

Online Training 24x7 Availability

# Certified Mitre Att&ck Training

Training for SIEM | SOC Analysts | InfoSec Professionals



Intelligence Analyst



Malware Reverse Engineer



Attack Simulation Specialist



Incident Responder



Security Threat Protection Analyst



Security Program Analyst



# Cyber Threat Intelligence Training for Information Security Professionals

V1

—

# Syllabus: Certified Mitre Att&ck Training

Pre-Requisite: Basic Knowledge of Cyber Threat Intelligence, Network Security concepts and Vulnerability Assessment

**Level:** Intermediate => Advanced

**Training Fee:** 6,000 INR (India Only) 100 USD (International Price)

## Why you Join us :

01. **Certified and Experienced Instructors**
02. **40 Hours of Online Live Instructor-Led Training**
03. **Personalized Training for Individuals and Corporates**
04. **Weekdays and Weekends Training Schedule Available**
05. **Live training session along with their recording will be provided**
06. **Post-training completion, you will be awarded 15 CPE credits.**



### ON DEMAND TRAINING

Learn on Your Own Time  
1-to-1 learning  
Customized Solutions

[CONTACT US](#)



### ONLINE TRAINING

Flexibility, Convenience & Time Saving  
More Effective  
Learning Cost Savings

[ENROLL NOW](#)



### CORPORATE TRAINING

Anytime, Anywhere – Across The Globe  
Hire A Trainer  
At Your Own Pace  
Customized Corporate Training

[CONTACT US](#)

## Why SIEM Intelligence™



Certified | Experienced  
InfoSec Instructors



Post Training Support



Tailor Made Training



Flexible Schedule



Access to the  
Recorded Sessions

## MITRE ATT&CK Training will be Focused on

- MITRE ATT&CK – Cyber Attack Lifecycle
- Pyramid of pain
- MITRE PRE-ATT&CK threat modelling methodology for pre-exploit activities
- MITRE's ATT&CK Matrix
- Small and highly portable detection tests mapped to the MITRE ATT&CK
- MITRE ATT&CK Navigator
- How to use the MITRE ATTACK framework defensively
- Install/Setup MITRE Caldera the automated cyber adversary emulation system
- Utilizing the MITRE ATT&CK Matrix
- MITRE ATT&CK Use Cases
- Warming Up. Using ATT&CK for Self-Advancement
- Getting started using MITRE ATT&CK for Threat Hunting
- Different TTP's on attacking Active Directory
- Atomic Red Team Test for MITRE-ATT&CK

## Introduction to Mitre Att&ck

- Intro to [attack.mitre.org](https://attack.mitre.org)
- What is the MITRE ATT&CK Framework?
- Where is the MITRE ATT&CK Framework Being Used?
- ATT&CK Tactics, Techniques, and Procedures
- Matrices of ATT&CK
  - Enterprise ATT&CK
  - Pre-ATT&CK
  - Mobile ATT&CK
- Preparing the Development Environment
  - Setting up a version control center (GitHub)
  - Downloading a project that hosts a to-do list system of data
  - Installing and configuring ATT&CK Navigator
  - Navigation and Review

## Introduction to Threat Informed Defense

- What Is A Threat Informed Defense?
- Cyber Threat Intelligence Analysis
- Defensive Engagement Of The Threat
- Focused Sharing and Collaboration

## Threat Intelligence

- ATT&CK Threat Groups Page
- MITRE ATT&CK Navigator
- Industry Search For More Mature Organizations

## Detection and Analytics

- Detection Process
- Analytics Process
- Collect Data
- Analyze Data
- Expand and Customize Analytics

## Initial Access

- What is Initial Access?
- External Remote Services
- Spearphishing Link
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Initial Access Case Study

## Execution

- What is Execution?
- Command Line Interface
- Execution Through API
- Control Panel Items
- Powershell
- Scripting
- User Execution
- Execution Case Study

## Persistence

- What is Persistence?
- Accessibility Features
- Bootkit
- Browser Extension
- Component Firmware
- Create Account
- Hooking
- New Service
- Persistence Case Study

## Privilege Escalation

- What is Privilege Escalation?
- Access Token Manipulation
- Elevation Escalation with Prompt
- Exploitation for Privilege Escalation
- File System Permission Weakness
- Scheduled Task
- Sudo

- Web Shell
- Privilege Escalation Case Study

## Defense Evasion

- What is Defense Evasion?
- Clear Command History
- Compile After Delivery
- Disabling Security Tools
- Hidden Files and Directories
- Hidden Users
- Process Hollowing
- Software Packing
- Defense Evasion Case Study

## Credential Access

- What is Credential Access?
- Bash History
- Brute Forces
- Credential Dumping
- Steal Web Session Cookie
- Credential Access Case Study

## Discovery

- What is Discovery?
- Account Discovery
- Browser Bookmark Discovery
- System Owner/User Discovery
- Discovery Case Study

## Lateral Movement

- What is Lateral Movement?
- Application Deployment Software
- Exploitation of Remote Services
- SSH Hijacking
- Lateral Movement Case Study

## Collection

- What is Collection?
- Audio Capture
- Clipboard Data
- Data from Local System
- Collection Case Study

## Command and Control

- What is Command Control?
- Commonly Used Port
- Custom Command and Control Protocol
- Uncommonly Used Ports
- Command and Control Case Study

## Exfiltration

- What is Exfiltration?
- Automated Exfiltration
- Data Compressed
- Data Transfer Size
- Data Transfer Limits
- Exfiltration Case Study

## Impact

- What is Impact?
- Account Access Removal
- Defacement
- Impact Case Study

## Monitoring a compromised system (WMI)

- Instating command line scripts to conduct a lateral attack
- Utilizing ATT&CK Navigator to identify the compromise
- Assessing the compromise through the ATT&CK framework
- Performing process monitoring
- Documenting and patching the holes in the defense architecture

## Monitoring a compromised system (EternalBlue)

- Instating command line scripts to conduct a lateral attack
- Utilizing ATT&CK Navigator to identify the compromise
- Assessing the compromise through the ATT&CK framework
- Performing process monitoring
- Documenting and patching the holes in the defense architecture

## Lab Exercises - MITRE ATT&CK Framework

- Lab 1: Mapping to ATT&CK from finished reporting
- Lab 2: Mapping to ATT&CK from raw data
- Lab 3: Storing and analyzing ATT&CK-mapped intel
- Lab 4: Making ATT&CK-mapped data actionable with defensive recommendations



**\*Contact us :**

-----

- Need technical assistance? Speak with a support representative by calling **+91-7737.131.337**

“