Global Information Assurance Certification Paper

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.

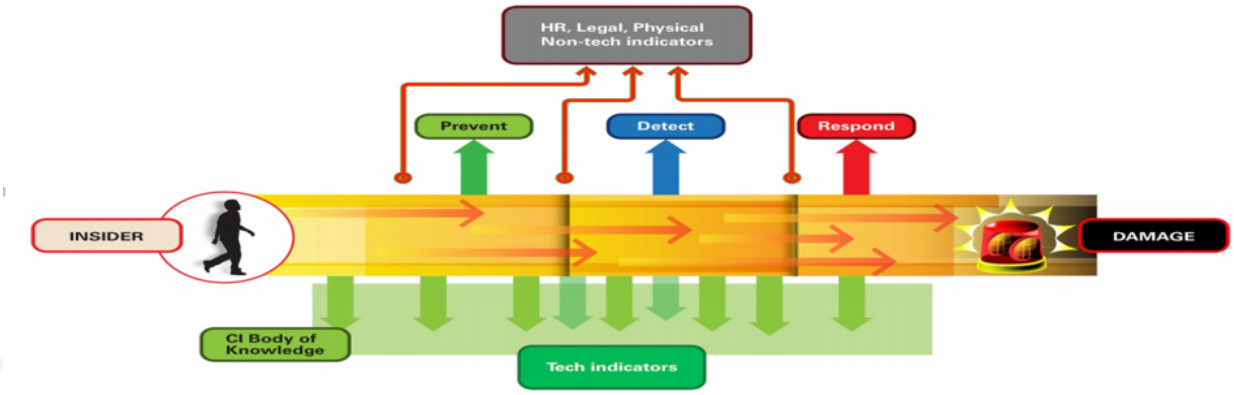
The first section provides reference frameworks for implementing an insider threat mitigation program with the Intelligence and National Security Alliance (INSA) Insider Threat roadmap, Carnegie Mellon University's Computer Emergency Response Team (CERT) insider threat best practices, CERT insider threat 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



Opportunities for prevention, detection, and response for an insider attack
Source: (CERT, 2013)

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

dfir.aaa@gmail.com

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.

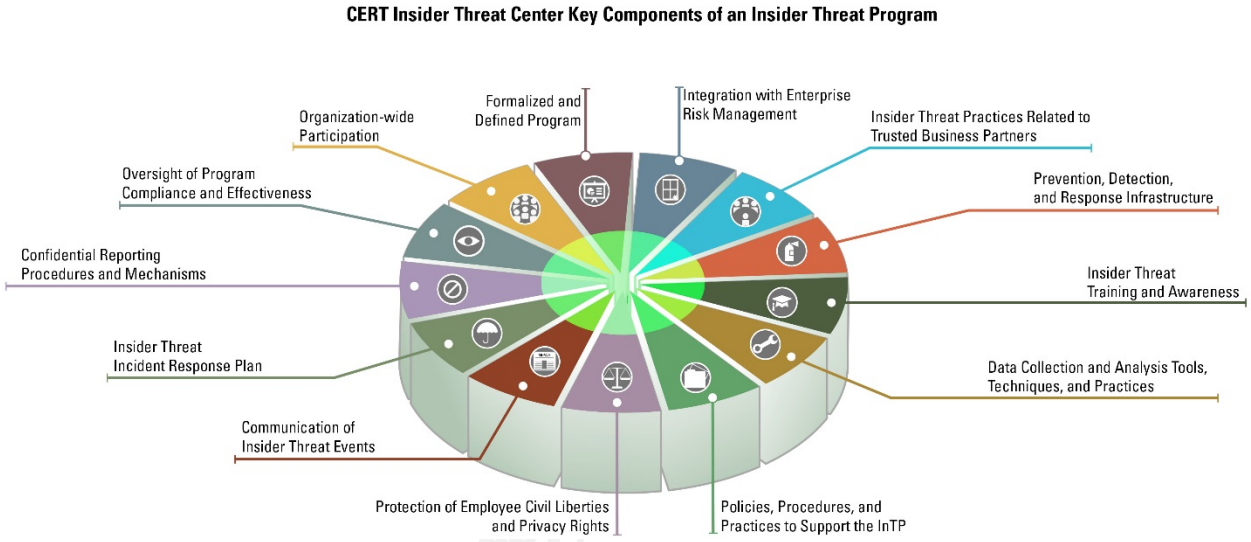
Figure 2 – INSA Insider Threat Road-map

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 reference[1] 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:

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

		monitoring capabilities. • Institute stringent access controls and monitoring policies on privileged users. • Institutionalize system change controls. • Develop a comprehensive employee termination procedure. • Implement secure backup and recovery processes. • Be especially vigilant regarding social media.	
ITMP Step 7 - Communication, Training & Awareness	• Training and Awareness • Communicating Insider Threat Events	• Incorporate insider threat awareness into periodic security training for all employees.	• Respond – Communications • Protect - Awareness & Training
ITMP Step 8 - Develop Detection Indicators	• Prevention, Detection, and Response	• Establish a baseline of normal network device behavior. Close the doors to unauthorized data exfiltration.	• Detect - Anomalies & Events • Detect - Security Continuous Monitoring • Detect - Detection Processes
ITMP Step 9 - Data & Tool Requirements	• Data Collection and Analysis	• Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.	• Protect - Access Control • Protect - Protective Technology
ITMP Step 10 - Data Fusion	• Data Collection and Analysis	• Not applicable	• Not applicable
ITMP Step 11 - Analysis and Incident Management	• Incident Response Planning Confidential Reporting	• Not applicable	• Respond - Analysis • Respond – Mitigation
ITMP Step 12 - Management Reporting	• Oversight of Program Compliance and Effectiveness	• Not applicable	• Not applicable
ITMP Step 13 - Feedback & Lessons Learned	• Not applicable	• Not applicable	• Recover - Recovery Planning • Recover - Improvements • Recover – Communications

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.

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.

dfir.aaa@gmail.com

Focus Areas	Recommendations from results of GIAC Corporation's Insider Threat Gap assessment
Policies and Procedures	▪ 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 ▪ Develop a tiered background vetting and validation framework for employees and contractors based on their role and access to key assets
Incident Response	▪ Establish an insider threat program to champion policies, frameworks, behavioral monitoring, and response requirements ▪ Enhance Incident Response plan to include specific procedures for handling incidents potentially involving insiders
Checkout Procedures	▪ Include enhanced monitoring of planned departing insiders as part of the insider threat monitoring program
Awareness Training	Enhance security awareness program to: ▪ Include themes specific to insider threats ▪ Reinforce the message with continuous campaigns ▪ Include modules targeting individual groups such as privileged users and management ▪ Additionally, encourage users to utilize secure alternatives to move sensitive data
Compliance and Enforcement	▪ 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
Technical Controls	▪ Develop a monitoring program to detect and respond to at-risk insider behavior; define use cases for behavioral indicators ▪ Develop criteria for enhancing the monitoring of privileged administrators ▪ Include enhanced monitoring of planned departing insiders as part of the insider threat monitoring program

The reference[3] 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.

dfir.aaa@gmail.com

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.

Type & Length	Description	Minimum Frequency	Possible Communication Method(s)

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
Flash Video / PowerPoint Slide - 10-15 seconds of animated characters or other graphical content	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.	Monthly	LCD Displays
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

dfir.aaa@gmail.com

Giveaways - Graphical content with limited text	A pen, mouse pad, mug, or another giveaway that have a security awareness tip or message depicted on them.	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

Indicator	Parameters (hypothetical)	Data Source Required
1. Excessive data upload to file-sharing service (Dropbox, Cloud) or Large data transfers	More than 100 uploads or 10 GB of data	○ Web Proxy/Next Generation Firewall ○ DNS ○ 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	○ MS Windows ○ 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	○ MS Windows ○ Unix ○ Network devices ○ Document Repositories
4. Attempts to access segregated/escalated systems/file shares/databases	More than three attempts to access a segmented or unauthorized system	○ MS Windows ○ Unix ○ Network devices ○ 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	○ Web Proxy/Next Generation Firewall ○ DNS ○ E-mail Gateway
6. Transactional triggers on business systems	Business logic triggers that would capture misuse of access and rights	○ MS Windows ○ Unix ○ Network devices ○ Document Repositories
7. Sensitive keyword searching	Designated confidential or sensitive keywords or data	○ MS Windows ○ Unix ○ Network devices ○ Document Repositories
8. Excessive printing	Exceeding 200 pages/day	○ MS Windows

9. Abnormal work hours (IT Access/physical)	After hours and weekends Correlate with Badge + Terminal mismatch	○ Badge card reader logs ○ MS Windows ○ Unix

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[4] 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.

dfir.aaa@gmail.com

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.

Splunk Command	Explanation	Logic
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	1.Defines source and provides all results with action=purchase for one day 2.Calculates distinct count(dc) of JESSIONID by clientIP 3.Stores the distinct count for each clientip per day in summary index sstats	Query all purchases made and calculate how many unique session id's was assigned for client IP.
source=access.log method=POST action=purchase | bin _time span=1d | stats dc(useragent) by _time clientip | rename dc(useragent) as useragentcount | collect index=uastats	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	Query all purchases made and calculate how many unique user agents for single client IP.
index=sstats | eventstats avg(sessioncount) as avgsessioncount, stdev(sessioncount) as stdevsc | where (sessioncount > avgsessioncount + 2 * stdevsc) or (sessioncount < avgsessioncount – 2 * stdevsc) | eval Risk_Score=0 | eval Risk_Score=Risk_Score+20 | table _time,clientip,Risk_Score | collect index=ipriskscore	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	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.
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	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	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.
index=ipriskscore | stats sum(Risk_Score) by _time clientip | rename sum(Risk_Score) as Total_Risk_Score | sort---Risk_Score	Calculate total risk score per day for each clientip and sort the results	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.

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.

Splunk Command	Explanation	Logic
source=http.csv dropbox.com | bin _time span=1d | stats dc(id) by _time user | rename dc(id) as count | collect index=dcount	1.Defines source and provides all results with dropbox.com for one day 2.Calculates distinct count(dc) of id by user 3.Stores the distinct count for each user per day in summary index dcount	Query all web traffic to dropbox.com and calculate how many times the user has accessed the site.
source=logon.csv | bin _time span=1d | transaction user startswith="activity=Logon" endswith="activity=Logoff" | table _time,duration,user | collect index=loginduration	1.Defines source and provides all results for one day 2.Calculates login duration for user with transaction command 3.Stores the duration for each user per day in summary index loginduration	Calculates login duration for all users for each day.
index=dcount | eventstats avg(count) as avgcount , stdev(count) as stdevc | where (count > avgcount + 2 * stdevc) or (count < avgcount – 2 * stdevc) | eval Risk_Score=0 | eval Risk_Score=Risk_Score+20 | table _time,user,Risk_Score | collect index=userriskscore	1.Calculates the average count per day 2. If count is 2 standard deviations more or less than the average add risk score by 20 3. Stores the risk score for each user in summary index userriskscore	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.
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	1. If login duration is greater than 8 add risk score by 20 3. Stores the risk score for each user in summary index userriskscore	If login duration greater than 8, add risk score by 20. In this use case, login duration greater than 8 hours considered anomalous.
index=userriskscore | stats sum(Risk_Score) by _time user | rename sum(Risk_Score) as Total_Risk_Score | sort---Risk_Score	Calculate total risk score per day for each user and sort the results	Calculate total risk score per day for each user based on browsing history and login duration. This step calculates the aggregate risk score for each user.

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.

Splunk Command	Explanation	Logic
sourcetype=”WinEventLog:Security” | bin _time span=1d | eval Risk_Score=0 | eval Risk_Score=if((EventID=1102 OR EventID=517),Risk_Score+3,Risk_Score+0) | eval Risk_Score=if((EventID=4663 AND Accesses = "DELETE" AND Object_Type=File),Risk_Score+1,Risk_Score+0) | 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) | table _time,Account_Name,Risk_Score | collect index=adriskscore	Defines log source as Windows security event log Defines Time duration as one day Assigns Risk_Score value zero Increase Risk_Score value by three if event id is related to audit log cleared Increase Risk_Score value by one if event id is related to file deletions by user account. Increase Risk_Score value by two if event ids are related to	Query all Windows events and assigns risk scores if there are any anomalous events for the user account.

	privilege escalation for the user account.	
index=adriskscore | stats sum(Risk_Score) by _time Account_Name | rename sum(Risk_Score) as Total_Risk_Score | sort---Risk_Score	Calculate total risk score per day for each user account and sort the results	Calculate total risk score per day for each user based on suspicious windows events. This step calculates the aggregate risk score for each user.

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.

At-Risk Activity	Daily Calculated Values	Splunk Query Example
Data upload	• Egress Bytes [SUM] • Egress Packets [COUNT] • URL string [LENGTH] • DNS query [LENGTH] • DNS query [COUNT] • User agent string [LENGTH] • User agent string [COUNT] • Egress IPs[COUNT] • URL domain [COUNT] • Protocols used [COUNT]	Egress Bytes [SUM] • sourcetype=firewall| stats sum(bytes) by clientip URL string [LENGTH] • sourcetype=proxy | eval url_length=len(url) | stats count(clientip) by Length DNS query [LENGTH] • sourcetype=dns | eval Length=len(query) | stats count(clientip) by Length
Removable media	• Unique serial numbers [COUNT] • Unique systems accessed with Removable Media [COUNT] • Bytes transferred [SUM] • Files transferred [SUM]	Unique systems accessed with Removable Media [COUNT] • sourcetype=WinRegistry key_path="HKLM\\system\\controlset*\\enum\\usbstor*" registry_type=CreateKey | eval Date=strftime(_time, "%Y/%m/%d %H:%M:%S") | rex "key_path.*usbstor\S(?<DeviceType>.*)&ven\S(?<Vendor>.*)&prod\S(?<Product>\S*)&rev\S" | stats count by Date, host, Vendor, Product, DeviceType
Print	• Number of printers utilized[COUNT] • Number of print jobs [COUNT] • Number of pages printed [SUM]	Number of pages printed [SUM] • sourcetype=WinPrintMon type=PrintJob operation=add | stats sum(page_printed) by user

Data consolidation	• Number of systems accessed [COUNT] • Unique user agent string [COUNT] • Bytes downloaded, for all systems [SUM] • Bytes downloaded, per system accessed [SUM] • Packets downloaded [COUNT] • Document access, total [COUNT] • Document access, by classification [COUNT]	Number of systems accessed [COUNT] • sourcetype=”WinEventLog:Security” EventCode=4769 | bin _time span=1d | stats dc(ServiceName) by _time user | rename dc(ServiceName) as count | collect index=userstats
User actions	• Login Match, Miss-Match [COUNT] • Login Location [COUNT] • User Position Change [COUNT] • Two-factor token use [COUNT] • Badge scan, Total [COUNT] • Badge scan, Per scan location [COUNT]	VPN Login Location [COUNT] • sourcetype=vpn | transaction user | table type,_time,user,country | collect userstats
File Share	• Number of shares accessed [COUNT] • Unique user agent string [COUNT] • Bytes downloaded, for all shares [SUM] • Bytes downloaded, per share accessed [SUM] • Packets downloaded [COUNT] • Document access, total [COUNT] • Document access, by classification [COUNT]	Document access, total [COUNT} • sourcetype="WinEventLog:Security" EventID=560 OR EventID=4656 Object_Type=File | eval Date=strftime(_time, "%Y/%m/%d") |eval UserName=coalesce(Primary_User_Name, Client_User_Name)| search UserName!="*$" AND UserName!="NETWORK SERVICE"| stats count by Date, Image_File_Name, UserName, Type, host

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.

dfir.aaa@gmail.com

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 suck 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.

dfir.aaa@gmail.com

References

[1] "Discussion Draft of the Preliminary Cybersecurity Framework Illustrative Examples" 28 Aug. 2013. Retrieved (2015, 07 30) from <http://www.nist.gov/itl/upload/discussion-draft_illustrative-examples-082813.pdf>.

[2] Flynn, L. (2013). Best practices against insider threats in all nations. Retrieved (2015, 07 30) from http://resources.sei.cmu.edu/library/asset-view.cfm? Assetid=59082.

[3] "Insider Threat Mitigation Micro-Assessment Template" 5 May. 2015. Retrieved (2015, 07 30) from <http://www.go-rbcs.com/insider-threat-micro-assessment-template>.

[4] Using Splunk Software as Part of a Government Insider Threat (2014, November). Retrieved July 25, 2015, from http://www.splunk.com/web_assets/pdfs/secure/Using_Splunk_Software_as_Part_of_a_Government_Insider_Threat_Detection_Program.pdf

Cole, E. (2015). Insider threats and the need for fast and directed response. Retrieved (2015, 07 30) from Https://www. Sans. Org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892

Insider Threat Resource Directory. (2014, October 4). Retrieved July 24, 2015, from http://www.insaonline.org/insiderthreat

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/

National Insider Threat Policy. (2015, April 14). Retrieved July 24, 2015, from http://www.ncsc.gov/nittf/docs/National_Insider_Threat_Policy.pdf

Insider Threat DoD Directive. (2014, October 31). Retrieved July 24, 2015, from http://www.dtic.mil/whs/directives/corres/pdf/520516p.pdf

INSA Cyber Insider Threat Task Force. (2013, March 5). Retrieved July 24, 2015, from http://www.insaonline.org/i/c/b/CITTF/i/c/cyber/d/index.aspx?hkey=2027ecfc-65fc-4641-877f-dbef05f9de4b

INSIDER THREAT BEST PRACTICES GUIDE – SIFMA. (2014, July 24). Retrieved July 24, 2015, from http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/insider-threat-best-practices-guide.pdf

Common Sense Guide to Mitigating Insider Threats - CERT. (2013, October 8). Retrieved July 24, 2015, from http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

dfir.aaa@gmail.com

Flynn, L. (2013). Best practices against insider threats in all nations. Retrieved (2015, 07 30) from Http://resources. Sei. Cmu. Edu/library/asset-view. Cfm? Assetid=59082

Cappelli, D., & Trzeciak, R. (2014, July 17). Keeping Up with the Joneses: How Does Your Insider Threat Program Stack Up? Retrieved July 24, 2015, from http://www.rsaconference.com/writable/presentations/file_upload/hum-w02-keeping-up-with-joneses-v2.pdf

Admin. of Barack Obama, Memorandum on the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012), available at http://www.fas.org/sgp/obama/insider.pdf. ["Minimum Standards for Executive Branch Insider Threat Programs"].

Armed Forces Commc'n & Elecs. Ass'n Cyber Comm., Insider Threat: Protecting U.S. Business Secrets and Sensitive Information (2013). ["AFCEA Insider Threat: Protecting U.S. Business Secrets"].

Richard C. Brackney and Robert H. Anderson, RAND Nat'l Sec. Research Div, Understanding the Insider Threat: Proceedings of a March 2004 Workshop (2004), http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAND_CF196.pdf. ["Understanding the Insider Threat"].

Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (2012). ["The CERT Guide to Insider Threats"].

Dawn Cappelli et. al, Common Sense Guide to Prevention and Detection of Insider Threats 3rd Ed. – Version 3.1, Carnegie Mellon, Software Engineering Institute (2009), p. 62, available at https://www.cylab.cmu.edu/files/ pdfs/CERT/CSG-V3.pdf. ["Common Sense Guide, 3rd Ed."]

Deanna D. Caputo et al., Human Behavior, Insider Threat, and Awareness: An Empirical Study of Insider Threat Behavior, MITRE Corp., Institute for Information Infrastructure and Protection (2009). ["Human Behavior, Insider Threat, and Awareness"].

"Discussion Draft of the Preliminary Cybersecurity Framework Illustrative Examples." 28 Aug. 2013. Retrieved (2015, 07 30) from <http://www.nist.gov/itl/upload/discussion-draft_illustrative-examples-082813.pdf>.

CERT Insider Threat Ctr., Unintentional Insider Threats: Social Engineering (2014), available at http://resources. sei.cmu.edu/library/asset-view.cfm?AssetID=77455

Matthew L. Collins et. al, Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations, Carnegie Mellon, Software Engineering Institute (2013), available at http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_48680.pdf. ["Collins, Spotlight On Insider Theft of IP"].

Cyber Council: Insider Threat Task Force, Intelligence and Nat'l Sec. Alliance, A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector, (2013). Adam Cummings et al., Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector (2012),

available at http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=27971. ["Insider Threat Study: Fraud in the Financial Services Sector"].

Defense Intelligence Agency, Your Role in Combating the Insider Threat, http://www.hsdl.org/?view&did=441866. ["Your Role in Combating the Insider Threat"].

Prosecuting Computer Crimes, Office of legal Education, Executive Office for United States Attorneys (2007), available at http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf. ["Prosecuting Computer Crimes"]

Dept't of Justice and Federal Trade Comm'n, Antitrust Policy Statement on Sharing of Cybersecurity Information, available at http://www.justice.gov/atr/public/guidelines/305027.pdf. ["DOJ/FTC Antitrust Policy Statement"].

Ernst & Young, Identity and Access Management: Beyond Compliance (May 2013), available at http://www. ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_ and_access_management_Beyond_compliance_AU1638.pdf. ["Identity and Access Management"].

FBI, U.S. Department of Justice, The Insider Threat: An Introduction to Detecting and Deterring An Insider Spy, http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat. ["FBI: Detecting and Deterring an Insider Spy"].

Lori Flynn et al., Best Practices Against Insider Threats in All Nations, Carnegie Mellon, Software Engineering Institute (2013), available at http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_59084. pdf. ["Best Practices Against Insider Threats in All Nations"].

Lori Flynn et al., International Implementation of Best Practices for Mitigating Insider Threat: Analyses for India and Germany, Carnegie Mellon, Software Engineering Institute (2014), available at http://resources.sei. cmu.edu/asset_files/TechnicalReport/2014_005_001_88427.pdf. ["International Implementation of Best Practices"].

Frank L. Greitzer et al., Pac. Nw. Nat'l Lab., Predictive Modeling for Insider Threat Mitigation, Dep't of Energy (2009), http://www.pnl.gov/coginformatics/media/pdf/tr-pacman-65204.pdf. ["Predictive Modeling for Insider Threat Mitigation"].

Stephen J. Hadley, Assistant to the President for Nat'l Sec. Affairs, Memorandum on Adjundicative Guidelines from to William Leonard, Director, Info. Sec. Oversight Office (Dec. 29, 2005), http://www.fas.org/sgp/isoo/ guidelines.pdf.

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

Insider Threat Team, CERT, Unintentional Insider Threats: A Foundational Study (2013), available at http:// resources.sei.cmu.edu/library/asset-view.cfm?AssetID=58744

dfir.aaa@gmail.com

Todd Lewellen et al., Spotlight On: Insider Threat from Trusted Business Partners Version 2: Updated and Revised (2012) available at http://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_53417.pdf. ["Spotlight On Insider Threat: Trusted Business Partners"]

Michelle Keeney, J.D., Ph.D. et al., Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors (2005), available at http://resources.sei.cmu.edu/asset_files/CERTResearchReport/2005_013_001_51946.pdf. ["Insider Threat Study: Computer System Sabotage"].

Microsoft, How to Protect Insiders from Social Engineering Threats (August 18, 2006), http://technet.microsoft. com/en-us/library/cc875841.aspx.

National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214. pdf. ["NIST Cybersecurity Framework"].

National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Dep't of Justice, 2nd Ed. (2008), available at https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. ["Electronic Crime Scene Investigation"].

Fahmida Y. Rashid, Insider Threat: Limit Privileged Access, BankInfoSecurity (Aug. 23, 2013), http://www.bankinfosecurity.com/insider-threat-limit-privileged-access-a-6014.

Raytheon, Best Practices for Mitigating and Investigating Insider Threats (2009), available at http://www.raytheon. com/capabilities/rtnwcm/groups/iis/documents/content/rtn_iis_whitepaper-investigati.pdf. ["Raytheon Whitepaper"].

Andree Rose et al., Developing a Cybervetting Strategy for Law Enforcement (2010), http://www.iacpsocialmedia. org/Portals/1/documents/CybervettingReport.pdf. ["Developing a Cybervetting Strategy"].

Securities and Exchange Commission, Office of Compliance Inspections and Examinations, "National Exam Program Risk Alert, Cybersecurity Examinations" (April 15, 2014), http://www.sec.gov/ocie/announcement/ Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf. ["SEC Cybersecurity Risk Alert"].

Eric D. Shaw and Harley V. Stock, Symantec, Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall (2011), available at https://www4.symantec.com/mktginfo/ whitepaper/21220067_GA_WP_Malicious_Insider_12_11_dai81510_cta56681.pdf. ["Behavioral Risk Indicators"].

George Silowash et al., Common Sense Guide to Mitigating Insider Threats 4th Edition (2012), available at http:// resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017. ["Common Sense Guide, 4th Ed."]

dfir.aaa@gmail.com

Sara Sinclair et al., Information Risk in Financial Institutions: Field Study and Research Roadmap, FinanceCom 2007, available at http://www.cs.dartmouth.edu/~sws/pubs/sstjp07.pdf. ["Information Risk in Financial Institutions"].

Suitability and Sec. Clearance Performance Accountability Council, Report to the President (2014), http://www. whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf. ["Suitability and Security Clearance Report"].

Raytheon. (2015, July). Meeting the Demands of Government Policies & Regulations. Retrieved from http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_266010.pdf

CPNI. (2013, April). CPNI INSIDER DATA COLLECTION STUDY. Retrieved from http://www.cpni.gov.uk/documents/publications/2013/2013003-insider_data_collection_study.pdf

SIFMA. (2014, November). SIFMA CYBERSECURITY: INSIDER THREATS BEST PRACTICES. Retrieved from http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/sifma-cybersecurity-insider-threat-best-practices.pdf

Splunk References

Purdue, R. (2015, May 14). Detecting Fraud and Suspicious events using Risk Scoring. Retrieved July 25, 2015, from http://blogs.splunk.com/2015/05/14/conf2014-highlight-series-detecting-fraud-and-suspicious- events-using-risk-scoring/

Gill, S. (2014, November 1). Improving Targeted Attack Detection. Retrieved July 25, 2015, from http://conf.splunk.com/sessions/2014/conf2014_SylvainGil_Exabeam_Security.pdf

Roberts, Carrie. "Discovering Security Events of Interest Using Splunk." N.p., 10 July 2013. Web. 30 July 2015. <http://www.sans.org/reading-room/whitepapers/logging/discovering-security-events-interest-splunk-34272>.

Data Theft via USB: Combating the Insider Threat. (2014, January 28). Retrieved July 24, 2015, from http://community.websense.com/blogs/securitylabs/archive/2014/01/28/combating-the-insider-threat.aspx

User Behavior Analysis with Splunk: Detecting Threats and Fraudulent Activity in the Ocean of Behaviors: Part 1 – Setting Alerts on User Session Risk Factors | Mensk Technologies Inc. (2015, May 10). Retrieved July 25, 2015, from http://www.mensk.com/user-behavior-analysis-with-splunk-detecting-threats-and-fraudulent-activity-in-the-ocean-of-behaviors-part1-calculating-risk/

User Behavior Analysis with Splunk: Detecting Threats and Fraudulent Activity in the Ocean of Behaviors: Part 2 – Detecting Abnormal User Session Velocity and Density | Mensk Technologies Inc. (2015, May 10). Retrieved July 25, 2015, from http://www.mensk.com/user-behavior-analysis-with-splunk-detecting-threats-and-fraudulent-activity-in-the-ocean-of-behaviors-part-2-detecting-abnormal-user-session-velocity-and-density/

Splunk, . (2014). Usb and removable media detection. Retrieved (2015, 07 30) from Http://gosplunk. Com/usb-and-removable-media-detection/

dfir.aaa@gmail.com

Splunk, . (2014). Windows File Access Attempts. Retrieved (2015, 07 30) from http://gosplunk.com/windows-file-access-attempts/

Splunk, . (2014). Advanced threat detection and response. Retrieved (2015, 07 30) from Https://www. Splunk. Com/content/dam/splunk2/pdfs/technical-briefs/advanced-threat-detection-and-response-tech-brief. Pdf

Splunk, . (2014). Windows print monitoring in splunk 6. Retrieved (2015, 07 30) from Http://blogs. Splunk. Com/2014/04/21/windows-print-monitoring-in-splunk-6/

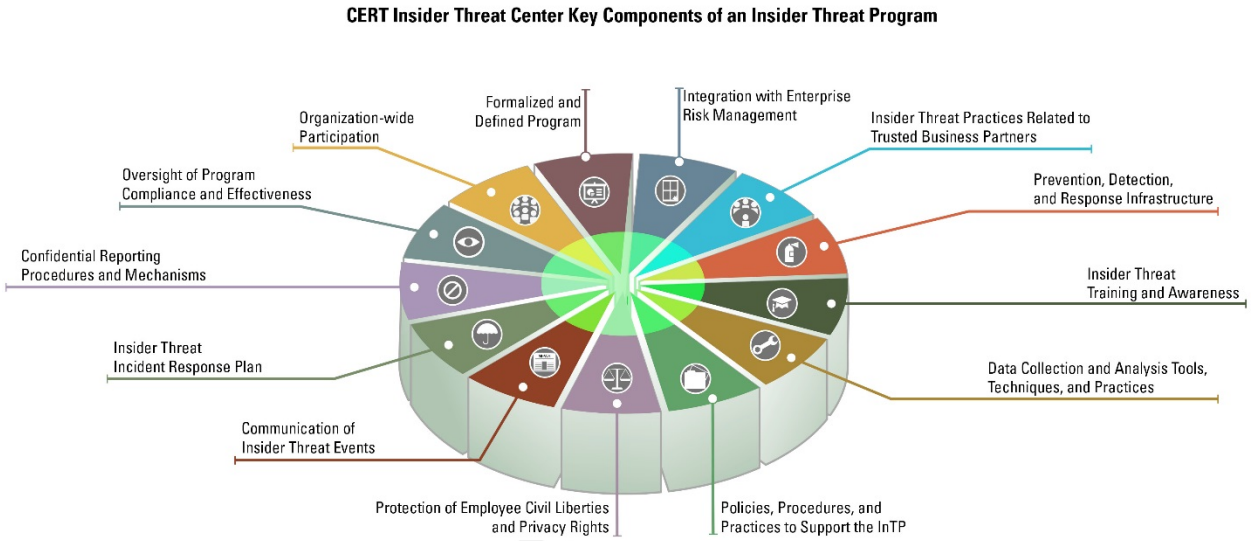
Using Splunk Software as Part of a Government Insider Threat (2014, November). Retrieved July 25, 2015, from from http://www.splunk.com/web_assets/pdfs/secure/Using_Splunk_Software_as_Part_of_a_Government_Insider_Threat_Detection_Program.pdf

"Search Manual." Use the Stats Command and Functions. Splunk, 01 Dec. 2014. Web. 04 Oct. 2015. http://docs.splunk.com/Documentation/Splunk/6.2.0/Search/Usethestatscommandandfunctions

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)

CERT. (2015, March). InTP Series: Establishing an Insider Threat Program (Part 1 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/03/intp-series-establishing-an-insider-threat-program-part-1-of-18.html

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

CERT. (2015, March). InTP Series: Key Elements of an Insider Threat Program (Part 2 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/03/intp-series-key-elements-of-an-insider-threat-program-part-2-of-18.html

The Formalized Program (Part 3 of 18) -

CERT. (2015, March). InTP Series: The Formalized Program (Part 3 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/03/-intp-series-the-formalized-program-part-3-of-18.html

Participation of Business Areas (Part 4 of 18)

CERT. (2015, March). InTP Series: Participation of Business Areas (Part 4 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/03/intp-series-participation-of-business-areas-part-4-of-18.html

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

CERT. (2015, April). InTP Series: Oversight of Program Compliance and Effectiveness (Part 5 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/04/-intp-series-oversight-of-program-compliance-and-effectiveness-part-5-of-18.html

Integration with Enterprise Risk Management (6 of 18)

CERT. (2015, April). InTP Series: Integration with Enterprise Risk Management (6 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/04/-intp-series-integration-with-enterprise-risk-management-6-of-18.html

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

InTP Series: Prevention, Detection, and Response (Part 7 of 18). (2015, April). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/04/intp-series-prevention-detection-and-response-part-7-of-18.html

Training and Awareness (Part 8 of 18)

CERT. (2015, April). InTP Series: Training and Awareness (Part 8 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/04/intp-series-training-and-awareness-part-8-of-18.html

Confidential Reporting (Part 9 of 18)

CERT. (2015, April). InTP Series: Confidential Reporting (Part 9 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/04/intp-series-confidential-reporting-part-9-of-18.html

Trusted Business Partners (Part 10 of 18)

InTP Series: Trusted Business Partners (Part 10 of 18). (2015, May). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/05/intp-series-trusted-business-partners-part-10-of-18.html

Data Collection and Analysis (Part 11 of 18)

CERT. (2015, May). InTP Series: Data Collection and Analysis (Part 11 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/05/-intp-series-data-collection-and-analysis-part-11-of-18.html

Incident Response Planning (Part 12 of 18)

CERT. (2015, May). InTP Series: Incident Response Planning (Part 12 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/05/-intp-series-incident-response-planning-part-12-of-18.html

Communicating Insider Threat Events (Part 13 of 18)

CERT. (2015, May). InTP Series: Communicating Insider Threat Events (Part 13 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/05/-intp-series-communicating-insider-threat-events-part-13-of-18.html

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

CERT. (2015, June). InTP Series: Policies, Procedures, and Practices (Part 14 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/06/-intp-series-policies-procedures-and-practices-part-14-of-18.html

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

CERT. (2015, June). InTP Series: Protection of Employee Civil Liberties and Privacy Rights (Part 15 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/06/-intp-series-protection-of-employee-civil-liberties-and-privacy-rights-part-15-of-18.html

The Insider Threat Framework (Part 16 of 18)

CERT. (2015, June). InTP Series: The Insider Threat Framework (Part 16 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/06/intp-series-the-insider-threat-framework-part-16-of-18.html

Implementation Planning (Part 17 of 18)

CERT. (2015, June). InTP Series: Implementation Planning (Part 17 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/07/intp-series-implementation-planning-part-17-of-18.html

Conclusion and Resources (Part 18 of 18)

CERT. (2015, June). InTP Series: Conclusion and Resources (Part 18 of 18). Retrieved from https://insights.sei.cmu.edu/insider-threat/2015/07/intp-series-conclusion-and-resources-part-18-of-18.html

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.
http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

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

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 end points, 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.

dfir.aaa@gmail.com

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

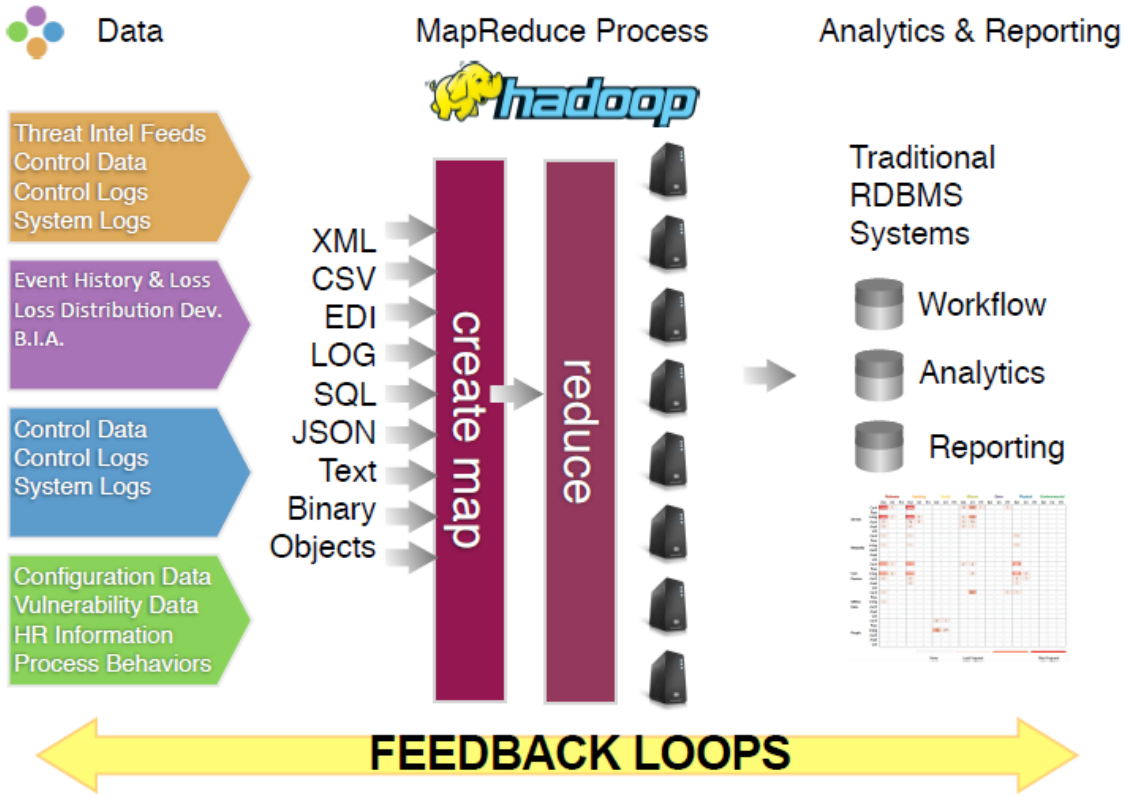
"3 Vs"—volume, velocity, and variety—are distinguishing characteristics of Big Data. Simply put, it is the volume (amount of data), velocity (the speed of processing and the pace of change to data), and variety (sources of data and types of data) that most notably distinguish Big Data from the traditional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

(Hutton, A. (n.d.). TOWARDS A MODERN APPROACH TO RISK MANAGEMENT. Retrieved May 26, 2015, from http://rvasec.com/slides/2013/Hutton-Towards_A_Modern_Approach.pdf)



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

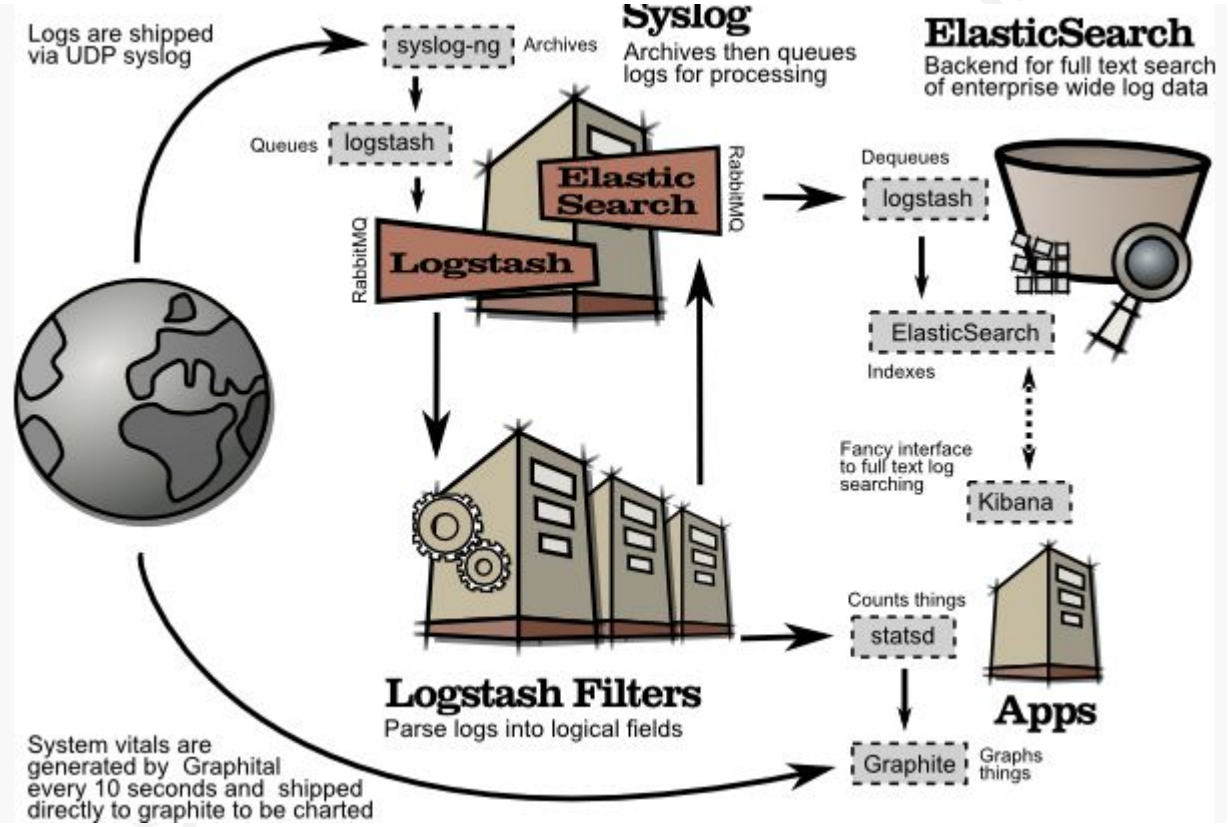
Logstash is a flexible, open source data collection, parsing, and enrichment pipeline. With connectors to common infrastructure for easy integration, Logstash is designed to efficiently process a growing list of log, event, and unstructured data sources for distribution into a variety of outputs, including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

dfir.aaa@gmail.com

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

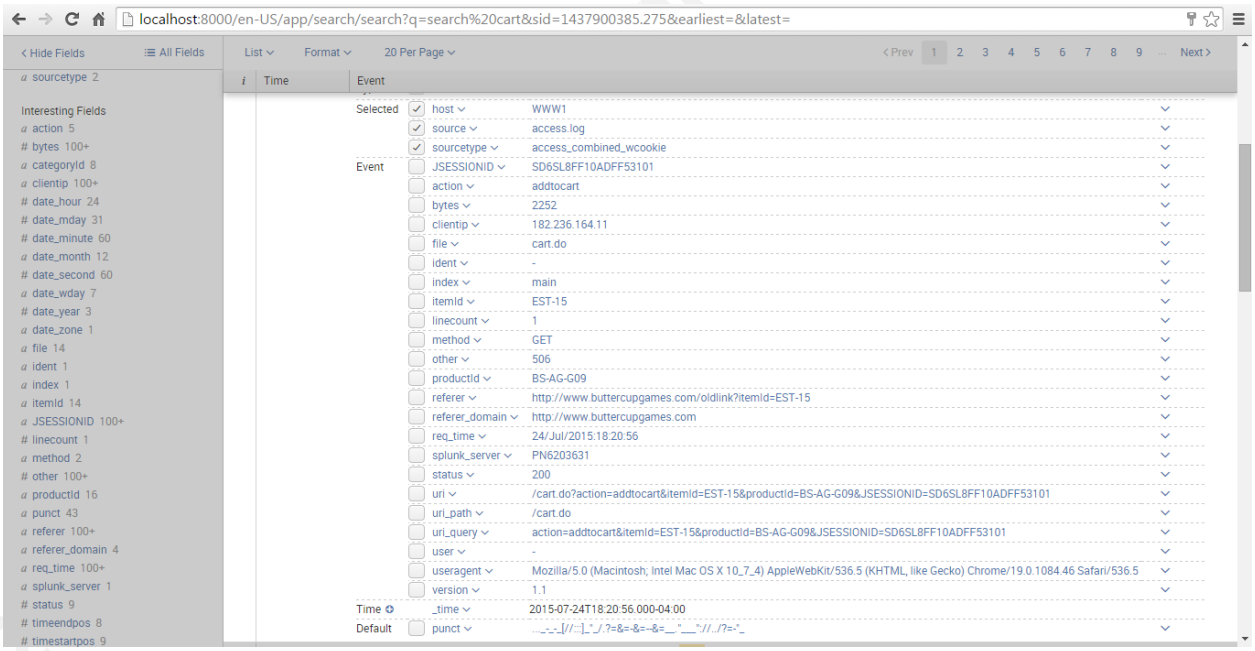
Download and upload the tutorial data from splunk which has sample data -

http://docs.splunk.com/images/Tutorial/tutorialdata.zip

Sample log

182.236.164.11 - - [24/Jul/2015:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "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

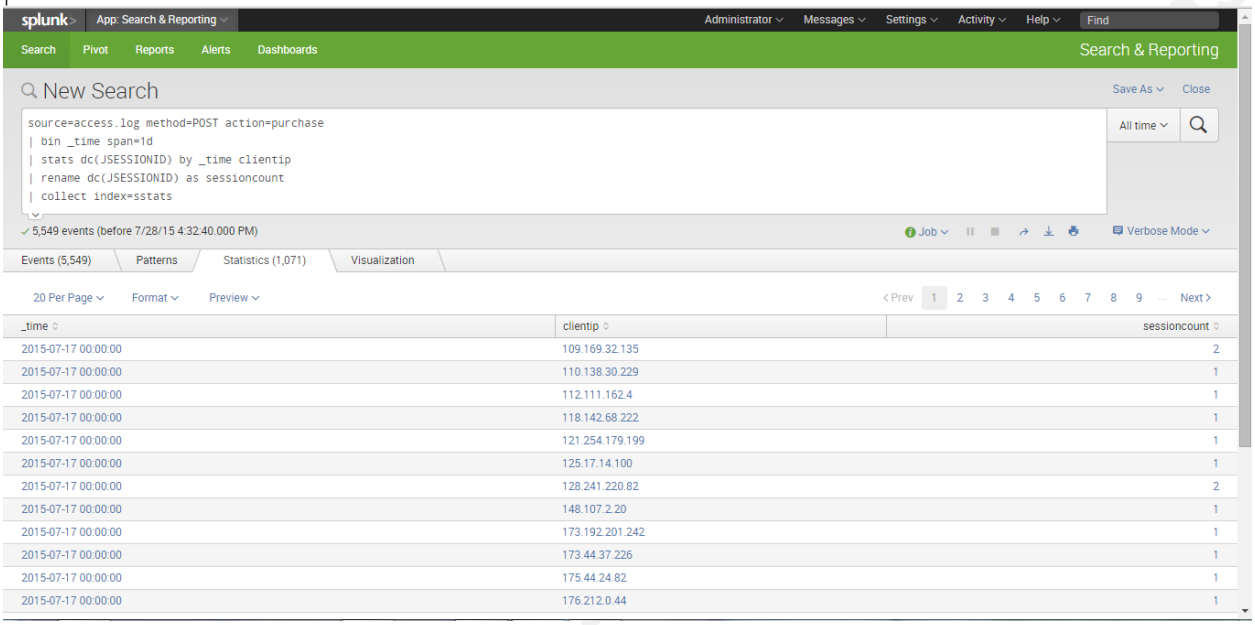
Splunk fields



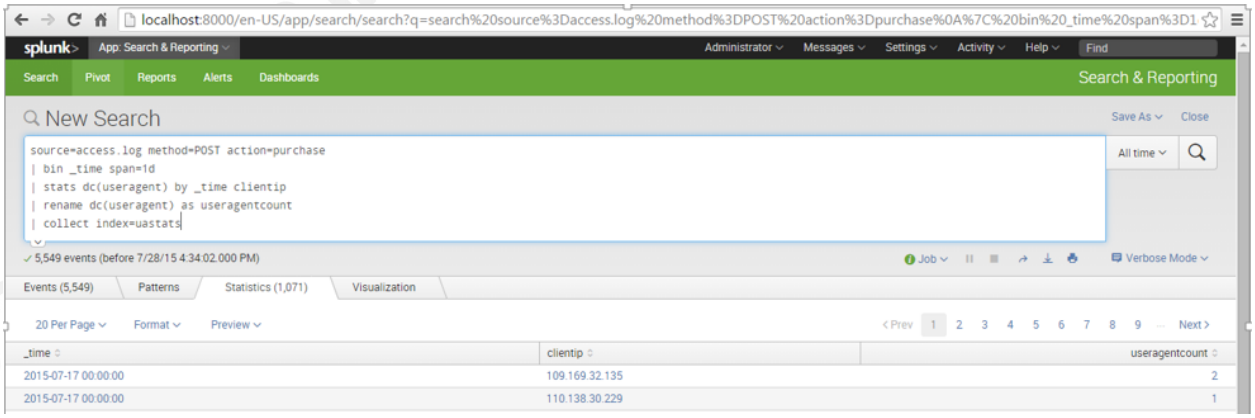
The summary indexes should be created before running the Splunk queries.

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
```



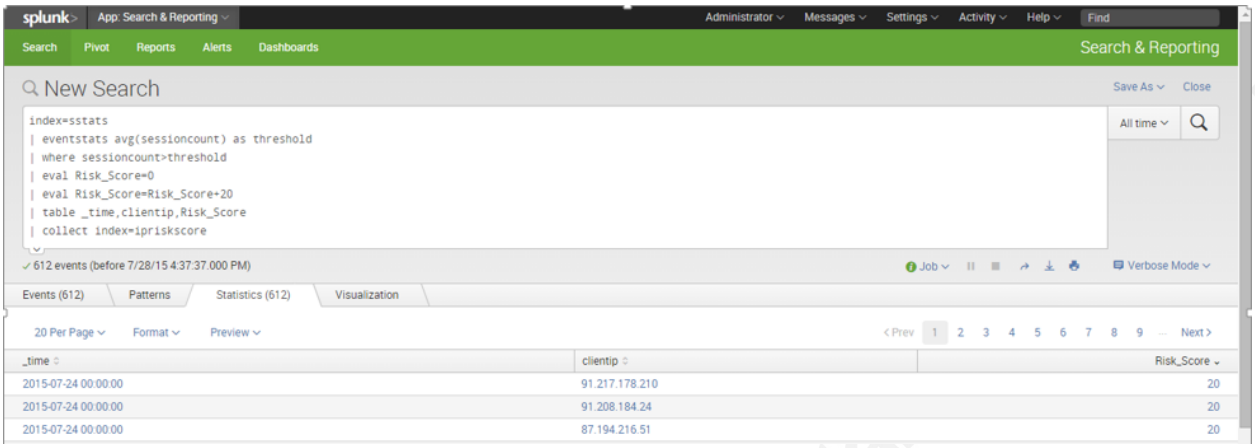

```
source=access.log method=POST action=purchase
| bin _time span=1d
| stats dc(useragent) by _time clientip
| rename dc(useragent) as useragentcount
| collect index=uastats
```



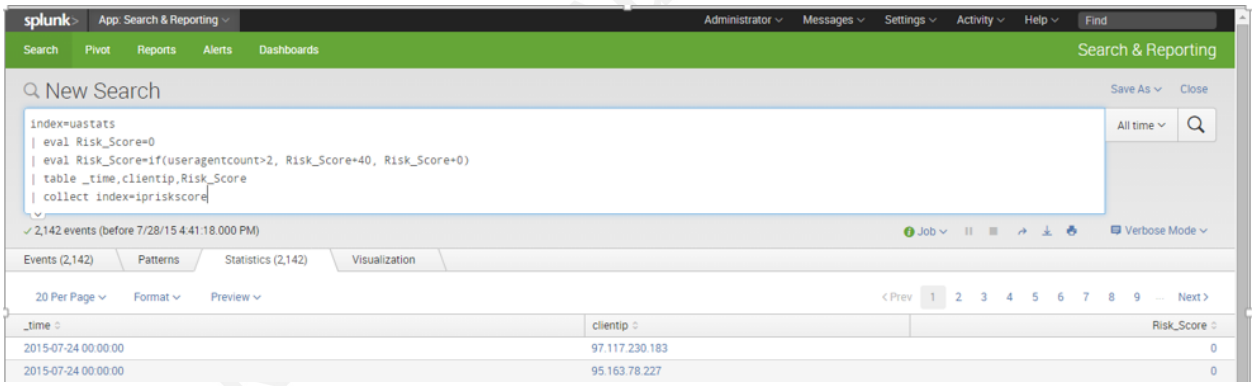

```
index=sstats
| eventstats avg(sessioncount) as threshold
| where sessioncount>threshold
| eval Risk_Score=0
| eval Risk_Score=Risk_Score+20
```

dfir.aaa@gmail.com

```
| table _time,clientip,Risk_Score
| collect index=iprisksсore
```

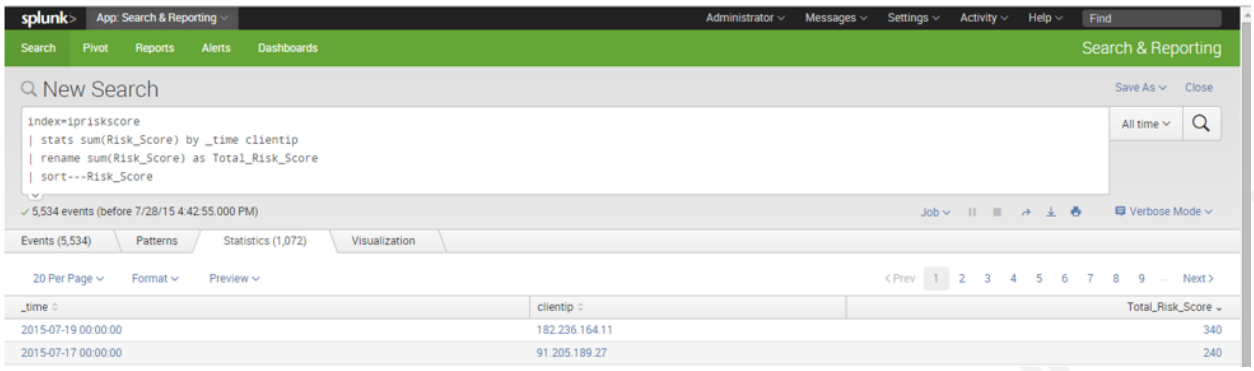



```
index=uastats
| eval Risk_Score=0
| eval Risk_Score=if(useragentcount>2, Risk_Score+40, Risk_Score+0)
| table _time,clientip,Risk_Score
| collect index=iprisksсore
```




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

dfir.aaa@gmail.com



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

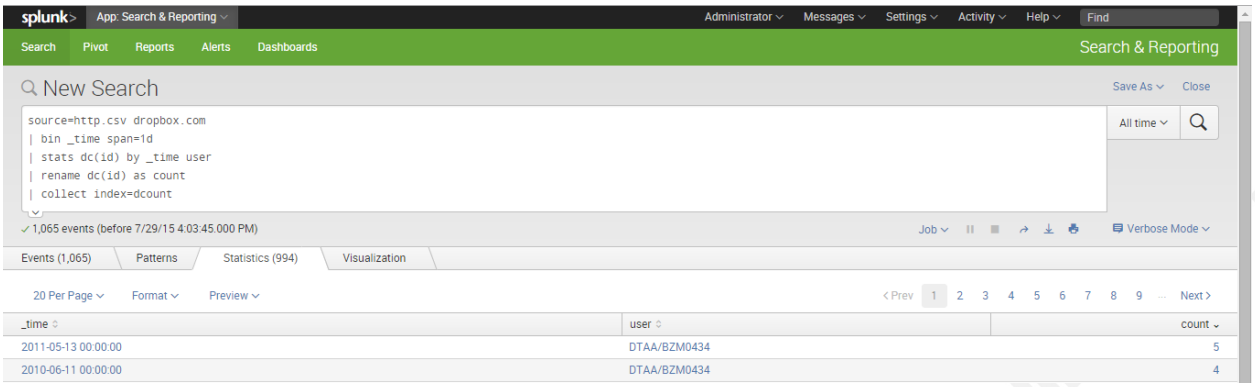
Sample log - Logon.csv
id,date,user,pc,activity
{Y6O4-A7KC67IN-0899AOZK},01/04/2010 00:10:37,DTAA/KEE0997,PC-1914,Logon
{O5Y6-O7CJ02JC-6704RWBS},01/04/2010 00:52:16,DTAA/KEE0997,PC-1914,Logoff
HTTP.CSV

Sample log – HTTP.csv
id,date,user,pc,url
{M8H9-W9NL75TH-1322KOLO},01/04/2010 07:08:47,DTAA/AMA0606,PC-1514,"http://cnet.com"
{V0E1-R0FE91SC-2381GTDZ},01/04/2010 07:35:19,DTAA/DBM0698,PC-1444,"http://force.open.com"

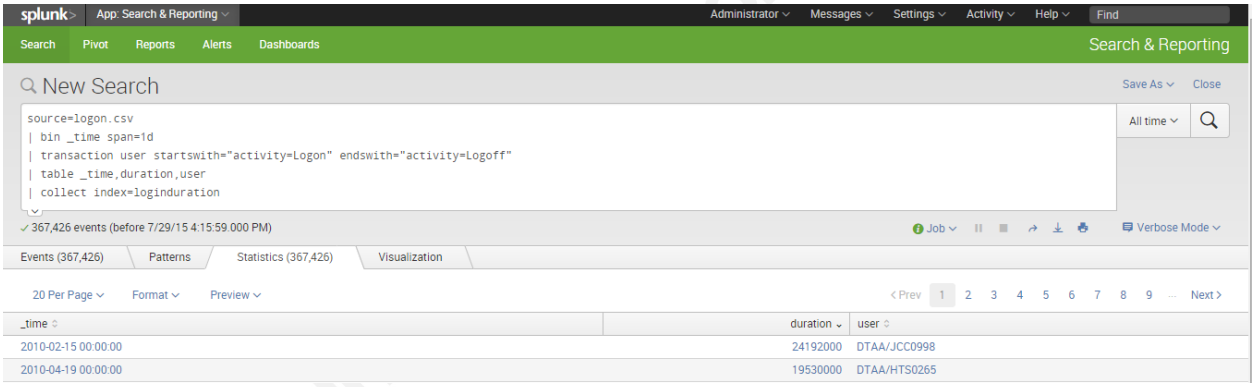
Splunk Query Screenshots

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

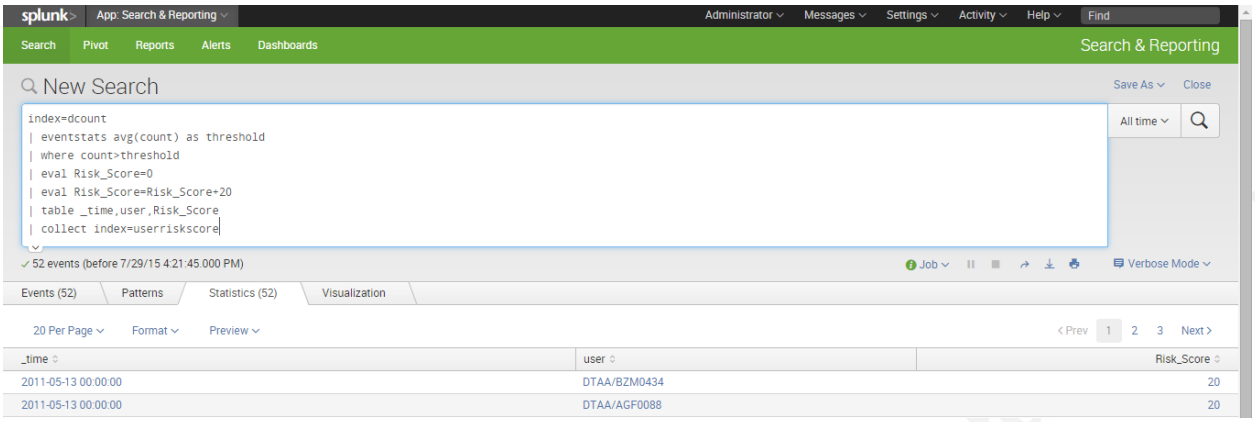



```
source=logon.csv
| bin _time span=1d
| transaction user startswith="activity=Logon" endswith="activity=Logoff"
| table _time,duration,user
| collect index=loginduration
```

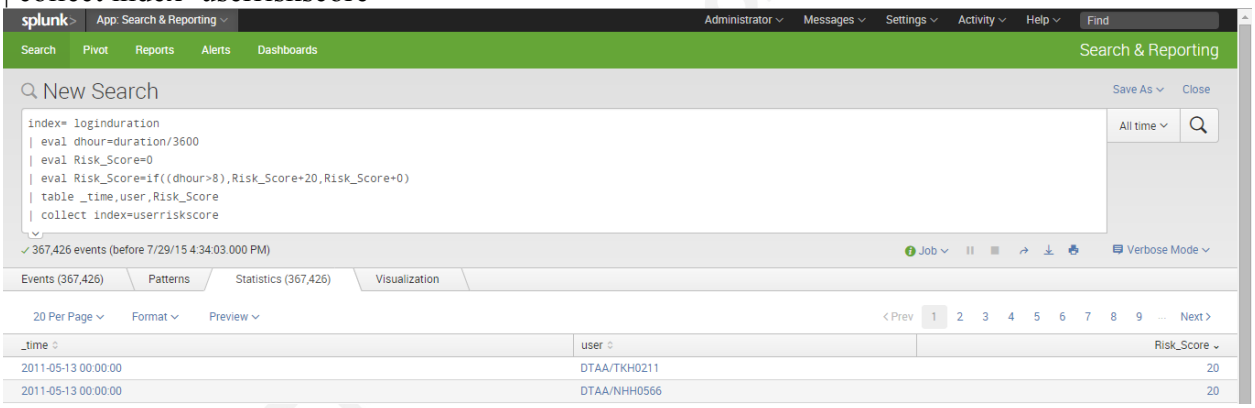



```
index=dcount
| eventstats avg(count) as threshold
| where count>threshold
| eval Risk_Score=0
| eval Risk_Score=Risk_Score+20
| table _time,user,Risk_Score
| collect index=userriskscore
```

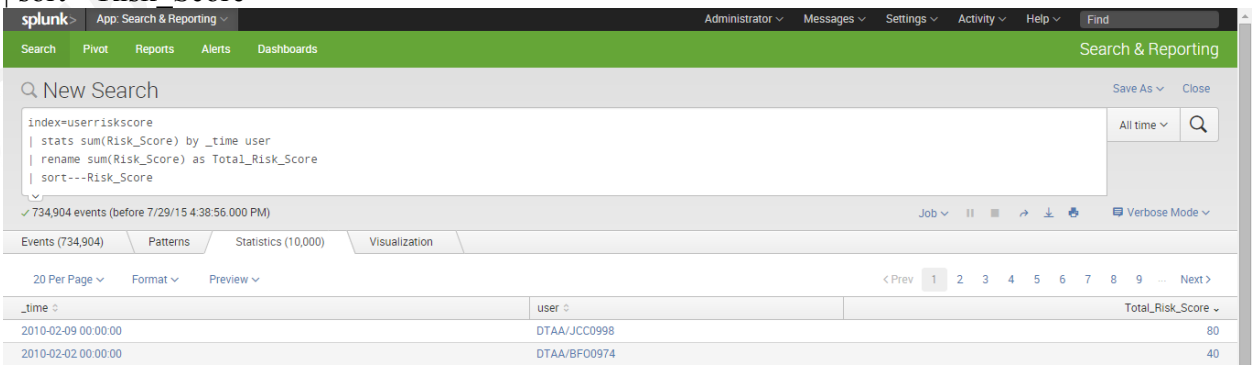
dfir.aaa@gmail.com




```
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