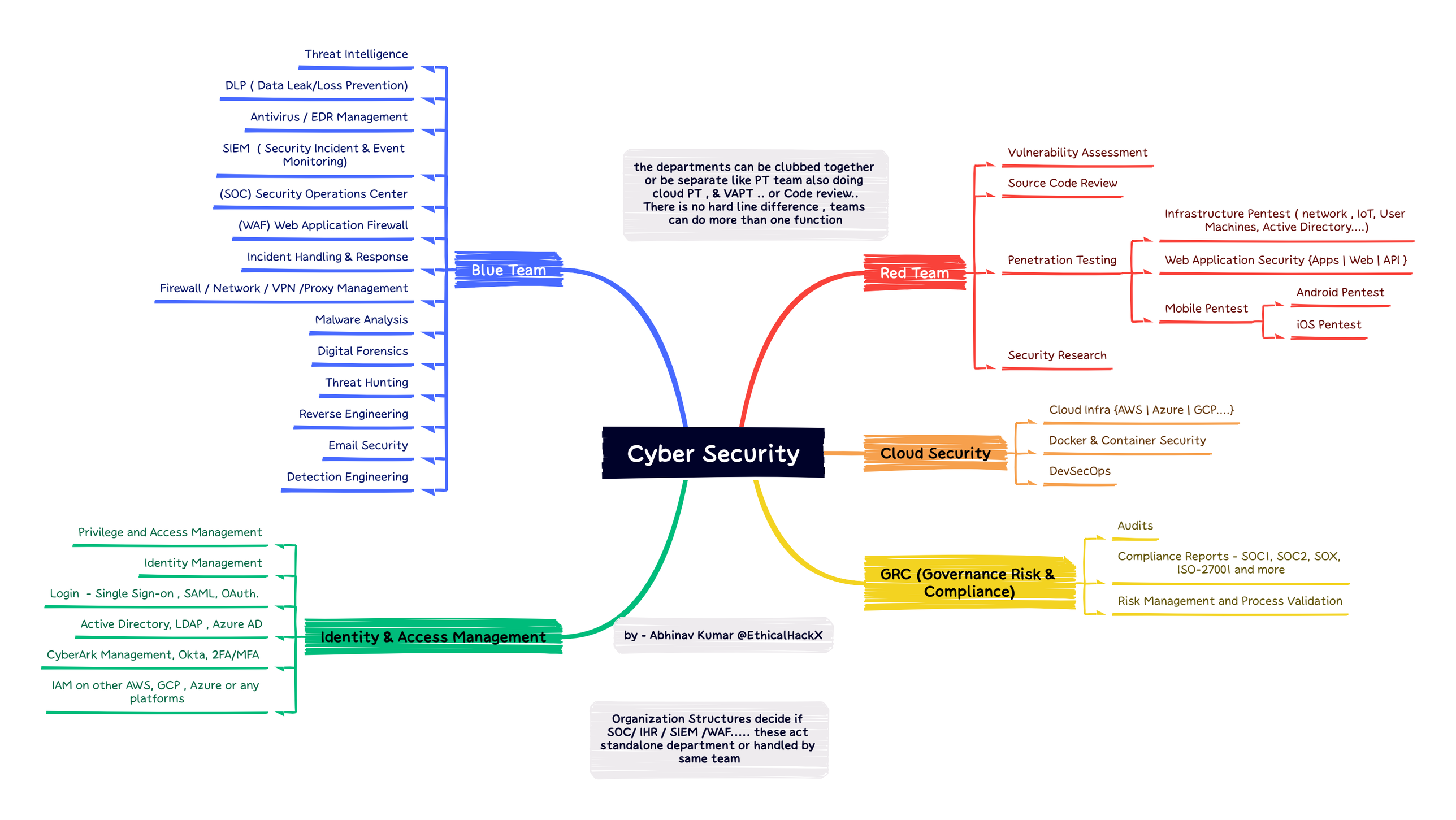
Cyber Security
Blue Team
Threat Intelligence
DLP (Data Leak/Loss Prevention)
Antivirus / EDR Management
SIEM (Security Incident & Event Monitoring)
(SOC) Security Operations Center
(WAF) Web Application Firewall
Incident Handling & Response
Firewall / Network / VPN /Proxy Management
Malware Analysis
Digital Forensics
Threat Hunting
Reverse Engineering
Email Security
Detection Engineering
the departments can be clubbed together or be separate like PT team also doing cloud PT , & VAPT .. or Code review.. There is no hard line difference , teams can do more than one function
Red Team
Vulnerability Assessment
Source Code Review
Penetration Testing
Infrastructure Pentest (network , IoT, User Machines, Active Directory....)
Web Application Security {Apps | Web | API }
Mobile Pentest
Android Pentest
iOS Pentest
Security Research
Cloud Security
Cloud Infra {AWS | Azure | GCP....}
Docker & Container Security
DevSecOps
GRC (Governance Risk & Compliance)
Audits
Compliance Reports - SOC1, SOC2, SOX, ISO-27001 and more
Risk Management and Process Validation
Identity & Access Management
Privilege and Access Management
Identity Management
Login - Single Sign-on , SAML, OAuth.
Active Directory, LDAP , Azure AD
CyberArk Management, Okta, 2FA/MFA
IAM on other AWS, GCP , Azure or any platforms
by - Abhinav Kumar @EthicalHackX
Organization Structures decide if SOC/ IHR / SIEM /WAF..... these act standalone department or handled by same team