

Enterprise SIEM and Log Aggregation

Project Scope and Schedule

Business Case	Capturing and analyzing system and networking logs is a cornerstone of an enterprise's ability to detect and respond to cybersecurity incidents. Security Information and Event Management (SIEM) is a software solution that aggregates and analyzes activity from many different resources across the entire IT infrastructure. The State currently has some stand-alone capability in areas of the network that hold sensitive data, but the overall coverage of these systems is limited to about 60% of the enterprise and is labor intensive. Unifying the multiple systems performing logging and including the unmanaged system logs into one complete system will increase visibility and detection of system security issues and allow the limited number of personnel monitoring those systems to have an out-sized influence on the overall security of the enterprise.
Scope	The initial scope will incorporate an assessment of current logging and the logging requirements necessary to inform incident identification and to meet Federal requirements. The follow-up will size the logging system to meet overall use, ingestion, and reporting needs. Assessment, design, procurement, implementation, and management are all in scope for the duration of this service.
Schedule	The first three months will entail information gathering, system design, and procurement. Implementation should take a further three months to install the system, train personnel, and verify operations. Once fully operational, the system logs will be evaluated for any changes to the overall structure of State technology and adjustments/additions will occur to ensure that the system is complete.

Project Estimate

Implementation	\$2,300,000
Operating	\$1,000,000/year
Total	\$3,300,000
Notes	