NATIONAL INSIDER THREAT TASK FORCE

NITTF Tech Bulletin 20180427: How CNSSD 1015 Defines EAM

ABSTRACT:

This Tech Bulletin considers the definition of enterprise audit management (EAM) provided by CNSSD 1015. According to CNSSD 1015, EAM is the “the identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring and maintenance of this capability.”

GUIDANCE:

The Committee on National Security Systems Directive 1015 (CNSSD 1015) on *Enterprise Audit Management Instruction for National Security Systems (NSS)*, September 2013, defines enterprise audit management (EAM) the “the identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring and maintenance of this capability. An Enterprise Audit Management solution should be deployed to collect, store, and provide access to audit data. For each type of audit (specific to system/mission/data), auditable events are identified, auditing is conducted to properly capture and store that data, and analysis and reporting are performed. Certain high-profile events trigger automated notification to designated individuals, such as system security officers or D/As incident response center/team."

CNSSD 1015 also states that EAM, "provides a framework for decision makers to continuously monitor asset integrity, manage risk in order to maintain system security, and develop meaningful enterprise situational awareness. EAM applies the general concepts, processes and activities of audit management with a focus on outcomes that affect the security posture of the information system via automation."

Essentially, EAM is a structured, consistent and continuous collection and reporting process across the whole of an organization for identifying, assessing, deciding upon responses to, and reporting upon the efficiencies of, or upon threats that affect the operational continuance of functionality. **However, EAM cannot be a substitute for user activity monitoring (UAM), because it does not collect, report, or otherwise act upon specific analysis of employee threat behaviors.**

For more information, please contact the NITTF Technical Team at nittftechnical@dni.ic.gov.