K7

Building an Effective SOC: People, Process, Technology

3 pages • CyberK7 Whitepaper

What it actually takes to run a SOC that catches real threats — staffing models, SIEM tuning philosophy, and escalation processes that work under pressure.

- 1. People
- 2. Process
- 3. Technology
- 4. Metrics That Matter
- About CyberK7

CyberK7 | Delhi, India | cyberk7.com

1. People

A SOC is only as effective as its analysts. Invest in ongoing training and realistic escalation paths.

2. Process

Tuned SIEM use-cases specific to your environment matter more than generic vendor rule packs.

3. Technology

SIEM, EDR and threat intelligence should be integrated, not run as siloed tools.

4. Metrics That Matter

Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) are the two metrics that matter most.

About CyberK7

CyberK7 provides managed SOC services tailored to your environment. Contact us at info@cyberk7.com or +91 98990 62199.

Quick Reference

Metric	Good Benchmark	Why It Matters
MTTD	Under 1 hour	Limits attacker dwell time
MTTR	Under 4 hours	Reduces incident impact
Coverage	24/7	Attackers do not work business hours

For a tailored consultation, contact CyberK7 at info@cyberk7.com or +91 98990 62199.