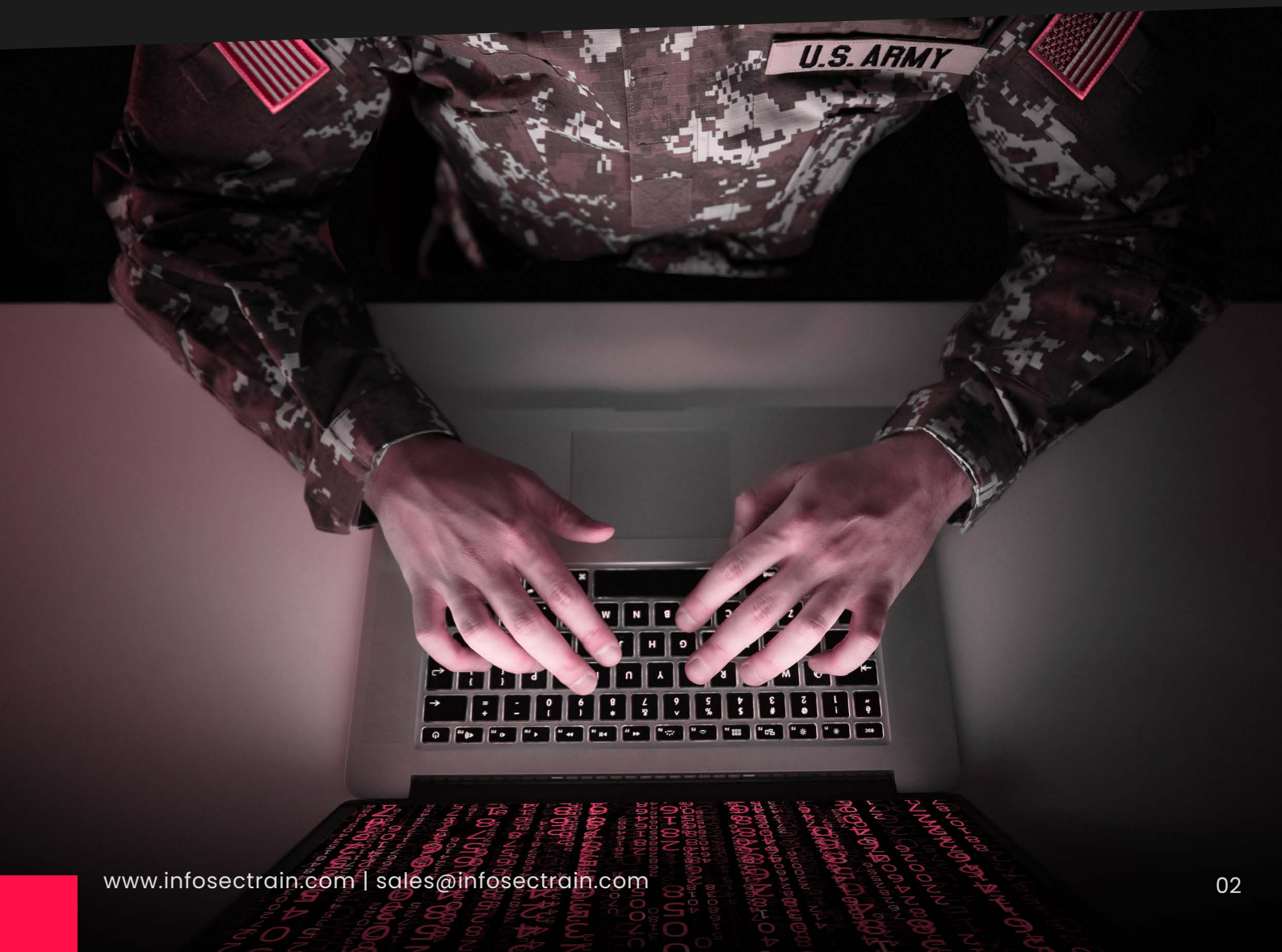
In-depth knowledge sharing on different matrices to enhance the skill.

Complete awareness is raised about an organization's security, identifying holes in defenses and prioritizing risks.

## Why MITRE ATT&CK Training?

MITRE ATT&CK Framework is a popular way to help organizations, end users, and the government share threat intelligence by offering a common language that's standardized and globally accessible. Professional's with ATT&CK Training are trusted for their latest skills to deal with the cyber threats. Thus, they get best of the jobs available for network defending. on the successful completion of this training, the candidates will be able to

- Set up the necessary development environment to start implementing MITRE ATT&CK.
- Classify how attackers interact with systems.
- Document adversary behaviors within systems.
- Track attacks, decipher patterns, and rate defense tools already in place.



## Target Audience

This course is beneficial for:

- Blue Team
- SOC analyst
- Security Analyst

## Pre-Requisite

Basic attack and defence knowledge and an understanding of information system security is recommended for this training.

# MITRE ATT&CK Course Content

## Introduction to MITRE ATT&CK

- MITRE ATT&CK – Cyber Attack Lifecycle
- Pyramid of pain
- Cyber Kill Chain
- Threat Intelligence using MITRE ATT&CK
- Intro to attack.mitre.org

## MITRE's ATT&CK Matrices

- MITRE PRE-ATT&CK threat modelling methodology for pre-exploit activities
- Enterprise Matrix: Windows, MacOS, Linux, Etc.
- Mobile
- ICS

## Mapping Data to ATT&CK

- Small and highly portable detection tests mapped to the MITRE ATT&CK
- Raw Data vs Finished Reports
- Case Studies

## Storing & Analysing the ATT&CK Mapped Data

- MITRE ATT&CK Navigator
- Utilizing the MITRE ATT&CK Matrix
- MITRE ATT&CK Use Cases
- Warming Up Using ATT&CK for Self-Advancement

## Defend with MITRE ATT&CK

- Concept of Active Defense
- MITRE SHIELD
- Defensive Recommendation with SHIELD
- MITRE CAR
- Getting started using MITRE ATT&CK for Threat Hunting
- Different TTP's on attacking Active Directory

## Red Team Emulation

- Install/Setup MITRE Caldera the automated cyber adversary emulation system
- Atomic Red Team Test for MITRE-ATT&CK
- Use Cases using different MITRE LAB Practical

www.infosectrain.com | sales@infosectrain.com