NATIONAL INSIDER THREAT TASK FORCE

NITTF Tech Bulletin 20180527: How CNSSD 504 Defines UAM

ABSTRACT:

This Tech Bulletin considers the definition of user activity monitoring (UAM) provided by CNSSD 504, and it notes the technical functionality that a UAM solution must have to meet the Directive's requirements.

GUIDANCE:

The Committee on National Security Systems Directive 504 (CNSSD 504) on *Protecting National Security Systems from Insider Threat*, 4 February 2014, defines user activity monitoring (UAM) as the "technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threats and to support authorized investigations." CNSSD 504 Annex B also states that every executive branch department and agency (D/A) should have five minimum technical capabilities to collect user activity data: keystroke monitoring, full application content (e.g., email, chat, data import, data export), screen capture, and file shadowing for all lawful purposes (i.e., the ability to track documents when the names and locations have changed). The fifth capability is that the collected UAM data must be attributable to a specific user. The D/A should incorporate UAM data into an analysis system that is capable of identifying anomalous behavior.

Essentially, UAM is a structured, consistent, and continuous collection and reporting process across the whole of an organization at the device level for identifying, assessing, deciding upon responses to, and acting upon specific analysis of employee threat behaviors. The purpose of UAM is to gather detailed and substantive content about behavioral activity, which may be indicative of an insider threat.

For more information about UAM, please see NITTF Tech Bulletins on UAM or contact the NITTF Technical Team at nittftechnical@dni.ic.gov.