NATIONAL INSIDER THREAT TASK FORCE

NITTF Tech Bulletin 20180322: Security Information and Event Management for Insider Threat Programs.

Abstract:

Security information and event management (SIEM) refers to a cyber tool for the collection and analysis of security events and threat management.

GUIDANCE:

Security Information and Event Management (SIEM) tools provide a holistic view of an organization's information technology (IT) and security infrastructure. A SIEM tool combines all of the security information management and security event functions into one centralized location. By bringing these two functions together, SIEM tools provide identification analysis of system alerts, and recovery of security events.

SIEM tools support compliance reporting and incident investigation through the analysis of historical data. The core capabilities of SIEM technology provides a broad range of event collection and the ability to correlate and analyze events across disparate sources of data in real time.

SIEM is implemented via software, systems, appliances, or some combination of these items. The following are the six main attributes of a SIEM tool.

Correlation: Sorts data into packets that are meaningful, similar and share common traits. The goal is to turn data into useful information.

Compliance: Enables the establishment of protocols that automatically collect data necessary for compliance with company, government, or organizational policies.

Data Aggregation: Assembles data from any number of sites, including servers, networks, databases, application software, and email systems. The aggregation also serves as a consolidating resource before data is sent to be correlated or retained.

Dashboards: Provides a dashboard to analyze and visualize data to discover patterns or target activity or data that does not fit into a normal pattern.

Retention: Stores data indefinitely so that decisions can be made from more complete or robust data sets.

Alerts: Activates protocols (e.g., dashboard notifications, automated email or text messages) when the data triggers alerts such potential security incidents.

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