Insider Threat Mitigation Guidance

Balaji Balakrishnan
Insider Threat Mitigation Guidance

GIAC GLEG Gold Paper

Author: Balaji Balakrishnan <dfir.aaa@gmail.com>
Advisor: Stephen Northcutt
Accepted: October 6, 2015

Abstract

Insider threats are complex and require planning to create multi-year mitigation strategies. Each organization should tailor its approach to meet its unique needs. The goal of this paper is to provide relevant best practices, policies, frameworks and tools available for implementing a comprehensive insider threat mitigation program. Security practitioners can use this paper as a reference and customize their mitigation plans according to their organizations’ goals.

The first section provides reference frameworks for implementing an insider threat mitigation program with the Intelligence and National Security Alliance (INSA) Insider Threat roadmap, Carnegie Mellon University's Computer Emergency Response Team (CERT) insider threat best practices, CERT insider threat program components, National Institute of Standards and Technology (NIST) Cybersecurity Framework, and other relevant guidance. This section provides an implementation case study of an insider threat mitigation program for an hypothetical organization.

The second section of this paper will present example use cases on implementing operational insider threat detection indicators by using a risk scoring methodology and Splunk. A single event might not be considered anomalous, whereas a combination of events assigned a high-risk score by the methodology might be considered anomalous and require further review. A risk scoring method can assign a risk score for each user/identity for each anomalous event. These risk scores are aggregated daily to identify username/identity pairs associated with a high risk score. Further investigation can determine if any insider threat activity was involved. This section explains how to implement a statistical model using standard deviation to find anomalous insider threat events. The goal is to provide implementation examples of different use cases using a risk scoring methodology to implement insider threat monitoring.
Introduction

An insider threat mitigation program is a top priority for senior executives. According to the 2015 Vormetric Insider Threat Report, "92 percent of IT leaders felt their organizations were either somewhat vulnerable to insider threats, while 49 percent said they felt very or extremely vulnerable to insider threats". An insider threat incident is typically caused by authorized individuals who have unfettered access to sensitive data. Insider threat mitigation requires a coordinated effort from many stakeholders including the C-Suite, human resources (HR), ethics, legal counsel, compliance, physical security, information technology (IT), information security, and data owners. The insider threat mitigation approach should have a structured program with senior management support addressed by policies, procedures, and technical controls. The goal of an insider threat mitigation program is to reduce the risk related to insider threats to an acceptable level. The kill chain model provides a framework for understanding various activities and stages which the adversary goes through from reconnaissance to exfiltration of data. Due to the nature of the threat, an insider threat is far more complicated and does not have defined stages, similar to the kill chain model. Figure 1 below, is a good representation of the activities involved in mitigating an insider threat risk.

Figure 1 – Goal of Insider Threat Mitigation Program

Security practitioners should align the insider threat mitigation program elements with the people, process, data and technology requirements of the organization.
Section I

1.0 Insider Threat Mitigation Best Practices

An organization can develop an insider threat mitigation program by tailoring and mapping the organization-specific elements to the INSA roadmap, CERT best practices, CERT Insider Threat program components, and the NIST Cybersecurity Framework. The frameworks are briefly explained in the section below.

1.0.1 INSA Insider Threat Mitigation Program Roadmap

The Insider Threat team from the Intelligence Community (IC) Analyst-Private Sector Partnership Program developed a resource that provides the essential elements required to initiate an insider threat mitigation program. The graphic below, figure 2, represents the 13 elements involved in implementing an insider threat mitigation program.

Figure 2 – INSA Insider Threat Roadmap

These 13 steps in the INSA road-map are explained with practical guidance in the references section of this paper, which cover all the required elements of establishing an insider threat mitigation program. The reference section has a mapping of 200 insider threat publications for the 13 essential elements.
1.0.2 CERT Insider Threat Program Best Practices & Components

The CERT Insider Threat Center has identified a set of key components that are necessary to produce a fully functioning insider threat program. The graphic below, Figure 3, represents the key components identified by CERT. Source: (CERT, 2015)

Figure 3 – CERT Insider Threat Components

The CERT Insider Threat program component references can be used to strengthen the insider threat mitigation work program. Please refer to Appendix B for CERT Insider Threat mitigation program elements and CERT Common Sense Guide to Mitigating Insider Threats.

1.0.3 NIST Cybersecurity Framework

The NIST Cybersecurity Framework can be utilized to implement an insider threat mitigation program. The NIST Cybersecurity Framework emphasizes processes/capabilities and supports a broad range of technical solutions. While organizations may develop overall threat profiles, this insider threat mitigation profile example illustrates how organizations may apply the framework to mitigate insider threat risks. The NIST reference¹ provided below demonstrates how organizations may use the NIST Cybersecurity Framework to mitigate Insider Threat.

1.0.4 Best Practices for Insider Threats – SIFMA

Focusing on the banking sector, the Securities Industry and Financial Markets Association (SIFMA) has created a comprehensive set of best practices guide to provide a framework to
create an effective insider threat mitigation program. This guide recommends using the NIST Cybersecurity Framework for implementing an insider threat mitigation program. This guide has relevant information on legal aspects related to insider threat mitigation program. The reference section has the download links for this best practice guide.

For additional information on these frameworks, the reference section has further guidance.

1.1 Mapping the Insider threat implementation frameworks

A key advantage of mapping the organization-specific insider threat mitigation program elements to industry standards is that each organization can ensure that industry best practices are incorporated. The insider threat program implementation can be benchmarked and improved in the future with this mapping as the industry standards evolve. The below table provides mapping between the different insider threat implementation frameworks for reference:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ITMP Step 1 - Initial Planning</td>
<td>• Establishing an Insider Threat Program</td>
<td>• Develop a formalized insider threat program.</td>
<td>• Identify - Asset Management</td>
</tr>
<tr>
<td></td>
<td>• The Insider Threat Framework</td>
<td>• Know your assets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Implementation Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The Formalized Program</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITMP Step 2 - Identify Stakeholders</td>
<td>• Participation of Business Areas</td>
<td>• Not applicable</td>
<td>• Not applicable</td>
</tr>
<tr>
<td></td>
<td>• Not applicable</td>
<td>• Not applicable</td>
<td></td>
</tr>
<tr>
<td>ITMP Step 3 - Leadership Buy-in</td>
<td>• Not applicable</td>
<td>• Not applicable</td>
<td>• Not applicable</td>
</tr>
<tr>
<td>ITMP Step 4 - Risk Management Process</td>
<td>• Integration with Enterprise Risk Management</td>
<td>• Consider threats from insiders and business partners in enterprise-wide risk assessments.</td>
<td>• Identify - Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>• Not applicable</td>
<td>• Identify - Risk Management Strategy</td>
<td></td>
</tr>
<tr>
<td>ITMP Step 5 - Detailed Project Planning</td>
<td>• Not applicable</td>
<td>• Not applicable</td>
<td>• Not applicable</td>
</tr>
<tr>
<td>ITMP Step 6 - Develop Governance Structure, Policy, and Procedures</td>
<td>• Policies, Procedures, and Practices</td>
<td>• Clearly document and consistently enforce policies and controls.</td>
<td>• Identify – Governance</td>
</tr>
<tr>
<td></td>
<td>• Protection of Employee Civil Liberties and Privacy Rights</td>
<td>• Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.</td>
<td>• Protect - Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Anticipate and manage negative issues in the work environment.</td>
<td>• Protection Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Implement strict password and account management policies and practices.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enforce separation of duties and least privilege.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Define explicit security agreements for any cloud services, especially access restrictions, and</td>
<td></td>
</tr>
</tbody>
</table>
Insider Threat Mitigation Guidance

<table>
<thead>
<tr>
<th>ITMP Step 7 - Communication, Training &amp; Awareness</th>
<th>• Training and Awareness</th>
<th>• Incorporate insider threat awareness into periodic security training for all employees.</th>
<th>• Respond – Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Communicating Insider Threat Events</td>
<td></td>
<td>• Protect - Awareness &amp; Training</td>
</tr>
<tr>
<td>ITMP Step 8 - Develop Detection Indicators</td>
<td>• Prevention, Detection, and Response</td>
<td>• Establish a baseline of normal network device behavior. Close the doors to unauthorized data exfiltration.</td>
<td>• Detect - Anomalies &amp; Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Detect - Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Detect - Detection Processes</td>
</tr>
<tr>
<td>ITMP Step 9 - Data &amp; Tool Requirements</td>
<td>• Data Collection and Analysis</td>
<td>• Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.</td>
<td>• Protect - Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Protect - Protective Technology</td>
</tr>
<tr>
<td>ITMP Step 10 - Data Fusion</td>
<td>• Data Collection and Analysis</td>
<td>• Not applicable</td>
<td>• Not applicable</td>
</tr>
<tr>
<td>ITMP Step 11 - Analysis and Incident Management</td>
<td>• Incident Response Planning Confidential Reporting</td>
<td>• Not applicable</td>
<td>• Respond - Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Respond – Mitigation</td>
</tr>
<tr>
<td>ITMP Step 12 - Management Reporting</td>
<td>• Oversight of Program Compliance and Effectiveness</td>
<td>• Not applicable</td>
<td>• Not applicable</td>
</tr>
<tr>
<td>ITMP Step 13 - Feedback &amp; Lessons Learned</td>
<td>• Not applicable</td>
<td>• Not applicable</td>
<td>• Recover - Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Recover - Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Recover – Communications</td>
</tr>
</tbody>
</table>

1.2 Legal Considerations for Insider Threat Mitigation Program

Although the insider threat mitigation programs can protect organizations from potentially crippling theft and system damage, they may also expose the organizations to some legal risk. Section V in Insider Threat Best Practice - SIFMA report (SIFMA, 2014) details the primary laws that may apply to an insider threat mitigation program in the United States. It also provides an overview of some of the relevant legislation in the U.K., Germany, Hong Kong, and India. There may be other applicable laws and regulations depending on the relevant facts and circumstances. CERT CMU has excellent references for legal aspects related to insider threat in many countries similar to this research paper\(^2\). This section is not intended to provide legal advice. Prior to instituting any insider threat mitigation program, organizations should engage in a thorough legal analysis and consult with their legal counsel.

dfir.aaa@gmail.com

© 2015 The SANS Institute  Author retains full rights.
1.3 Case Study - Implementing Insider Threat Mitigation program for GIAC Corporation

This section provides a detailed case study for implementing an insider threat mitigation program for a hypothetical company, GIAC Corporation, using the insider threat mitigation frameworks.

1.3.0 Background

The GIAC Corporation is a software services company that has been performing well (double-digit revenue growth), and recently, it started supporting US federal government projects. In November 2012, U.S. President Obama issued a MEMORANDUM FOR ALL AGENCIES UNDER HIS JURISDICTION entitled, “The National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.” The policy requires all U.S. government executive departments and agencies that access classified information to establish insider threat detection programs. Now it is becoming even more important for private sector organizations supporting the U.S. government to implement the insider threat mitigation program. There was a recent mandate to have all sub-contractors and private organizations supporting the federal government implement an insider threat program. The GIAC Corporation is facing this regulatory compliance requirement to implement an insider threat program. The GIAC Corporation appointed an experienced senior person as the insider threat program manager to implement the insider threat program. The insider threat program manager developed the insider threat mitigation program by tailoring and mapping the GIAC organization-specific insider threat mitigation program elements to the INSA road-map, CERT best practices, CERT Insider Threat program components, and the NIST Cybersecurity Framework.

1.3.1 ITMP Step 1 - Initial Planning

As one of the first steps, the newly appointed insider threat program manager in the GIAC Corporation gathered input from the existing program and performed a comprehensive assessment of the current state and recommended a future state to mitigate insider threats.

As an example, the table below shows recommendations from the gaps assessment of GIAC Corporation’s focus areas. The focus areas are grouped according to GIAC Corporation’s needs.
### Focus Areas

<table>
<thead>
<tr>
<th>Policies and Procedures</th>
<th>Recommendations from results of GIAC Corporation’s Insider Threat Gap assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Enhance policies to explicitly require the GIAC Corporation to monitor and/or prevent the movement of sensitive data to insecure locations including external devices and outbound connections</td>
</tr>
<tr>
<td></td>
<td>- Develop a tiered background vetting and validation framework for employees and contractors based on their role and access to key assets</td>
</tr>
<tr>
<td>Incident Response</td>
<td>- Establish an insider threat program to champion policies, frameworks, behavioral monitoring, and response requirements</td>
</tr>
<tr>
<td></td>
<td>- Enhance Incident Response plan to include specific procedures for handling incidents potentially involving insiders</td>
</tr>
<tr>
<td>Checkout Procedures</td>
<td>- Include enhanced monitoring of planned departing insiders as part of the insider threat monitoring program</td>
</tr>
<tr>
<td>Awareness Training</td>
<td>- Enhance security awareness program to:</td>
</tr>
<tr>
<td></td>
<td>- Include themes specific to insider threats</td>
</tr>
<tr>
<td></td>
<td>- Reinforce the message with continuous campaigns</td>
</tr>
<tr>
<td></td>
<td>- Include modules targeting individual groups such as privileged users and management</td>
</tr>
<tr>
<td></td>
<td>- Additionally, encourage users to utilize secure alternatives to move sensitive data</td>
</tr>
<tr>
<td>Compliance and Enforcement</td>
<td>- Develop a sensitive data monitoring program where the organization affirms that users are properly classifying and storing sensitive information and conduct a regular review of where sensitive information is being stored</td>
</tr>
<tr>
<td>Technical Controls</td>
<td>- Develop a monitoring program to detect and respond to at-risk insider behavior; define use cases for behavioral indicators</td>
</tr>
<tr>
<td></td>
<td>- Develop criteria for enhancing the monitoring of privileged administrators</td>
</tr>
<tr>
<td></td>
<td>- Include enhanced monitoring of planned departing insiders as part of the insider threat monitoring program</td>
</tr>
</tbody>
</table>

The reference is a template for the initial gap assessment based on the CERT best practices.

### 1.3.2 ITMP Step 2 - Identify Stakeholders

The GIAC Insider threat program manager identified all the key stakeholders in the GIAC Corporation who need to participate in the insider threat program. Every organization may have different departments responsible for dealing with insider threat risks, so it is critical to identify and involve the appropriate stakeholders in the insider threat program. The GIAC Insider threat program manager incorporated stakeholder groups to include key members from human resources (HR), legal counsel, physical security, information technology (IT), communications and ethics and compliance teams. Some of the key members included are the Chief Information Officer, Chief Information Security Officer, Business Unit Leads, HR Vice President, Chief Counsel, Chief Privacy Officer, Infrastructure Lead, and the Application Development Lead.
1.3.3 ITMP Step 3 - Leadership Buy-in

After determining the stakeholders who need to be involved, the GIAC insider threat program manager formed the insider threat steering committee with the senior executive management team from each primary function. The role of this steering committee is to provide guidance and prioritize the insider threat mitigation program. The GIAC insider threat program manager obtained a buy-in from the steering committee by explaining the risk involved and how the insider threat mitigation program reduces risk. The GIAC insider threat program manager also established the insider threat working group at the operational level with the primary team members who handle the implementation of the insider threat program.

1.3.4 ITMP Step 4 - Risk Management Process

The GIAC insider threat program manager worked closely with the CISO and the information security/risk team to integrate the insider threat mitigation program with the overall organizational cyber security strategy and risk management plan. The risk management plan, including the insider threat risks, will provide the complete risk picture to senior executives. The GIAC Organization followed the ISO 3100 risk management framework and a three-tier risk rating model. The Insider threat mitigation program applied the risk management process, and the activities were prioritized based on the risk ratings.

1.3.5 ITMP Step 5 - Detailed Project Planning

The GIAC insider threat program manager worked with the IT program management office (PMO) to submit the project charter and the detailed project plan for the insider threat mitigation project. The GIAC insider threat program manager obtained the GIAC organizational framework, templates and process for managing projects and programs. The detailed project plan includes all the resources that were required for implementation. This phase is critical since every organization has program governance for managing projects, releasing funds and managing resources. The GIAC insider threat program manager aligned the insider threat mitigation program with GIAC organizational processes and metrics. As an example, the GIAC insider threat program manager created six projects as per initial assessment and recommendations: Policies and Procedures, Incident Response, Checkout Procedures, Awareness Training, Compliance and Enforcement and Technical Controls.
1.3.6 ITMP Step 6 - Develop Governance Structure, Policy, and Procedures

Based on prior experience, the GIAC insider threat program manager understands that every phase of the insider threat mitigation program involves a human element, so an insider threat is a highly sensitive topic in many aspects. The clear definition of policy and procedures with inputs from all stakeholders is vital. The GIAC insider threat program manager’s goal was to enhance policies to require the GIAC Corporation to monitor and/or prevent the movement of sensitive data to insecure locations, including external devices and outbound connections. The enforcement of insider threat policies should be implemented with the support of the associated stakeholders. The GIAC insider threat program manager consulted and worked with all the interested parties to finalize the policy. The insider threat policy and procedures were defined by taking into account all the considerations including organizational culture and legal and privacy concerns. While it is important to implement technical solutions for monitoring, the GIAC insider threat program manager ensured appropriate policies and procedures are in place before establishing a dedicated monitoring program.

1.3.7 ITMP Step 7 - Communication, Training & Awareness

The GIAC Corporation has established teams responsible for information security awareness, communication, and employee learning/training. The GIAC Insider threat program manager works with the information security awareness team leader to ensure that the insider threat components are incorporated as a part of the awareness program and is continuously updated. The GIAC insider threat program manager worked with the corporate communications team leader to establish a communication strategy for the insider threat mitigation program’s roll-out.

As an example, the GIAC insider threat program manager created the updated security awareness and communication plan by working with the information security team members and the communication team members.

<table>
<thead>
<tr>
<th>Type &amp; Length</th>
<th>Description</th>
<th>Minimum Frequency</th>
<th>Possible Communication Method(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Quick Tips - One paragraph** | An Insider threat-related information security tip about countermeasures that mitigate risks or reminders about security awareness policies or compliance deadlines. Examples include steps to locking a desktop, proper disposal of confidential data, and never to open email from unknown sources. | **Biweekly** | Tip of the Day "Did You Know?"

LCD Displays |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flash Video / PowerPoint Slide - 10-15 seconds of animated characters or other graphical content</strong></td>
<td>Attention grabbing a video or slide to increase users' awareness of the importance of information security, countermeasures that mitigate risks, or compliance deadlines. Examples include theme based cartoons showing the outcomes of bad security practices, illustrated steps to locking a desktop, and dos and don'ts of security.</td>
<td><strong>Monthly</strong></td>
<td>LCD Displays</td>
</tr>
</tbody>
</table>
| **Newsletters - Two or more multi-paragraphed articles** | Information about latest insider threats to the GIAC Corporation, countermeasures that mitigate risks or reminders about security awareness policies or compliance deadlines. | **Quarterly** | Newsletter

Targeted Communications |
| **PowerPoint Presentation - 30-60 minutes** | The insider threat awareness presentation can be focused on questions and answers from the business regarding information security or a formal presentation on a security topic. Examples include role-based training lunch-and-learns, a how to protect personal data and identity, and a walkthrough of available security tools. | **Quarterly** | Brown Bag Lunches

Hard Copy Handouts |
| **Regular Publications - Multi paragraphed publication** | Insider threat focused publication located on Intranet Portal. This could include articles, policies, guidelines, or standards published. | **Semi-Annually** | Intranet Site |
| **Posters - Graphical content with limited text** | Tips and other insider threat focused content that is delivered with a fun and engaging graphic. Examples include a fun graphic depicting a good and bad security situation, and multiple graphics showing illustrated quick tips. | **Semi-Annually** | Poster Holders |
| **eLearning Computer Based Training (CBT) - Multiple pages and/or modules, including video, text, and graphical animations no longer than 45 minutes.** | Computer-based training (CBT) courses to enhance user's level of security awareness, increase role based security knowledge, and meet awareness and training compliance requirements. | **Annually** | Learning Management System |
| **Pamphlets and Fliers - Limited bulleted text with graphics** | Handouts for staff to use as a reference that capture information security procedures, guidelines, or countermeasures that mitigate insider threat risks. Examples include tri-folds for staff to use as security reference material, quick reference guide for data classification. | **Annually** | Hard Copy Handouts |
1.3.8 ITMP Step 8 - Develop Detection Indicators

The GIAC insider threat program manager worked with the information security team to develop a user activity monitoring solution using existing log sources in Splunk. As an example, the table below shows some of the sample detection indicators developed by the GIAC insider threat program manager for discovering insider threat activity.

Sample Detection Indicators for Discovering Insider Threats with Data Sources

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Parameters (hypothetical)</th>
<th>Data Source Required</th>
</tr>
</thead>
</table>
| 1. Excessive data upload to file-sharing service (Dropbox, Cloud) or Large data transfers | More than 100 uploads or 10 GB of data | o Web Proxy/Next Generation Firewall  
o DNS  
o E-Mail Gateway |
| 2. Unauthorized Removable Media use (USB Thumb Drive, External Hard Drives, digital cameras) | Large amount of data being transferred and any additional, unauthorized use | o MS Windows  
o Unix |
| 3. Excessive data alteration and deletion/wiping, especially by high-risk groups (e.g. administrators) | Use of non-approved tools, More than 10 GB in a 24 hour period | o MS Windows  
o Unix  
o Network devices  
o Document Repositories |
| 4. Attempts to access segregated/escalated systems/file shares/databases | More than three attempts to access a segmented or unauthorized system | o MS Windows  
o Unix  
o Network devices  
o Document Repositories |
| 5. Unauthorized user web activity (hate sites, pornography, pirated, job search sites) that indicate low productivity, job discontent, and potential legal liabilities | Monitor external Internet activity and track access attempt to blacklisted sites | o Web Proxy/Next Generation Firewall  
o DNS  
o E-mail Gateway |
| 6. Transactional triggers on business systems | Business logic triggers that would capture misuse of access and rights | o MS Windows  
o Unix  
o Network devices  
o Document Repositories |
| 7. Sensitive keyword searching | Designated confidential or sensitive keywords or data | o MS Windows  
o Unix  
o Network devices  
o Document Repositories |
| 8. Excessive printing | Exceeding 200 pages/day | o MS Windows |
Section II shows examples using Splunk that can be used in correlation with other events to detect anomalies in individual users. Any SIEM software solution can be used to capture and create alerts on an insider threat. Some of these detection indicators might be considered intrusive in some organizations so careful consideration should be given in the selection of these detection indicators. As explained in the policies and procedures section earlier these detection indicators should be approved by the steering committee, legal, human resources and other required stakeholders before implementation.

1.3.9 ITMP Step 9 - Data & Tool Requirements

Insider threat detection involves obtaining a diverse set of data, from proxy logs to HR records. The GIAC Corporation has a mature implementation of Splunk to collect logs from various data sources. The GIAC insider threat program manager worked with the information security team to identify gaps in the collection of logs and created a plan to make sure all the required logs are captured as part of the insider threat mitigation program. A reference from Splunk has explained the ICS 500-27 audit data requirements.

1.3.10 ITMP Step 10 - Data Fusion

There are several databases designed specifically for efficient storage and query of Big Data, including Splunk, Hunk, ELK, OpenSOC, Hadoop, Cassandra, CouchDB, Greenplum Database, HBase, MongoDB, and Vertica. Since the GIAC Organization had Splunk implemented, for the first phase, the insider threat program manager decided to use Splunk for insider threat-detections. The GIAC Organization also has an in-house Hadoop implementation, which includes a Hadoop integration with Splunk for further enhancement of insider threat detection. That was considered for future phases of the insider threat program. Appendix B explains in detail some Big Data solutions for building customized solutions for reference.
1.3.11 ITMP Step 11 - Analysis and Incident Management

The GIAC insider threat program manager understands the importance of a well-established incident management process incorporating insider threat components. The HR, compliance and ethics teams were involved in following the GIAC organizational framework for insider threat investigations. During the beginning of the investigation, most of the incidents might seem harmful. Careful examination should be performed to understand the context and the investigations should be very objective. During an external attack and exfiltration, it might be very clear in most of the cases that the bad actors are trying to steal data. During insider threat based incidents, there is a possibility that smart and motivated employees sometimes bend the rules to get things done. Especially with Shadow IT, some of the IT savvy GIAC employees copy data to cloud drives to work from home. For example, one incident investigation that initially had indications of data theft finally turned out to be a minor policy violation. In this case, a script was used by the senior employee to copy data to an external cloud drive during off hours. After proper investigations, the senior employee revealed that he/she had run the script to copy data during off hours so the latest data would be available the next day when he/she works from home. There was no malicious data theft; this is a minor policy violation, and appropriate remediation action should be taken according to the established framework.

The GIAC insider threat program manager ensured that the incident framework would provide access to log data to investigators only after obtaining proper approvals. The roles and responsibilities were also clearly defined, so there was enough authority established for the investigations team to perform the required investigative and remediation activities.

1.3.12 ITMP Step 12 - Management Reporting

Management reporting is vital to obtaining continued support from management and understanding what keeps them up at night. It also enables the continuous updating of the insider threat mitigation program accordingly. The GIAC insider threat program manager ensures that the program is on the radar of the management by highlighting the progress and risks at the right time. The GIAC program manager used business intelligence tool Tableau to highlight the improvements to the risk posture.
1.3.13 ITMP Step 13 - Feedback & Lessons Learned

Constant feedback and lessons learned ensure that the insider threat mitigation program adapts to organizational changes and external best practices and frameworks as they become available. The GIAC insider threat program manager obtained the buy-in to continue to ensure the insider threat working group has consistent communications and feedback from the different stakeholders.

As seen in the above case study, one of the major investments was appointing a senior insider threat program manager for leading the insider threat mitigation program. All the other program activities were performed by utilizing the existing people, process and technology in the GIAC Corporation. This case study should be considered an example highlighting some critical aspects of the implementation of an insider threat mitigation program. Each organization should tailor its insider threat mitigation program based on their environment and requirements.

Section II

This section of the paper will provide example insider threat activity detection use cases using Splunk. The use cases will demonstrate the implementation of operational insider threat detection indicators by using risk scoring methodology. A single event might not be considered anomalous. However, a combination of events assigned a high-risk score might be considered anomalous and might require further review. Risk scoring method assigns risk scores for each user/identity for each anomalous event. These risk scores are aggregated daily to identify username/identity pairs associated with a high risk score. Further investigation can determine if any insider threat activity was involved.

2.1 Risk Scoring Methodology

Step 1 – Identify anomalous events based on baseline or threshold

The baseline or threshold can be designed based on analyzing data from past events. Depending upon the organization and prior experience, in some cases, a simple numeric threshold like transferring more than 1 GB of data to an external drive can be considered anomalous event. In some cases, a statistically significant event like the total amount of data (in bytes) transferred to
USB drive that is three standard deviations more or less than the average can be considered anomalous event.

Step 2 – Assign risk scores for each user/identity for each anomalous event

The risk score can be assigned depending upon the organization’s data and the environment. In some cases, there can be higher risk scores if sensitive data or people are involved.

Step 3- Aggregate all the risk scores per day to identify top user/identity that requires further investigation to determine any Insider threat activity involved.

2.2 Use Case - Risk Score for fraud detection with web server access logs

The use case provided below is for creating a baseline and assigning risk scores for purchases made from web server based on suspicious session-id and user agents found in the web server access logs.

<table>
<thead>
<tr>
<th>Splunk Command</th>
<th>Explanation</th>
<th>Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>source=access.log method=POST action=purchase</td>
<td>1. Defines source and provides all results with action=purchase for one day 2. Calculates distinct count(dc) of JSESSIONID by clientIP 3. Stores the distinct count for each clientip per day in summary index sstats</td>
<td>Query all purchases made and calculate how many unique session id’s was assigned for client IP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Defines source and provides all results with action=purchase for one day 2. Calculates distinct count(dc) of useragent by clientIP 3. Stores the distinct count for each clientip per day in summary index uastats</td>
<td>Query all purchases made and calculate how many unique user agents for single client IP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>index=sstats</td>
<td>1. Calculates the average and standard deviation of the session id’s per day 2. If session id is 2 standard deviations more or less than the average session id add risk score by 20 3. Stores the risk score for each clientIP in summary index ipriskscore</td>
<td>If the number of unique session id’s per day is 2 standard deviations more or less than the average, then add risk score by 20. In this use case, session id greater than average considered anomalous.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>index=uastats</td>
<td>1. If user agent count is greater than 2 add risk score by 40 3. Stores the risk score for each clientIP in summary index ipriskscore</td>
<td>If the number of user agents greater than two, add risk score by 40. In this use case user agents greater than 2 considered anomalous.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>index=ipriskscore</td>
<td>Calculate total risk score per day for each clientip and sort the results</td>
<td>Calculate total risk score per day for each clientip that accessed the website and made purchases. This step calculates the aggregate risk score for each client IP.</td>
</tr>
<tr>
<td>source=access.log method=POST action=purchase</td>
<td>1. Defines source and provides all results with action=purchase for one day 2. Calculates distinct count(dc) of JSESSIONID by clientIP 3. Stores the distinct count for each clientip per day in summary index sstats</td>
<td>Query all purchases made and calculate how many unique session id’s was assigned for client IP.</td>
</tr>
</tbody>
</table>

Source: dfir.aaa@gmail.com
2.3 Use Case – Risk score for user activity based on login duration and browsing activity

The following use case is creating a baseline and assigning risk scores based on browsing activity and login duration.

<table>
<thead>
<tr>
<th>Splunk Command</th>
<th>Explanation</th>
<th>Logic</th>
</tr>
</thead>
</table>
| source=\texttt{http.csv
dropbox.com} | 1. Defines source and provides all results with dropbox.com for one day | Query all web traffic to dropbox.com and calculate how many times the user has accessed the site. |
| \texttt{\textbackslash bin\_time span=1d} | 2. Calculates distinct count (dc) of id by user | |
| \texttt{\textbackslash stats dc(id) by \_time user} | 3. Stores the distinct count for each user per day in summary index dcount | |
| \texttt{\textbackslash rename dc(id) as count} | | |
| \texttt{\textbackslash collect index=dcount} | | |

<table>
<thead>
<tr>
<th>Splunk Command</th>
<th>Explanation</th>
<th>Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>source=\texttt{logon.csv}</td>
<td>1. Defines source and provides all results for one day</td>
<td>Calculates login duration for all users for each day.</td>
</tr>
<tr>
<td>\texttt{\textbackslash bin_time span=1d}</td>
<td>2. Calculates login duration for user with transaction command</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash transaction user \textbackslash startswith=&quot;activity=Logon&quot;}</td>
<td>3. Stores the duration for each user per day in summary index loginduration</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash endswith=&quot;activity=Logoff&quot;}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash table _time,duration,user}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash collect index=loginduration}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Splunk Command</th>
<th>Explanation</th>
<th>Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{\textbackslash index=dcount}</td>
<td>1. Calculates the average count per day</td>
<td>If the number of visit to dropbox.com per day is 2 standard deviations more or less than the average, then add risk score by 20.</td>
</tr>
<tr>
<td>\texttt{\textbackslash eventstats avg(count) as avgcount, stdev(count) as stdevc}</td>
<td>2. If count is 2 standard deviations more or less than the average add risk score by 20</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash where (count &gt; avgcount + 2 * stdevc) or (count &lt; avgcount - 2 * stdevc)}</td>
<td>3. Stores the risk score for each user in summary index userriskscore</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=Risk_Score+20}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=Risk_Score+0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash table _time,user,Risk_Score}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash collect index=userriskscore}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Splunk Command</th>
<th>Explanation</th>
<th>Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{\textbackslash index=loginduration}</td>
<td>1. If login duration is greater than 8 add risk score by 20</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval dhour=duration/3600}</td>
<td>2. Stores the risk score for each user in summary index userriskscore</td>
<td>If login duration greater than 8, add risk score by 20. In this use case, login duration greater than 8 hours considered anomalous.</td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td>3. Stores the risk score for each user in summary index userriskscore</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.4 Use Case – Risk score for user activity based on Windows Active Directory events

The following use case is creating a baseline and assigning risk scores based on user activity in Windows active directory logs.

<table>
<thead>
<tr>
<th>Splunk Command</th>
<th>Explanation</th>
<th>Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{\textbackslash sourcetype=&quot;WinEventLog:Security&quot;}</td>
<td>Defines log source as Windows security event log</td>
<td>Query all Windows events and assigns risk scores if there are any anomalous events for the user account.</td>
</tr>
<tr>
<td>\texttt{\textbackslash bin_time span=1d}</td>
<td>Defines Time duration as one day</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=0}</td>
<td>Assigns Risk_Score value zero</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=if(EventId=1102 OR EventId=517),Risk_Score+3,Risk_Score+0}</td>
<td>Increase Risk_Score value by three if event id is related to audit log cleared</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=if(EventId=4663 AND Accesses = &quot;DELETE&quot; AND Object_Type=File),Risk_Score+1,Risk_Score+0}</td>
<td>Increase Risk_Score value by one if event id is related to file deletions by user account.</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash eval Risk_Score=if(EventCode=576 OR EventCode=4672 OR EventCode=577 OR EventCode=4673 OR EventCode=578 OR EventCode=4674), Risk_Score+2, Risk_Score+0}</td>
<td>Increase Risk_Score value by two if event ids are related to</td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash table _time,Account_Name,Risk_Score}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\texttt{\textbackslash collect index=adriskscore}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In these three examples, summary indexes were used to capture the results of risk scores and append the risk scores. A lookuptable or KV store can also be used to accomplish the task in Splunk. The example is developed to meet the sample log data. In real use cases, Splunk queries can be modified for relevant use cases unique to a Splunk implementation (e.g., identify maximum bytes transferred by the user).

These queries are designed for sample data. The Splunk queries are tested with sample data, and screenshots are provided in Appendix D. These Splunk queries are good examples of how Splunk can be used to trend and baseline user activity and assign risk scores. Hopefully, some of the examples above would be useful to create baselines. Splunk queries can be used to extend risk score model to different use cases. In real use cases, Splunk queries can be modified for relevant use case covered in the Data & Tool requirements section.

Capturing User Activity - Daily Per-User Calculations

Baselining user activity examples are highlighted in the table below. Daily aggregated risk score can be assigned once the daily calculations are performed, using summary indexes or lookup tables. Daily aggregated risk scores can be used to detect insider threat activities/anomalies.

<table>
<thead>
<tr>
<th>At-Risk Activity</th>
<th>Daily Calculated Values</th>
<th>Splunk Query Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data upload</td>
<td>• Egress Bytes [SUM]</td>
<td>Egress Bytes [SUM]</td>
</tr>
<tr>
<td></td>
<td>• Egress Packets [COUNT]</td>
<td>source=firewall</td>
</tr>
<tr>
<td></td>
<td>• URL string [LENGTH]</td>
<td>source=proxy</td>
</tr>
<tr>
<td></td>
<td>• DNS query [LENGTH]</td>
<td>source=dns</td>
</tr>
<tr>
<td></td>
<td>• User agent string [LENGTH]</td>
<td>source=WinRegistry</td>
</tr>
<tr>
<td>Removable media</td>
<td>• Unique serial numbers [COUNT]</td>
<td>Unique systems accessed with Removable Media [COUNT]</td>
</tr>
<tr>
<td></td>
<td>• Unique systems accessed with Removable Media [COUNT]</td>
<td>source=WinRegistry</td>
</tr>
<tr>
<td></td>
<td>• Bytes transferred [SUM]</td>
<td>source=WinRegistry</td>
</tr>
<tr>
<td></td>
<td>• Files transferred [SUM]</td>
<td>source=WinRegistry</td>
</tr>
<tr>
<td>Print</td>
<td>• Number of printers utilized [COUNT]</td>
<td>Number of pages printed [SUM]</td>
</tr>
</tbody>
</table>
Different user populations have various levels of abnormality present. Peer groups can be calculated by assessing user’s activities for each estimated value (bytes out of network, removable media count, sensitive document access, etc.) in addition to their assigned roles. This additional comparison allows users own past actions to self-define who they operate most like and then to perform comparisons against like-acting peers.

**Model using Statistical Deviations**

With visibility of the user actions on a daily basis, a complete statistical model can be applied to the daily user activity to calculate anomalous events using the following rules:

- Calculate the Average and the Standard Deviation for each of the Calculated Values for each User on Daily, Weekly, and Monthly time windows
- Daily comparison of the User’s actions for each activity on that assessed Day, the prior Week from the current day, and previous Month from the current day
- All calculated values that are sufficiently different from the average via standard deviation comparison are to be identified as anomalous and assigned a risk score
- The user(s) on a daily basis with the highest risk scores across the Daily, Weekly, and Monthly measurements are to be identified as highest potential risk

A standard deviation of 2.5 can be used for the initial threshold of calculated value deviation. This allows for the most common activities to be ignored but in the initial review period of the...
analysis doesn’t require excessively anomalous activity to be identified. Also the calculation of average / standard deviation should exclude the most recent activity (15% of total days measured not included) so that emerging changes will be identified based on the profile from past actions, not present. This statistical model explained above can be implemented using Splunk.

The Splunk examples above are modified queries to match the test data. Security practitioners should modify all the examples according to the Splunk implementation and configuration of the particular instance used by the organization. Splunk also had numerous apps that will assist with insider threat use cases such as the Splunk Enterprise Security(ES), Windows security operations center, and the Palo Alto app that has dashboards that can be utilized. Splunk Dashboards can be created to display queries that are developed related to insider threat monitoring. Alerts can also be configured based on daily aggregate risk scores for immediate action by the dedicated insider threat monitoring team. For further guidance, see the Splunk references section.

There are many developments happening in this solution space and many vendors are offering commercial solutions like Prelert, DarkTrace, Niddel, Securonix, Novetta, Dtex, Niara to name a few companies. Some of them use machine learning algorithms to identify normal and based on the baseline they detect anomalies for detecting both insider and external threats.

Some of this user activity monitoring might be considered intrusive in some organizations so careful consideration should be given in the selection of these models and rules. As explained in the policies and procedures section earlier these monitoring rules should be approved by the insider threat steering committee, legal, human resources and other required stakeholders before implementation.
3.0 Conclusion

Insider threats are complex and require a multi-year strategy with planning. Each organization should tailor their approach to meet their needs. The goal of this paper is to provide relevant best practices, policies, frameworks and tools available for implementing good insider threat mitigation program. The appendixes in this paper cover additional topics and references that will be useful in the implementation of an insider threat mitigation program.

Information security teams can develop comprehensive insider threat mitigation program by combining the INSA road-map with CERT best practices, CERT Insider Threat program components, NIST Cybersecurity Framework and other relevant references. This paper is only meant to provide an overview of frameworks, tools and policies for implementing an insider threat mitigation program. External consultants can provide more tailored and detailed assistance and feedback. In addition to private consultants, there are a number of non-profit and government resources that can provide support. The CERT Insider Threat Division of the Software Engineering Institute at Carnegie Mellon University, a federally funded research, and development center is one such example. The CERT Insider Threat Division hosts workshops on developing insider threats, works with organizations on program development, and provides training and certification courses to insider threat program managers and assessors.

Security practitioners can use this paper as a reference and customize the tools and frameworks according to their organizational needs.
References


92 percent of IT leaders felt their organizations were either somewhat vulnerable to insider threats, while 49 percent said they felt very or extremely vulnerable to insider threats. #2015InsiderThreat. (2015, March 19). Retrieved July 24, 2015, from http://www.vormetric.com/campaigns/insiderthreat/2015/


dfir.aaa@gmail.com


dfir.aaa@gmail.com


Carly L. Huth and Robin Ruefle, Components and Considerations in Building an Insider Threat Program (Nov. 7, 2013), http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69076


Splunk References


dfir.aaa@gmail.com


Appendix A

CERT Insider Threat Program Components

CERT Insider Threat Center has identified a set of key components that are necessary to produce a fully functioning insider threat program. Source: (CERT, 2015)

CERT Insider threat program component references can be used to strengthen the Insider threat mitigation work program.

Establishing an Insider Threat Program (Part 1 of 18)


Key Elements of an Insider Threat Program (Part 2 of 18)


The Formalized Program (Part 3 of 18)


Participation of Business Areas (Part 4 of 18)

Oversight of Program Compliance and Effectiveness (Part 5 of 18)


Integration with Enterprise Risk Management (6 of 18)


Prevention, Detection, and Response (Part 7 of 18)


Training and Awareness (Part 8 of 18)


Confidential Reporting (Part 9 of 18)


Trusted Business Partners (Part 10 of 18)


Data Collection and Analysis (Part 11 of 18)


Incident Response Planning (Part 12 of 18)


Communicating Insider Threat Events (Part 13 of 18)

Policies, Procedures, and Practices (Part 14 of 18)


Protection of Employee Civil Liberties and Privacy Rights (Part 15 of 18)


The Insider Threat Framework (Part 16 of 18)


Implementation Planning (Part 17 of 18)


Conclusion and Resources (Part 18 of 18)


Common Sense Guide to Mitigating Insider Threats

The fourth edition of the Common Sense Guide to Mitigating Insider Threats provides the most current recommendations from the CERT® Program, part of Carnegie Mellon University’s Software Engineering Institute, based on an expanded database of more than 700 insider threat cases and continued research and analysis. Each practice lists several recommendations that organizations of various sizes should implement immediately to mitigate (prevent, detect, and respond to) insider threats.


This edition of the guide describes 19 practices that organizations should implement across the enterprise to prevent and detect insider threats, as well as case studies of organizations that failed to do so. Each practice includes features new to this edition: challenges to implementation, quick wins and high-impact solutions for small and large organizations, and relevant security standards. This edition also focuses more on six groups within an organization—Human Resources, Legal, Physical Security, Data Owners, Information Technology, and Software Engineering—and provides quick reference tables noting which of these groups each practice

dfir.aaa@gmail.com
applies to. The appendices provide a revised list of information security best practices, a new mapping of the guide’s practices to established security standards, a new breakdown of the practices by organizational group, and new checklists of activities for each practice.

Fourth edition of the Common Sense Guide to Mitigating Insider Threats

Best practices:
1. Consider threats from insiders and business partners in enterprise-wide risk assessments.
2. Clearly document and consistently enforce policies and controls.
3. Incorporate insider threat awareness into periodic security training for all employees.
4. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5. Anticipate and manage negative issues in the work environment.
6. Know your assets.
7. Implement strict password and account management policies and practices.
8. Enforce separation of duties and least privilege.
9. Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
10. Institute stringent access controls and monitoring policies on privileged users.
11. Institutionalize system change controls.
12. Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
13. Monitor and control remote access from all endpoints, including mobile devices.
14. Develop a comprehensive employee termination procedure.
15. Implement secure backup and recovery processes.
16. Develop a formalized insider threat program.
17. Establish a baseline of normal network device behavior.
18. Be especially vigilant regarding social media.
19. Close the doors to unauthorized data exfiltration.
Appendix B

Big Data Solutions for Data Fusion

Big Data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making. (Gartner. IT Glossary. 2013. http://www.gartner.com/it-glossary/big-data/.)

Big Data Characteristics

“3 Vs”—volume, velocity, and variety—are distinguishing characteristics of Big Data. Simply put, it is the volume (amount of data), velocity (the speed of processing and the pace of change to data), and variety (sources of data and types of data) that most notably distinguish Big Data from the traditional approaches used to capture, store, manage, and analyze data.

The onslaught of Big Data necessitates that information governance (IG) be implemented to discard unneeded data in a legally defensible way.

Security Data Analytics implementation

Below figure shows the implementation of security big data analytics using Hadoop.

ELK (Elasticsearch Logstash Kibana) overview

**Elasticsearch**

Elasticsearch is a distributed, open source search and analytics engine, designed for horizontal scalability, reliability, and easy management. It combines the speed of search with the power of analytics via a sophisticated, developer-friendly query language covering structured, unstructured, and time-series data.

**Logstash**

Logstash is a flexible, open source data collection, parsing, and enrichment pipeline. With connectors to common infrastructure for easy integration, Logstash is designed to efficiently process a growing list of log, event, and unstructured data sources for distribution into a variety of outputs, including Elasticsearch.
**Kibana**

Kibana is an open source data visualization platform that allows you to interact with your data through stunning, powerful graphics. From histograms to geomaps, Kibana brings your data to life with visuals that can be combined into custom dashboards that help you share insights from your data far and wide.

**ELK Architecture**

These are just two examples of security data analytics implementation using Hadoop, and ELK. There are several databases designed specifically for efficient storage and query of Big Data, including Cassandra, CouchDB, Greenplum Database, HBase, MongoDB, and Vertica. There are lots of solutions from vendors which provide security big data analytics capability. Thus there are numerous solutions that can be selected and implemented depending upon the goals of the organization implementing security big data analytics solution.
Appendix D

Use Case - Risk Score for fraud detection with web server access logs

Download and upload the tutorial data from splunk which has sample data -
http://docs.splunk.com/images/Tutorial/tutorialdata.zip

Sample log

```
"http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506
```

Splunk fields

The summary indexes should be created before running the Splunk queries.
Splunk Query Screenshots

source=access.log method=POST action=purchase
| bin _time span=1d
| stats dc(JSESSIONID) by _time clientip
| rename dc(JSESSIONID) as sessioncount
| collect index=sstats

index=sstats
| eventstats avg(sessioncount) as threshold
| where sessioncount>threshold
| eval Risk_Score=0
| eval Risk_Score=Risk_Score+20

dfir.aaa@gmail.com
| table _time,clientip,Risk_Score
| collect index=ipriskscore

index=uastats
| eval Risk_Score=0
| eval Risk_Score=if(useragentcount>2, Risk_Score+40, Risk_Score+0)
| table _time,clientip,Risk_Score
| collect index=ipriskscore

index=ipriskscore
| stats sum(Risk_Score) by _time clientip
| rename sum(Risk_Score) as Total_Risk_Score
| sort---Risk_Score
Use Case – Risk score for user activity based on login duration and browsing activity

Download Insider threat test dataset r1.tar.bz2 from https://www.cert.org/insider-threat/tools/ and upload the data to the Splunk instance.

Sample log - Device.csv
id,date,user,pc,activity
{S7A7-Y8QZ65MW-8738SAZP},01/04/2010 07:12:31,DTAA/RES0962,PC-3736,Connect
{G7A8-G1OB94NR-3006NTXH},01/04/2010 07:35:40,DTAA/BJC0569,PC-2588,Connect

Sample log - Logon.csv
id,date,user,pc,activity
{Y6O4-A7KC67IN-0899AOZK},01/04/2010 00:10:37,DTAA/KEE0997,PC-1914,Logon
{O5Y6-O7CJ02JC-6704RWBS},01/04/2010 00:52:16,DTAA/KEE0997,PC-1914,Logoff

HTTP.CSV

Sample log – HTTP.csv
id,date,user,pc,url

Splunk Query Screenshots

source=http.csv dropbox.com
| bin _time span=1d
| stats dc(id) by _time user
| rename dc(id) as count
| collect index=dcount

dfir.aaa@gmail.com
source=logon.csv
| bin_time span=1d
| transaction user startswith="activity=Logon" endswith="activity=Logoff"
| table_time,duration,user
| collect index=loginduration

index=dcount
| eventstats avg(count) as threshold
| where count>threshold
| eval Risk_Score=0
| eval Risk_Score=Risk_Score+20
| table_time,user,Risk_Score
| collect index=userriskscore
Insider Threat Mitigation Guidance

```bash
index= loginduration
| eval dhour=duration/3600
| eval Risk_Score=0
| eval Risk_Score=if((dhour>8),Risk_Score+20,Risk_Score+0)
| table _time,user,Risk_Score
| collect index=userriskscore

index=userriskscore
| stats sum(Risk_Score) by _time user
| rename sum(Risk_Score) as Total_Risk_Score
| sort---Risk_Score
```

dfir.aaa@gmail.com
## Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>SANS OnDemand</th>
<th>OnlineUS</th>
<th>Anytime</th>
<th>Self Paced</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>