Defensive Security – Complete Guide with Diagrams

1. What is Defensive Security?

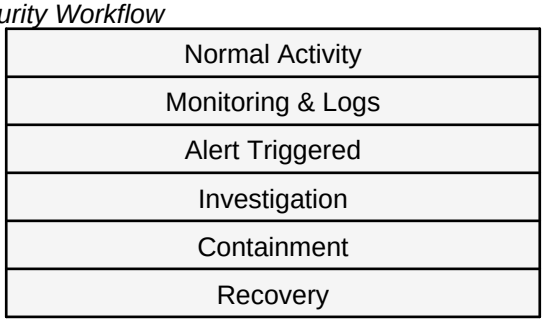
Defensive Security is the cybersecurity discipline focused on protecting systems, networks, and data from attacks. It ensures confidentiality, integrity, and availability by preventing threats, detecting malicious behavior, responding to incidents, and recovering systems safely.

Diagram 1: Defensive Security Lifecycle

2. How Defensive Security Works

Defensive security works as a continuous monitoring and response cycle. Systems are observed to establish normal behavior. Any deviation triggers alerts which are analyzed by security teams.

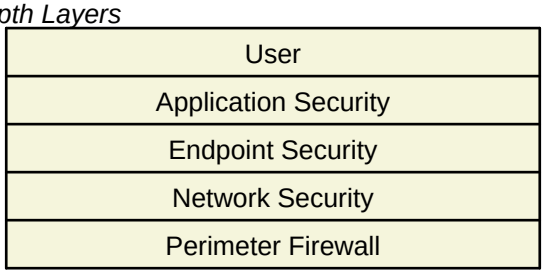
Diagram 2: Defensive Security Workflow



3. Core Functional Components

- Prevention: Firewalls, access control, patching, endpoint protection
- Monitoring: Log collection, SIEM, network visibility
- Detection: IDS/IPS, anomaly detection, threat intelligence
- Incident Response: Identify, contain, eradicate, recover
- Hardening: Configuration fixes, policy updates, lessons learned

Diagram 3: Defense-in-Depth Layers



4. Real-World Use Cases

- Detecting brute-force attacks using authentication logs
- Stopping ransomware by isolating infected endpoints
- Detecting data exfiltration through abnormal traffic
- Monitoring insider threats via behavior analysis
- Ensuring recovery using backups and disaster recovery plans

Diagram 4: SOC Operational Flow