From ***Internet***

Cybersecurity Layers

1. Perimeter Security Layer

What It Does: Protects the organization's network from external threats by controlling what enters and exits the network.

Examples:

- **Firewalls: Filter incoming and outgoing traffic to block unauthorized access.**
  - ***Examples*: Cisco ASA, Palo Alto Networks Firewalls**
- **Intrusion Detection Systems (IDS): Monitors network traffic for suspicious activity.**
  - ***Examples*: Snort, Suricata**
- **Intrusion Prevention Systems (IPS): Actively prevents detected threats from entering the network.**
  - ***Examples*: Cisco Firepower, McAfee Network Security**
- **Virtual Private Network (VPN): Secures remote access to the network by encrypting data.**
  - ***Examples*: OpenVPN, Cisco AnyConnect**
- **Web Application Firewalls (WAF): Protects web applications from threats like SQL injection and cross-site scripting (XSS).**
  - ***Examples*: Cloudflare, AWS WAF**

2. Network Security Layer

What It Does: Secures the internal network by preventing unauthorized access, detecting threats, and ensuring the integrity of communications.

Examples:

- **Network Access Control (NAC): Ensures that only authorized devices can access the network.**
    - ***Examples*: Cisco ISE, Aruba ClearPass**
- **Segmentation: Divides the network into smaller, isolated segments to contain threats.**
    - ***Examples*: VLANs, Firewalls**
- **IDS/IPS: Monitors network traffic and prevents intrusions.**
    - ***Examples*: Snort, Suricata, Cisco Firepower**
- **VPNs: Encrypts network traffic for secure communication over public networks.**
    - ***Examples*: OpenVPN, Cisco AnyConnect**

3. Endpoint Security Layer

What It Does: Secures devices such as laptops, desktops, and mobile phones that access the network, ensuring that they are protected from malware and unauthorized access.

Examples:

- **Antivirus/Antimalware: Protects against malicious software and malware.**
    - ***Examples*: Symantec, McAfee, Windows Defender**
- **Endpoint Detection and Response (EDR): Detects and responds to threats on endpoints.**
    - ***Examples*: CrowdStrike, Carbon Black, SentinelOne**
- **Mobile Device Management (MDM): Manages and secures mobile devices that access the network.**
    - ***Examples*: VMware AirWatch, MobileIron**

4. Application Security Layer

What It Does: Secures software applications from vulnerabilities that could be exploited by attackers.

Examples:

- **Web Application Firewalls (WAF): Protects web applications from common attacks like SQL injection.**
    - ***Examples*: Cloudflare, AWS WAF**
- **Static/Dynamic Application Security Testing (SAST/DAST): Scans code for vulnerabilities during development.**
    - ***Examples*: Veracode, Checkmarx, Burp Suite**
- **Secure Code Review: Manual or automated review of code to find security flaws.**
    - ***Examples*: GitHub security features, SonarQube**

---

5. Data Security Layer

What It Does: Protects data both at rest (stored) and in transit (during communication) from unauthorized access and breaches.

Examples:

- **Encryption: Encrypts data to ensure confidentiality and integrity.**
    - ***Examples*: AES, TLS/SSL**
- **Data Loss Prevention (DLP): Monitors and prevents unauthorized data transfer.**
    - ***Examples*: Symantec DLP, Digital Guardian**
- **Backup and Recovery: Ensures that data is regularly backed up and recoverable in case of an attack or disaster.**
    - ***Examples*: Veeam, Acronis**

---

6. Identity and Access Management (IAM) Layer

What It Does: Manages user identities and controls access to network resources based on roles and policies.

Examples:

- **Multi-Factor Authentication (MFA): Requires multiple verification methods before granting access.**
    - ***Examples*: Google Authenticator, Microsoft Authenticator**
- **Single Sign-On (SSO): Allows users to authenticate once and gain access to multiple systems.**
    - ***Examples*: Okta, Microsoft Azure AD**
- **Role-Based Access Control (RBAC): Assigns access based on roles to limit user permissions.**
    - ***Examples*: Azure AD, AWS IAM**

---

7. Cloud Security Layer

What It Does: Secures cloud-based infrastructures, applications, and data, protecting them from threats unique to cloud environments.

Examples:

- **Cloud Access Security Brokers (CASB): Enforces security policies for cloud services.**
    - ***Examples*: Netskope, McAfee MVISION**
- **Cloud Firewalls: Protects cloud resources from malicious access.**
    - ***Examples*: AWS Security Groups, Azure Firewall**
- **Cloud Security Posture Management (CSPM): Ensures compliance and secures cloud configurations.**
    - ***Examples*: Prisma Cloud, Dome9**

---

8. Monitoring and Response Layer

What It Does: Monitors network traffic and system activities in real-time to detect, investigate, and respond to incidents quickly.

Examples:

- **Security Information and Event Management (SIEM): Collects and analyzes security logs to detect threats.**
  - ***Examples*: Splunk, IBM QRadar**
- **Security Orchestration, Automation, and Response (SOAR): Automates response actions and orchestrates incident management workflows.**
  - ***Examples*: Palo Alto Networks Cortex XSOAR, Splunk Phantom**
- **Endpoint Detection and Response (EDR): Detects and investigates security threats on endpoints.**
  - ***Examples*: CrowdStrike Falcon, SentinelOne**

---

9. Security Awareness and Training Layer

What It Does: Educates employees and users on cybersecurity best practices, potential threats, and how to avoid common risks.

Examples:

- **Phishing Simulations: Simulates phishing attacks to train users on how to identify suspicious emails or messages.**
  - ***Examples*: KnowBe4, Cofense**
- **Security Awareness Programs: Provides regular training sessions and resources to educate employees on cybersecurity threats and best practices.**
  - ***Examples*: SANS Security Awareness, CybSafe**
- **Compliance Training: Educates users on industry-specific regulations and security compliance, such as GDPR or HIPAA.**

  - ***Examples*: Proofpoint, Infosec Skills**

- **Password Management Training: Educates employees on creating strong passwords and using password managers to store them securely.**

  - ***Examples*: LastPass, Dashlane**