Advent Of Cyber 2022 Day-1 FrameWorks

Security frameworks are documented processes that define policies and procedures organisations should follow to establish and manage security controls. They are blueprints for identifying and managing the risks they may face and the weaknesses in place that may lead to an attack.

NIST Framework

The Cybersecurity Framework (CSF) was developed by the National Institute of Standards and Technology (NIST)

The framework focuses on five essential functions:

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover.**

ISO27000 Series

The International Organization of Standardization (ISO)

The ISO 27001 and 27002 standards are commonly known for cybersecurity and outline the requirements and procedures for creating, implementing and managing an information security management system (ISMS).

MITRE ATT&CK

The MITRE ATT&CK framework is a knowledge base of TTPs, commonly known as Tactics, Techniques and Procedures carefully curated and detailed to ensure security teams can identify attack patterns.

CyberKill Chain

This framework was adopted from the military with the terminology kill chain.
Developed by Lockheed Martin
Stages:

- **Recon**
- **Weaponization**
- **Delivery**
- **Exploitation**
- **Installation**
- **Command & Control**
- **Actions On Objectives**

Unified KillChain

The Unified Kill Chain can be described as the unification of the MITRE ATT&CK and Cyber Kill Chain frameworks. Published by Paul Pols in 2017
The Unified Kill Chain describes 18 phases of attack based on Tactics, Techniques and Procedures (TTPs). The individual phases can be combined to form overarching goals, such as gaining an initial foothold in a targeted network, navigating through the network to expand access and performing actions on critical assets.

CYCLE-1

Reconnaissance
Weaponisation
Delivery
Social Engineering
Exploitation
Persistence
Defence Evasion
Command & Control

IN

CYCLE-2

Pivoting
Discovery
Privilege Escalation
Execution
Credential Access
Lateral Movement

THROUGH

CYCLE-3

Collection
Exfiltration
Impact
Objectives

OUT

Prathamesh Satam
https://t.me/cybersecuritycare
https://instagram.com/cyber.mesh?igshid=ZDdkNTZiNTM=