K>FIVEFOUR™
POWERED BY MARKON

WHERE OPERATORS ARE FORGED—NOT LECTURED

k>fivefour™ delivers **mission-ready cyber operator training** through a unified ecosystem that supports Red Teams, defenders, and emerging cyber leaders. Our ranges, scenarios, and automated adversary simulations give them the **hands-on experience** they need—in the cloud or on-prem—with environments built for real-world threats, not theory.

PROGRESSIVE TRAINING TRACKS

Our training tracks provide a clear, disciplined progression from foundational skills to technical mastery across the full spectrum of cyber operations. Each course builds on the last, immersing operators in hands-on, scenario-driven challenges that develop real mission capability.

MISSION-READY BY DESIGN

- DEFENSIVE CYBER SCENARIOS AND COURSES
- INSTRUCTOR-LED AND SELF-PACED TRAINING OFFERINGS
- ALWAYS-ON, ZERO-INSTALL LAB AND SCENARIO ACCESS
- SCALABLE FROM PERSONAL TO ENTERPRISE USE
- TRUSTED BY DOW, ALLIED NATIONS, AND FORTUNE 500 TEAMS
- BUILT FOR OPERATIONAL RELEVANCE — NOT THEORY

BATTLEGROUNDS™

REALISTIC, ALWAYS-ON ADVERSARY SIMULATION

- Browser-based student and administrator access — no installs required
- Available cloud-hosted or on-prem with the same operator experience
- Seamless delivery of on-demand or instructor-led courses, labs, exams, and scenarios
- Custom AD forests, Linux/Windows hosts, and C2 infrastructure
- Automated adversary simulation for realistic operational pressure
- Team mode with shared environments for collaborative scenarios
- Used across the **k>fivefour** curriculum or available for standalone use

HYDRA™

ON-PREMISES, FULL-STACK, CONTAINERIZED, EXTENSIBLE CYBER RANGE ENABLING ADVANCED CYBER OPERATIONS FROM ANYWHERE

- Realistic Battlegrounds™-enabled training scenarios
- High-availability, clustered, scalable architecture
- Mission-specific customization, including operational technology (OT) and air-gapped enclaves
- Supports multi-role training and exercises
- Automated attack simulation and scoring integrations

SHADOW BREACH™

AUTOMATED & THREAT-INFORMED SIMULATIONS FOR ADVERSARY BEHAVIOR, THREAT REPLICATION, & VULNERABILITY DISCOVERY

- AI simulation creation from CTI, artifacts, and operator input
- Cloud or on-premises deployment, including HYDRA™-powered environments
- Standalone or Battlegrounds-integrated execution
- Pre-engagement recon for pentesters and cyber operators
- Defender-visible artifacts and telemetry for detection validation

SECURE ON ALL FRONTS

K>54

Scan the QRC or visit
markonsolutions.com/k54
to learn more about training

Markon