1. Introduction

Currently, there is no community-accepted standard for an insider threat mitigation program. While these programs have developed organically or ad hoc over time, no agency has developed and made available a model program that other agencies can use to determine which best practices to implement and which components to prioritize, depending upon their environment, budget, and other such inherent constraints. The authors have been increasingly asked to assist in developing, reviewing, or implementing insider threat programs of varying degrees across the Intelligence Community (IC) and the Department of Defense (DoD). The authors have gathered a set of best practices from a variety of organizations with insider threat programs to build and present a model insider threat auditing and mitigation program described herein. These best practices are most applicable to the DoD/IC, but are also relevant to civilian organizations.

2. Scope

This document develops a "straw man" program model for the mitigation of insider threats. In the context of this paper, insider threat means:

_A current or former employee, contractor, or other individual who has or had authorized access to an organization’s network, systems(s), or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems._ [1]

The paper outlines the components needed for an insider threat auditing and mitigation program, implementation strategies and options, and methods of program validation that agencies can use for both initiating a program or reviewing an existing program. The paper concludes with descriptions of the best practices derived from the model program.

3. High-Level Program Aspects

Insider threat programs vary in scope and function from one organization to another. In general, an insider threat program has certain key aspects: policy, authority, collection, prevention, personnel review, threat awareness, analysis, attribution, incident response, and investigations. Depending on certain factors, including the type of program or responsible entities, some programs may not implement all aspects described in the model. Effort should be made to identify and address missing aspects.

4. Contributing Entities

The contributing entities in an insider threat program typically are Computer Network Defense (CND), Security, and Law Enforcement (LE) or Counterintelligence (CI). The key aspects of the model program typically are performed by different entities within an organization or a combination of internal and external entities, as is the case of the inclusion of an LE or CI entity in many organizations’ programs. Figure 1 shows the model program aspects and identifies the entity type providing that aspect.

CND generally describes the information assurance entity within an organization. This group implements and maintains monitoring capabilities, prevention, and analysis as well as responds to incidents before law enforcement would be involved. CND organizations also perform any remediation and damage assessment upon incident conclusion.
An organization’s Security Policies and Personnel Vetting entities provide key aspects of the model program. Security policies should outline responsibilities and acceptable use for an organization’s users. An organization’s Personnel Vetting entities should interface with the CI entities to cross reference potential insiders against emerging threats.

LE/CI entities may or may not be part of an organization. Generally, for civilian government organizations, the Federal Bureau of Investigation (FBI) has the authority to investigate potential malicious insiders. The DoD has its own authorities, but it also can coordinate with the FBI. The Authority, Policies, and Guidance section below describes the authorities for various government organizations. Each aspect of the model program is described below.

4.1 Policy

An organization’s security policies and guidance set both responsibilities and direction in terms of how the organization will implement prevention and monitoring controls and will respond to incidents.

4.2 Authority

When an incident is escalated to the level of an investigation, a law enforcement entity typically would run the investigation, citing applicable laws and regulations that may have been broken. The law enforcement entity has the ability to collect certain types of data for specific purposes, far beyond what can be typically collected by an organization’s CND element.

4.3 Collection

Insider threat programs typically are built upon a strong monitoring and auditing program within an organization. The continued collection and retention of relevant events or contextual information is critical to performing monitoring and response for insider threat mitigation.

4.4 Prevention

Many organizations skip preventative controls and instead only implement monitoring for malicious insiders. Unfortunately, monitoring is prone to false positives and takes a significant time investment to make accurate. If the organization only implements detective controls, then the analytical loop (collection, analysis, response) may take longer time than the duration of certain insider attacks. Anytime an organization wants to restrict their users’ behavior in the enterprise, it is best to be addressed by preventative controls. These controls should complement any detective controls implemented. Monitoring then can be concentrated where preventative controls cannot be utilized.

4.5 Personnel Review

Organizations with strong personnel security vetting through periodic updates of financial data, foreign contacts and trips, and polygraph examinations can use this data to identify organization members who may be more likely to commit misuse or espionage or may be more likely to be targeted for recruitment by a foreign intelligence service (FIS).

4.6 Threat Awareness

Counterintelligence can play an important role in insider threat mitigation. Understanding the current threats against an organization, combined with personnel review, may identify employees more likely to be targeted and may allow an organization to refocus its efforts on threat awareness or specific gaps in security.

4.7 Analysis

Data analysis is crucial to timely and accurate incident response. There are many analysis techniques that vary in complexity, from rule based detection to the application of machine learning algorithms. Some of these can be automated, and others will be human driven. This is the program aspect that will require the most time and resources, as this is the cornerstone of effective insider threat programs. Data analysis—building analytical capabilities that are accurate and reproducible—is a challenging problem. All analytic capabilities need to be continually validated for effectiveness against the amount of resources an organization applies to them [2]. This topic is covered in more detail in the Program Validation section.

4.8 Attribution

All collected events must be attributed to a person in an organization. As time goes by, the various attributes describing a person will change. An attribution system needs to be flexible enough to audit these changes and bound them by start and end times.
Overlaying this attribution data on events enables an organization’s analysts to understand more about the person or persons involved in an investigation. This rich attribution data typically is best understood and gathered by an organization’s Human Resources department. There may be privacy implications for its inclusion in an insider threat program.

4.9 Incident Response

Once continuous monitoring is in place, there will be events that will trigger escalation, triage, and response, which typically will be performed by an organization’s CND group. An escalation process should be in place so that any response does not adversely impact the ability of either law enforcement or counterintelligence to conduct an effective investigation.

4.10 Investigation

Once an event leads to an investigation, LE/CI entities take over from the responding CND group. The appropriate authorized investigative agency will lead the investigation but could call upon or coordinate with an organization’s CND group for additional support or information.

5. Characterization of Insiders

The insider threat problem covers a broad range of activities, with policy violation at one end of the spectrum and espionage at the other [6]. The mechanisms used for detection and prevention vary, depending on the specific concern being addressed. While some violations may be redressed via better policy enforcement or oversight, other activities require more in-depth analysis and preventative mechanisms. Another variable that comes into play is the number of activities that will be seen across that same spectrum. Policy violations will be significantly more numerous than cases of espionage, but in some cases, the potential damage from a single case of espionage can easily dwarf that of policy violators. Figure 2 shows a graph of various types of insider activity and the comparative amount of incidents that an organization will address.

![Figure 2. Load versus Insider Threat Types](image)

Insider threat programs must address how to manage investments of time and resources into detection, prevention, and analysis across that spectrum of potential violation and damage. The actual number of cases for a specific enterprise will vary, but in most cases, an insider threat analytical group will spend the bulk of its time dealing with policy violations and other activities that are at the low end of both the complexity and damage spectrums. To be able to manage analysts’ time and ensure that the analysis concentrates on what policy makers want, the program will need to understand how analysts are reviewing potential insiders. There also will need to be processes in place to capture the analysts’ findings and conclusions. The Program Validation section discusses approaches to measuring success in this regard.

6. Authorities, Policies, and Guidance

Many laws address the different types of insider threats, including misuse, sabotage, or espionage. For civilian government and IC members, these laws fall under Title 18 of the United States Code. The DoD and military members would be bound under the Uniform Code of Military Justice. Table 1 describes some of the important sections of the U.S. code and applicable authorization acts that are relevant to building an insider threat program.
### Table 1. Applicable Sections of U.S. Code/Authorization Acts

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title 18, USC 793</td>
<td>Gathering, transmitting, or losing defense information.</td>
</tr>
<tr>
<td>Title 18, USC 794</td>
<td>Gathering or delivering defense information to aid a foreign government.</td>
</tr>
<tr>
<td>Title 18, USC 798</td>
<td>Disclosure of classified information.</td>
</tr>
<tr>
<td>Section 811, 1995 Intelligence Authorization Act</td>
<td>Immediate notification to the FBI whenever there are indications that classified information may have been disclosed without authorization to a foreign power (non-DoD).</td>
</tr>
<tr>
<td>Article 106a, UCMJ, Espionage (Title 10, USC Section 906a)</td>
<td>Espionage by a member of the U.S. military. Not required to adhere to Section 811, 1995 Intelligence Authorization Act.</td>
</tr>
<tr>
<td>Section 922, 2012 National Defense Authorization Act</td>
<td>The DoD is required to establish a program for information-sharing protection and insider threat mitigation for all DoD systems.</td>
</tr>
<tr>
<td>Executive Order #13587</td>
<td>This Executive Order is intended to improve the security of classified information in government computer networks as part of the government’s response to WikiLeaks. EO is supposed to reduce the feasibility and likelihood of the unauthorized release of classified information. It addresses gaps in policy for information systems security, including characterization and detection of insider threats.</td>
</tr>
</tbody>
</table>

Lesser incidents may only be considered violations of policy. It is important that organizations set up a series of policies that cover acceptable use of their networks and systems. The policies can take the form of a Rules of Behavior document. Organizations have commonly developed Rules of Behavior documents for both privileged users as well as the general user population. These documents should be signed before any employee is able to gain access to a network resource. An organization’s workstations also should contain banners upon login that describe and link to the governing rules of behavior.

Large organizations with many disparate information systems that are pursuing consolidated auditing programs have benefitted from an organizational auditing policy. This policy establishes ownership of the audit mission and responsibilities for each information system to supply auditing information to a central log-gathering and aggregation component. This policy also will describe for the audit mission owner how long logs must be retained.

The audit mission owner will have to deal with privacy issues for some data/data sets. Whether auditing systems of record or dealing with sensitive personnel issues, the audit mission owner will have to handle personally identifiable information (PII). Large organizations have groups that perform Privacy Impact Assessments (PIA) and help establish policies for dealing with privacy information. Typically, a program collaborates with these groups to establish a privacy policy for its record data.

The Office of the National Counterintelligence Executive (NCIX) recently made available applicable policies and guidance for establishing an insider threat program. Intelligence Community Standard (ICS) 700-2 describes the use of audit data for insider threat detection. NCIX also has made available an insider threat concept of operations that provides guidance on establishing an insider threat program, including capabilities, requirements, and planning. Government organizations can take advantage of these documents for launching their insider threat programs. Organizations also can take part in the Insider Threat Task Force, which has been established to provide coordination across all government insider threat programs.

### 7. Technology

A robust, mature insider threat program has significant technology needs. One of the constant challenges facing active programs is weighing the cost of investing in new technology against developing other resources, such as analytical depth or training programs. Being able to make that decision requires an insider threat program to understand what the new technology will provide and how it will affect the program’s other components.

In most cases, technology investments can be divided into the following categories:

- Infrastructure
- Data exploitation/analytics
- Policy enforcement
- Sensors.

As a program makes technology investment decisions, it needs to understand how the technology will benefit its mission and what the trade-offs are. While decisions of this sort are not unique to insider threat, sometimes legal, policy, or other constraints inhibit what a program can do.
For example, policy and legal realities can fundamentally affect what an insider threat program can and cannot do. While technology may exist to collect specific types of data, the use of that technology may be constrained. This is especially true when an insider threat program looks to expand its data collection capabilities, as all capabilities will be scrutinized by an organization’s legal department.

8. Data Sources

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Category</th>
<th>Insider Threat Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter firewall, IDS logs,</td>
<td>Audit</td>
<td>Of limited use, given that the majority of insider threat activity occurs within an enterprise’s perimeter [4]</td>
</tr>
<tr>
<td>web/proxy logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog, event logs</td>
<td>Audit</td>
<td>In most cases, log events do not map well to user actions</td>
</tr>
<tr>
<td>Host-based monitoring</td>
<td>Audit</td>
<td>Can augment system logs with more user-oriented events and can provide insight into application use not captured elsewhere</td>
</tr>
<tr>
<td>Data loss prevention</td>
<td>Audit/Prevent</td>
<td>Can block, prompt, encrypt, or log any user-oriented event</td>
</tr>
<tr>
<td>Application logs</td>
<td>Audit</td>
<td>Can provide audit of critical enterprise application functions and data access</td>
</tr>
<tr>
<td>Badge logs</td>
<td>Physical Security</td>
<td>Provides insight to the timing of entering/exitng of buildings and other badge access-controlled areas (e.g., SCIFs, labs, elevators, etc.)</td>
</tr>
<tr>
<td>Personnel information (including</td>
<td>Human Resources and Security</td>
<td>Can include potential behavior indicators that are of interest to insider threat analysts</td>
</tr>
<tr>
<td>citations, polygraph inconclusives/failures, financial distress, demotions, letters of censure, reportable incidents, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Travel reporting</td>
<td>Security</td>
<td>Discrepancies between reported and actual travel are of interest, as is unreported travel</td>
</tr>
<tr>
<td>Privileged user monitoring</td>
<td>Audit</td>
<td>Gives finer-grained insight into the activities of users who have the potential to cause more damage</td>
</tr>
</tbody>
</table>

Table 2. Common Insider Threat Data Sources

For the most part, data sources drive which malicious activities an insider threat program is capable of detecting and analyzing. Along with access to various data sources, an insider threat program needs to understand the business context of the data. Table 2 shows a number of common data sources either provided to or collected by an insider threat program, along with a brief explanation of their potential use related to insider threat.

9. Staff Roles

Most components of an insider threat program will be performed at an organization’s central auditing facility, which is typically one or more security operations centers (SOC). The SOC will deploy sensors, log collectors, and aggregators across the enterprise. Some SOCs may have a LE entity incorporated as part of the audit process, or they may coordinate with an external LE entity. Once an incident occurs, one or more of these roles could be included as part of an incident response team.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>CND Administrator</td>
<td>Deploys and operates auditing and preventative data sources</td>
<td>Responsibilities are to deploy and maintain the sensor grid. Would likely be used during incident remediation. Has permission to make changes to enclaves and systems that they are responsible for.</td>
</tr>
<tr>
<td>Insider Threat Analyst</td>
<td>Performs technical analysis of the data to assess for any escalation</td>
<td>Typically these are tiered subject matter experts at interpreting information from organizational auditing sources that could be indicative of a problem.</td>
</tr>
<tr>
<td>Insider Threat Engineer</td>
<td>Architects and engineers advanced technical capabilities for pursuing the malicious insider.</td>
<td>Engineers with subject matter expertise in insider threat prevention, auditing, correlation, large data sets and databases, and building complex automation systems.</td>
</tr>
<tr>
<td>LE/CI Agent</td>
<td>Government agent who is chartered and empowered to enforce the law.</td>
<td>Typically leads the counterintelligence, espionage, or misuse investigation. May not be a technical role.</td>
</tr>
</tbody>
</table>

Table 3. Roles for Insider Threat Program

Table 3 describes the minimal roles required for an insider threat program.
10. Program Validation

Program implementers need to continually validate different aspects of the program to determine if capabilities are performing adequately or are improving. This can be difficult, especially during an intense operational tempo. As programs mature, there is a need to continually assess data source inclusion, analytical processes and detectors, and even investigative outcomes. Program implementers should include this validation as part of the program’s standard operating procedures.

For diverse organizations with many data sources, these data sources will be in various states of inclusion into a log-consolidation application, such as a Security Information and Event Manager (SIEM). Some programs have tracked these different states. This tracking helps those programs to assess data source priorities derived from their analysts’ needs and the complexity of higher stages of inclusion.

Each analytic process needs to be measured for its effectiveness. This effectiveness is best measured by calculating both true positives and false positives over some sample time. In an operational environment, establishing ground truth can be difficult: it is unknown just how many malicious insiders may exist in the sample. Organizations should incorporate analytical outcomes and investigative results during the sample timeframe to build an understanding of the effectiveness that can be compared to other sample timeframes. They then have a basis for making changes and measuring how those changes perform on other sample time frames.

Metrics can be important for validating investigative outcomes. The bulk of an analytical group’s time is spent dealing with policy violations and other activities on the low end of the complexity and damage spectrums; therefore, it is important to manage that time. Metrics tracking the amount of time an analyst spends based upon investigation type or complexity can shape tier resourcing. Metrics for the different types of investigations performed and for tracking analyst conclusions and investigative outcomes can shape program emphasis, data source inclusion, and training opportunities. A program could structure its metrics to help identify effective and comparatively ineffective detectors, by identifying noisy detectors with too few analytical outcomes. Metrics are important beyond supporting management reporting. They should be of substance to be periodically reviewed and acted upon by program implementers.

11. Best Practices

The program best practices, derived from the model program, are described below.

1. Have an organizational audit policy establishing responsibilities for auditing and monitoring that all information systems in an organization must adhere to. Large government agencies typically have numerous information systems scattered across the enterprise. Instituting an auditing policy that outlines the responsibilities and expectations of the insider threat program, system owners, and security oversight makes it possible for these disparate information systems to provide valid and timely audit data to the auditing group. It is important that an organization’s audit policy is implemented and adhered to so that the auditing group can gain a complete and accurate picture across the entire enterprise.

2. Issue rules of behavior to all users and implement banners on all systems. Rules of behavior provide users with critical information about what is allowed and not allowed on an organization’s systems. Typical government Rules of Behavior documents outline that there is no expectation of privacy for users’ actions on government networks and information systems. All users should sign these Rules of Behavior before being allowed on an organization’s systems. Signed Rules of Behavior documents supply organizations with proof that users have been made aware of what can and cannot be done on the organization’s systems. Banners that need to be clicked before accessing workstations should reaffirm and link to these Rules of Behavior.

3. Properly handle privacy information that is instrumental for insider threat audit. An organization needs to understand and track many attributes concerning individuals that may be involved in an insider attack. This may only be achieved by cross referencing a person’s identity or persona inside and outside of an organization. Much of this persona information may be considered privacy data. For example, a person’s home telephone number or personal email address could be part of an incident and may raise privacy concerns. Certain affiliations may even be important in an incident, for example, where people of a certain nationality are more likely to be targeted for recruitment from a specific FIS. This information needs to be properly handled and protected. Organizations typically have a requirement to perform a PIA before this information may be used during monitoring for indications of insider misuse.
4. Immediately notify the FBI for non-DoD government entities. Upon suspicion that someone may be committing espionage in a non-DoD government organization, the organization should immediately contact the FBI pursuant to Section 811 of the 1995 Intelligence Authorization Act. The FBI then has authority over any subsequent investigation. Section 811 of the 1995 Intelligence Authorization Act applies to most IC members and civilian government agencies that process national defense information.

5. Apply active prevention to complement monitoring. Monitoring and response alone cannot mitigate all insider misuse, especially if that misuse is time sensitive in nature. Applying preventative controls to limit access to an organization’s network may help avoid an incident or may motivate an attacker to operate in an area of the network where monitoring then can be applied for best effect. Many organizations have found that data loss prevention (DLP) technologies harmonize with the goals of insider threat monitoring. DLP focuses on ways to prevent or audit data that may be leaving a network. Applying a solid DLP policy that may restrict removable media or network services (email, web, etc.) usage can prevent misuse and also may deter potential insiders.

6. Focus on cyber observables. When performing monitoring and analysis, organizations should identify how changes in a subject’s behavior may be recorded in its information systems or observed on the network. There are times when data may need to be recorded so a system then can audit it, as is the case with an individual’s foreign contacts or travel. Open source research on malicious insiders has shown that most will perform some cyber observable activity. When building or expanding an analytic capability for observing this insider misuse, organizations have used past insider misuse and espionage cases for identifying these cyber observables.

7. Make insider threat monitoring part of a mature auditing program. Organizations can audit systems for a variety of reasons. Typically, an organization would have implemented a mature auditing program before insider threat monitoring is performed. Perimeter monitoring, operating system auditing, and application auditing are types of auditing with varying application to insider threat monitoring. Auditing special systems (network logon/logoff, public key infrastructure, building badging) can have significant impact on an organization’s insider threat monitoring program. Generally, organizations that have more mature auditing programs can describe data, storage, or information systems that are considered high-value targets (HVT). Inputting these data sources into a SIEM and understanding an organization’s HVTs can be critical for a successful insider threat monitoring strategy.

8. Collect and merge disparate data sources. An organization may have to collect and merge many data sources before any analysis can occur. These disparate data sources each will be in their own format and will have a separate structure. SIEM technology’s purpose is to ingest the disparate data sources into a common event repository. A SIEM provides data normalization for time synchronization, attribution, or correlation. Many SIEM technologies take advantage of scalable storage solutions in order to scale and perform in even the most complex enterprise environments.

9. Publish integration guidance to organizational elements. While every information system or application in an organization may be different, they typically are similar in their audit requirements. Rather than treat every system distinctly, it is advantageous to treat similar systems alike in terms of audit and security requirements—as standard enclaves having similar requirements for like systems. This guidance should be published so that any system or application owner can understand the audit requirements from the organization’s CND group.

10. Apply continuous monitoring. Focused observation, as opposed to continuous monitoring, describes an increase in monitoring that targets a specific person based upon certain initial criteria. Some organizations have favored this approach because of relative ease of implementation rather than applying a solid monitoring strategy across an organization. Focused observation is a poor replacement for continuous monitoring, especially if the initial criterion is missed. Continuous monitoring provides an ability to gather related data after an incident that would not have been collected through focused observation.

11. Understand business context. When a significant event occurs, a responder should try to understand the event’s business context. In large organizations, this could be difficult, but it could mean the difference between a successful or an unsuccessful response. Organizations should collect enough data leading up to and after an event to understand the circumstances for event occurrence and who and why a person is involved. Contextual information derived from human resources data about employees (job function, job title, job area of focus, etc.) will help support this understanding.
12. Store collected information for later retrieval. Malicious insiders can be in place in an organization for many years before any indication of a problem is observed. Some organizations that have had employees who committed espionage have had those employees in their environment for more than 20 years, as was the case for infamous spies Ana Montes and Robert Hanssen [3]. Organizations need to construct a long-term storage and retention plan for any collected data that can enable them to retrieve supporting data if a future need arises. Organizations have typically implemented retention policies of 10 years, 25 years, as long as the longest active employee's tenure, or for a certain number of years after an employee leaves that organization. Considerations need to be made for the storage type and location.

13. Actively engage with counterintelligence entities during continuous monitoring. An organization’s employees may be actively targeted by a FIS for a variety of reasons. Some sponsor programs actively engage CI entities to understand these threats, enabling them to implement more dynamic monitoring controls. This allows for much-needed situational awareness during monitoring.

14. Use past insider cases for developing new indicators [5]. As part of their continual business, the best sponsor programs have a research and development team that regularly develops new indicators for use during operations. This group typically analyzes past insider threat cases from the pool of investigations that they have run or been a part of, from community partners that have shared investigations to open source intelligence sources that track prosecuted insider threat investigations. This team will identify the tactics, techniques, and procedures (TTPs) used by the subjects of those investigations.

15. Focus on “low-hanging fruit” first, then increase analytic sophistication. When developing an initial analytical capability, organizations should develop less-sophisticated techniques for detecting malicious insiders. These detectors normally are applied to easily collected audit sources and are binary in nature. In any organization, there will be many of these detectors to implement. Once a cadre of simple detectors is applied, more refined techniques, such as correlative indicators, trending, or machine learning techniques, can be designed and implemented.

16. Continually validate analytical processes. One of the hardest questions any organization can ask is, “Is my analytical process getting better?” Organizations with active programs have identified ways of validating their analytical processes. Every detector needs to be validated for accuracy on an ongoing basis. This topic is covered in greater detail in the Program Validation section.

17. Implement solid attribution for all events. Nearly every collected event should be associated with one or more employees in an organization. This requires sustained collection of identity information against which to cross reference collected events of interest. Audit data from disparate systems may use different identity information. Organizations need to implement a system that tracks these different identity attributes about employees. A system such as this will need to track an attribute’s state in relation to a person and bind the state changes by start and end times.

18. Bind events and attribution information with start and end times. Some events may occur for long periods of time and may require an understanding of the state change to properly comprehend the event. A good example of this is an instance of employee foreign travel. During the trip, the employee may not have produced other network events. Once the trip is completed, the employee’s activity will most likely resume. Analytic processes may need an understanding of the state change due to the trip and a resumption of activity after.

19. Instrument a bounded process for tiered triage. Depending on their population, some organizations have implemented a tiered analytic process, with a more cursory search being performed during lower tier analysis and more in-depth analysis being performed at the higher tiers. Efforts should be made to bound each tier level by how long a single process takes to perform and the amount of analytical resources required at that tier to perform the process. The highest tier should be the most in depth, and will require the most senior analysts. It will most likely also take the longest amount of time to perform, but the outcome should determine the appropriate response.

20. Establish a clear escalation path for response. Once an incident occurs, there should be an established escalation plan for all involved parties. Leads will need to be established for each responding group. The investigative lead, typically an LE agent, will need to coordinate any network response from the CND group so that no response affects the investigation. Once the investigation is completed, the CND group will need to perform a damage assessment.
21. Perform both “reactive” and “proactive” responses. An organization’s monitoring group may be asked to respond to referrals from other parts of the organization, in addition to responding to incidents found solely through their analysis. These referrals could be from personnel security vetting or an LE/CI group, or they could even result from employee tips. Response based off referrals typically is considered a reactive response. Responses based solely off internal analysis are more proactive in nature.

12. Summary

Based on experiences with different organizations having insider threat programs, we described and outlined the components needed for an insider threat auditing and mitigation program and methods of program validation that agencies can use when both initiating a program and reviewing an existing program. This paper concludes with descriptions of each of the best practices derived from the model program. This final section is meant to be a standalone section that readers can detach and incorporate into their insider threat mitigation program guidance.

13. References


