DATALOCK
CONSULTING GROUP

ISO
ISO/IEC 17020:2012

ISO
9001:2015

RMF | Security Operations | Cloud Security

CAPABILITIES BRIEF

CAGE: 7AMZ6 | UEI: GM2HRFT252M3

Zyad Nabbus | CEO | (571) 216.6059 | zyad.nabbus@datalockcg.com | www.datalockcg.com

Company Overview

Leadership & Focus

- 35+ Years of Experience in Cybersecurity
- Securing Mission-Critical Systems
- Protecting Supply Chains
- Safeguarding Digital Assets
- Ensuring Regulatory Compliance

Contract Vehicles, Certifications, & Team Members

- GSA MAS - 54151HACS SIN
- FedRAMP (3PAO)
- FISMA
- ISO 17020:2012 & 9001:2015
- A2LA Accredited for NIST 800-53 & 800-171

DATALOCK
CONSULTING GROUP

Core Competencies

1 *Risk Management Framework (RMF)*

- FISMA / FedRAMP / NIST 800-79
- Security Assessment & Authorization (SA&A)
- Authority to Operate (ATO)

2 *Security Operations*

- Security Program Development
- Pen Testing / Vulnerability Mgmt.
- Identity & Access Mgmt. (IAM)
- Vulnerability/Compliance Scanning

3 *Cloud Security*

- Cloud Automation
- Cloud Engineering
- Cloud Architecture
- DevSecOps

Company Experience

Trusted Relationships

Proven Performance

- NIST 800-79 PIV Assessment of HSPD-12
- ISSO Support / Continuous Monitoring for High Value Assets (HVAs)
- FISMA Assessments / Pen Testing
- ATO for SCADA / HVAs
- Cyber Supply Chain Risk Assessment
- Enterprise Security Architecture Analysis including Zero Trust
- IAM Support Services using SailPoint
- Security Operations & Engineering

DATALOCK
CONSULTING GROUP

OCC | Risk Management Framework Implementation & Execution

Situation

The Office of the Comptroller of the Currency (OCC) sought support in developing and maturing a comprehensive risk management program based on the Risk Management Framework (RMF) outlined in NIST 800-37.

Approach

DataLock Consulting Group has supported the enhancement of security policies, procedures and practices to help accelerate the proper implementation of the Risk Management Framework (RMF). In addition, our team has conducted the security assessments for each information system based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 to identify risks in support of decisions to grant or deny an Authority to Operate (ATO). In addition, our team has supported the development and execution of the Continuous Monitoring program, as well as the Independent Verification & Validation program.

Outcome / Value Delivered

Through our engagement with the OCC, the agency was able to implement a robust security program meeting FISMA standards and fostering a resilient cybersecurity infrastructure. The implementation of the Continuous Monitoring program resulted in significantly improved FISMA metrics, As a value add, our team was able to organize critical artifacts to help OCC quickly respond to external audits requirements

Solutions

- Continuous Monitoring
- Authority to Operate (ATO)
- NIST 800-37
- NIST 800-53

DATALOCK
CONSULTING GROUP

NOAA | Independent NIST Based Security Assessments

Situation

The National Oceanic and Atmospheric Administration (NOAA) required security assessment support for unique mission critical assets, to include their Hurricane Hunters (air craft), vessels, High Value Assets (HVA) and Supervisory Control and Data Acquisition (SCADA) systems. These unique assets require a broad range of skill sets to conduct a thorough assessment in order to properly identify risks to these assets and the agency.

Approach

DataLock Consulting Group, executed a comprehensive security assessment on each asset, and all associated systems on board each unique asset. The assessments included Security Control Assessments (SCA) as well as comprehensive Penetration Testing and social engineering assessments. Several critical deficiencies were identified and unique recommendations were provided to support the remediation of unique vulnerabilities. Furthermore, the assessment results were diligently compiled for a comprehensive briefing to the Deputy CIO of DOC NOAA.

Outcome / Value Delivered

DataLock Consulting Group was able to identify critical vulnerabilities within these mission critical systems for the NOAA. Given the unique types of information systems being assessed as a part of our engagement with the NOAA, DataLock Consulting Group was able to support the agency's approach in managing risks associated with these unique assets. Our team provided comprehensive recommendations for managing vulnerabilities for systems with limited patch capabilities when deployed at sea. Our risk prioritization approach helped the agency apply threat intelligence to understand real risks instead of perceived risk.

Solutions

- Penetration Testing
- Social Engineering Assessments
- Phishing Tests
- Vulnerability Management

DATALOCK
CONSULTING GROUP

GSA | ISSO Support and Continuous Monitoring for High Value Assets (HVA)

Situation

The General Services Administration (GSA) required Information System Security Officer (ISSO) support for several mission critical systems deployed in the cloud. Among the systems entrusted to our team include Login.gov and SAM.gov.

Approach

Our responsibilities covered a comprehensive array of security domains, emphasizing compliance with the Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), and agency-specific requirements. This involved executing Continuous Monitoring procedures, offering support for Security Assessments, and the regular provision of detailed weekly and monthly security and status reports.

Outcome / Value Delivered

The outcome of our ISSO support services was the sustained compliance of the assigned information systems with the stringent standards of FISMA and the specific requirements of the General Services Administration. The execution of Continuous Monitoring activities ensured a proactive stance towards security, and the support provided for Security Assessments contributed to a robust and resilient security posture. The regular dissemination of detailed security and status reports facilitated transparency and informed decision-making within the agency.

Solutions

- FISMA
- Continuous Monitoring
- Cloud Based Assessments
- FedRAMP

DATALOCK
CONSULTING GROUP

USDA | Security Engineering Operations & Assessment Services

Situation

The United States Department of Agriculture (USDA) Food and Nutrition Service (FNS) required a full suite of cyber security services for their cyber security program including security engineering, security operations, security documentation and security assessment support for all assets owned by the Mission Area (MA).

Approach

DataLock analyzed FNS’ security program to identify gaps in the program to include identification of current security tools, processes, personnel expertise and governance structure. DataLock developed & implemented a strategy to improve the security program We ensured security documentation complied with USDA standards and assessed systems to comply with Departmental timelines.

Outcome / Value Delivered

DataLock improved the FNS cyber security program, increasing visibility into all assets delivering an improved monitoring and incident response capability. We improved FNS’ Departmental compliance score resulting in FNS being recognized as a Center of Excellence for multiple cyber security program areas. FNS is now sought after for their best practices throughout USDA.

Solutions

- Security Engineering
- Security Operations
- Continuous Monitoring
- FISMA
- Authority to Operate

ISO
ISO/IEC 17020:2012

DATALOCK
CONSULTING GROUP

ISO
9001:2015

RMF | Security Operations | Cloud Security

CAPABILITIES BRIEF

CAGE: 7AMZ6 | UEI: GM2HRFT252M3

Zyad Nabbus | CEO | (571) 216.6059 | zyad.nabbus@datalockcg.com | www.datalockcg.com