Blue Team Tools by Joas and Fabacab
Windows-based defenses
macOS-based defenses
Threat signature packages and collections
Threat intelligence
Threat hunting
Preparedness training and wargaming
Phishing awareness and reporting
Operating System distributions
Network perimeter defenses
Honeypots
Tarpits
Policy enforcement
Compliance testing and reporting
Application or Binary Hardening
Communications security (COMSEC)
Kubernetes
Fuzzing
Distributed monitoring
Cloud Platform Security
DevSecOps
Automation
Code libraries and bindings
Supply chain security
Host-based tools
Sandboxes
Security monitoring
Network Security Monitoring (NSM)
Security Information and Event Management (SIEM)
Incident Response tools
IR management consoles
Evidence collection
Tor Onion service defenses
Transport-layer defenses
Security configurations
SOAR