CYBERSECURITY PROFESSIONAL SERVICES

Service Offerings

MORGANFRANKLIN
CONSULTING
A Vaco Company

STRATEGY, GOVERNANCE, RISK & COMPLIANCE (GRC)

STRATEGY AND PLANNING

Advisory to Executives and Boards
Make informed decisions and set priorities regarding cybersecurity investments and risk management based upon insights provided by a team of experienced cyber advisors.

Financial and Business Planning
Quantify cyber risks using techniques such as Factor Analysis of Information Risk (FAIR) and define cybersecurity risks in business terms accessible to departments across the organization, and develop automated metrics and reporting of event analysis using decision-bot reasoning to be integrated into SIEM tools and workflow.

Strategy Development
Develop a cybersecurity strategy, roadmap, and operating model to optimize the organization's security investment based upon comprehensive cybersecurity risk analysis, access to cybersecurity expertise, and knowledge of an organization's unique regulatory requirements.

Virtual CISO Services
Partner with a senior executive, with a strong background in IT leadership and organization design, supported by a team of cybersecurity specialists, including security architects, analysts, and project managers, for flexible, including part-time, interim, or fully outsourced cybersecurity leadership.

GRC AND ENTERPRISE RISK MANAGEMENT

Third-Party Risk Management
Identify external dependencies and analyze the associated risk. Develop policies that focus on Network Access, Code Vulnerability and Supply Chain Risk.

Cyber Policy and Framework Development
Design or update cybersecurity strategies to ensure alignment with industry frameworks, such as NIST CSF, FFIEC CAT, ISO 27001, PCI DSS, NY Dept of FS, HIPAA, and HITRUST, while also providing protection against real-world cyber threats.

Business Continuity and Cyber Resilience
Ensure business security resilience in the face of natural disasters, cybersecurity incidents, and other events by developing response and recovery strategies aligned with both IT and business objectives.

Security Awareness, Training and Communications
Drive security culture and employee awareness through a combination of traditional approaches, such as phishing simulations and computer-based training (CBT) and innovative methods, using gamification, incentives, and fun.

IDENTITY & ACCESS MANAGEMENT (IAM)

Identity Governance Solutions (IAG/IGA)
Improve cyber and data security by implementing a zero-trust security model based upon a scalable and automated foundation for compliance controls, access requests, automated provisioning, certification, password management, and identity enabled visibility.

Access Management
Create policies to secure, control, manage and monitor permissions across users, accounts, processes, and systems based upon how the organization currently accesses data and best practices for data security and access management.

Strong Authentication
Secure and simplify employee access to digital accounts by deploying solutions such as single-sign on (SSO), passwordless authentication, and multi-factor authentication using biometrics or physical security tokens.

Privileged Access Management (PAM)
Monitor and restrict access to critical assets and privileged accounts by using a PAM solution to secure, control, manage and monitor permissions for users, accounts, processes, and systems with elevated privileges.

MANAGED SECURITY SERVICES PROVIDER (MSSP)

Regulatory Compliance
Ensure compliance with a growing number of data protection regulations by partnering with cybersecurity advisors with deep regulatory experience to design a compliance strategy, implement necessary security controls, and automate common compliance reporting practices.

SOC as a Service Offerings
Fill gaps in security expertise by taking advantage of flexible SOC-as-a-Service offerings, including a fully-outsourced SOC, a la carte offerings, or management of security solutions already deployed and customized to an organization's network environment.

Alert Management
Decrease alert overload by taking advantage of an alert triage system that uses multiple levels of machine learning to eliminate false positive detections and provide security teams with a manageable number of curated, aggregated alerts.

Advanced Threat Detection
Detect advanced threats that can evade traditional security controls by designing and deploying a security architecture that provides a wealth of contextual data and implementing a proactive threat hunting program to find attackers resident on an organization's systems.

CYBERSECURITY OPERATIONS

Perimeter Defense

Update network perimeter defenses to account for new deployment scenarios (cloud, IoT, and mobile) and to take advantage of advanced cybersecurity solutions for Data Loss Prevention (DLP), Endpoint Protection (AV, NGAV, and EDR), intrusion detection and prevention (IDS/IPS and honeypots), and secure networking (SD-WAN).

Network Security

Enhance datacenter security, performance, and connectivity by taking advantage of deployment and maintenance of proxy servers, network access control (NAC), wireless networking, VPN integration, insider threat detection, managed security services, and security control assessment, designed, and implementation.

Monitor and Detect

Minimize potential cybersecurity incident costs by partnering with cybersecurity advisors to identify potential security vulnerabilities before a breach occurs, support SIEM deployment and management, and provide access to a flexible and affordable third-party SOC and security expertise.

SIEM & SOAR Deployment and Management

Partner with security advisors who can provide advice on SIEM and SOAR solution selection and deployment and maintenance support to enable rapid threat detection and response and full or partial incident response workflow automation based upon built-in playbooks.

Cloud Security Infrastructure

Enforce security controls across multiple cloud environments and use cases with a security plan created in Azure, AWS, O365, and Google Cloud Platform (GCP) that includes access management with a Cloud Access Security Broker (CASB) and defined change and defect management processes.

APPLICATION SECURITY

Vulnerability Management

Select and use the correct tools and techniques to ensure that vulnerabilities are identified and remediated through patching programs, network security policy updates, software reconfigurations, and education of application owners.

Static and Dynamic Code Analysis & Review (SAST/DAST)

Minimize vulnerabilities in application code using static, dynamic, and interactive application security testing (SAST, DAST, and IAST) in development and deploying runtime application self-protection (RASP) to identify and block attempted exploitation of production code.

Database Security

Partner with security experts to assess, design, implement, and maintain database security solutions in on-premises and cloud-based deployment environments using CASB, DLP, data at rest, data in motion, and data encryption solutions.

DevOps/Open Source Security

Transition from DevOps to DevSecOps by integrating application security solutions into automated continuous integration, testing, and deployment workflows and building a “security culture” within the development team.

INCIDENT RESPONSE & RISK INTELLIGENCE

Incident Response (CIRT)

Ensure that the organization can respond rapidly and correctly to a cybersecurity incident by developing an incident response plan based upon industry best practices and partnering with a team that can provide executive guidance, communications support, and response coordination.

Cyber Intelligence

Leverage industry-specific expertise and cybersecurity experience to identify reputable cybersecurity threat intelligence feeds, such as FS-ISAC, FireEye, RecordedFuture, and ThreatStream, and integrate tactical, operational, and strategic intelligence into an organization’s cybersecurity architecture and risk management strategy.

Penetration Testing

Ensure security against the cyber threats that the organization is most likely to encounter by simulating attacks covering the internal network, external network, web applications, insider threat, wireless networks, cloud infrastructure, and physical security.

Red, Blue, Purple Teaming

Perform realistic assessments of the effectiveness of the organization’s cybersecurity policies, procedures, and controls by evaluating it using simulated attacks by experienced ethical hackers (red team) against the organization’s in-house security team (blue team), including coordination between both teams to evaluate the effectiveness of new or existing security tools or policies (purple team).

Cyber Exercise Planning

Develop and perform a variety of different simulated cybersecurity exercises, including tabletop exercises and roleplaying, to create or improve the organization’s incident response playbook and improve employee responses to various cybersecurity incident scenarios.