COALFIRE

COALFIRE HELPS FEDERAL NATIONAL LABORATORY ACHIEVE FISMA COMPLIANCE FOR 5 SYSTEMS

THIS ORGANIZATION IS DEDICATED TO IMPROVING HUMAN HEALTH THROUGH INNOVATION IN BIOMEDICAL SCIENCE, INCLUDING EMERGING INFECTIOUS DISEASES

Customer Challenge:

As a federal national laboratory, a Coalfire client needed to meet the Federal Information Security Management Act (FISMA) standards, which is a federal law designed to improve the security posture of government agency federal systems, bureaus, departments, and such supporting entities as vendors and subcontractors.

This process involved working directly with each agency to achieve an Authority to Operate (ATO), which would be assessed to controls based on FIPS 199, FIPS 200, and NIST SP 800-53 Revision 4.

Coalfire Proposal: To support the organization's research mission by protecting critical research data, personally identifiable information, and protected health information, Coalfire conducted FISMA assessments on five systems/applications and performed cybersecurity tasks on the Biomedical Informatics Development Cloud General Support System (BIAD Cloud GSS) and four hosted applications.

Coalfire provided full advisory support, Information System Security Officer (ISSO) support, FISMA assessment services, continuous monitoring assessment services, threat hunting, and penetration testing to help this organization meet FISMA and other compliance goals for a new AWS-based BIAD Cloud GSS.

Information Security Officer Support: Coalfire provided a full-time ISSO to oversee security and maintain ATO for the organization's general support system and four applications that it hosts. Additionally, our deployed ISSO continues to support the organization's overall cybersecurity and compliance strategies throughout their environment and is working with client leadership to develop and maintain cloud security and strategy by creating and maintaining policies, procedures, and compliance documents. ISSO responsibilities also include creating initial drafts the documentation and updating documentation.

For this project, Coalfire guided all compliance tasks—from completing all Security Assessment Plans (SAPs) to tracking and handling Plan of Actions & Milestones (POA&Ms). In addition, Coalfire continues to meet with both the organization's leadership and government personnel onsite to solicit feedback and track overall program management needs. When the organization requested full-time ISSO support, Coalfire was able to provide personnel already familiar with the unique needs and challenges of this program.

Threat Hunting: Coalfire conducts threat hunting to analyze all environments for susceptibility to threat actors and identifies and implements tools that can block common tactics, techniques, and procedures (TTPs) deployed by these actors. Threat hunter analysis also allows Coalfire to identify Indicators of Compromise (IOCs) to determine if the organization has already been compromised.

Coalfire automates detection of TTPs through the appropriate security instrumentation whenever possible. If an activity is determined to be an actual or potential threat, we assess the level of risk and forward the activity to the NCI CERT for active incident response. Coalfire threat hunters work in conjunction with our penetration testing team to ensure that instrumentation is operating as designed and make improvements based on testing results. Threat hunting includes detection of new threats and identification of weaknesses that may not be readily apparent through vulnerability assessment activities.

Penetration Testing: Although FISMA Moderate-level systems do not require penetration testing, the organization requested a penetration test to ensure that both the general system and four systems hosted by the organization were protected from today's modern threat actors. Coalfire leveraged our in-house penetration testing experts to assess target systems from both an internal and external perspective. Our team emulated a threat which would have already gained access to the system, such as a compromised employee account, and used phishing tactics and physically compromised laptops to meet external penetration testing requirements. At the end of the test, our team provided a report of findings in accordance with Open Web Application Security Project (OWASP) and NIST best practices, and also provided recommendations and fielded follow-up questions with system stakeholders and the organization's leadership.

Full Advisory Support: Initially, Coalfire performed advisory and assessment work for the general support system, which was a new system on AWS Cloud. Based on findings, Coalfire identified two systems that required compliance support.

Coalfire support for the organization kicked off with a gap analysis for three of the company's existing major applications to determine their compliance with FISMA requirements and controls across the 800-53 control families. Coalfire planned future documentation and artifacts development, and reviewed network diagrams and other systems documentation to determine the scope and identify boundaries of what components and interconnections were a part of the boundaries of one of the systems. To determine the security impact of the system, Coalfire performed validation of the FIPS 199 and NIST SP-800-60 data types and validated that the system was properly categorized as a Moderate impact system.

Coalfire scheduled and conducted working sessions with system stakeholders to develop five tailored documentation packages for the organization's general support system and four hosted applications. For each FISMA-Moderate system, Coalfire worked with key stakeholders to ensure system security documentation accurately described the control implementations of the environment. Our team implemented a review process for each document to ensure proper stakeholder involvement, tracking,

and acknowledgement. Coalfire also created policies and procedure documentation as well as FISMA-required artifacts to prepare the GSS, and reliant applications for Compliance Assessment services.

Compliance Assessment Support: Coalfire performed the FISMA compliance assessments for the organization's general support system and corresponding applications. Once advisory support was complete for the organization's GSS and each of the four applications, Coalfire deployed independent assessment teams to assess compliance with FISMA controls in accordance with NCI practices and NIST SP 800-53 requirements. We ensured assessment reliability by deploying an assessment team independent of our advisory team and by undergoing rigorous independent review of our findings by the NCI ISCM.

Conduct Vulnerability Scanning / Management: Coalfire worked with the organization to identify vulnerabilities within the assessment boundary, including hosts, devices, databases, and web applications. The scanning team utilized Tenable Nessus to ensure that all tools are updated and configured to run in a safe manner such as by setting relative limits of tool bandwidth usage and scanning devices in a random order to reduce the number of IDS/IPS alerts. Vulnerability scanning activities included validation of the system boundary and that all IP-addressable system hosts and devices are identified. Coalfire performed a network discovery scan on the defined boundary with the automated vulnerability scanning tools to validate the components and test the boundary protection mechanisms. Coalfire created scan groups and directed scans to extract vulnerability details from all in-scope hosts and devices to include any software, databases, and web applications running on them.

AWS Solutions: The applications developed by the organization are all hosted in the AWS East Region and have all attained an Authority to Operate (ATO) from the NCI Authorizing Official. The AWS East/West FedRAMP authorization has been key to achieving security compliance. Not only is the data center FedRAMP compliant, but also many of the AWS services used for the applications are FedRAMP compliant or in the process of becoming FedRAMP compliant, allowing the applications to inherit security control compliance from these services. The use of AWS services continues to evolve the architecture as new and better solutions are implemented. AWS services utilized by the organization include VPC, EC2, Fargate, ELB, Lambda, S3, Glacier, CloudWatch, CloudTrail, RDS, Redshift, DynamoDB, IAM, Certificate Manager, KMS, GuardDuty, Macie, SNS, and SQS.

Third-Party Apps Used: The organization has leveraged several third-party apps that integrate with AWS for operations and maintenance purposes, including Docker Hub, Loggly, and Slack. The organization endeavors to implement third-party apps that can be implemented/integrated with the AWS environments wherever possible due to contractual obligations. AS such, the organization periodically reviews tools that are not FedRAMP compliant and evaluates products that are FedRAMP compliant. The process for selecting a SaaS also takes into consideration requirements for security and monitoring.

Outcomes & Results: In just one year, Coalfire helped this organization meet FISMA and other compliance goals for a new AWS-based BIAD Cloud GSS, helping support the organization's research mission by protecting critical research data, personally identifiable information, and protected health information. The organization has attained five formal ATO declarations for five systems.

Lessons Learned: The organization learned during initial assessment for ATO that they needed a full-time ISSO to oversee security and maintain ATO for the organization's general support system and four applications that it hosts. The organization's cloud engineers and developers also gained many key learnings and continue to learn about AWS services and how best to utilize them for security and monitoring purposes. Because AWS is optimally positioned for continuous integration and continuous development, the organization is able to better review and implement AWS services as their architecture grows.

In addition to the organization's positive feedback on Coalfire's high quality of work, the NCI ISSO deployed by Coalfire has positioned us to perform all assessments thanks to our standing as an approved FedRAMP Third Party Assessment Organization (3PAO).