MorganFranklin CONSULTING

TECHNOLOGY

SECURITY SERVICE OFFERINGS

Security Service Offerings

MorganFranklin Consulting has security teams and experts ready to execute on your next project. From consulting, implementation and managed services, contact us to speak with our security practice experts who will provide you with the expertise needed to successfully deliver, execute, and manage end-to-end cybersecurity solutions.

	SERVICE	DESCRIPTION
Strategy, Governance, Risk & Compliance (GRC) Services	**Virtual CISO Services**	Manage or partner with senior executives that are well versed in security strategy, planning, budgeting and delivery while possessing a strong background in IT leadership and organization design. The vCISO engages as part-time, interim or fully outsourced executive, providing specialized knowledge, resources and experiences to define and implement a unique security strategy.
	Advisory to Executives & Boards	Improve overall performance with management consulting for executives or the board on presentations, strategy, and industry focus through complex analysis, operations and business plan development.
	Strategy, Roadmap & Operating Model Development	Close the gap between strategy and execution with thoughtfully developed differentiating capabilities, the building blocks to creating strategically defined operating models, roadmaps and delivery plans. Clarify elements, timelines and responsibilities in 3-year roadmaps to ensure action and implement delivery plans based on priorities.
	Financial & Business Planning, Metrics & Measurement	Establish budget expectations and control ongoing costs. Gain insight into risk analysis and quantification using methods such as Factor Analysis of Information Risk (FAIR). Provide the ability to analyze and quantify cyber risk in financial terms and business language all departments can understand. Develop automated metrics and reporting of event analysis using decision-bot reasoning; establish or integrate into SIEM tools and workflow.
	Security Awareness, Training & Comms	Drive security culture and employee awareness through administration of traditional approaches (Phishing, CBT) and innovative methods (gamification, incentives, fun).
	Continuity and Cyber Resilience	Work closely with our cyber exercise assurance team, develop an integrated approach for disaster recovery solutions before, during, and after a threat or breach occurs. Prevent, respond and recover quickly from disruptions.
	Cyber Policy & Framework Development	Advise, develop, and maintain IS policies, procedures and guidelines. Perform policy audits once well-established. Assess organization against industry frameworks such as NIST CSF, FFIEC CAT, ISO 27001, PCI DSS, NY Dept of FS, HIPAA, & HITRUST. Provide a structure that can be applied to help understand, prevent, and recover from extreme-but-plausible scenarios that may disrupt critical business services.
Identity & Access Management (IAM)	**Identity Governance Solutions**	Build, integrate and deploy platforms that provide a scalable foundation for compliance controls, access requests, automated provisioning, certification, password management, and identity enabled visibility.
	Identity Innovation	Evaluate and recommend new identity and authentication solutions such as biometrics, face recognition, FIDO, zero trust, and other tools.
	Privileged Access Management	Expertise in implementing privilege access management platforms and policies to secure, control, manage and monitor permissions for users, accounts, processes, and systems with elevated access to critical assets.
	Security Administration (IAM)	Offer security administration support for identity and access requests. Assist with internal or external framework, policies and technologies to promote appropriate access to data and resources. Develop scenario playbooks and automation to help reduce costs.
	Authentication Services	Facilitate authentication strategy and implement industry leading technologies such as HOTP/TOTP, password-less solutions, YubiKey, tokens, and/or biometric authentication.

SECURITY SERVICE OFFERINGS

MSSP (Managed Security Service Provider)
Cyber Fusion Center (SOC)

Comprehensive or flexible services offered as a package, custom approach or hybrid solution that meets individual security needs including incident monitoring, L1 incident response and playbook development.

Implement SIEM and SOAR capabilities to protect from threats both minor and advanced, or monitor the technology and tools already present to ensure any 24/7 gaps are covered. 24/7/365 threat monitoring by dedicated security experts; robust 24/7/365 SOC providing the right technologies and knowledgeable, well-trained experts that detect, investigate and respond quickly and accurately to threats.

	SERVICE	DESCRIPTION
Cybersecurity Operations	**Perimeter Defense**	Audit and improve firewall management, IDS/IPS, Data Loss Prevention, A/V, DMZ honeypot. Provide resources and insight into selecting the right controls and solutions for all environments.
	Network Security	Assess or manage datacenter security, Proxy, NAC, Wireless, Remote/VPN, and insider threats. Improve security effectiveness or establish new security controls.
	Detect, Monitor	Provide L1, L2, or L3 SOC team expertise to monitor, develop content, and operationalize threat intelligence, incorporating it into existing procedures, SIEM integration, outline detection capabilities for SOC.
	SIEM Deployment & Management	Develop expertise in common SIEM tools (Splunk, Qradar, LogRhythm, etc.). Evaluate environment for SIEM and SOAR implementation. Provide deployment, integration, administration services and continued evolutionary support.
	Cloud Security Infrastructure	Deliver cloud strategy that will minimize risks and vulnerabilities. Implement a CASB for control and enforcement; outline and identify change management workflow and defect remediation processes. Provide expertise with AWS, Azure & O365, and Google GCP.
Application Security	**Vulnerability Management**	Consultants will work with your teams to implement a vulnerability management program that scans the environment while driving remediation through patching programs, changes in network security policy, recommendations on software reconfiguration, and application owner education.
	Static and Dynamic Code Analysis & Review (SAST/DAST)	A widely effective technique in identifying vulnerabilities, code review will uncover security flaws and concerns. Code is reviewed, analyzed and verified to be free from potential known exploits for both non-executing code and within executing programs.
	Database Security	Strengthen information repositories by integrating security solutions into database environments either internally or through the cloud. Collaborate and review with security access and monitoring controls, solutions and deployment of reliable tools (CASB, DLP, Data in Motion, Data at Rest, and Encryption technologies).
	DevOps/Open Source Security	Consultants will work with your teams to coordinate the application security process within Agile/ DevOps teams to ensure proper analysis and review before apps or updates deploy. Conceive and implement full "DevSecOps" programs for more efficient collaboration and encourage a "security culture" within DevOps.
Incident Response & Risk Intelligence	**Incident Response (CIRT)**	Provide expertise to appropriately and effectively manage, investigate and gather evidence on events or incidents involving breaches. Guides executives on appropriate actions, response and communi¬cation during an incident. Coordinates with cyber forensics, on-site security/IT, public relations and disaster recovery teams.
	Cyber Intelligence	Integrate third-party Tactical, Operational and Strategic intelligence that's easy to understand and act. Provide resources to integrate and select intelligence feeds from reputable sources including FS-ISAC, FireEye, RecordedFuture, ThreatStream, and many more.
	Penetration Testing	Determine most likely adversaries and coordinate pen testing, including standalone testing services such as internal network, external network, web application, insider threat, wireless and physical; in addition to Red, Blue and Purple team services - to evaluate environment, people and processes against possible threats.
	Red, Blue, Purple Teaming	Evaluate the effectiveness of a cybersecurity program by putting it through a simulated, persistent attack by an appointed Red team. Evaluate blue team's (the defenders) response, both automated and human-driven. Purple teaming brings both teams together to coordinate their actions and responses (TTPs) in order to evaluate new technology or policies.
	Cyber Exercise Planning	Provide multiple scenario injects based on real world events, plan for extreme-but-plausible scenarios, role play through situations, create playbooks geared towards specific events including cyber-attack, cyber breach and crisis management.