Enabling Cybersecurity
through the lens of Business

Cost-Effective | Transformative | Proven

STARTER

9K– 40K*

(In USD / Entity)

2 – 4 weeks

Deliverables

Canned reports on

- ✓ Top Attack Vectors and Financial Impacts
- ✓ Controls Recommendations based on NIST CSF
- ✓ CyberMinds Executive Summary

Ideal for

- ✓ Cyber Risk Quantification for critical apps
- ✓ Budget Planning
- ✓ Executive/Board-level Presentations
- ✓ Validation of current Controls plan
- ✓ Measure the progress of Controls implementations

STANDARD

Starter package add-on (+ 8K)

(In USD / Entity)

2 – 5 weeks

Deliverables

Starter Package +

- ✓ Short-term Recommendations targeting CVEs that reduce the most financial risks

Ideal for

- ✓ Insights on long-term & short-term recommendations based CVE and its Financial Impact
- ✓ Requires input/integration from/with Vulnerabilities Scanning tools used within the Entity

S – FLEXIBLE

25K+

(In USD / Entity)

3 – 6 weeks

Deliverables

Customized deliverables from Starter/Standard Package +

- ✓ What-if Scenario Analysis (3)
- ✓ Investment Analysis
- ✓ Controls Analysis to interpret results into prioritized & executable roadmap
- ✓ Controls mapping to specific Industry Standards
- ✓ Custom Reporting

Ideal for

- ✓ Actioning the CRQ outcomes into Executable road maps
- ✓ Alignment to Cyber and Business Objectives
- ✓ Custom Reporting
- ✓ Continuous Reporting (1-3-6-12)

ADVANCED

CUSTOM**

(In USD / Entity)

10 – 25 weeks

Deliverables

Customized Package based on CyberMinds' The Fabric

- ✓ End to End analysis of the critical Business Stack (Processes, and underlying systems)
- ✓ Threat & Risk Modeling
- ✓ What-if Scenario Analysis (3)
- ✓ Third-Party Intelligence (add-on)
- ✓ Threat Intelligence (add-on)
- ✓ Vulnerability Intelligence
- ✓ Controls analysis with prioritized roadmap
- ✓ Executive Presentation

Ideal for

- ✓ Cyber Risk Assessment and quantification for critical business processes and systems
- ✓ Executive Cyber Risk Dashboards
- ✓ Validation of current Cybersecurity Strategy & Plans
- ✓ Detailed Attack/Threat, Risk and Controls Profiling for the **entire business stack**
- ✓ Enabling Shared responsibility model between Business, IT, Cyber and Third parties
- ✓ Alignment of the Outcomes to Cyber and Business Objectives
- ✓ Operationalize Applied Cyber Risk Management

&AbREIciT ChifCbhFlalVFRVPi WVVVeTDIbi WO3VdRdRIC VF(Wb/iaaSRECdRWVVc dCbdIAE CPIi eWdi abWfRIFi OWbiidW)Vi CaaSRCdRWVaibi 3VdRdh'i
&&imecdWTiaCE CPIciRVESeFIi Rc iCVCShcRciWOid IiEbRdRECSiDecRVIccIabWEIccIciCVFiOeVEdRWViCid IieVFIbShRVPiCaaSRECdRWVci-iceaaWbdichcdIT'

Contact us for additional questions and for a sample report.

Powered by

CyberMinds® WHERE BUSINESS MEETS CYBER | ThreatConnect™