

Course Title: Threat Intelligence

LTPC: 3-0-2-4

Dr. Ashu Sharma,

Founder CyberSecSociety

WHAT IS CYBER THREAT INTELLIGENCE (CTI) ?

- Cyber Threat Intelligence (CTI) is the **precise and contextualized information** about **emerging or existing cyber threats** that have been refined and analyzed to provide **actionable advice** which allows the organizations to take informed **decision to proactively defend or mitigate** any cyber threats.

WHAT IS CYBER THREAT INTELLIGENCE (CTI) ?

- Red Team
- Blue team
- Purple team
- White team

Topics to be covered

Introduction to Cyber Threat Intelligence(CTI):

- Understanding about the Intelligence,
- Definition and History of CTI,
- Concept behind the CTI,
- Requirements of CTI, Stages of CTI,
- Types of CTI, CTI Frameworks
- Lifecycle, Benefits of CTI and How CTI help the organization.

Topics to be covered

Cyber Kill Chain Methodology and Threats: -

- Cyber Threats overview, Categories of Cyber Threats,
- Understanding Cyber kill chain methodology,
- techniques
- procedures, Scenario of Kill Chain Deep Dive.

Topics to be covered

CTI Requirements, Planning and Review: -

- Understanding Organization's Current Threat Landscape,
- requirements of CTI Analysis,
- Planning of Threat Intelligence Program,
- Threat Intelligence Team building,
- Cyber Threat Intelligence Program Review.

Cyber Threat Intelligence Data Collection and It's Processing: -

Topics to
be covered

- Introduction of CTI Data Collection, Methods of Data Collection,
- Data Types, CTI Data Collection Management,
- Describe the Data Collection through different methods,
- Data Collection in Bulk,
- Data Collection Processing.

Topics to be covered

CTI Data Analysis: -

- Introduction of Data Analysis,
- Techniques of Data Analysis,
- Understanding of Threat Analysis,
- Process of Threat Analysis,
Perform Threat Modeling,
- Methodologies
of Threat Modeling,
- Evaluation of Threat Intelligence.

Topics to be covered

Understating Report and Dissemination of Cyber Threat Intelligence: -

- Introduction of CTI Reports, Types of CTI Reports,
- Template of CTI Report, Overview of Dissemination,
- Preferences for Dissemination, Operational of Dissemination,
- Sharing Intelligence Benefits, Challenges,
- Overview of Sharing CTI, CTI Sharing Platforms,
- CTI Acts and Regulations,
- CTI Integration,
- Overview of Delivery Mechanisms.

Expectation

Evaluation scheme- not yet decided

Weight on theory & Practical- suggestion??

Classes timings ; Monday series 6:00pm – 7:00pm

Theory Session timings ; weekdays

Lab timings ; weekend (mostly on Saturday) 6:00pm to 8:00pm

Projects; deadline: last day of lectures