SOC OPTIMISATION CHECKLIST

Use this comprehensive checklist to ensure you're covering all bases when optimising your Security Operations Centre:

Assessment & Evaluation

[ ] Schedule and conduct quarterly SOC capability assessments
[ ] Review and update SOC metrics and KPIs (MTTD, MTTR, etc.)
[ ] Analyze recent security incidents for lessons learned
[ ] Evaluate SOC tool effectiveness and integration
[ ] Assess current threat detection coverage against MITRE ATT&CK framework
[ ] Review compliance with relevant industry regulations
[ ] Conduct gap analysis between current capabilities and industry best practices

Team Development

[ ] Update training plan for SOC personnel based on identified skills gaps
[ ] Schedule regular tabletop exercises and incident response drills
[ ] Ensure SOC staff have appropriate certifications (CISSP, GCIA, etc.)
[ ] Implement mentorship program for knowledge transfer
[ ] Conduct burnout assessment and workload balancing
[ ] Evaluate team structure and roles for optimal coverage
[ ] Schedule team participation in industry conferences and workshops



SOC OPTIMISATION CHECKLIST

Technology & Tools

[ ] Review and update SIEM use cases and correlation rules
[ ] Evaluate and implement new detection technologies where needed
[ ] Assess automation opportunities in existing workflows
[ ] Review and optimize alert thresholds to reduce false positives
[ ] Test backup and recovery procedures for critical SOC systems
[ ] Evaluate integration between security tools
[ ] Review and update threat intelligence feeds

Processes & Procedures

[ ] Update incident response playbooks for emerging threats
[ ] Test and refine escalation procedures
[ ] Update documentation for all SOC procedures
[ ] Review and optimize alert triage processes
[ ] Implement or update threat hunting procedures
[ ] Review and update on-call schedules and procedures
[ ] Test communication protocols during incidents



SOC OPTIMISATION CHECKLIST

Stakeholder Management

[ ] Schedule regular SOC performance reviews with executive leadership
[ ] Develop or update SOC metrics dashboards for various stakeholders
[ ] Establish regular communication channels with IT and development teams
[ ] Review and update service level agreements (SLAs)
[ ] Collect feedback from stakeholders on SOC performance
[ ] Schedule executive-level tabletop exercises for major incidents

Continuous Improvement

[ ] Implement a formal process for capturing and implementing lessons learned
[ ] Establish a roadmap for SOC capability enhancement
[ ] Schedule regular review of industry best practices and standards
[ ] Implement a suggestion program for SOC team improvements
[ ] Benchmark your SOC against industry peers
[ ] Create a formal change management process for SOC improvements

Looking for advice on how to optimise and continually improve your SOC. Check out this guide or contact us some free, no obligation advice.

Enquiries@RiverSafe.co.uk

