APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

TECHNICAL REPORT, VERSION 2

Insights from Insider Threat Detection Tools Workshop

Marilyn J. Maines, Kelly M. Jones, Michelle E. Morrison, and Petra A. Bradley

Applied Research Laboratory for Intelligence and Security (ARLIS)

Prepared for OUSD(I) • March 10, 2020

Background

On June 5, 2019, the National Insider Threat Special Interest Group (NITSIG), in partnership with the University of Maryland's Applied Research Laboratory for Intelligence and Security (ARLIS) and the Johns Hopkins Applied Physics Laboratory (APL) held a workshop on Insider Threat Detection Tools (ITDTs). Fourteen (14) individuals from the Insider Threat Community attended the workshop and contributed to the formulation of the set of key challenges facing the Insider Threat Community discussed below. All attendees have a role in administering an insider threat program, have conducted research on insider threat, have served as an end-user/analyst of detection tool output, or have experience in some combination of these functions. Participants represented government agencies and industry. Vendors were excluded from the workshop to allow open discussion of user experiences with current tools. Participants' names and organizational affiliations are not included in this summary and there is no attribution of contributions to individual participants or to the agencies/organizations they represent. On February 11, 2020 the NITSIG in partnership with University of Maryland, held a follow-up Workshop on Insider Threat Detection Tools, at which the conclusions from this technical report were included in the discussion and a Checklist for Insider Threat Detection Tools Acquisition was developed. The Checklist is included in the recommendations section of this report. [1]

Workshop Goals and Topics

The goal of the workshop was to answer key questions related to procurement and use of software tools designed to support insider threat identification and mitigation efforts. Workshop participants' responses to those questions are summarized in the report below.

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

[1] The University of Maryland would like to acknowledge and thank Jim Henderson, NITSIG Chairman, for his partnership and support in organizing the two Insider Treat Detection Tools workshop within the NITSIG auspices. Jim is also a primary contributor to the "Checklist for Insider Threat Detection Tools Acquisition," contained in the recommendations section of this technical report.

Additional Workshop discussion topics included:

5. Program management issues related to insider threat efforts
6. Terminology related to insider threat programs

Executive Summary

The goal of the original Insider Threat Detection Tools Workshop discussed in this Technical Report was to answer key questions related to procurement and use of software tools designed to support insider threat identification and mitigation efforts and to discuss organizational experiences and lessons learned in setting up Insider Threat monitoring programs. On February 11, 2020 the NITSIG held a follow-up Workshop "Insider Threat Detection for Computer Systems/Networks" on Insider Threat Detection," at which the conclusions from this technical report were included in the discussion and a Checklist for Insider Threat Detection Tools acquisition was developed. The Checklist is included in the recommendations section of this report. These workshops respond to a growing need for clarity and understanding regarding the huge numbers of INDTs available with diverse functions and capabilities on the market today and the lack of guides and manuals to assist new users in determining which tools to purchase.

Key Workshop Findings

The list below summarizes some of the most significant take away findings identified and discussed during the original Workshop. They highlight a growing awareness of the complex environment in which INDTs operate and the need for successful integration of more advanced analytic capabilities to meet the insider threat challenges of the future. Additionally, the comments focus on the need for balance between technical capabilities of monitoring tools and concepts and approaches from the social and behavioral sciences for understanding the data that the tools identify.

- Finding out what data you have (identifying the "crown jewels") and what you need to know from existing data is of primary importance 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.
- Successful insider threat detection requires a balance between technological detection of insider threat and understanding human factors. This includes 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.
- 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.

- It is necessary to consider how disaster recovery/Continuity of Operations Plan (COOP) impact insider threat detection.
- It is useful to 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. A process to change or incorporate a second tool after considerable investment in a first tool that does not satisfy all needs may be required.

Focus Area 1: Major Issues related to current insider threat monitoring tools.

Identifying suitable Insider Threat Detection Tools (INDTs) is an overarching problem. Some technologies currently marketed as "insider threat detection" products were originally designed for other applications including (data loss prevention) DLP, (user analytic metrics) UAM, or Security Information and Event Management (SIEM) tools, making it difficult to fully examine the range of products that contribute to insider threat monitoring and detection. While these applications are often related to, if not intrinsic to, the challenge of detecting and managing insider threat in the workplace, most of them were not originally designed for use by security personnel. One opinion expressed was that the industry is primarily interested in selling tools and makes it difficult to determine easily whether a tool is truly designed to address the problem of insider threat or just marketed as such.

DATA LAKES are large storage repositories that store data in the format it was collected and do not use file trees to organize data.

Incompatibility issues with existing systems. Not all currently available off-the-shelf insider threat detection products work with existing configurations within agencies and organizations. Some products cannot be fed data directly. This can necessitate software adaptations and newly developed connection solutions that require time and money to develop and install. For example, some products cannot draw from current "data lakes." This is a serious issue that can force organizations to substantially reconfigure their systems, which may be costly and involve substantial time investments.

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. One participant commented that Insider Threat offices do not care about organizational productivity, time, or use of resources.

Problems related to adapting tools to cloud configuration. Converting currently available products to a cloud version sometimes results in not being able to use certain product features. Loss of several features may degrade the desired capability of the product. Some products, especially when used in the cloud, cannot secure data or provide sufficient protection for Personally Identifiable Information (PII) or other sensitive data. This is a particularly troublesome issue for government agencies that have strict requirements for protection of PII and other sensitive data.

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 cannot 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. Most organizations do not have the resources to ensure forensic imaging of computers of departing personnel or personnel who may be demonstrating suspect behavior, and no enterprise tool exists to examine such images. Additionally, there may be little or no network activity data to monitor for employees who don't regularly use monitored IT systems. People who do not access the monitored nevertheless, be a source of insider threat. The proportion of personnel not on the network and the most appropriate ways to monitor those individuals varies by organization.

MISSING DATA PROBLEM
Some personnel may never touch the monitored network and are "invisible" to the tools. These include:

- Personnel who do not use IT systems for their jobs (e.g., housekeeping)
- Personnel who work on remote platforms, use personal devices, or use handheld devices

Other methods must be used to monitor these personnel.

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 (e.g., classified networks) 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 (e.g. login times may be meaningless, other countries have different data collection laws.)

Focus Area 2: Monitoring and Maintenance Issues

In regard to monitoring and maintenance, 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 organization.

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.

Focus Area 3: Challenges Associated with Managing Insider Threat Data

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 9000 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 are needed into privileged users.

Focus Area 4: Identified Requirements for a Future Insider Threat Tool

Workshop participants identified the following features and capabilities as necessary for the development of a successful tool for detection of insider threat. The list is not intended as a complete listing of all features needed for a future tool, but as a starting point to guide future developers.

- 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 at cyber behavior, learn baseline, and then detect changes or deviations.
- Ability to be able to see if VPNs from foreign travel match logged travel.
- Need for improved case-management tools, but there were differences in opinion about whether these should be part of the insider threat tool or a separate system.
- Automatic case management built into tools would provide a big-time savings.
- **Improved Ticket creation for CER/CERT**
    - Some users voiced a need for a case solution that is not tied to the UEBA tool.
    - Some users rely on Archer for case management, but do not want it tied to other tools.
    - It would be useful to have inter-operability between systems to track multiple data sources.
    - Some use Lexis/Nexis to search for information when conducting an investigation.
    - Some users expressed reluctance to use personal data.
    - Some users voiced issues with tying employee to identity (e.g. how do you know if "John Smith" and "beaniebaby0123" is your John Smith). Social security numbers or other user-specific information increase fidelity.

- **Ability to monitor open source information** about employees and dark web presence
  - One organization decided not to monitor employee social media data except during an investigation; one reason for this is the issue of multiple accounts for a single individual.
  - Some users find link and peer analysis (social networks) not very beneficial, while others pointed out that it can be critical in espionage cases.
- **Ability to "drill down" to make sense of the data.** There is sometimes need for a CI analyst to understand the context of alerts.
- **Improved risk level assessment.**
  - How useful are the risk scores? The weighting of factors is not yet mature. For example, being late to complete security training should not weigh the same as attempts to exfiltrate data.
  - Some believed there is a need for two scores, one for observed behavior and one for predicted future behavior.
  - Some felt there is a need ability to home in on jumps in scores that indicate PRI (potential risk indicator).
  - Some saw need for an ability to "white list" activities that have been identified as low risk, either for individuals or for the whole organization.
- **Integration of scenario-based models.**
  - There are different scenarios for different risk issues (e.g. Is an employee at risk for data loss? Suicide? Retention?).
  - Do not report on someone in first 60 days, since no baseline means too many false positives.
  - Use data scientists and FBI profiles to indicate risk.
  - There are times when individuals offer no indicators in the context of workplace behavior due to compartmentalization.
  - Weighted behaviors as indicators should be closely held; you don't want employees changing their behavior based on what causes alerts.
- **Ability to measure distinctive elements.**
  - This includes reduction in false positives (reports do not equal false positives)
  - Elements should be organized by types of cases.
  - There was a strong desire for more metrics overall.
  - For example, alerts sometimes capture "true positive/not actual" case (e.g. large print job) but it's not actually indicative of threat if there is a legitimate explanation)
- **Improved Review Dashboard.**
  - Desire for a tool that provides the ability to look at multiple cues without having to write the queries.
  - Several users do not 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.

Additional Workshop Discussion Topics

In addition to the five primary focus areas discussed above the workshop also included two closely related areas that impact adoption and use of insider threat tools. These include:

5. Program management issues related to insider threat efforts
6. Terminology related to insider threat programs

Focus Area 5. Program Management Issues related to Insider Threat Efforts

Workshop participants discussed a set of program management issues that impact insider threat tool adoption and use at government agencies and industry organizations. Some issues in this set have the potential to significantly impact adoption, use, and acceptance as well as effectiveness of InT tools.

- **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.** 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 Insider Threat Programs in response to Executive Order 13587, issued in 2011 by President Obama that requires each federal agency to establish an insider threat detection and prevention program covering all employees with access to classified networks, 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. Some organizations may also have external requests from legal and HR, especially when hiring new employees. Some organizations turn background checks over to investigators but then do not have those data to include in day to day monitoring. 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 insider threat tool needs and there are effectively no guides or manuals to assist in determining which tools to purchase.
- **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 based only upon current insider threat monitoring technology, which tracks patterns of behavior and indicates areas of possible risk. Most agreed that tools with more sophisticated analytic capabilities, including machine learning and AI, will be needed in order to answer questions of intent.
- **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."
- **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 insider

threat programs are located within an organization can create differences in funding, visibility, trust from employees, and access to data.

- **Monitoring leaks.** Monitoring leaks is usually considered relatively easy to identify —you can see files leaving. In other cases, it is harder to know what we are seeing. Exfiltration of protected information is generally considered a reliable indicator of threat.
- **Vendor investment concerns.** Organizations may become locked into a vendor because of contracts or money already spent on a particular tool or solution. Is there process to change or incorporate a second tool after considerable investment in a first tool does not satisfy all needs?

Focus Area 6: 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 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. Balancing the two approaches of protecting against insider threat while encouraging and promoting "insider trust" is one of the core decisions in establishing a successful monitoring program.

Conclusions

The goal of the original Insider Threat Detection Tools Workshop discussed in this Technical Report was to answer key questions related to procurement and use of software tools designed to support insider threat identification and mitigation efforts and to discuss organizational experiences and lessons learned in setting up insider threat monitoring programs. Based on the response to this initial workshop, NITSIG, with co-sponsorship from University of Maryland, scheduled a second follow-on Workshop on February 11, 2020 "Insider Threat Detection for Computer Systems/Networks." These workshops respond to a growing need for clarity and understanding regarding the huge numbers of insider threat detection tools available with diverse functions and capabilities on the market today and the lack of guides and manuals to assist new users in determining which tools to purchase.

Key Workshop Findings

- Finding out what data you have (identifying the "crown jewels") and what you need to know from existing data is of primary importance 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.

- Successful insider threat detection requires a balance between technological detection of insider threat and understanding human factors. This includes 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.
- 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 monitoring programs.
- It is necessary to consider how disaster recovery/Continuity of Operations Plan (COOP) impact insider threat detection.
- It is useful to 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. A process to change or incorporate a second tool after considerable investment in a first tool that does not satisfy all needs may be required.

Recommendations

In an effort to make the findings and comments from this technical report usable to recipients, ARLIS has developed a list of key questions to guide organizations when initially setting up an insider threat monitoring program and making decisions on acquisition of specific insider threat detection tools and a chart of key decision points in this process. We hope that these resources will highlight useful considerations when initiating Insider Threat Programs and provide a framework for further dialogue on the issues and concerns surrounding InT Detection Tool selection and management.

List of Key Questions to Consider when Setting Up Insider Threat Monitoring Programs and Acquiring Insider Threat Detection Tools (INDTs)

1. What critical data does my organization currently have and what do we need to know from this data in order to establish a successful Insider Threat Monitoring Program? (Define organizational needs)
2. Does my organization have a policy or plan to balance technical detection of insider threat and understanding human factors involved? (integrate social and behavioral sciences approaches with technical monitoring capabilities)
3. What are the estimated costs –both for initial start-up of a technical monitoring/detection program and ongoing operational and maintenance costs? How will these costs be funded by the organization? (program funding)
4. How will my organization identify suitable insider threat detection tools from the wide range of products available? Does the organization have a need for all five basic types of INDTs a) Data Loss Prevention (DLP); b) Privileged Access Management (PAM); c) User Activity Monitoring (UAM); 4) User Behavior Analytics (UBA) or User Entity Behavior Analytics (UEBA; and 5) Security Information and Event Management (SIEM) ? What

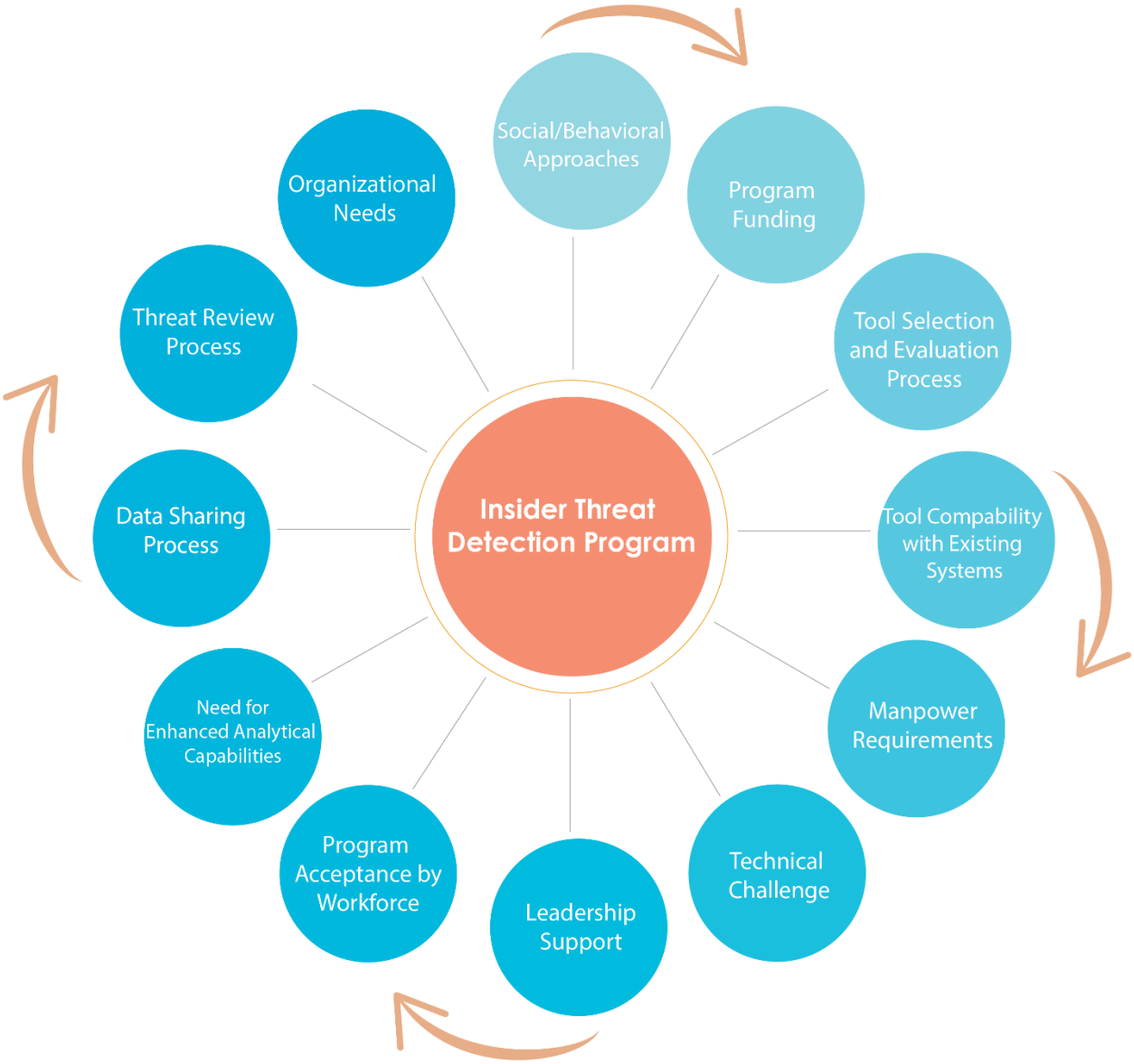
selection criteria, technical review process and selection process will be used? (tool selection)

5. Is the set of tools that my organization is considering compatible with the organization's existing data systems and processes that are currently running or will reconfiguration and adaptation be needed? (compatibility gaps)
6. What are the manpower requirements associated with an InT Monitoring Program? This includes manpower needs to set-up and maintain equipment, as well as manpower needs to sort, manage and analyze the data? Will manpower needs be met by in-house personnel or will vendor-provided support be necessary? (manpower requirements)
7. What are the specific technical challenges that my organization is likely to face regarding current organizational functions? This includes adapting insider threat detection tools to cloud configuration, logon and keystroke monitoring, end point monitoring (remote and international locations, different time zones), and dealing with employees who don't access the computer network. (technical challenges)
8. What is the level of leadership support for insider threat monitoring within my organization? What office or group will oversee the introduction and management of an insider threat program with its associated HR, security and legal concerns? (leadership support of program)
9. What level of acceptance will an Insider Threat Monitoring Program have within my organization? This includes employee training, participation and compliance, and organizational acceptance of intrusive measures that may slowdown operational functions. What level of slowdown will be acceptable? (program acceptance by workforce)
10. Does my organization have a need to look beyond observed behaviors detected by insider threat monitoring tools? Do we need additional, more advanced analytic tools to help understand motivation and intent of employees? If yes, what investment in artificial intelligence or machine learning are we prepared to make? (enhanced analytic capabilities)
11. Is my organization prepared to incorporate and share many types of data across the organization to increase the effectiveness of the Insider Threat Monitoring Program? This would include HR data, security data, and other sensitive data to develop an integrated picture of the person. (data sharing)
12. Does my organization have a policy (or need to develop one) on how to deal with identified possible insider threats? This includes a range of HR and legal issues, a clear process to deal with false positives, and to bring in additional data on the employee as needed while still protecting the individual's rights and privacy. (threat review process)

Table 1. Insider Threat Detection Program and Tool Acquisition Decision Points

Define organizational needs	**Integrate social/behavioral approaches with technical monitoring**	**Establish program funding**	**Define tool selection and evaluation process**
Assess tool compatibility with current systems	**Assess manpower requirements**	**Identify technical challenges**	**Assure leadership support of the program**
Build program acceptance by workforce	**Assess need for enhanced analytic capabilities**	**Establish data sharing processes**	**Create threat review process**

Figure 1. Insider Threat Detection Program and Tool Acquisition Decision Points



Checklist for Insider Threat Detection Tools (ITDT) Acquisition

This checklist was developed during two Insider Threat Detection Tools Workshops held on June 5, 2019 and February 11, 2020 by the National Insider Threat Special Interest Group (NITSIG) in partnership with the University of Maryland's Applied Research Laboratory for Intelligence and Security (ARLIS). Primary compilers of this list are Jim Henderson, NITSIG Chairman, and Marilyn Maines, ARLIS Insider Trust Team, based upon comments and contributions of workshop participants.

1. Understanding your organizational needs

Which ITDT tool addresses insider threats the best for your organization? This is not an easy question since one size does not fit all.

- ☐ How does your organization define Insider Threat? (going beyond NITP, NCC2 regulations) The definition can be different for each organization.
- ☐ What behaviors/activities are you trying to detect/mitigate? (Define your requirements before beginning evaluations of ITDTs)
- ☐ Do any of your existing network security tools meet some of your requirements? (conduct network security tool(s) inventory)

What does your organization want the ITDT to do?

- ☐ Report on observed behaviors / activities (policy violations)
- ☐ Report on deviations from normal behaviors / activities
- ☐ Report on predictive behaviors / activities
- ☐ Prevent /block activities of concern (i.e. data exfiltration)
- ☐ Be interactive (display warning message to employees)
- ☐ Employee threat risk scoring
- ☐ Keystroke logging
- ☐ Video recording of employee activities on computer

Are Advanced Features required?

- ☐ Import/use of external data sources (TransUnion, TR-Clear, etc.)
- ☐ Machine Learning /Artificial Intelligence

2. ITDT Evaluation and Management

ITDT Compatibility Problems

- ☐ Interoperability with existing operating systems, software applications, network security tools
- ☐ ITDT agent installed on computers
- ☐ Test and evaluation of ITDT before purchasing (try before buy, pilot phase)

ITDT Management

- ☐ Role based access (administrator (full control), Insider Threat analyst)
- ☐ Data anonymization (hide identity of individual being monitored)

ITDT User Interface

- ☐ Ease of use, learning curve, training required (training provided /costs)

3. ITDT Installation, Configuration, and Deployment

Initial Start-up Considerations

- ☐ Scalability (# of computers/ networks)
- ☐ Bandwidth requirements /usage
- ☐ Endpoint data throttling to server
- ☐ Silent agent installation (agent hidden from operating system)
- ☐ Installation: Plug & Play (plug & pray), ease of configuration / Customization (vendor help provided? / in-house support? / costs?)
- ☐ Default rule sets / Custom rule sets (vendor support needed for creating? / costs?)

Integration / Interoperability with other Network Security Tools

- ☐ Importing and integrating data from other network security tools (additional plug-in costs?)
- ☐ Data mining, correlation, analysis
- ☐ External data ingestion (badge systems, human resources data, public data such as financial, law enforcement and social media data (i.e. Endera, TransUnion, etc.)

ITDT Data Storage

- ☐ Organization data storage retention requirements (how many years?)
- ☐ Data retention access (real time, cold storage?)
- ☐ Data location (On-site or vendor cloud?)
- ☐ Data ownership (organization, vendor?)
- ☐ Charges from vendor based on amount of data collected (cost?)
- ☐ Type of database required for storage (cost?)
- ☐ Database storage requirements (size, access, controls?)

Detection, Prevention & Alerting / Reporting

- ☐ Managing / Analyzing the large amounts of data generated by ITDTs.
- ☐ Event / Alert overload problems with ITDT server
- ☐ Impact or slow-down of routine operations and functions

- ☐ Number of dedicated insider threat analysts required
- ☐ Established process for handling event alerts

4. Identifying Computer-Network Activities that are indicators of concern for your organization

Basic Areas of Concern

- ☐ Login / Logoff of user accounts (general & privileged users)
- ☐ File Events (computer / network access - add, copy, move, modify, rename, delete)
- ☐ File Activity / high volume copying of files from network to computer
- ☐ USB / DVD-CD usage
- ☐ E- mail / web mail usage
- ☐ Network print events (large print jobs, printing during non-business hours)
- ☐ Printing to local printer (bypass network printer monitoring)
- ☐ Software applications usage (to include installs, self-running executables)
- ☐ Operating system changes (processes, services)
- ☐ Network bandwidth usage (large file transfers)
- ☐ Internet usage (websites visited, searches, uploads, downloads, social networking usage, cloud storage, etc.)
- ☐ Web browser plug-ins (screen sharing, VPN, etc.)
- ☐ Web browser incognito / private browsing mode
- ☐ VPN / FTP usage
- ☐ Use of virtual machines (file uploads)
- ☐ Facebook Messenger, Go to Meeting, Skype (file uploads)
- ☐ Local network use vs. WIFI access (mobile hotspot use for data exfiltration)

Other Areas of Concern

- ☐ Using web file sharing services to upload large files (Bypass N/W Security Tools)
- ☐ Copier usage / Fax usage
- ☐ Multi-function device usage (printer, fax, e-mail, scan)
- ☐ Charging cell phones / MP3 players with computer (use as storage device)
- ☐ Phone PBX systems
- ☐ Facility access systems

Appendix A: List of Insider Threat Detection Tools

Basic Types of Insider Threat Detection Tools[2] There are five basic types of tools that support insider threat detection: 1) Data Lost Prevention (DLP); 2) Privileged Access Management (PAM); 3) User Activity Monitoring (UAM); 4) User Behavior Analytics (UBA) or User Entity Behavior Analytics (UEBA); and 5) Security Information and Event Management (SIEM). Most organizations draw from some or all of these categories of tools when establishing an insider threat monitoring program. Within each category there are numerous tools available. This is, in fact, part of the problem that organizations and insider threat specialists are facing – a plethora of tools available to users with no real system for evaluating how effective the tools offered are or how well they corelate to individual organizational needs.

1. Data Loss Prevention Tools (DLP). Data Loss Prevention Software is regarded as the first line of defense against files and data illegitimately leaving an organization's control. DLP software is intended to address loss from multiple channels, including email, endpoint, web, network and cloud. DLP tools accomplish this through classification and tracking of individual files but does not provide any insight into how a file (or data) is leveraged by users.

How DLP works and what it provides. DLP software is typically set up by an organization to detect data policy violations, and to prevent data loss (i.e., "data leaks"). Implementation involves an extensive data discovery and classification process established to find, categorize and understand sensitive data. These settings must be managed on an ongoing basis as needs change, requiring teams to fine-tune their policy rules to ensure that source and definitions around sensitive data are properly updated on a regular basis.

2. Privileged Access Management (PAM) Tools Privileged Access management (PAM) is a solution that helps organizations restrict privileged access within an existing Active Directory environment. The primary purpose of PAM software is to understand who has access to specific systems and applications at any given time. PAM software accomplishes this by provisioning and deprovisioning user identities and using password vaulting and access management techniques for critical systems and applications.

How PAM works and what it provides. PAM software focuses on "privileged users," those employees with high level access to servers, applications, or sensitive areas of an organization's private networks. A PAM solution will frequently include the following components:

- **Password management.** These systems can be used to generate temporary credentials to a system without requiring the user to memorize lengthy, complex passwords. Vaulting helps to prevent individual passwords from being easily discovered or cracked.
- **Session Management.** This software can track individual sessions to visually ensure that their actions are within the organization's cybersecurity policy.
- **Access Management.** An access manager can act as a point of entry to a system or network, where a user can request access to perform tasks. Super Admins (a.k.a. "privileged users") can control who has access to specific areas of a system or network.

[2] This characterization of the five basic types of insider threat tools draws from two articles "Fact or Fiction: Which Cybersecurity Tools Really Address Insider Threat?" ObserveIT 2018. https://www.observeit.com/resources/fact-or-fiction-which-cybersecurity-tools-really-address-insider-threat/ and "Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump Start an Insider Threat Program," 2018 IEEE Symposium of Security and Privacy Workshops.

3. User Activity Monitoring (UAM). User Activity Monitoring (UAM) is the "technical capability to observe and record the actions and activities of an individual at any time, on any device accessing US Government information."[3] UAM tools focus on the user rather than the data. UAM captures user actions, including the use of applications, windows opened, system commands executed, checkboxes clicked, text entered/edited, URLs visited, and nearly every other on-screen event. UAM does not limit access or reject any activity. Instead, UAM continuously monitors user behavior for policy compliance. Suspicious actions or trends are documented and analyzed on a case-by-case basis.

How UAM works and what it provides. UAM software looks at what users are doing on any given endpoint, helping cybersecurity teams answer questions such as:

- How are users working with files?
- Are they moving files or folders?
- What are the user's application privileges?
- Do users have access, or are they granting access, to files they should not?

UAM also uses session recordings and visual capture to provide the organization's cybersecurity team with the ability to understand the context of an incident.

For example, a typical insider threat behavior of a user who is about to exfiltrate data is moving files around systems or assigning different names to a file or folder. UAM is able to detect this and to create a forensic evidence record or trail of suspicious behavior.

4. User Behavior Analytics (UBA). User Behavior Analytics (UBA), also known as User and Entity Behavior Analytics (UEBA), takes threat monitoring to the analytic level and allows users to identify anomalies and analyze potential insider threat activity within an organization. UBA tools seek to understand user behavior as the key to discovering intent. They are designed to have a predictive capability and promise to identify potential insider threats or problems before they happen, based on previous behavior. UBA software also promises to be useful for detecting user behaviors thought to be outside the norm of an organization's cybersecurity policies.

How UBA works and what it provides. UBA technologies use machine learning to group users together to try to find outliers, allowing cyber teams to develop a list of users to monitor. This technology brings in log data sets from endpoints, networks, hosts and cloud environments. UBA does not focus on the data itself or the value of the data, but rather the behavior of the user, which is compared with previous behaviors. These tools are able to provide an alert when an insider threat risk is detected but cannot provide any action to stop further damage.

5. Security Information and Event Management System (SIEM). Security Information and Event Management (SIEM) tools centralize, correlate, and analyze data across IT networks to detect security issues. SIEM is also sometimes known as SEIM (Security Event and Information Management). SIEM tools provide the basic structure for most Secure Operations Centers (SOC). Core functions of SIEM tools include the collection, aggregation, consolidation and management of data logs from many types of devices and environments, data regulatory systems and audit control for compliance programs, security event detection and reporting, and search capabilities.

How SIEM works and what it provides. SIEM systems are often set up with event-based alerting and provide the technology to act on potential cybersecurity threats. SIEM tools may be configured to reveal similar data to UBA tools, but this requires extensive programing and rule sets and tuning

[3] 2014 report published by the National Insider Threat Task Force.

to get comparable information. SIEM can provide value to organizations by analyzing large volumes of logs data, ingested from multiple sources across the organization.

6. Case Management Systems Although not considered one of the five categories of insider threat detection tools, which primarily focus on collection of data that could indicate a potential threat, several comments were made by workshop attendees regarding case management systems used by CER Teams responding to incidents. These systems are used to aggregate data from several sources, track incident responses, or both.

Applied Research Laboratory for Intelligence and Security (ARLIS)
• 7005 52nd Avenue, College Park, Maryland 20742 •

Points of Contact

Technical Lead
Marilyn Maines, MA
Research Faculty
(301) 226-9198 | mmaines@arlis.umd.edu

Technical Lead
Kelly M. Jones, PhD
Research Associate
(301) 226-8850 | kjones@arlis.umd.edu

Executive Director
William Regli, PhD
(301) 405-6615 | regli@umd.edu

Contract Officer
Ms. Monique Anderson
Assistant Director, Office of Research Administration
(301) 405-6272 | manders1@umd.edu