Types of Monitoring in DevOps

**1. Infrastructure Monitoring**  
Infrastructure monitoring involves tracking the performance and health of physical and virtual servers, containers, VMs, and other infrastructure components.  
Focus Areas: CPU usage, memory usage, disk I/O, network I/O, uptime, and availability.  
Tools: Prometheus, Nagios, Zabbix, Datadog.  
Purpose: Ensures that the underlying infrastructure is functioning properly and supports the applications running on it.  
  
**2. Application Performance Monitoring (APM)**APM focuses on monitoring the performance and availability of applications, tracking metrics like response times, error rates, and user satisfaction.  
Focus Areas: End-user experience, transaction tracing, application dependencies.  
Tools: New Relic, Dynatrace, AppDynamics.  
Purpose: Helps in detecting and diagnosing performance issues within applications, ensuring they meet user expectations.  
  
**3. Log Monitoring**  
Log monitoring involves collecting, aggregating, and analyzing logs generated by applications, servers, and network devices.  
Focus Areas: Error logs, access logs, system logs, security logs.  
Tools: ELK Stack (Elasticsearch, Logstash, Kibana), Splunk, Fluentd.  
Purpose: Provides insights into system behavior and helps in troubleshooting issues by analyzing detailed event logs.  
  
**4. Network Monitoring**  
Network monitoring tracks the performance and health of network components such as routers, switches, firewalls, and load balancers.  
Focus Areas: Bandwidth usage, packet loss, latency, network traffic.  
Tools: Nagios, SolarWinds, PRTG Network Monitor.  
Purpose: Ensures that the network infrastructure is operating efficiently, with minimal latency and no bottlenecks.  
  
**5. Security Monitoring**  
Security monitoring involves tracking and analyzing security-related data to detect and respond to potential threats and vulnerabilities.  
Focus Areas: Intrusion detection, firewall logs, authentication logs, security event logs.  
Tools: SIEM tools (Security Information and Event Management) like Splunk, IBM QRadar, and LogRhythm.  
Purpose: Helps in maintaining the security posture of the organization by identifying and mitigating security risks in real-time.