SYLLABUS

12 Weeks. 55+ Topics.

A complete path from threat intelligence foundations to operational tradecraft. Every week builds toward one of six real deliverables, from a threat actor profile report to a full intelligence platform build, so you finish job ready.

#ThreatIntelligence #OSINT #MalwareIntel #ThreatHunting #MITREATTCK

03	12	55+	06
MONTHS	WEEKS	TOPICS	DELIVERABLES

PROGRAM PHASES

01

Foundations

Weeks 01 to 04. Understand the discipline, then collect and analyse intelligence.

02

Advanced

Weeks 05 to 08. Track infrastructure, study malware and hunt for threats.

03

Tradecraft

Weeks 09 to 11. Dark web, leaked credentials, ransomware and platform building.

04

Capstone

Week 12. Automate the workflow and run a full intelligence operation.

info@techonquer.org · +91 6367098233

ELIGIBILITY

Who can join this course

This program is built for anyone who wants to move into threat intelligence, whether you are starting from a security foundation or coming in fresh. No prior intelligence experience is required, only a genuine interest in how threats are tracked and understood.

Students and freshers

Anyone from a computer science, IT or cybersecurity background who wants to enter threat intelligence as a first career path.

SOC analysts

Analysts already working in a Security Operations Center who want to move from alert triage into intelligence driven work.

IT and network professionals

Working professionals from IT, networking or system administration backgrounds who want to shift into cybersecurity.

Security enthusiasts

Self-taught learners with basic networking and security knowledge who want a structured, job-focused path forward.

RECOMMENDED BEFORE YOU START

- Basic understanding of networking concepts such as IP addresses, DNS and ports
- Familiarity with how the internet and web infrastructure work
- Comfort using a computer at a technical level, no coding experience required
- Curiosity about how attackers operate and how that behaviour is tracked

M01 · Foundations

Week 01 of 12

Introduction to Threat Intelligence

This is where the discipline itself gets defined. Before you can collect or analyse anything, you need a working vocabulary: what separates raw data from information, and information from intelligence that is actually decision ready. The module walks through the four types of threat intelligence, strategic, operational, tactical and technical, so you can tell which one a given piece of reporting belongs to and why that matters for who reads it. It closes with the intelligence lifecycle, the direction, collection, processing, analysis and dissemination loop that every later module in this program plugs into, plus a grounding tour of the current threat landscape.

WHAT YOU WILL COVER

- What is threat intelligence
- Data vs information vs intelligence
- Types of TI: strategic, operational, tactical, technical
- Intelligence lifecycle
- Threat landscape overview

PRACTICAL LAB

Reading threat reports

Read a public threat report the way an analyst does, and pull out its type, confidence level and audience.

M02 · Foundations

Week 02 of 12

Threat Actors and APTs

Intelligence is ultimately about people and groups, not just indicators, so this week moves from the landscape into the adversaries themselves. You will learn how threat actors are classified, from opportunistic criminals to state sponsored Advanced Persistent Threat groups, and how their behaviour gets documented in a structured, repeatable way. The MITRE ATT&CK framework and the Cyber Kill Chain are introduced as the two shared languages the industry uses to describe an attack, and you will practise breaking an intrusion down into its Tactics, Techniques and Procedures.

WHAT YOU WILL COVER

- Threat actor types
- MITRE ATT&CK framework
- TTPs: tactics, techniques, procedures
- APT groups overview
- Cyber Kill Chain

PRACTICAL LAB

Mapping an APT to ATT&CK

Take a real APT profile and plot its known behaviour onto the ATT&CK matrix, tactic by tactic.

M03 · Foundations

Week 03 of 12

Intelligence Collection and Feeds

No analysis is better than the collection that feeds it, so this module covers where intelligence actually comes from. You will work through the major collection disciplines, OSINT, TECHINT, HUMINT and SOCMINT, and understand what each one is genuinely good and bad at. Alongside that, the module introduces commercial and open intelligence feeds and the discovery tooling named in the syllabus, Shodan, Censys, theHarvester and SpiderFoot, so you can start building a repeatable collection pipeline.

WHAT YOU WILL COVER

- OSINT
- TECHINT
- HUMINT
- SOCMINT
- Dark web intelligence
- Intelligence feeds
- Shodan, Censys, theHarvester, SpiderFoot

PRACTICAL LAB

Building a collection pipeline

Combine two or more collection sources into one pipeline you can reuse in later modules.

info@techonquer.org · +91 6367098233

M04 · Foundations

Week 04 of 12

Analysis and Reporting

This is the module that turns everything collected so far into something a decision maker can actually use. You will learn structured analytic techniques including Analysis of Competing Hypotheses, a method for testing your own assumptions instead of confirming the first theory that fits, along with link analysis and timeline analysis for mapping relationships and sequences of events. The module also covers confidence levels, professional report writing, and the technical side of extracting IOCs and writing your first YARA and Sigma rules.

WHAT YOU WILL COVER

- Structured analytic techniques
- Analysis of Competing Hypotheses (ACH)
- Link analysis
- Timeline analysis
- Intelligence confidence levels
- Intelligence report writing
- IOC extraction
- YARA basics
- Sigma rules

PRACTICAL LAB

Full intelligence cycle simulation

Run one dataset through collection, analysis and reporting end to end, and write a short brief.

M05 · Advanced

Week 05 of 12

Infrastructure Tracking

Attackers reuse infrastructure far more than they would like you to think, and this module teaches you to exploit that habit. You will learn to pull domain intelligence and passive DNS history to see how a domain has been used over time, track SSL and TLS certificates as a fingerprint that follows an actor across different hostnames, and correlate IP addresses across campaigns rather than treating a single indicator as the whole finding.

WHAT YOU WILL COVER

- Domain intelligence
- Passive DNS
- SSL/TLS certificate tracking
- IP correlation
- Infrastructure fingerprinting

PRACTICAL LAB

Complete infrastructure mapping

Start from a single domain and build out a full infrastructure map using DNS and certificate history.

info@techonquer.org · +91 6367098233

M06 · Advanced

Week 06 of 12

Attribution and Infrastructure Analysis

Building on last week's infrastructure work, this module moves toward the harder question of who is actually behind an operation. You will learn the attribution techniques analysts use to connect infrastructure back to a specific actor or group, including geolocation signals and language analysis. Attribution is treated as probabilistic here, not absolute, so the emphasis is on a defensible chain of correlated evidence rather than jumping straight to a name.

WHAT YOU WILL COVER

- Attribution techniques
- Geolocation and language analysis
- Infrastructure correlation and mapping

PRACTICAL LAB

Complete infrastructure mapping

Extend last week's map with attribution signals and document your confidence in each connection.

info@techonquer.org · +91 6367098233

M07 · Advanced

Week 07 of 12

Malware Intelligence

Malware is one of the richest sources of threat intelligence available, if you know how to read it. This module starts with malware types and families, then moves into the practical difference between static analysis and dynamic analysis in a sandbox. You will study how malware communicates with its command and control infrastructure, what that traffic tends to look like on the wire, and how to connect samples back to a broader campaign.

WHAT YOU WILL COVER

- Malware types and families
- Static vs dynamic analysis
- Sandbox analysis
- Behavioral analysis
- C2 communication patterns
- Network traffic analysis

PRACTICAL LAB

Malware campaign tracking

Take a sample from initial triage through to identifying which broader campaign it belongs to.

info@techonquer.org · +91 6367098233

M08 · Advanced

Week 08 of 12

Threat Hunting and Detection

This is where intelligence stops being descriptive and starts being used to actively find things. You will learn three approaches to hunting, hypothesis driven, IOC based and TTP based, hunting for behaviour patterns instead of static artifacts. The second half of the module is hands-on detection engineering, taking what you find and turning it into durable Sigma and YARA rules that keep catching the same behaviour long after the hunt is over.

WHAT YOU WILL COVER

- Hypothesis-driven hunting
- IOC-based hunting
- TTP-based hunting
- Anomaly detection
- Detection engineering
- Sigma rules deep dive
- YARA rules deep dive

PRACTICAL LAB

Full hunt simulation

Run a complete hunt from hypothesis to a working detection rule against a simulated environment.

M09 · Tradecraft

Week 09 of 12

Dark Web Intelligence

The tradecraft phase opens with the part of the internet most collection tools never touch. This module covers how to access and monitor dark web sources safely and responsibly, and how to build a structured, repeatable process for watching underground forums over time rather than making one-off visits, while keeping yourself and your organisation safe throughout.

WHAT YOU WILL COVER

- Dark web intelligence
- Underground forum monitoring

PRACTICAL LAB

Underground forum monitoring

Set up a structured, safe process for tracking activity on an underground forum over time.

info@techonquer.org · +91 6367098233

M10 · Tradecraft

Week 10 of 12

Credential and Ransomware Intelligence

Two of the most operationally urgent intelligence areas in the field get their own dedicated week. You will learn how leaked credentials move through breach dumps, combolists and stealer logs, and how to track that exposure back to real organisational risk. Alongside that, the module covers ransomware intelligence, following the ecosystem of ransomware groups, their leak sites and their negotiation behaviour.

WHAT YOU WILL COVER

- Leaked credential tracking
- Ransomware intelligence

PRACTICAL LAB

Threat intelligence investigation

Combine credential exposure and ransomware group tracking into one focused investigation.

info@techonquer.org · +91 6367098233

M11 · Tradecraft

Week 11 of 12

Intelligence Platform

Everything you have collected and analysed so far has lived in notes, spreadsheets and one-off reports. This module moves that work into a real intelligence platform, so it can be shared, searched and correlated automatically. You will get hands-on with MISP for structured indicator sharing and OpenCTI for connecting intelligence into a knowledge graph, thinking about a platform as the backbone of a team's program, not one analyst's archive.

WHAT YOU WILL COVER

- Building an intelligence platform
- MISP
- OpenCTI

PRACTICAL LAB

Building the intelligence platform

Stand up a working MISP or OpenCTI instance and load in indicators from earlier modules.

info@techonquer.org · +91 6367098233

M12 · Capstone

Week 12 of 12

Automation and Capstone

The program closes by making everything you have learned repeatable at scale. You will use Python to automate the parts of the intelligence workflow that do not need a human in the loop, so your time goes toward analysis instead of manual data entry. The capstone then asks you to run a full intelligence operation end to end, collection, analysis, infrastructure tracking, reporting and platform entry, against a realistic scenario.

WHAT YOU WILL COVER

- Automation with Python
- Capstone: full intelligence operation

PRACTICAL LAB

Capstone: full intelligence operation

Run the entire intelligence cycle end to end against a realistic scenario as your final deliverable.

TECHNICAL TOOLKIT

The technical ecosystem covered in the syllabus

Named technologies and methodologies, preserved from the source curriculum.

Frameworks and analytic methods

- MITRE ATT&CK
- Cyber Kill Chain
- Structured analytic techniques
- ACH

Collection and discovery

- OSINT
- TECHINT
- HUMINT
- SOCMINT
- Shodan
- Censys
- theHarvester
- SpiderFoot

Detection

- YARA
- Sigma

Intelligence platforms

- MISP
- OpenCTI

Infrastructure analysis

- Passive DNS
- SSL/TLS certificate tracking
- IP correlation
- Infrastructure fingerprinting

Advanced intelligence

- Dark web intelligence
- Underground forum monitoring
- Leaked credential tracking
- Ransomware intelligence
- Automation with Python

CAREER OUTCOMES

What you can become after this course

By the end of the twelve weeks you will have six real deliverables in hand and a working knowledge of the full intelligence cycle. That combination opens up roles across the defensive and intelligence side of cybersecurity.

- **Cyber Threat Intelligence Analyst**
  Track adversaries, build actor profiles and turn raw indicators into reporting that decision makers actually use.
- **SOC Analyst (L2 / L3)**
  Move beyond alert triage into intelligence-informed investigation using ATT&CK, IOCs and structured analysis.
- **Threat Hunter**
  Proactively search environments for hidden threats using hypothesis-driven and TTP-based hunting techniques.
- **Malware Intelligence Analyst**
  Analyse malware samples, trace C2 infrastructure and connect individual samples back to broader campaigns.
- **OSINT Investigator**
  Run open source investigations using Shodan, Censys, theHarvester and SpiderFoot for reconnaissance and attribution.
- **Detection Engineer**
  Write and maintain YARA and Sigma rules that turn hunt findings into durable, reusable detections.
- **CTI Platform Engineer**
  Build and run threat intelligence platforms like MISP and OpenCTI as the shared backbone for a security team.

FINAL DELIVERABLES

What the syllabus specifies you will produce

These six deliverables are listed explicitly in the source syllabus.

01 **Threat actor profile report**

02 **Infrastructure map**

03 **Malware campaign report**

04 **Detection rules (YARA / Sigma)**

05 **Full intelligence platform**

06 **Capstone operation report**

Program format: 3 months, 12 weeks.

The 12 week structure organises the requested course duration while keeping the source syllabus terminology, topics and practical outputs intact.

info@techonquer.org · +91 6367098233