Insights from Insider Threat (InT) Detection Tools Workshop

Based upon University of Maryland Technical Report
(M. Maines, K. Jones, M. Morrison, and P. Bradley)

Insights from Insider Threat (InT) Detection Tools Workshop: Goals and Primary Focus Areas

The goal of the NITSIG workshop was to answer key questions related to procurement and use of software tools designed to support insider threat identification and mitigation efforts.

Primary areas of focus during the Workshop included:

1. Major issues related to current insider threat monitoring tools
2. Monitoring and maintenance issues
3. Challenges associated with managing data
4. Identified requirements for a future insider threat tool
5. Program management issues related to insider threat efforts
6. Terminology related to Insider Threat programs: moving from “insider threat” to “insider trust

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Focus Area 1: issues related to Current Insider threat detection tools

- **Identifying suitable Insider Threat Detection tools is an overarching problem.** Some technology currently marketed as "insider threat detection" products were originally designed for other applications making it difficult to fully examine the range of products that contribute to insider threat monitoring and detection.
- **Incompatibility issues with existing systems.** Not all currently available off-the-shelf insider threat detection products work with existing configurations within agencies and organizations. This can necessitate software adaptations and newly developed connection solutions that require time and money to develop and install.
- **Manpower requirements and costs associated with insider threat detection tools can be very high.** Using insider threat tools can create a manpower issue. Workshop participants indicated that two or more full time equivalents (FTEs) are often required just to set up and maintain the equipment. Manpower requirements to sort, manage, and analyze the data collected by the tools can also be extensive.
- **Capability gaps in basic internal threat tools.** Many behaviors associated with insider threat are not detected with simple tools and require more sophisticated applications. Many behaviors can't be detected without screen capture and keystroke data, which require endpoint monitoring and resources for data analysis. Even logon monitoring, which most organizations are able to do/collect, might not be a good indicator alone, as personnel may be putting in long or irregular hours due to a special assignment, or may alter their hours due to working abroad on a temporary assignment.
- **Endpoint monitoring challenges.** To collect detailed information about individuals, endpoint agents are usually required. Installation of such endpoint monitoring, plus the current practice of a mobile and remote workforce can create a heavy network burden. Many organizations have multiple networks to monitor and, by design, no way to collate data, making it difficult to get a full picture of each employee. Some agencies have employees across the globe, which entails its own complications in regard to login times and data collection.

Focus Area 2: Monitoring and Maintenance Tools

- **Inside vs. Outside.** Opinions varied on whether tool vendors provide adequate support. Some felt that having in-house engineering resources is extremely useful. One office has data scientists on staff; having people in-house leads to better understanding of the culture of the corporation and more tailored requirements.
- **Required internal support.** Generally, organizations have found that is necessary to create a team of individuals with specific responsibility for monitoring insider threat. One office spends 60% of its time maintaining tools. Another organization has 42 people maintaining the tool, just on the high side. It has taken one organization about a year to install, tune, and train a team to analyze the content of the company culture.
- **Vendor support.** Some vendors offer contractors to provide support in-house or allocated as a staff team. Having Professional services on call to trouble-shoot problems especially in early stages of an InT program, can be very useful, but there are many issues involved, including location of these representatives, cost for services, and time required for response.

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Focus Area 3: Challenges Associated with Managing Insider Threat

- **Extremely high number of detected events.** One common challenge with insider threat data is the huge intake of events (one attendee reported 118 million) resulting in a deluge of alerts (1.2 million) which would require at least 2 FTEs to sort and analyze. Another user reports that software is pulling in 9,000 events/sec and the system is often not functioning as a result of overload. There is simply no easy way to sample a more manageable intake.
- **Problems with risk ranking.** Another challenge is that risk ranking is reportedly not working; many systems treat all risk factors as equal. One user reports, "It feels like we are playing 'whack a mole' - we have security measures, but most of our alerts are false positives." Additionally, it is important to study different indicators for monitoring different threats. The indicators of violence are not the indicators of espionage, and are not the indicators of suicide.
- **Integration of Human Resources (HR) data.** There is a need to incorporate human resources (HR) data to get a full picture of employee risk levels. Such data for contractors is not always available. Data for individuals working remotely is also not always available.
- **Focusing on deviations from regular activity.** A risk matrix is needed for all personnel in a given agency or organization, which includes a baseline plus daily activity. There is a need to be able to differentiate "normal business" from when an individual diverges from his/her normal pattern. This provides an ability to look for change in behavior as a possible indicator. More detail and visibility is needed into privileged users.

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Focus Area 4: Program Management Issues Related to Insider Threat Efforts

- **Varying levels of organizational support.** While it is common to have management support for an insider threat program, there is often little or no money provided for this function. Once there is a perceived solution, even if this solution is preliminary and not fully evaluated, management appetite for spending on the insider threat problem may further deteriorate.
- **Limited understanding of function of insider threat tools when programs are first introduced and need to meet many different requirements.** Not many understand what an insider threat tool is or what it would need to be to provide real insight for their organization. Government organizations implement InT programs in response to Executive Order 13587, issued in 2011 by President Obama, or to the National Industrial Security Program Operating Manual (NISPOM) requirement, which covers requirements for DOD contractors. Hospitals and medical organizations are more focused on protection of sensitive patient data, and business and technical design companies are seeking to protect proprietary information related to their products. These many different reasons for establishing insider threat monitoring lead to very different tool requirements. There is not a "one size fits all" approach for sorting out InT tool needs and there are no guides or manuals to assist in determining which tools to purchase.
- **Cost and manpower issues.** Using insider threat tools can create a manpower issue. Often 2 or more FTEs are required just to set up and maintain the equipment. This is not always made clear when tools are described and offered for sale to organizations.
- **Acceptance of intrusive tools.** Some environments do not want intrusive tools. These types of tools can make formerly quick, essential tasks take far too long. Developers continuously push back against extreme slowing or in some cases against any slowing. One user stated, "We cannot deploy agents on the box in all scenarios because we cannot afford slowdowns for the warfighter."

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Focus Area 4: Program Management Issues Related to Insider Threat Efforts (continued)

- **Differences in how insider threats are monitored within organizations.** Some insider threat programs fall under cyber security, some under personnel security. Some units started as cyber intelligence teams with that posture and expertise. These difference in where InT programs are located within an organization can create differences in funding, visibility, trust from employees, and access to data.
- **Desire to look beyond behavior.** Several organizations expressed desire to know more about insiders than just their observed behavior - wanting to move on to understanding intent. For example several key questions identified include: Why are employees leaving? Are they planning to take data with them? What causes employees to consider removing sensitive material? These questions cannot be answered from current insider threat monitoring technology which can track patterns of behavior and indicate areas of possible risk. Most agreed that more tools with more sophisticated analytic capabilities, including machine learning and AI, will be needed in order to answer questions of intent.

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Focus Area 5: Identified Requirements for a future Insider Threat Tool

Workshop participants identified the following features and capabilities as necessary for the development of a future tool for detection of insider threat.

•Incorporation of HR data for a more complete picture; this could be limited for contractors where data is not as readily available.

•Ability to look for change rather than baseline.

•Ability to look at cyber behavior, learn baseline, and then detect deviations.

•Ability to be able to see if VPNs from foreign travel match logged travel.

•Improved case-management tools, but differences in opinion about whether these should be part of the InT tool or a separate system.

•Automatic case management would be a big time savings

•Improved Ticket creation for CER/CERT

•Ability to monitor open source information about employees and dark web presence

•Ability to “drill down” to make sense of the data – sometimes need a CI analyst to understand the context of alerts.

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Focus Area 5: Identified Requirements for a future Insider Threat Tool (continued)

- **Improved risk level assessment** - how useful are the scores? Weighting of factors is not yet mature.
- **Integration of scenario-based models** (e.g. is an employee at risk for data loss? Suicide? Retention?)
- **Ability to measure distinctive elements,** including reduction in false positives (reports do not equal false positives), organize by types of cases, more metrics overall. For example sometimes capture "true positive/not actual" case (e.g. large print job) but it's not actually indicative of threat (i.e. there is a legitimate explanation)
- Improved Review Dashboard, that provides the ability to look at multiple cues without having to write the queries, several users don't like the need to use advanced features to adjust monitoring and ensure that the tool is doing what you think it is and would appreciate a simpler monitoring approach.

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Terminology Related to Insider Threat Programs: Moving from Insider Threat to Insider Trust

- Terminology about any issue can be important, and some organizations are sensitive about using “insider threat,” which may not resonate with their work force.
- For some organizations preferred terms to refer to insider threat risks include: data loss prevention, information protection, trade secrets protection, and trusted workforce.
- Other organizations tend to like the term “insider threat” because it sets up clear expectations, i.e., “we are watching you.”
- Terminology preferences may be based to a considerable extent on context, workforce composition, and organizational culture.
- Some participants believe that shifting to a more positive emphasis on “data protection” and “trust placed in the workforce” has the potential to result in greater workforce acceptance of the need for insider threat detection programs as well as increased levels of employee participation in these programs.

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Key Findings from InT Tools Workshop

- Primary importance of finding out what data you have and what you need to know from the data in order to establish a successful insider threat monitoring program.
- Organizations may not be able to buy off-the-shelf insider threat technology as a solution. They may have to build a system to fit organizational needs (not all organizations will have resources for this).
- There are many terms in use for insider threat detection that are not well defined in the industry. It would be useful to develop an agreed set of standard definitions.
- The need to know your personnel is an over-arching requirement for insider threat monitoring. The more familiar supervisors are with the concerns and behaviors of their employees, the more likely it will be to develop a trusted work force.
- Is there a balance between technological detection of insider threat and understanding human factors? This demonstrates a clear need for the integration of concepts and approaches from the social sciences into technical threat monitoring.
- Anomalies in behavior are not in themselves meaningful – greater understanding is needed of what an anomaly might indicate.

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

Key Findings from InT Tools Workshop – Continued

- Approaches/techniques should be developed for using machine learning (ML) to learn when context is meaningful or explanatory
- It is necessary to consider both on-going and operational costs of insider threat monitoring and detection when designing and building Insider Threat programs.
- Consider how disaster recovery/Continuity of Operations Plan (COOP) impact insider threat detection.
- Consider charges or costs based on the amount of data collected and analyzed as a key Insider Threat program factor.
- Organizations may become locked into a vendor because of contracts or money already spent on a particular tool or solution . Is there a process to change or incorporate a second tool after considerable investment in a first tool that does not satisfy all needs?

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY