INSIDERTHREATDEFENSE.COM

Protecting Classified & Sensitive Information Is Our Business

COUNTERESPIONAGE - INSIDER THREAT AUDITING AND MONITORING RECOMMENDATIONS

The following are recommendations and guidance related to Insider Threat Auditing and Monitoring Tools.

Three important features need to be considered when considering an acquisition of an enterprise Insider Threat Auditing and Monitoring Tool(s).
1) Auditing and Monitoring: **Auditing** may be reviewing an Insider's computer activities to look for thresholds being exceeded; **Example**: Excessive printing or file copying to portable storage media. **Monitoring** may be reviewing and Insider's computer activities for suspicious or malicious activities; **Example**: A login to the Insider's computer outside of their normal working hours.

2) Preventative / Threshold: These features could support policy violations and prevent an Insider from performing certain actions after a policy violation is detected; Features; User lockout, computer shutdown, encryption when data is exported, data export blocking, USB port blocking, file quota copying limits, floppy/CD/DVD mount blocking, copy/paste blocking, print blocking, screen print blocking, block opening, modifying, deleting of files / e-mails, software application blocking/blacklisting, blocking use of administrative privileges, etc.

3) Data Discovery and Categorization: These features could support the ability to track files/data by locating and identifying the security classification of files/data and providing greater visibility and reporting on the usage of files/data by Insiders.

Press Release:
Insider Threat Defense, Inc. And Tanager, Inc. Announce Strategic Partnership For Insider Threat Program Risk Mitigation Services

Tanager, Inc: Small Business Leader In Insider Threat Implementation And Services
Tanager is a leading small business in insider threat program implementation for the U.S. Government. While many may talk about insider threat in general terms and as a conceptual problem, Tanager has implemented, operated, and performed Counterintelligence focused analysis and Information Technology solutions implementation on several U.S. Government insider threat programs since 2010. The Tanager team has been active in insider threat programs since 2005, with experience implementing insider threat capabilities and solutions in over 20 U.S. Government and commercial environments.

Tanager, Inc: Small Business Leader In Insider Threat Auditing And Monitoring Services
Tanager's Threat Mitigation Services provide a flexible turn-key technical and programmatic solution, utilizing the leading host-based insider threat audit and monitoring tools available. This managed service offering provides a quick and easy way for industry to leverage "U.S. government-grade" host-based audit and monitoring capabilities using a partner who has extensive hands-on experience. Tanager offers a full range of insider threat mission services including, training, and insider threat program implementation services.

To learn more about Tanagers insider threat capabilities, threat mitigation services, and how they can help you with your insider threat needs, visit:

Website: **www.tanagerinc.com**
E-Mail: **insiderthreat@tanagerinc.com**

NATIONAL INSIDER THREAT POLICY
DOD-IC REGULATIONS
RELATED TO
INSIDER THREAT AUDITING AND MONITORING

References to Insider Threat Auditing and Monitoring are found in the following DoD and IC regulations:

Reference # 1:
CJCSI 6510.01 IA And Support To CND (10-2013) / Page A-5 Enclosure A
8. Monitoring Information Systems. DOD ISs (e.g., enclaves, applications, outsourced IT-based process, and platform IT interconnections) shall be monitored to detect and react to incidents, intrusions, disruption of services, or other unauthorized activities **(including insider threat)** that threaten the security of DOD operations or IT resources, including internal misuse.

Reference # 2:
DoDD 8500.01—Cyber Security / Page 34
e. LE and CI (LE/CI)
(2) DoD component LE/CI agencies deploy capabilities on DoD networks with the intent to identify and investigate the human element posing a threat to DoD IT and DoD information. Cybersecurity will be used in support of countering espionage, international terrorism, and the **CI insider threat** in accordance with DoDI 5240.26 (Reference (cv)).

Reference # 3
NCIX / DNI Guidance ICS 700-2: Insider Threat Detection Capability On Classified Computing Environments
NCIX / DNI Guidance ICS 500-27: Collection And Sharing Of Information And Audit Data For IC Information

National Insider Threat Policy Requirements

E. INFORMATION INTEGRATION, ANALYSIS AND RESPONSE:
Agency Heads Shall:
1. Build and maintain an insider threat analytic and response capability to manually and/or electronically gather, integrate, review, assess, and respond to information derived from Cl, Security, lA, HR, LE, the monitoring of user activity, and other sources as necessary and appropriate.
2. Establish procedures for insider threat response action(s), such as inquiries, to clarify or resolve insider threat matters while ensuring that such response action(s) are centrally managed by the insider threat program within the agency or one of its subordinate entities.
3. Develop guidelines and procedures for documenting each insider threat matter reported and response action(s) taken, and ensure the timely resolution of each matter.

H. MONITORING USER ACTIVITY ON NETWORKS:
Agency Heads Shall Ensure Insider Threat Programs Include:
1 . Either internally or via agreement with external agencies, the technical capability, subject to appropriate approvals, to monitor user activity on all classified networks in order to detect activity indicative of insider threat behavior. When necessary, Service Level Agreements (SLAs) shall be executed with all other agencies that operate or provide classified network connectivity or systems. SLAs shall outline the capabilities the provider will employ to identify suspicious user behavior and how that information shall be reported to the subscriber's insider threat personnel.

2. Policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.

3. Agreements signed by all cleared employees acknowledging that their activity on any agency classified or unclassified network, to include portable electronic devices, is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding. Agreement language shall be approved by the Senior Official(s) in consultation with legal counsel.

4. Classified and unclassified network banners informing users that their activity on the network is being monitored for lawful United States Government-authorized purposes and can result in criminal or administrative actions against the user. Banner language shall be approved by the Senior Official(s) in consultation with legal counsel.

PLEASE NOTE:
An organization should seek legal guidance before undertaking any computer auditing and monitoring activities on it workforce.

Jim Henderson / CEO TopSecretProtection.Com, Inc., InsiderThreatDefense.Com
Cyber Threat-Insider Threat Risk Assessment Auditor / Analyst
Cyber Security-Information System Security Program Management Training Course Instructor
Counterespionage-Insider Threat Defense Program Training Course Instructor
Certified Information Systems Security Professional (CISSP)
Certified Chief Information Security Officer (CCISO)
Chairman Of Maryland InfraGard Insider Threat Special Interest Group
Phone: 561-809-6800 / 888-363-7241
E-Mail:
jimhenderson@insiderthreatdefense.com
jimhenderson@topsecretprotection.com
Connect With Me On LinkedIn:
http://www.linkedin.com/in/isspm
Websites:
Cyber Security Program Management Consulting
Cyber Threat Risk Assessments / Mitigation Strategies
Cyber Security-Information Systems Security Program Management Training Course
http://www.topsecretprotection.com
Insider Threat Defense Program Management Consulting
Insider Threat Risk Assessments / Mitigation Strategies
Insider Threat Defense Program Training Course
http://www.insiderthreatdefense.com