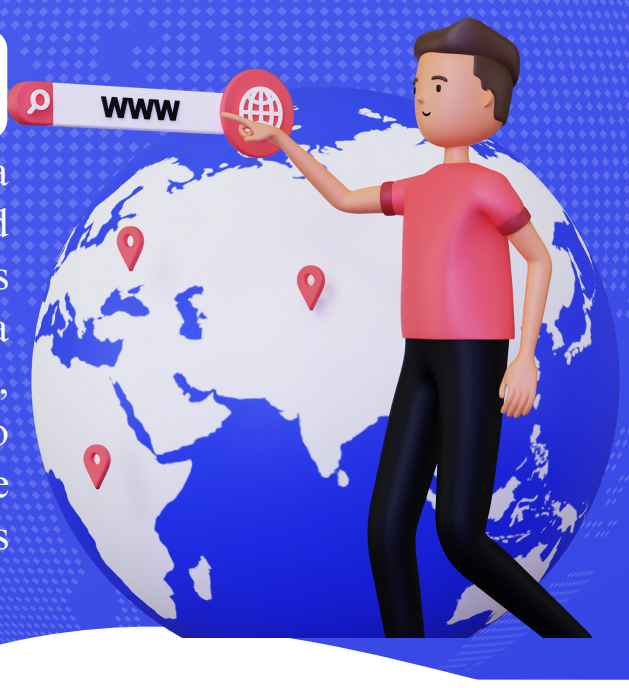
Virus and Malware Security

(DoS) this refers to an attack intended to flood a target system by overwhelming its capacity and rendering it inaccessible to legitimate users. This is achieved through sending large volumes of data requests, exploiting vulnerabilities to crash services, or flooding networks with traffic. The aim is to disrupt normal operations attacks that can be launched from a single source or coordinated across multiple devices (DDoS), amplifying their impact.



Malware and it Works.

Malware is a harmful program designed to infiltrate, disrupt, or damage computer systems and networks. It operates by exploiting vulnerabilities in software or tricking users into installing it. Once installed, malware can execute various malicious activities like stealing sensitive information,corrupting files, remotely controlling the infected system. Such malware can be categorized into different forms viruses, worms, Trojan horses, ransomware, and spyware. Malware can be spread through emails with attachments, websites that have been compromised,USB drives infected by malicious software. The main purpose is the appropriation of unauthorized access, resulting in damage or financial cyber criminals.

Malware & virus Mitigation at Application Level

1. Implement strong authentication systems such as (Multi-Factor Authentication) to confirm the user's identity who is residing on to your application.
2. Perform validation and filtering of all input data to protect against illegal injection attacks, like SQL injection, cross-site scripting (XSS), and command injection.
3. Implement whitelisting to authenticate only software permitted to run on your system thus mitigating software execution without any authorization
4. Encrypt data transiting across the network using algorithm such as SHA-1.

Virus and Malware Mitigation at Network Level

01.Consider using application whitelisting to only allow approved programs to run on your system, reducing the risk of malware execution.

02. Consider deploying into your system Endpoint Detection and Response (EDR).

03. Turn on the firewall of your system to discover and control traffic across the network from receiving and outgoing packets

04. Select popular antivirus software and ensure that it is up-to-date by installing the latest updates as they are released. Antivirus software is capable of detecting and removal of malwares that are identified by now.

05. Don't open any email attachments if they came from someone you don't know or the sender seem to be suspicious. The trojan horse in spam emails that use attachment or phishing links is the malware.

Causes of Virus and Malware

1. Phishing attacks: Through malicious email links.
2. Weak passwords: These are susceptible and easy to crack.
3. Sophisticated and targeted attacks by skilled hackers aiming to infiltrate specific organizations.
4. Users may inadvertently download and install malware disguised as legitimate software