CASE STUDY

Technical Support to FISMA Compliance @ USDA, Forest Service

Challenge

The Forest Service contracted NSG to Implement a Security Event Management System (SEM) that would aggregate security event information from 1300 servers and devices and retain events for 30 days online and 2 years offline. They also tasked NSG to assess the enterprise for data sources required for FISMA Compliance and integrate event monitoring with incident resolution.

Solution

NSG installed an information security event aggregation and reporting system to comply with FISMA policies and procedures. A SIM infrastructure was built using netForensics (nFx) products (SIM One, DataOne) to manage the events centrally for the majority of hosting service providers. The mission-critical applications of FS to nFX were integrated, providing a reporting dashboard. The solution deployment addressed the issues of high availability and disaster recovery planning as well as backup, and recovery. Overall, NSG provided the following solutions:

- Designed and implemented robust, fault-tolerant SEM
- Integrated custom data sources
- Implemented incident response management system
- Provided analysis of event data to assess progress toward compliance goals
- Provided effective security compliance management
- Provided technology/tools: NetForensics, SIMOne

Results

- Reduced cost of reaching security goals through centralized security monitoring and reporting
- Standardized environment that allows event information to be easily correlated
- Improved security posture and compliance
- Optimized resource investment