Your Challenge

Insider Threat Mitigation

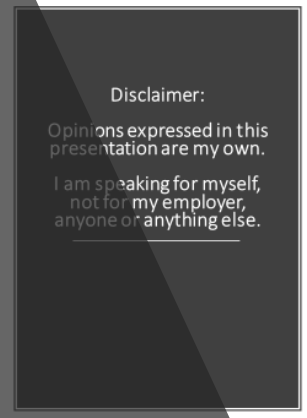
A Path Forward

Balaji Balakrishnan

Disclaimer:

Opinions expressed in this presentation are my own.

I am speaking for myself, not for my employer, anyone or anything else.



Agenda

- Introduction
- Insider Threat Mitigation Framework
- Risk Scoring Methodology Using Splunk
- Key Takeaways
- Conclusion

Introduction

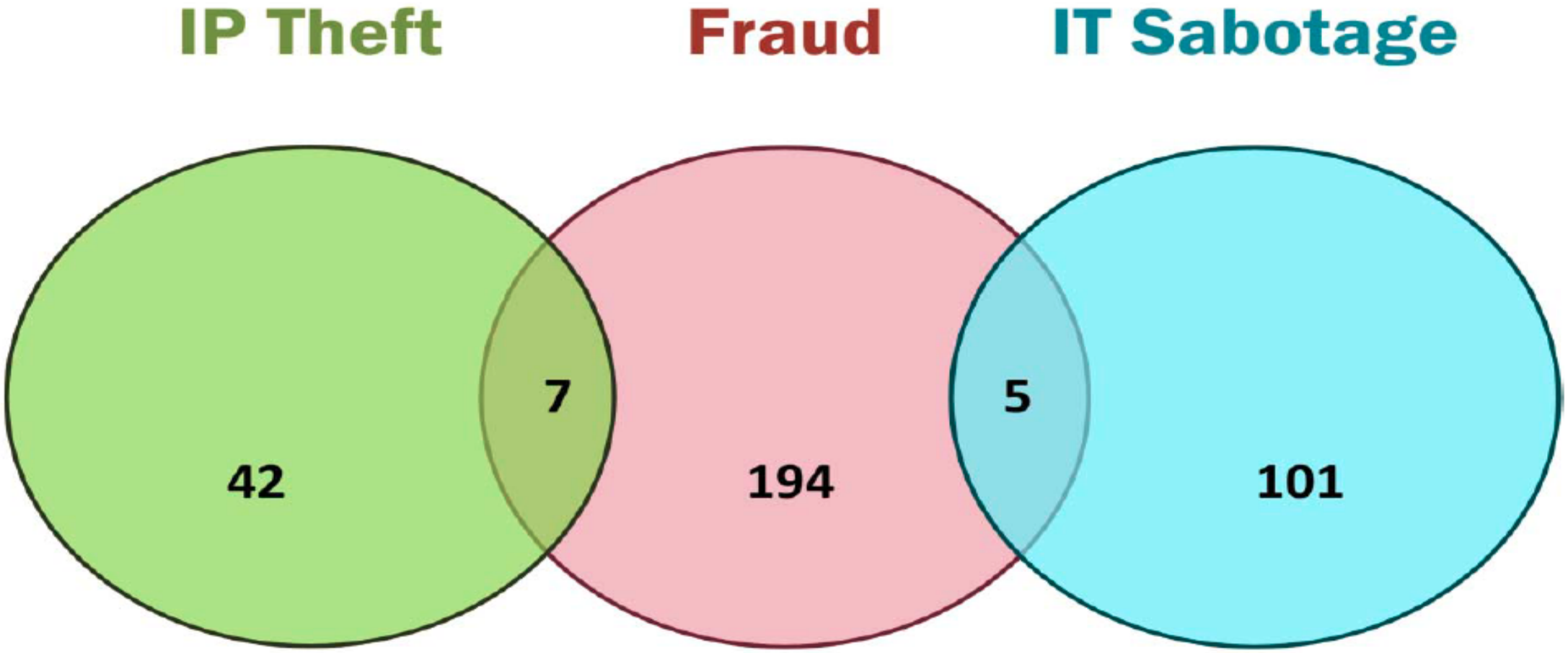
```
Main () {
        printf("I'm Balaji, and I have more than 16 years of
experience working in Information Technology and
Information Security, primarily in the financial services
space in security operations and incident response. ");
}
```

What is an Insider Threat ?

- "The CERT Program's definition of a malicious insider is a current or former employee, contractor, or business partner who meets the following criteria:
  - has or had authorized access to an organization's network, system, or data
  - has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

- The CERT Program's current analysis recognizes the following unique patterns of insider threat behavior: intellectual property (IP) theft, IT sabotage, fraud, espionage, and accidental insider threats. This guide focuses on IP theft, IT sabotage, and fraud." (CERT, 2013)

CERT Insider Threat Incident Database - Classification



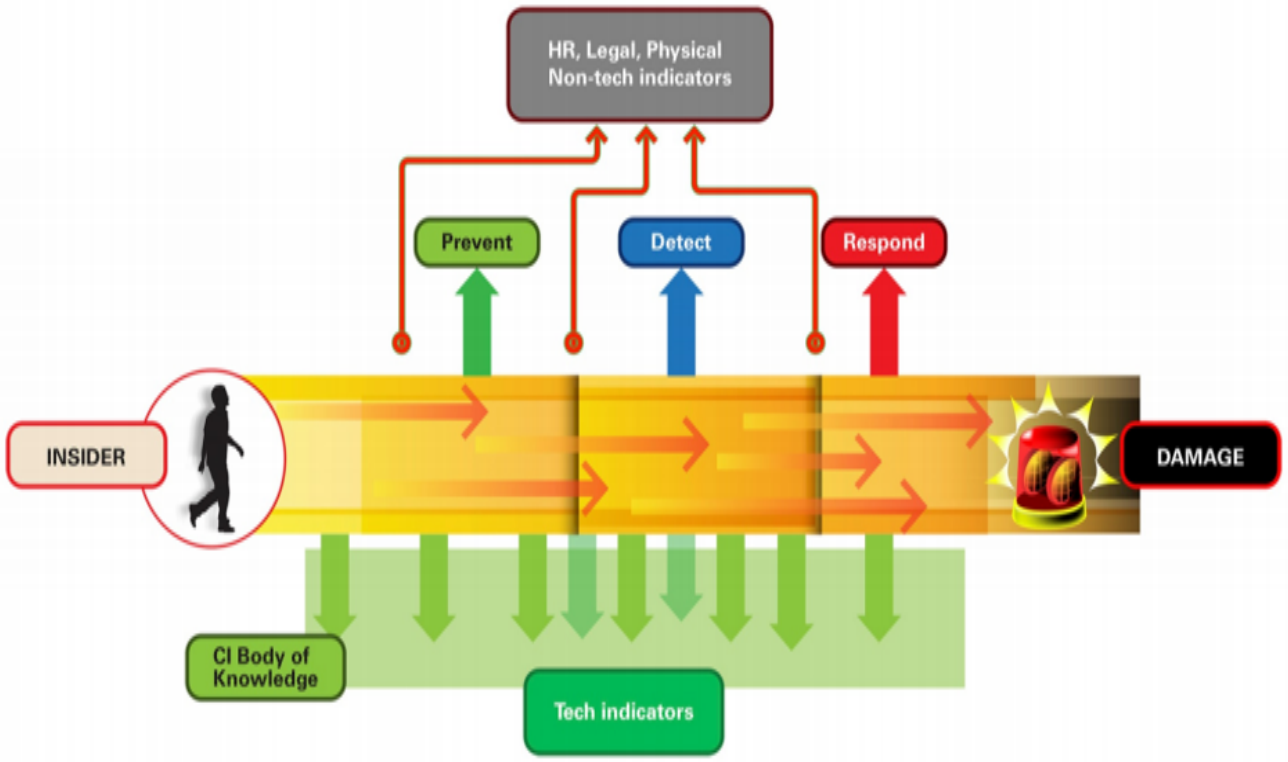
Source: CERT, 2016

How rampant is the problem of Insider Threats?

- 60% of all attacks are caused by insider threats
- 61% of organizations do not monitor privileged users more closely than regular users

Source:
(IBM, 2016)

How does an Insider Threat Mitigation Program work?



Opportunities for prevention, detection, and response for an insider attack

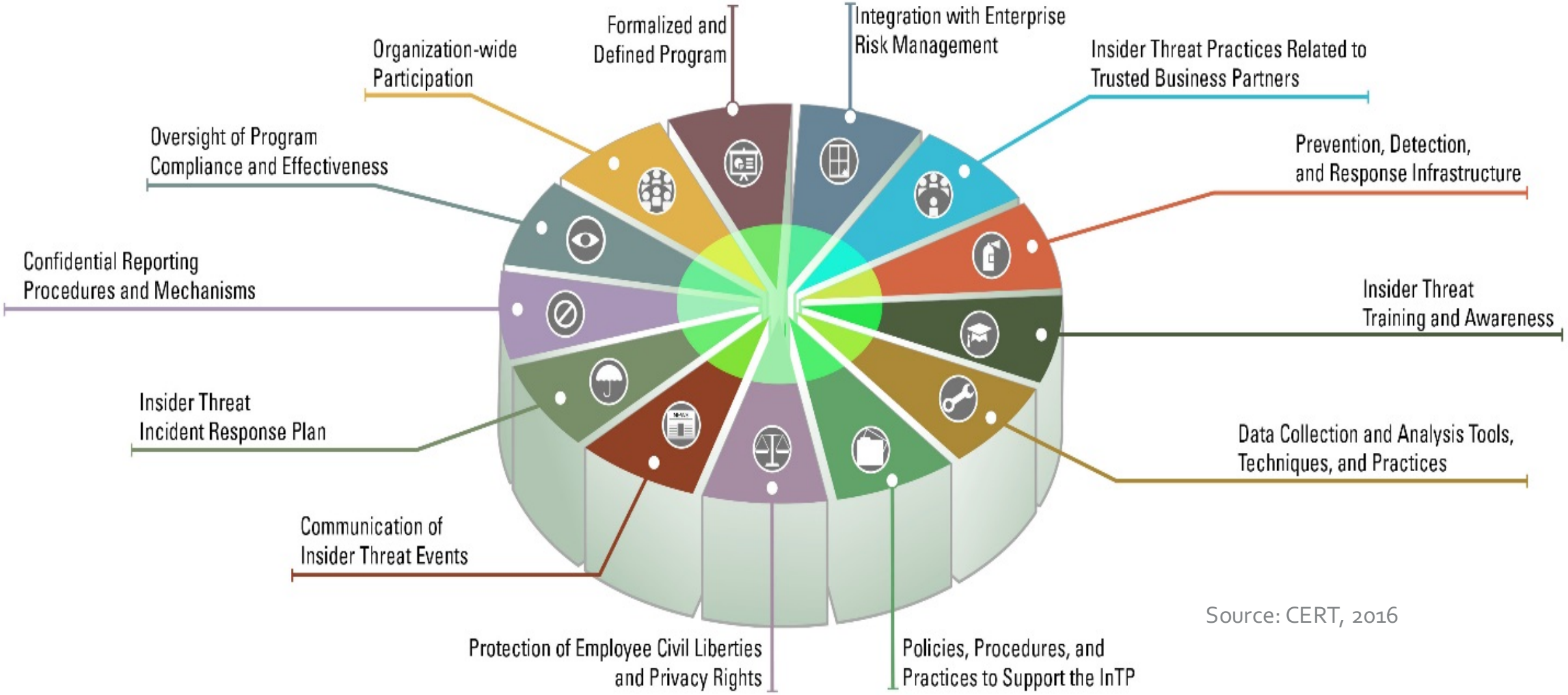
Source:
(CERT, 2013)

There are many Insider Agent Types

Attack Types \ Intent →	Non-Hostile			Multiple		Hostile							
	Reckless Individual	Untrained / Distracted Individual	Outward Sympathizer	Vendor	Partner	Irrational Individual	Thief	Disgruntled Individual	Activist	Terrorist	Organized Crime	Competitor	Nation State
Accidental Leak	X	X	X	X	X	X		X					
Espionage				X	X		X	X	X		X	X	X
Financial Fraud				X	X		X	X			X		
Misuse	X	X	X	X	X	X		X	X				
Opportunistic Data Theft				X	X		X	X	X		X	X	X
Physical Theft						X	X	X		X	X		
Product Alteration	X	X		X	X			X	X		X	X	X
Sabotage						X		X	X	X		X	X
Violence						X		X		X			

Source: (CERT, 2013)

CERT Insider Threat Center: Key Components of an Insider Threat Program



Source: CERT, 2016

INSA Insider Threat Mitigation Framework – Case Study

Source: INSA, 2014

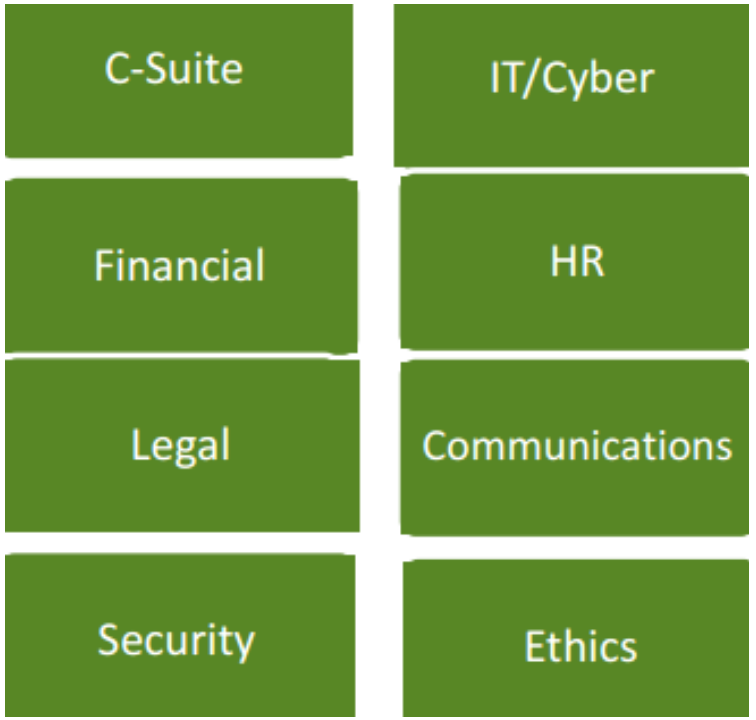
Initiation Phase

- Step 1: Initial Planning – Gather input from the existing program and perform a comprehensive assessment of the current state and recommend a future state to mitigate insider threats.

Source: INSA, 2014

Stakeholders

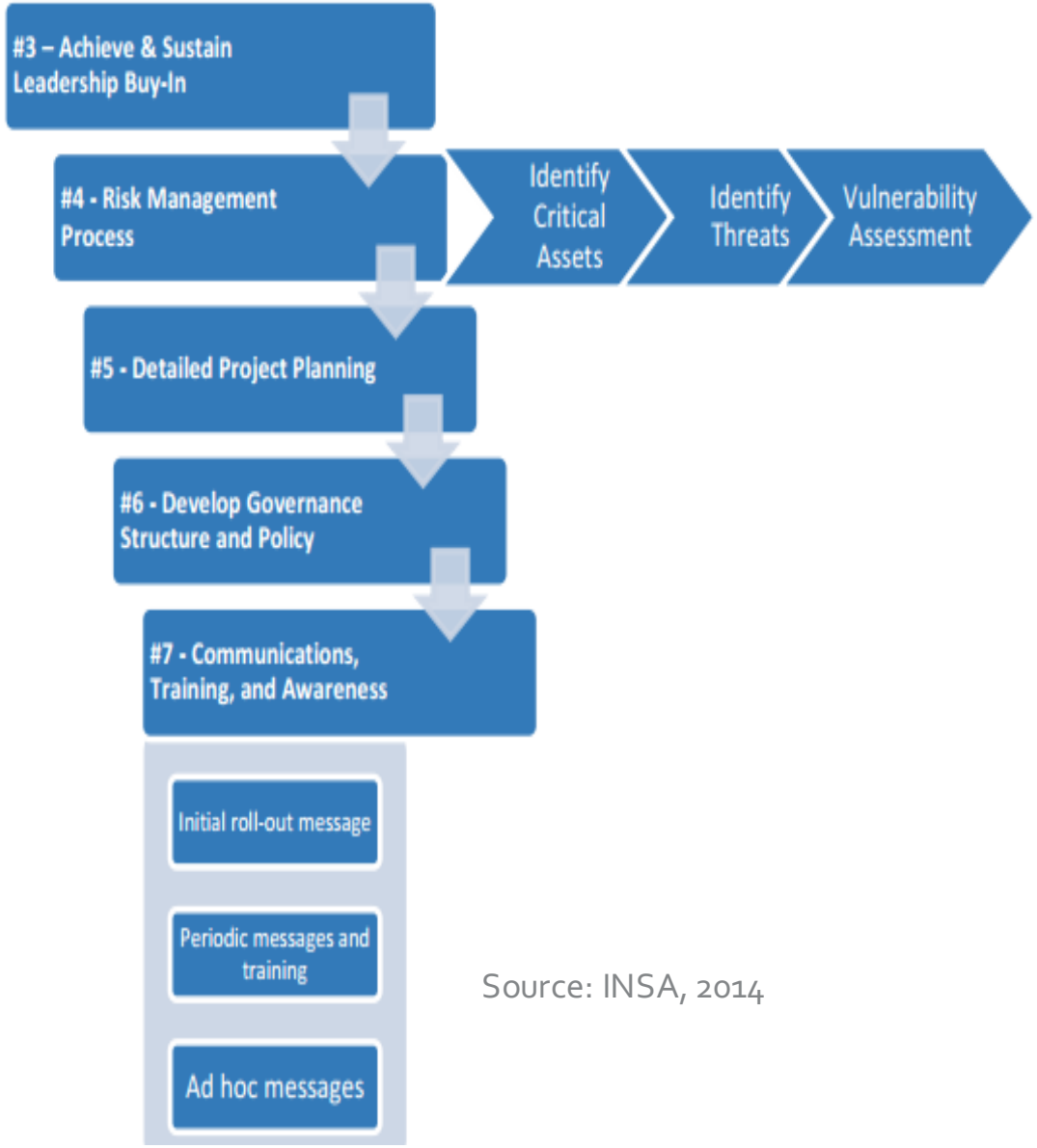
- Step 2: Identify Key Stakeholders - Some of the key members may include the Chief Information Officer, Chief Information Security Officer, Business Unit Leads, HR Vice President, Chief Counsel, Chief Privacy Officer, Infrastructure Lead, and the Application Development Lead.



Source: INSA, 2014

Planning Phase

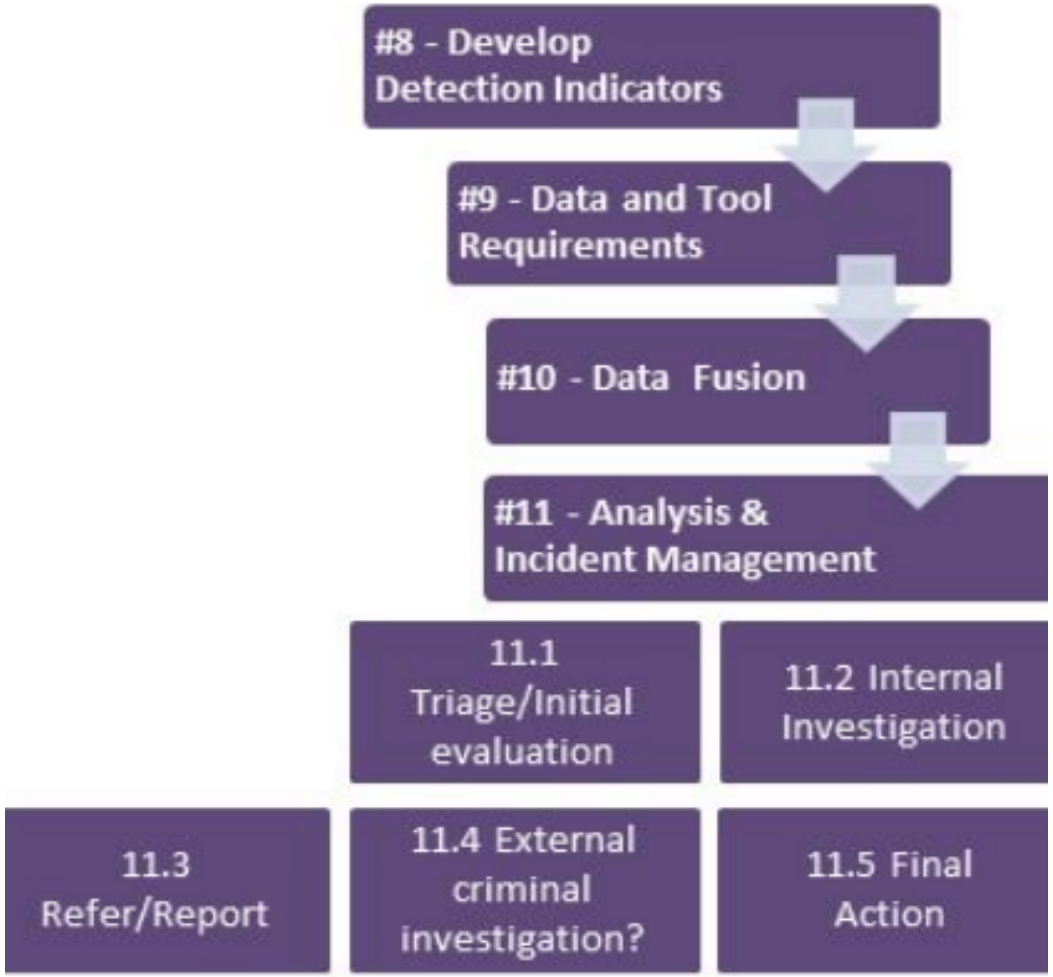
- Step 3: Leadership Buy-In – Ensure sign-off is received from the senior management team. It is important to "win the hearts and minds" of the leadership.
- Step 4: Risk Management Process – Follow a risk management process framework such as ISO 3100
- Step 5: Detailed Project Planning – Develop your project plan and include items such as phases, milestones, due dates, resources, etc.
- Step 6: Develop Governance Structure – Assign a Program Manager and Steering Committee
- Step 7: Communication, Training – Develop your communication and training plan.



Source: INSA, 2014

Operations Phase

- Step 8: Develop Detection Indicators - Determine your risk indicators and the associated parameters and data sources.
- Step 9: Data and Tool Requirements – Obtain a diverse set of data, from proxy logs to HR records for example, and then determine your tool requirements
- Step 10: Data Fusion – Bring your data together. 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
- Step 11: Analysis and Incident Management – Develop an incident management process that includes HR, ethics, and compliance.



Source: INSA, 2014

There are numerous analytic indicators of varying attack types

Analytic Indicator Category	Analytic Indicator	Attack Types								
		Accidental Leak	Espionage	Financial Fraud	Misuse	Opportunistic Data Theft	Physical Theft	Product Alteration	Sabotage	Violence
Activity-Based Analytics										
System	Authentication and Authorization Failure		1	1	1	1		1	1	
	Changes in Data Access Patterns		1	1	1	1		1	1	
	Access Inconsistent With User Class		1	1	1	1		1	1	
	Changes in Network Patterns	2	2	1		1			2	
	Network Patterns Inconsistent with User Class	1	1			1				
	Data Exfiltration	1	2	2		1			2	
	Unauthorized Data Access Methods	1	1		1	1				
	Privilege Change		1	2	1	1		2		2
	Erroneous Defensive Posture Changes	2			1	1		2		
	Improper Command Usage	2								
	Knowledge Access		1	2	1	1				
	Audit Log Modification		2	1	1			1	1	

Sample Indicators (Step 8 from the previous slide)

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

Understanding the Investigative Challenge of the Insider Threat

Raw Data → Observations → Indicators → Behaviors & Focus

Incoming Data is Processed to Create Observations

- Time Reporting
- E-mails
- Remote Access
- Building Access
- Phone Records
- Travel Records
- Financial Records Credit Reports
- File Downloads
- Inter/Intranet Traffic

Observations Processed to Infer Indicators

- File Size
- File Combinations
- Web Sites
- Authorization Attempts
- Trading Activity
- Usage Patterns
- HR/ Performance Information
- Install Scripts

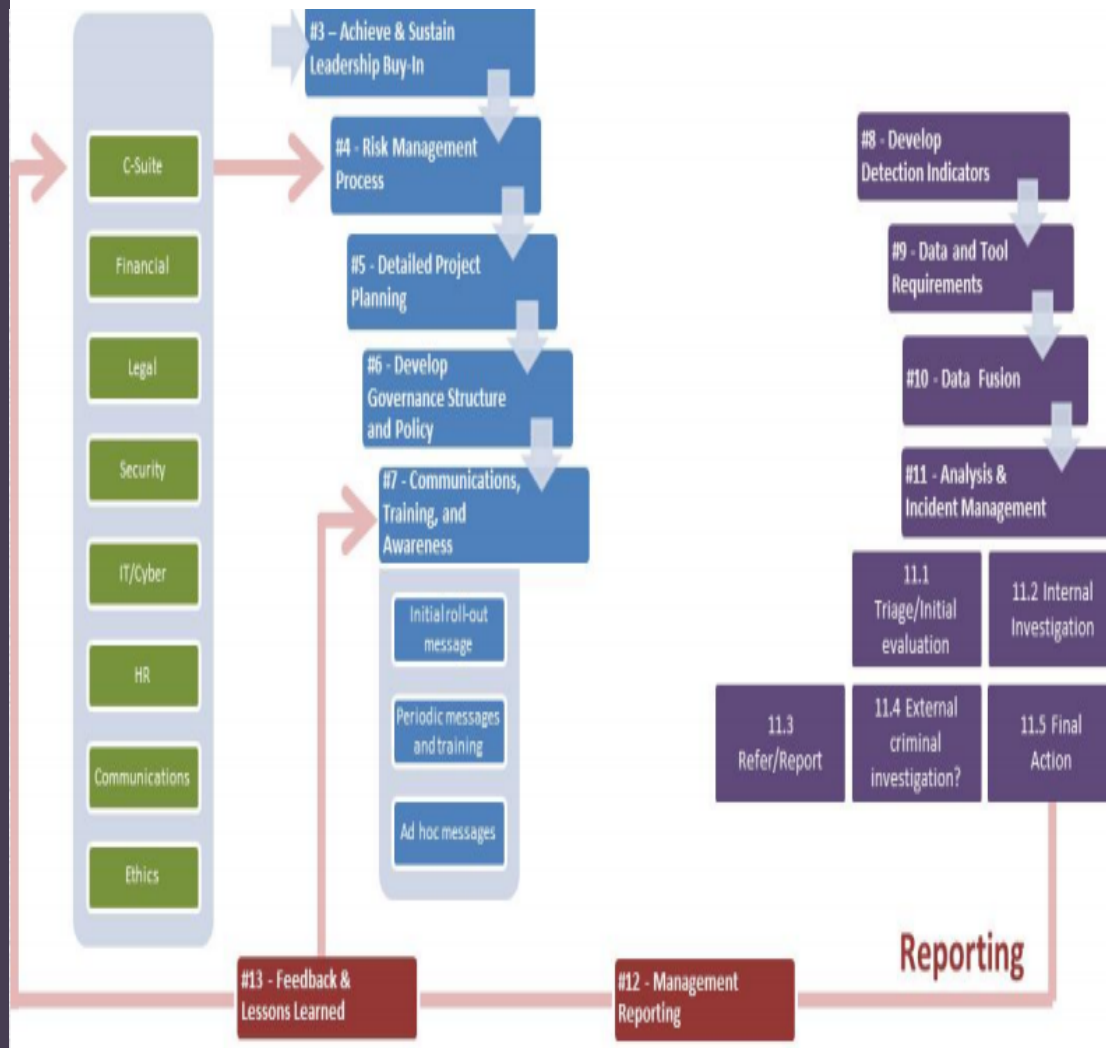
Indicators Assessed to Evaluate Threat

- Policy Violations
- Harvesting Property Data
- Access Attempts Outside of Pattern
- Attempts to Access Privileged Data
- Disgruntled Employee
- Suspicious Communications

Discover, Identify & Associate Actions that Fit a Malicious Profile

Management Reporting Phase

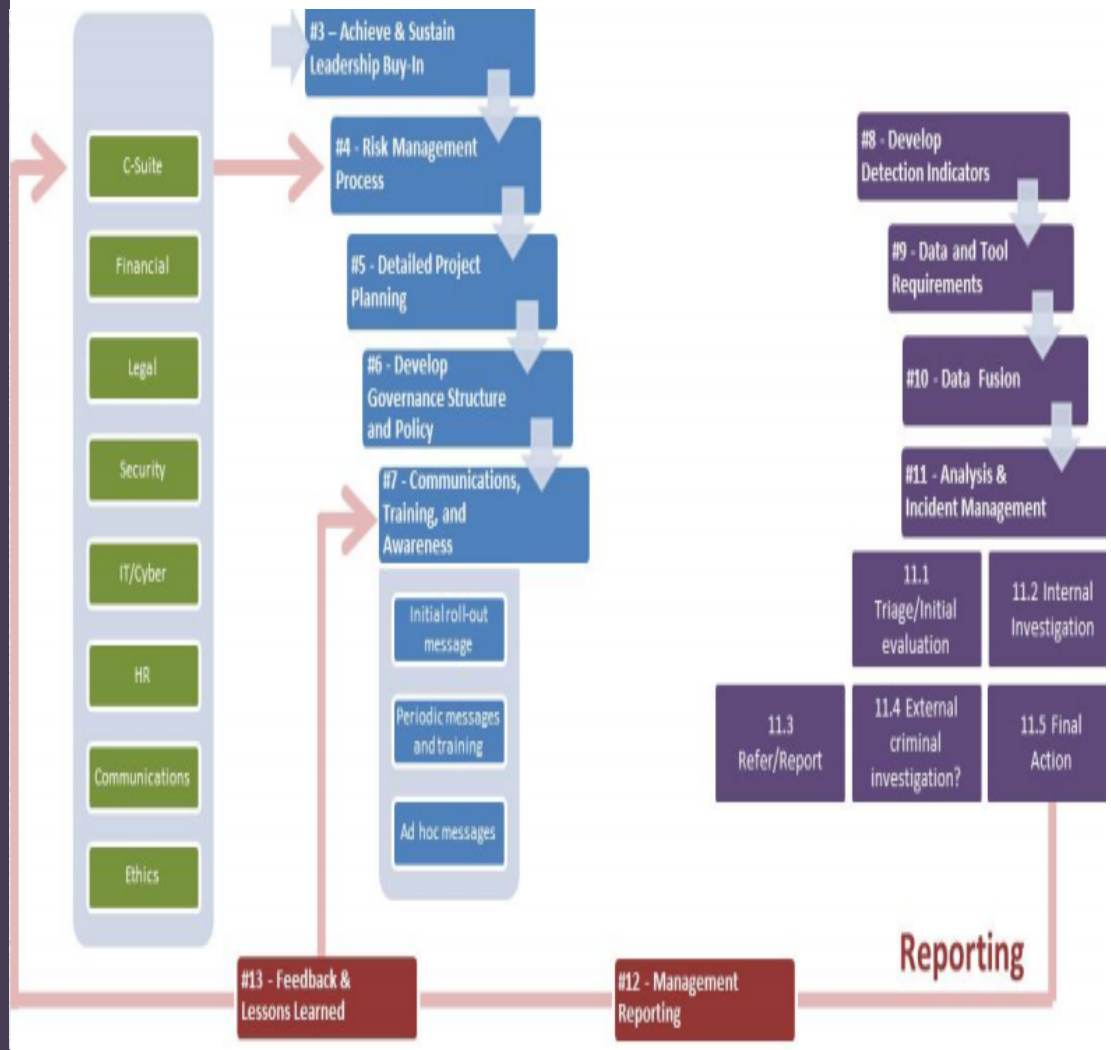
- Step 12: Management Reporting- Develop reports to ensure management fully understands the current state of the security operations



Source: INSA, 2014

Feedback and Lessons Learned

- Step 13: Feedback and 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.



Source: INSA, 2014

Statistical Analysis - Risk Scoring Methodology

- Step 1 – Identify anomalous events based on baseline or threshold
- Step 2 – Assign risk scores for each user/identity for each anomalous event
- Step 3- Aggregate all the risk scores per day to identify top user/identity that requires further investigation to determine the threat activity involved.

Risk Scores – Splunk Example

- Step 1 – Identify anomalous events based on baseline or threshold

```
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
```

Risk Scores – Splunk Example

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

```
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
```

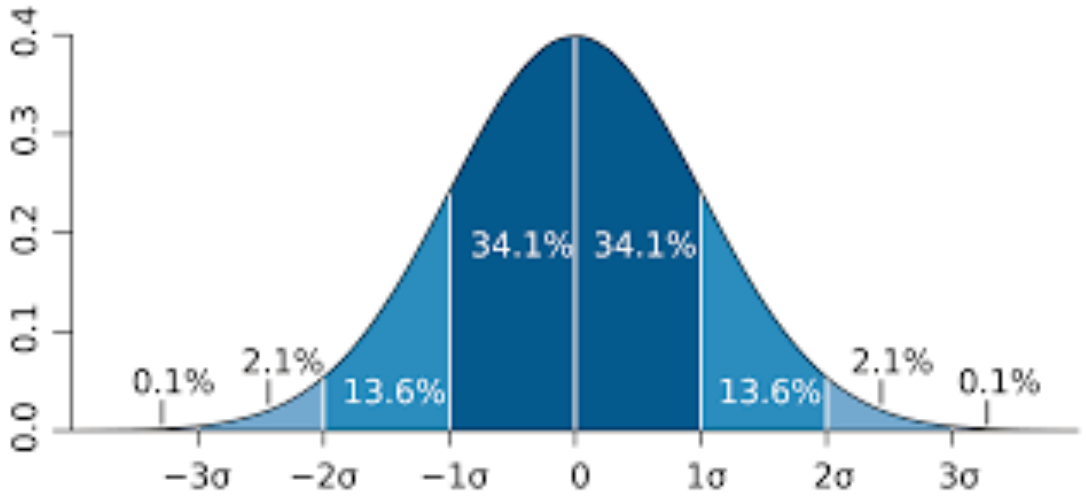
Risk Scores – Splunk Example

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

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

Risk Score Model using Statistical Deviations

- Simple User/Network Behavior Analytics - A complete statistical model can be applied to the daily user/network activity to calculate anomalous events :
  - Calculate the Average and the Standard Deviation for each User/network behavior value on Daily, Weekly, and Monthly time windows
  - Daily comparison of the User/network behavior 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/network behaviors on a daily basis with the highest risk scores across the Daily, Weekly, and Monthly measurements are to be identified as highest potential risk



Source: Wikipedia.org

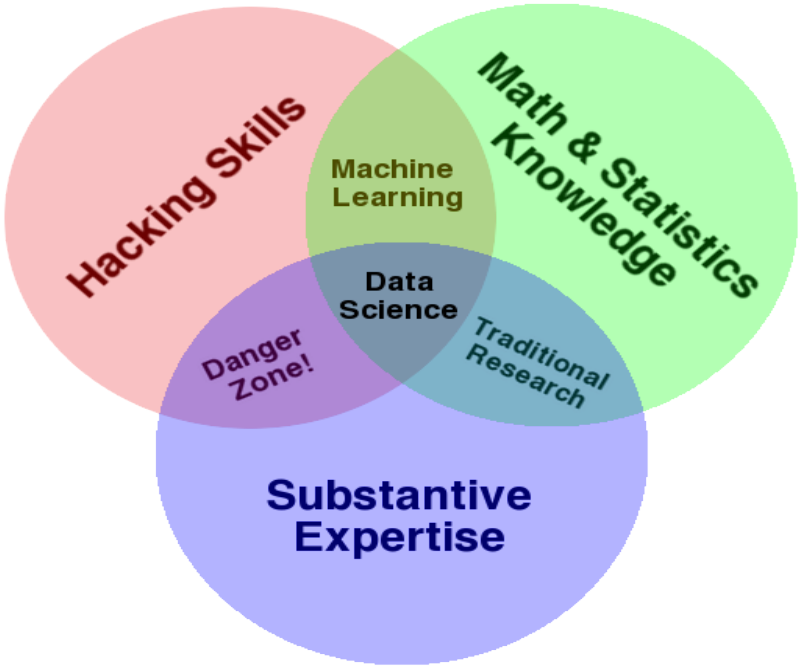
Big Data Security Analytics Platforms

- Big Data Security Analytics Platform Examples
    - Apache Metron, OpenSOC, ELK, RITA, Hadoop, ONI, Splunk, Sqrrl
- Data Collection(host, network, application, DLP, contextual)
- Cloud technologies rapidly evolving
- Big data analytics technologies rapidly evolving

Data Science Techniques

- Approaches
  - Exploration & Visualization
    - Graph
    - Parallel coordinates
  - Statistical Analysis
    - Top talkers & Long tail analysis
    - Using Baselines
    - Risk Scoring
    - Natural Language Processing
    - Time series analysis
  - Machine Learning
    - Supervised learning
      - Classification
      - Regression
    - Unsupervised learning
      - Clustering

….and Skills



Key Takeaways & Conclusion

- Top down- Support from senior executives mandatory
- Develop insider threat policy framework
- Develop Insider Indicators of Compromise with HR, Legal, Ethics teams
- Develop dedicated team with few senior members in the team
- Establish good, repeatable and verifiable insider threat investigation process with documentation
- Build Big data analytics platform integrating all data sources
- Create Insider threat detection process integrating all teams (HR, Legal etc.)

Questions