Blue Teaming

Blue Team Operations
- Attack Simulation
- Threat Hunting
- Detection Engineering
- Continuous Monitoring
- Security Automation

Security Monitoring
- Security Alerts
- Security Operations Center (SOC)
- Threat Detection
- Log Monitoring
- Endpoint Monitoring
- Network Monitoring

Compliance and Governance
- Security Awareness Training
- Security Policies
- Security Auditing
- Risk Management
- Regulatory Compliance

Threat Detection
- MITRE ATT&CK Mapping
- SIEM Analysis
- Signature Detection
- Behavior Analysis
- Threat Intelligence
- Anomaly Detection

Identity Security
- Identity Threat Detection
- Access Control
- Account Monitoring
- Multi-Factor Authentication
- Privileged Access Management

Incident Response
- Post-Incident Review
- Incident Identification
- Recovery
- Incident Analysis
- Eradication
- Containment

Security Tools
- Threat Intelligence Platforms
- SIEM Platforms
- Network IDS / IPS
- EDR Platforms
- SOAR Platforms

Log Management
- Log Correlation
- System Logs
- Centralized Logging
- Application Logs
- Authentication Logs
- Network Logs

Threat Intelligence
- Adversary Tracking
- Indicators of Compromise (IOC)
- Malware Analysis
- Indicators of Attack (IOA)
- Threat Feeds

Endpoint Security
- Host Intrusion Detection
- Endpoint Detection and Response (EDR)
- Patch Management
- Antivirus / Anti-Malware
- Device Control

Vulnerability Management
- Configuration Hardening
- Asset Discovery
- Patch Management
- Vulnerability Scanning
- Risk Assessment

Network Security
- VPN Monitoring
- Firewall Monitoring
- DNS Monitoring
- Intrusion Detection System (IDS)
- Network Traffic Analysis
- Intrusion Prevention System (IPS)

www.hackingarticles.in