



CYBERSECURE VERTEX™
REDUCED RISK ELEVATED CONFIDENCE

Security Services

Program Service Catalogue





CYBERSECURE VERTEX
REDUCED RISK ELEVATED CONFIDENCE

Contents

CyberSecure Vertex.....	3
SOC/SIEM/SOAR SERVICES	4
SIEM ENGINEERING/OPTIMIZATION	4
SOAR DEPLOYMENT	4
SOC PROCESS OPTIMIZATION	4
TRAINING & ENABLEMENT	4
SECURITY OPERATIONS ADVISORY	5
STRATEGIC ADVISORY	5
OT SECURITY INTEGRATION	5
SECURITY OPERATIONS ADVISORY	5
STRATEGIC ADVISORY	5
OT SECURITY INTEGRATION	5
SOC SERVICE PACKAGES	6
SOC OPTIMIZATION AUDIT	6
SIEM/SOAR ACCELERATOR	6
SIEM HEALTH CHECK	6
DETECTION & RESPONSE TUNING	6
CLOUD SECURITY	7
CLOUD SECURITY ASSESSMENT	7
DETECTION & RESPONSE ENABLEMENT	7
CLOUD COMPLIANCE & GOVERNANCE SUPPORT	7



CYBERSECURE VERTEX™
REDUCED RISK ELEVATED CONFIDENCE

CyberSecure Vertex™ is a deeply technical, precision-driven cybersecurity consulting firm built for organizations that demand uncompromising security standards. We combine enterprise-grade expertise with agile execution to deliver tailored solutions that address the complex challenges of today's digital threat landscape. Our team consists of seasoned practitioners who specialize in offensive security, incident response, secure architecture, and strategic advisory—ensuring every engagement is rooted in real-world experience and technical depth.

Whether you're securing cloud infrastructure, conducting red team operations, or navigating compliance frameworks, CyberSecure Vertex is your trusted partner in cyber resilience.





SOC/SIEM/SOAR SERVICES

SIEM ENGINEERING/OPTIMIZATION

- Architecture and deployment
- Integration and custom parsers
- Correlation rules creation and fine tuning
- Log volume optimization and cost control

SOAR DEPLOYMENT

- Custom playbook development and automated response orchestration
- Integration with EDR, ticketing, and threat intel platforms
- Automated enrichment and response flows
- Workflow streamlining for faster and reliable incident response

SOC PROCESS OPTIMIZATION

- Triage and escalation workflows
- Alert fatigue reduction strategies
- Use case development and lifecycle management
- Analyst productivity enhancement

TRAINING & ENABLEMENT

- Custom playbook and detection training for SOC teams
- Onboarding programs for entry-level and junior analysts
- SIEM/SOAR tool-specific workshops
- Advanced use case workshops



SECURITY OPERATIONS ADVISORY

- MSSP vs. captive consulting
- Detection content roadmap development
- Compliance assessments (PCI/DSS, GDPR, etc.)
- Maturity assessments (MITRE/ATT&CK, NIST, ISO)

STRATEGIC ADVISORY

- CISO/ExCo presentations
- Risk-centric design and thinking
- Guidance on SOC design, tool selection
- Designing detection roadmaps
- Compliance alignment and readiness assessment
- SOC maturity assessments (CMMI)
- Designing maturity roadmap

OT SECURITY INTEGRATION

- Deploying OT-aware firewalls
- Integrating OT telemetry and alerts with enterprise SIEM/SOC
- Ensuring compliance with OT security frameworks
- Assessment and hardening of industrial control systems (ICS) and SCADA networks
- Detections for OT-specific threats and use cases
- Development of tailored playbooks
- Compliance with IEC 62443 and other OT security standards



SOC SERVICE PACKAGES

Our service packages are designed to deliver rare, high-impact cybersecurity expertise that complements and amplifies your internal capabilities. From SOC audits to SIEM tuning and beyond, many of our offerings are most effective when engaged at regular intervals — providing sustained value and strengthening your security posture.

Engagements may be fixed-fee, project-based, or subscription-driven, depending on your needs and the maturity of your environment.

SOC OPTIMIZATION AUDIT

- Review and report on alerting, automation, and process efficiency

SIEM/SOAR ACCELERATOR

- Hands-on implementation
- Custom parsers/integrations
- Investigation enrichment integrations

SIEM HEALTH CHECK

- Ingestion rate and storage analysis
- Capacity analysis and roadmaps
- Performance issues analysis
- Rules efficiency analysis

DETECTION & RESPONSE TUNING

- SIEM rules authoring and tuning
- SOAR playbook improvements
- Incident response assistance

CLOUD SECURITY ASSESSMENT

- ## DETECTION & RESPONSE ENABLEMENT

- ## CLOUD COMPLIANCE & GOVERNANCE SUPPORT

- **Cloud-specific compliance readiness (ISO 27017, SOC 2, HIPAA, etc.)**
- **Cloud Security Baselines (CIS Benchmarks, NIST 800-53, etc.)**
- **Policy and control framework mapping**

+91 80763 09990