2016

Systems of Systems Approach to Insider Threat

Campbell, Willliam

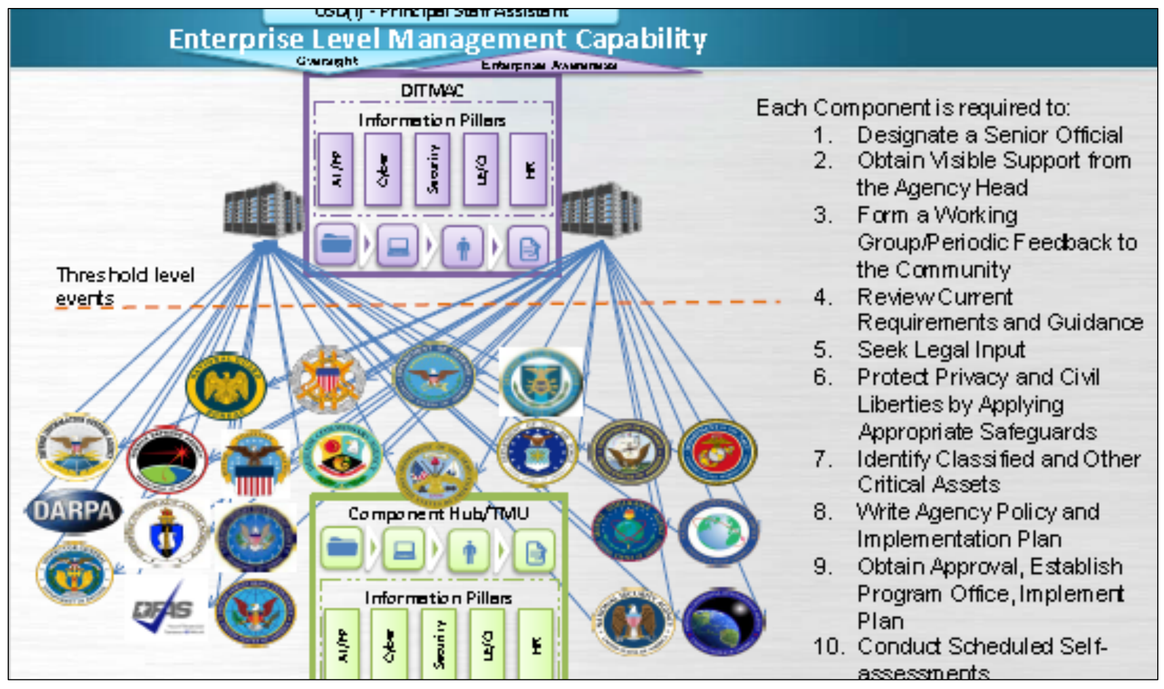
Monterey, California. Naval Postgraduate School

Systems of Systems Approach to Insider Threat

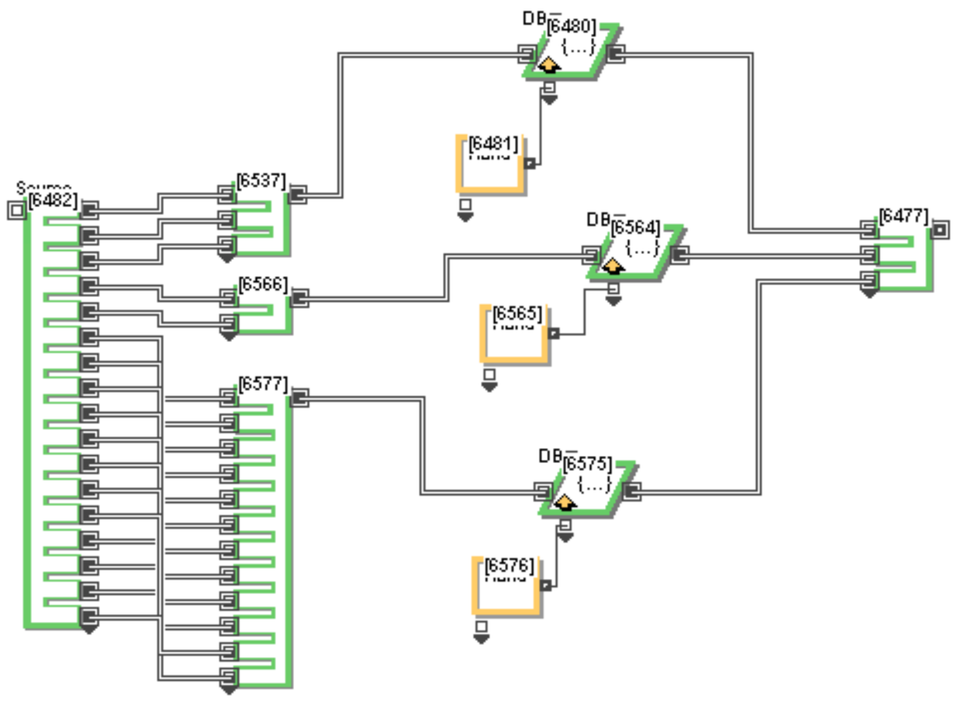
Naval Postgraduate School

Insider Threat Hubs

- Insiders pose a significant threat to our nations physical and cyber security. Detecting and mitigating this threat is important because insiders have been granted privileges that external threats do not have and can easily evade security protocols to conduct malicious acts. To combat these threats, organizations are creating centralized hubs designed to prevent, detect, and mitigate the actions of insiders. A critical element of these hubs is the analytical cell designed to identify malicious acts' anomalous behavior from ordinary behavior.
- Insider-threat hubs rely heavily on internal sources of data such as user activity monitoring. This ignores additional external data sources of insider-threat indicators. This thesis examines insider-threat detection and analysis processes and proposes an approach that may enhance the hub analytical cell.



DITMAC lead Insider Threat Hub

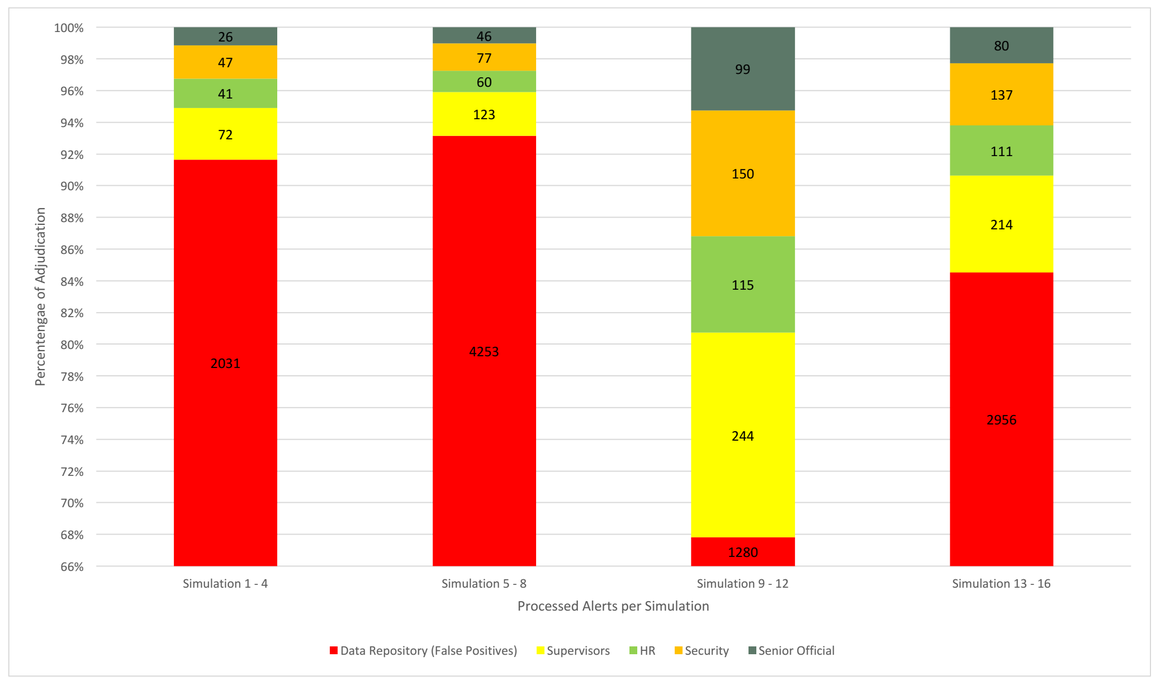


DSS vs NGA Insider Threat Hubs

- Analysis of the insider-threat hub ecosystems of two government agencies: the Defense Security Service (DSS) and the National Geospatial Agency (NGA) provides insight into the organizational structure of insider-threat hubs, technological systems currently utilized for threat inputs and analysis, as well as shortcomings associated with insider-threat detection and analysis.
- Shortcomings include the process of identifying insider-threat indicators with only UAM ignoring external sources of data and another involves technology that can enhance data collection and analysis.

Extend Sim Results

- ExtendSim software is used to simulate hub operations based on DSS and NGA insider-threat hubs.
- Each simulation tested the processing rates of the hub analytical cell in order to determine methods of lowering false positive rates. Alerts were processed based on:
  - Highest priority of first in first out basis
  - Source of the alert
  - Unique Identifier associating the alert with a specific user.



High False Positive Rate of Alerts

System of Systems Approach

- A System of Systems (SoS) is a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities (ODUSD[A&T], 2008).
- Main purpose of an SoS is to link autonomous systems for information sharing.
- Two critical components of SoS approach:
  - Components of an SoS must operate independently
  - Each component must be managed independently
- Current insider-threat detection relies on UAM and tip-line information, ignoring external sources of information. A SoS approach could feed external information to hub for analysis.

CPT William Campbell, USA
Graduate School of Operations and Information Sciences

Insider Threat Hub Operations

Faculty Advisors:
Dr. Shelley Gallup
Dr. Tom Anderson