

Prevent known threats

Blacklists

Reputation systems

Threat intelligence

Signature based network and endpoint methods

IPS = Intrusion Prevention Systems

Virtual keyboards

URL blockers

Host based firewalls

File and disk encryption

Parental control

Prevent unknown threats

Exploit prevention

Sandboxes

Isolation and compartmentalization

Application whitelisting

Access Control Lists

Software restriction Policies (SRP)

User Access Control (UAC)

Detect known threats

Antivirus

IDS = Intrusion detection system (snort)

HIDS = Host based intrusion detection systems

Web app Firewalls (WAF)

Vulnerability scanning

Anti-spam

Traffic monitoring

Detect unknown threats

Behavioral analysis

Machine learning

Heuristic detection

Canary Tokens

Respond /Recover

Backups

Snapshots

Roll-back

Automated response and remediation


Anti-virus

siem

Links

- <https://www.snort.org/>
- <https://zeek.org/>
- <https://github.com/thinkst/opencanary>
- <https://www.ossec.net/download-ossec/>
- <https://nst.sourceforge.net/nst/>
- <https://cybersecurity.att.com/products/ossim>

OSI model

 Cybersecurity Threats in OSI Model		
OSI Layer	 Functions	 Attack vectors
Application Layer	<ul style="list-style-type: none">✓ User interface & app-level service✓ Web browsing, email, file transfer✓ HTTP, SMTP, DNS protocols	<ol style="list-style-type: none">1 Malware injection2 Phishing attacks3 App-level DDoS attacks
Presentation Layer	<ul style="list-style-type: none">✓ Data encryption and decryption✓ Data compression and expansion✓ Data format conversion	<ol style="list-style-type: none">1 Attack for weak encryption2 File format exploits3 Malicious code injection
Session Layer	<ul style="list-style-type: none">✓ Create & terminate app sessions✓ Manage session state✓ Video conferencing session	<ol style="list-style-type: none">1 Session hijacking & replay2 Session fixation attack3 Cross-site request forgery
Transport Layer	<ul style="list-style-type: none">✓ End-to-end data delivery✓ TCP and UDP protocols✓ Error correction & congestion ctrl	<ol style="list-style-type: none">1 TCP/SYN & UDP flood attack2 TCP hijacking & MiTM attack3 Port scan for vulnerability
Network Layer	<ul style="list-style-type: none">✓ Routing and IP addressing✓ IPv4, IPv6 and routing protocols✓ IP network configuration	<ol style="list-style-type: none">1 IP spoofing & fragmentation2 Ping of death & ICMP flood3 Route poisoning attacks
Data Link Layer	<ul style="list-style-type: none">✓ Frames and physical addressing✓ Error detection and correction✓ Switching & VLAN configuration	<ol style="list-style-type: none">1 ARP spoofing & poisoning2 STP attack & MAC spoofing3 Wireless vulnerability attacks
Physical Layer	<ul style="list-style-type: none">✓ Electrical/optical signaling✓ Ethernet cables and fiber optics✓ Physical layer configuration	<ol style="list-style-type: none">1 Wiretapping & tampering2 Signal jamming3 Unauthorized device install