Insider Threat
Starting a Program

Deborah Pianko, SAS Detection & Investigation Division, Principal
Patrick Alcorn, SAS Government, Solutions Manager

01 The Threats Within

02 Recent News

03 Your 100 Day Plan

04 Technology Best Practices

05 Take-Aways

sas®
THE POWER TO KNOW®

The Disgruntled Employee

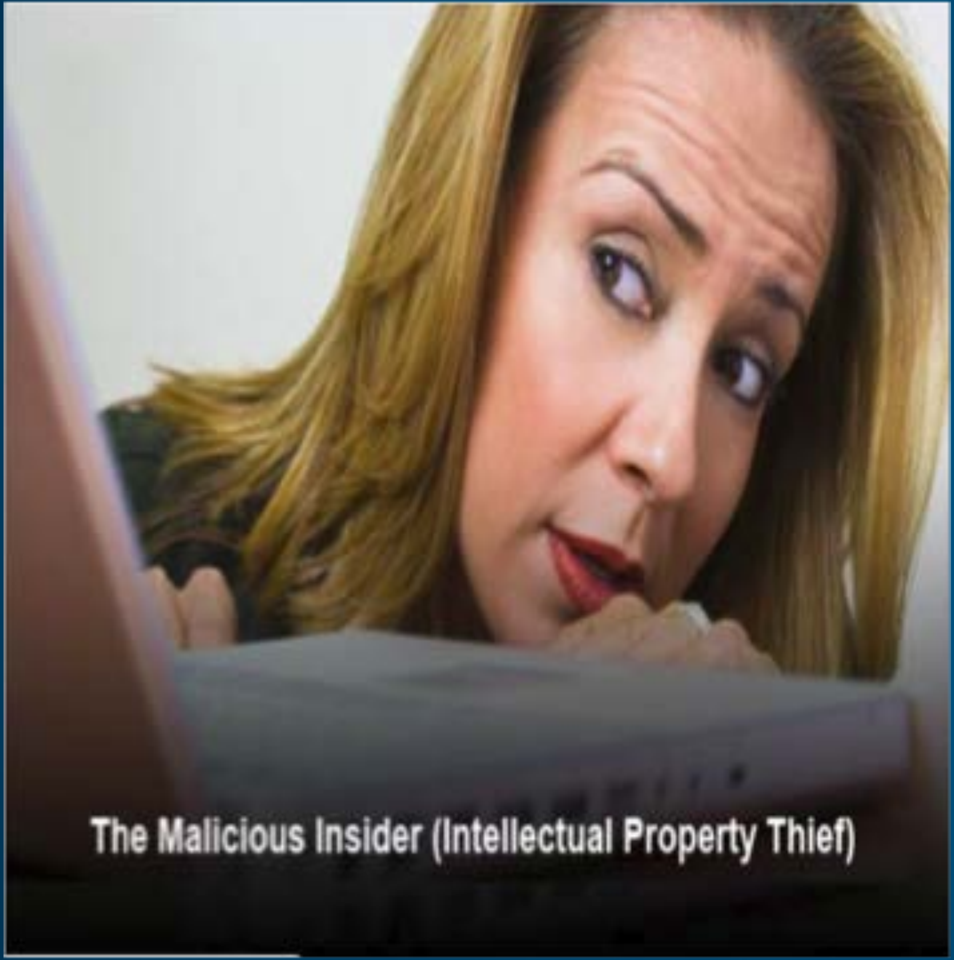
- Saboteur

Dossier

- May be introverted
- Detail oriented
- Feels underappreciated
- Frustrated; careless about work
- Job hunting
- Arguments with superiors
- Might leave a “time bomb”

Behaviors

- ✓ Access to servers outside normal business hours
- ✓ Sentiments reveal dissatisfaction
- ✓ Frequent rule violations



The Malicious Insider

- Intellectual Property Theft

Dossier

- Climbing corporate ladder
- No time for those “beneath”
- Still feels underappreciated
- Plans to leave for key competitor
- Taking valuable IP with them
- Typically senior team members with a lot of access to sensitive info

Behaviors

- ✓ Many inbound emails from external contacts
- ✓ Frequent abnormal communications outside normal channels
- ✓ Spikes of documents to external email (or dropbox)

The Absent Minded Manager

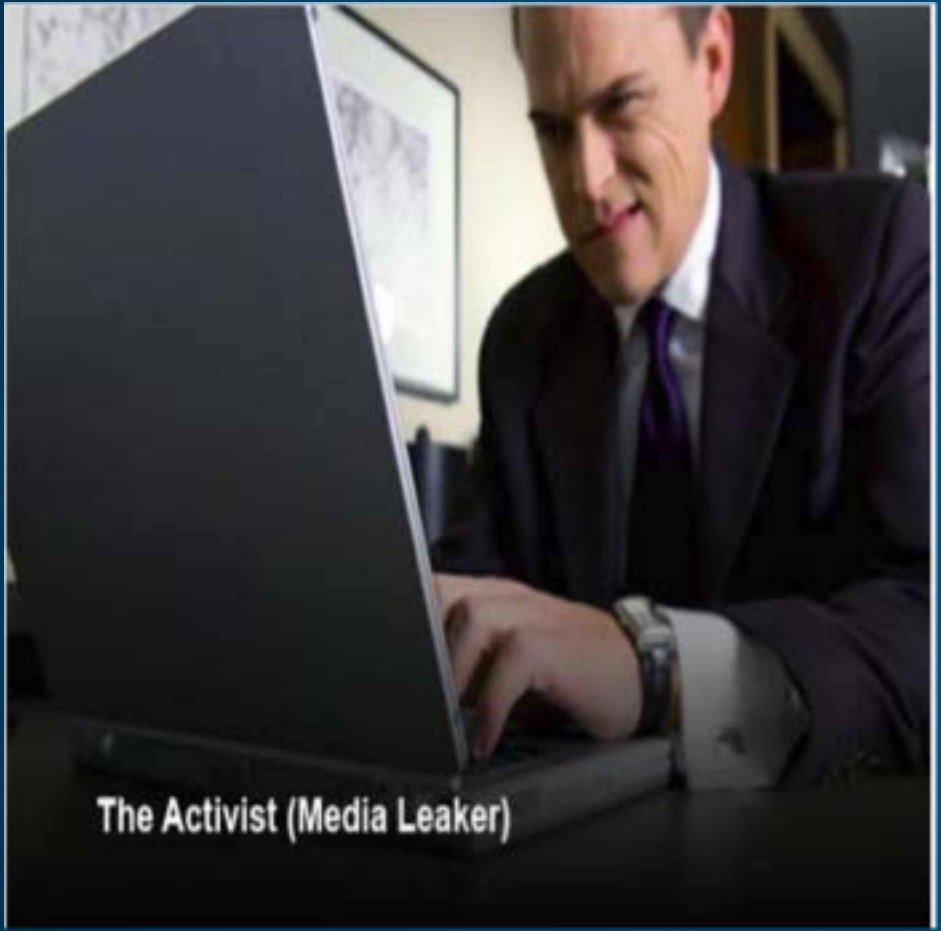
- Negligent Employee

Dossier

- This HR manager receives a request to email employees' personally identifiable information (PII) to a new accounting firm.
- The email address turns out to be fraudulent.
- This employee rarely takes the time to set up passwords and regularly emails himself/herself sensitive information.

Behaviors

✓ Sloppiness and inattentiveness
✓ Sharing passwords and sensitive information via email



The Activist

- Media Leaker

Dossier

- Top performer, privy to sensitive high level internal communications (e.g. executive pay, company spending, HR violations)
- Decides they've had enough
- Shifts working hours to he can secretly document activities
- Sends "dirt" on organization to national media organization and then quits

Behaviors

- ✓ Stressed or depressed
- ✓ Seeks access to sensitive company information
- ✓ Active on servers at unusual hours
- ✓ Spike in downloading activity

The Compromised Consultant
(Code and Intellectual Property Thief)

The Compromised Consultant

- Code and Intellectual Property Thief

Dossier

- In personal financial trouble
- Targeted by an organized crime network because of his technical position of trust
- Blackmailer may pose as technical recruiter and convince that person to steal sensitive PII information
- Will become more confident and aggressive about stealing information
- Will become sloppy and prepare to resign to avoid being caught

Behaviors

- ✓ Signs of financial instability (i.e., gambling, extravagance)
- ✓ Abnormally high level of downloads or copies of documents

The Planted Insider (Intellectual Property Thief)

The Planted Insider

- Intellectual Property Thief

Dossier

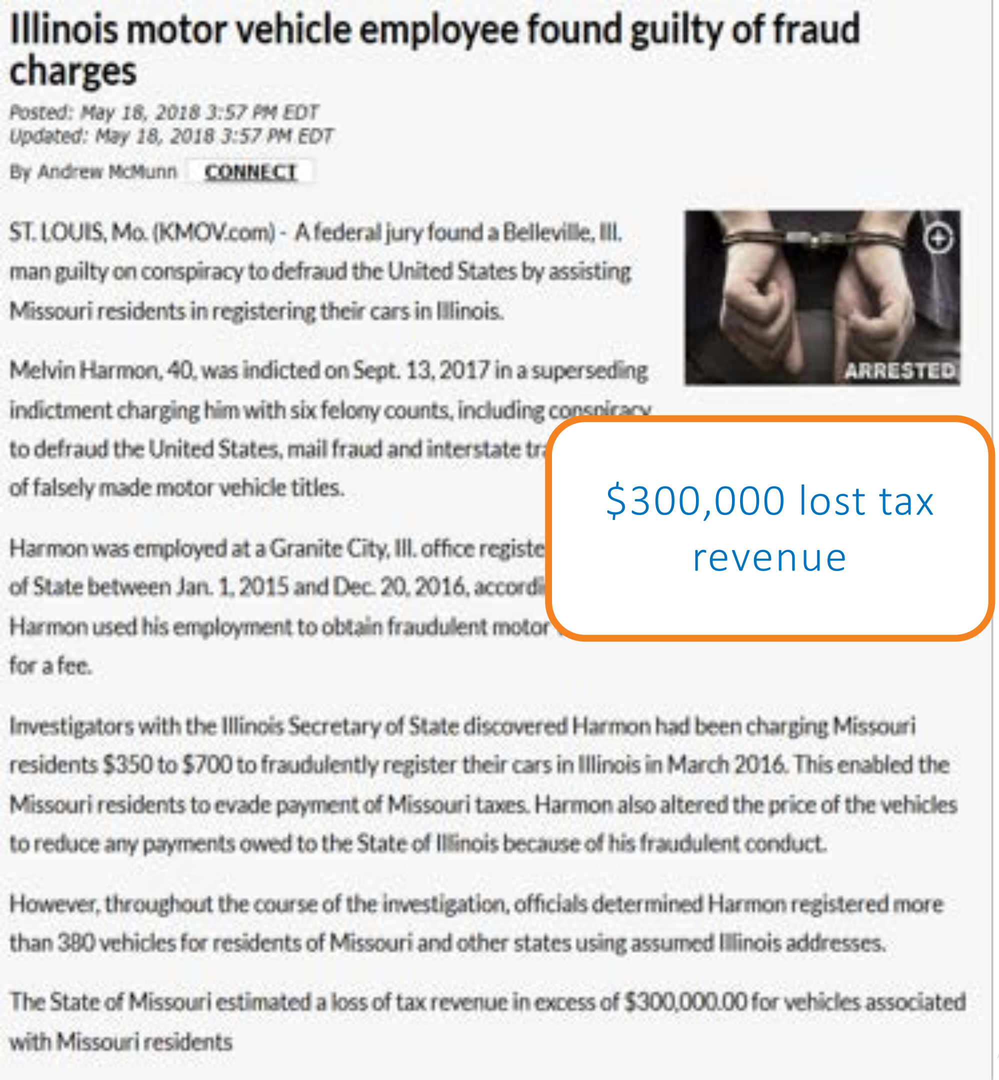
- Quickly promoted and well respected
- Approached by foreign national at conference
- Began frequent but casual communication on a regular basis
- With this employee's help, the foreigner lands an entry-level position on the equities trading floor.
- The two kept in touch but employee soon had doubts about him

Behaviors

✓ Communicates primarily with external contacts

✓ Motivated by money; skirts rules to get ahead

	IT Sabotage	Fraud	Theft of Intellectual Property
Current or former Employee?	Former; disgruntled	Current; stressed	Current (**within 30 days of resignation**); can be disgruntled but not necessarily
Type of position	Technical (e.g., sys admins, programmers, DBAs)	Non-technical (e.g., data entry, customer service) or their managers	Technical (e.g., scientists, programmers, engineers) or sales
Gender	Male	Male/Female 50%/50%	Male
Target	Network, systems, or data	PII or Customer Information	IP (trade secrets) or Customer Information
Access Used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At Work



Illinois motor vehicle employee found guilty of fraud charges

Posted: May 18, 2018 3:57 PM EDT
Updated: May 18, 2018 3:57 PM EDT

By Andrew McMunn CONNECT

ST. LOUIS, Mo. (KMOV.com) - A federal jury found a Belleville, Ill. man guilty on conspiracy to defraud the United States by assisting Missouri residents in registering their cars in Illinois.

Melvin Harmon, 40, was indicted on Sept. 13, 2017 in a superseding indictment charging him with six felony counts, including conspiracy to defraud the United States, mail fraud and interstate tr of falsely made motor vehicle titles.

Harmon was employed at a Granite City, Ill. office registe of State between Jan. 1, 2015 and Dec. 20, 2016, accordi Harmon used his employment to obtain fraudulent motor for a fee.

Investigators with the Illinois Secretary of State discovered Harmon had been charging Missouri residents $350 to $700 to fraudulently register their cars in Illinois in March 2016. This enabled the Missouri residents to evade payment of Missouri taxes. Harmon also altered the price of the vehicles to reduce any payments owed to the State of Illinois because of his fraudulent conduct.

However, throughout the course of the investigation, officials determined Harmon registered more than 380 vehicles for residents of Missouri and other states using assumed Illinois addresses.

The State of Missouri estimated a loss of tax revenue in excess of $300,000.00 for vehicles associated with Missouri residents

$300,000 lost tax revenue

- Illinois DMV employee charging Missouri residents $350-$700 to register cars in Illinois to avoid Missouri taxes - > **more than 380 vehicles**
- Also altered price of vehicles to reduce any payments owed to Illinois because of his misconduct
- **Missouri lost $300,000 in tax revenue** from January 1, 2015 – December 20, 2016 (term of his employment)
- Case investigated by Missouri DOR and ASUAs. Faces 20 years prison and huge financial fines.

Other Departments of Revenue in the News

DOR #1 (Dropbox):

- DOR employee uploaded work files to personal cloud storage.
- Discovered by IT team in routine log reviews

DOR #2 (Website):

- Software glitch (web portal) allowed taxpayers to see other taxpayer data (~39,000 TP).
- Issue noticed first by payroll company

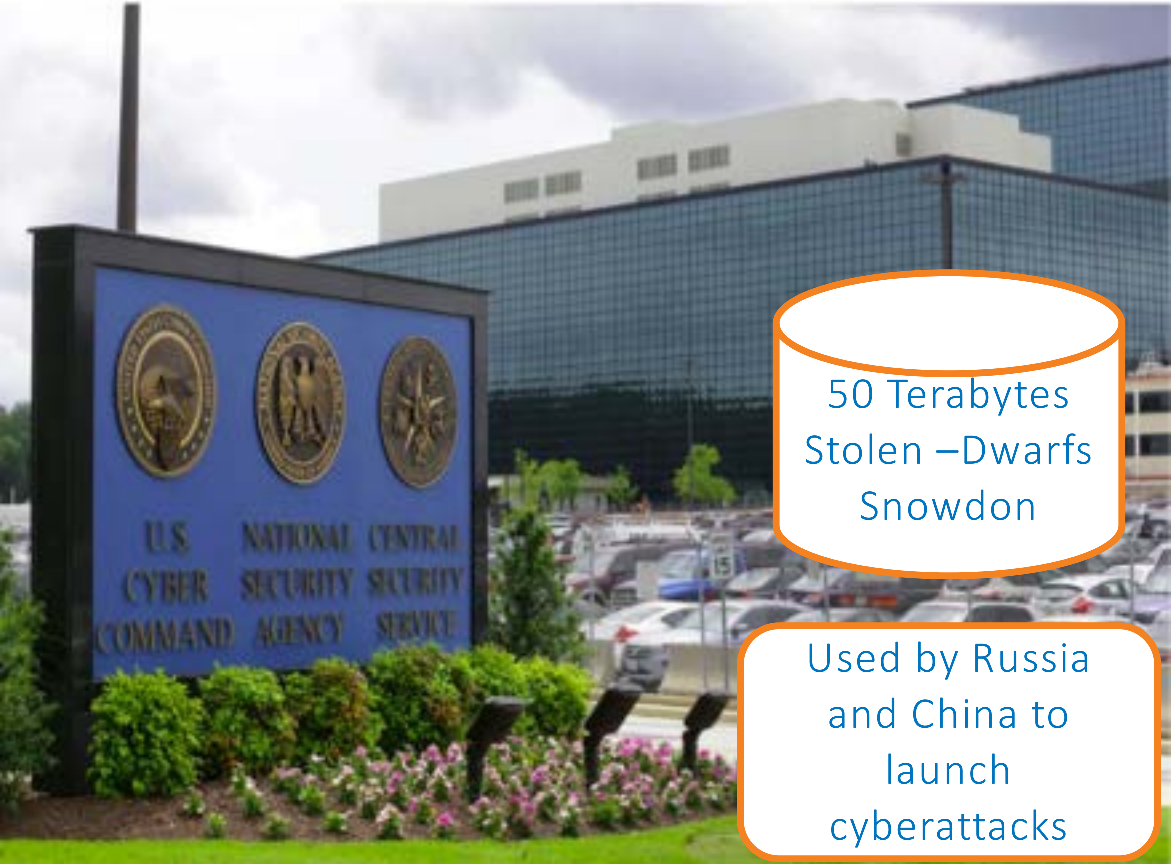
DOR #3 (Flash Drive):

- Flash drive stolen from car of auditor
- Contained names, addresses, SSNs of 2800 people employed by 6 businesses being audited

DOR #4 (Employee Credentials):

- Massive data breach by obtaining login credentials of employee – 3.6 Million Taxpayers

Ex-N.S.A. Worker Accused of Stealing Trove of Secrets Offers to Plead Guilty



50 Terabytes Stolen –Dwarfs Snowdon

Used by Russia and China to launch cyberattacks

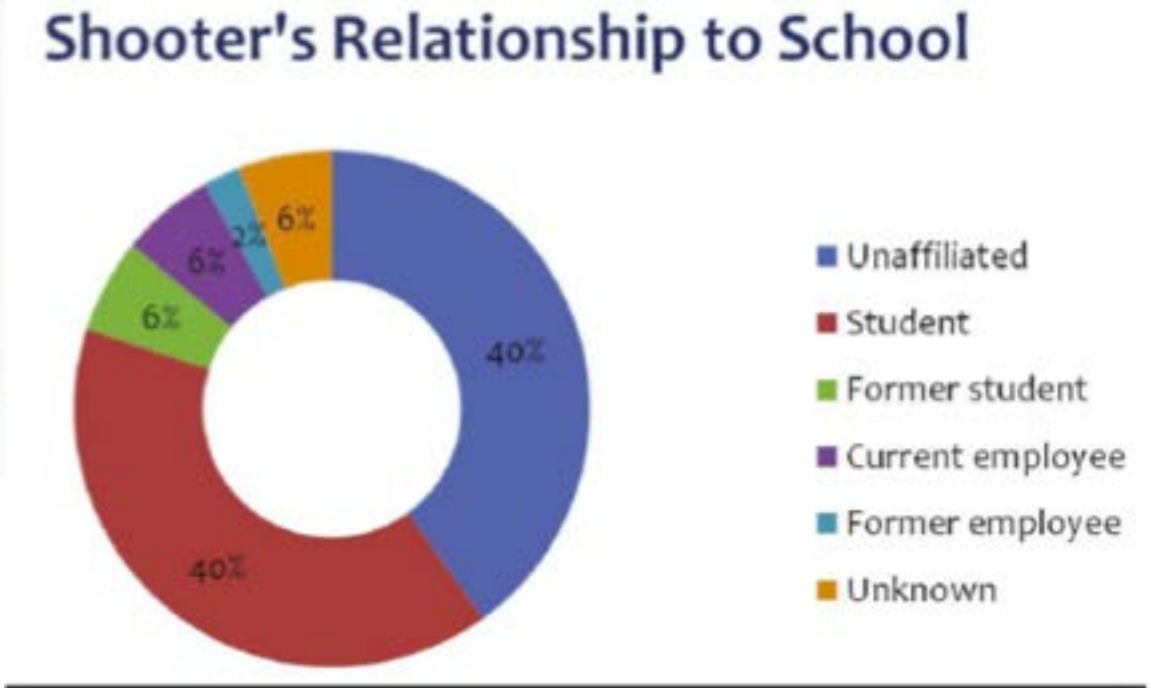
- Highly embarrassing case that exposed gaping holes in the government’s system for safeguarding secrets.
- Took home highly classified documents from the N.S.A. and other agencies beginning in the late 1990s (until 2016), stashing them on paper, hard drives and flash drives in his house in Glen Burnie, MD
- Included most or all of the agency hacking tools that ended up being offered for sale on the internet by a group calling itself the Shadow Brokers.

Insider Threat Detection
Can Extend into Safety Concerns

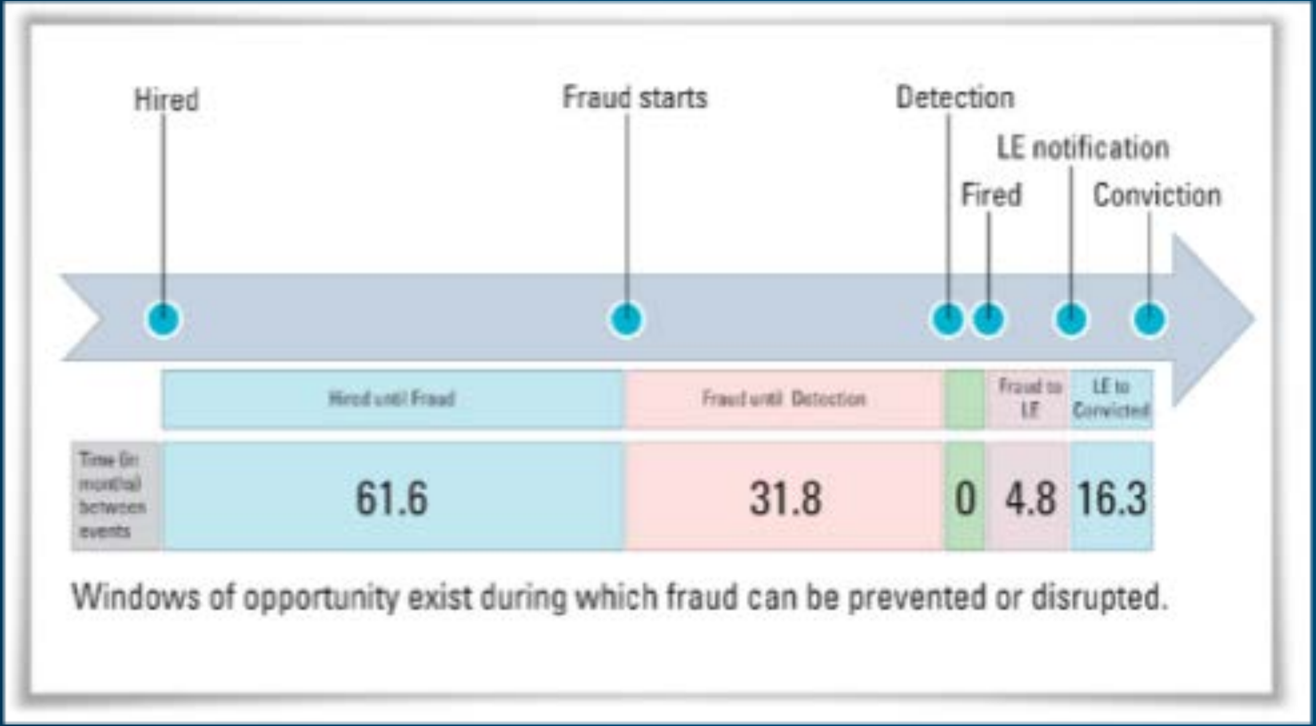
Fired worker kills five and himself in Orlando rampage

John Bacon and Rick Neale, USA TODAY NETWORK Published 10:59 a.m. ET June 5, 2017 | Updated 7:38 p.m. ET June 5, 2017

Law enforcement authorities said there were "multiple fatalities" following a Monday morning shooting in an industrial area near Orlando. (June 5) AP


Shooter's Relationship to School

Dwell Time Low and Slow – Early Detection is Key



	Hired until Fraud	Fraud until Detection		Fraud to LE	LE to Convicted
Time (in months) between events	61.6	31.8	0	4.8	16.3

Windows of opportunity exist during which fraud can be prevented or disrupted.

5 Years
HIRE -> FRAUD START

32 Months
FRAUD START-> DETECTION

Criminals who executed a “low and slow” approach accomplished more damage and escaped detection for longer – Career criminals/nation state actors are highly trained.

So Where Do I Start?

Your 100 Day Plan

100 Day Plan

Initiate (4 Weeks)

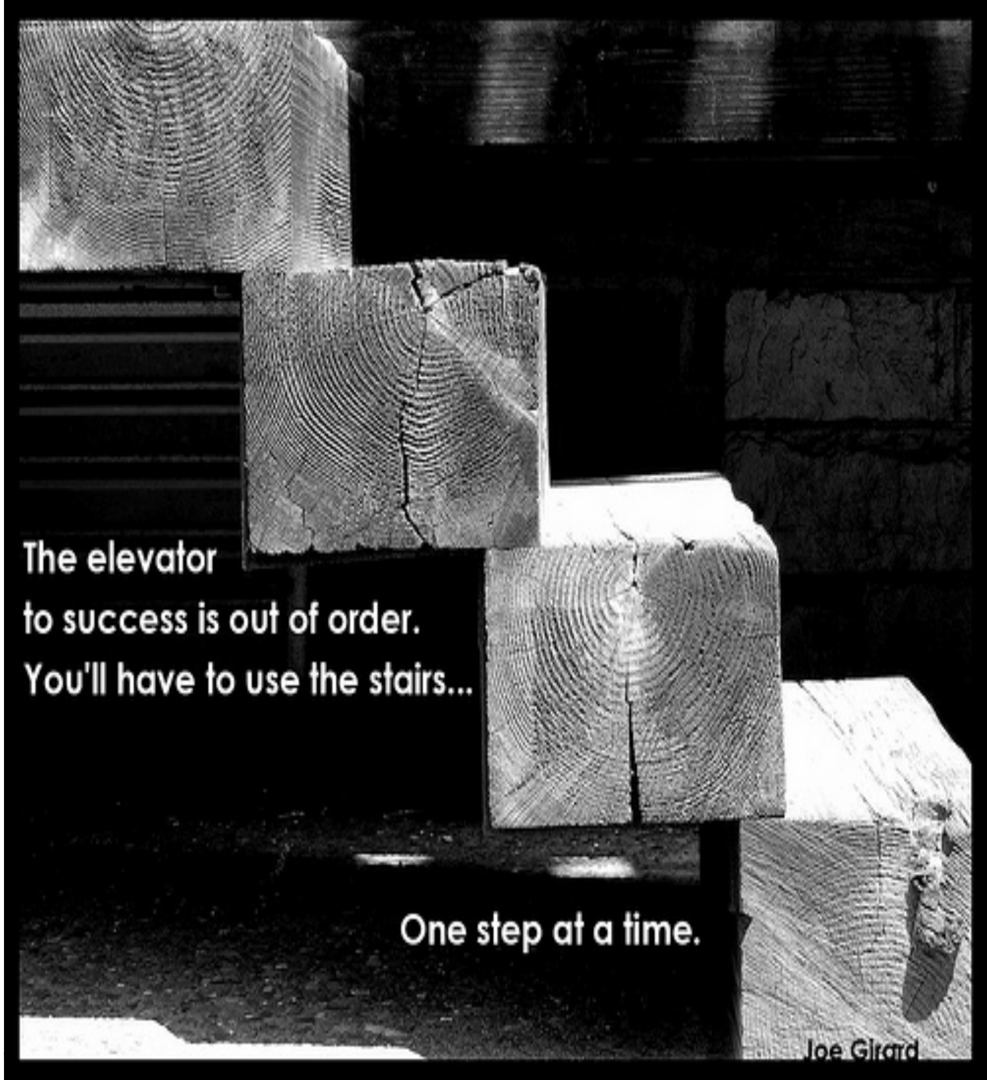
- Baseline Operations
- Identify Stakeholders
- Create Business Case
- Assemble Team

Develop (8 Weeks)

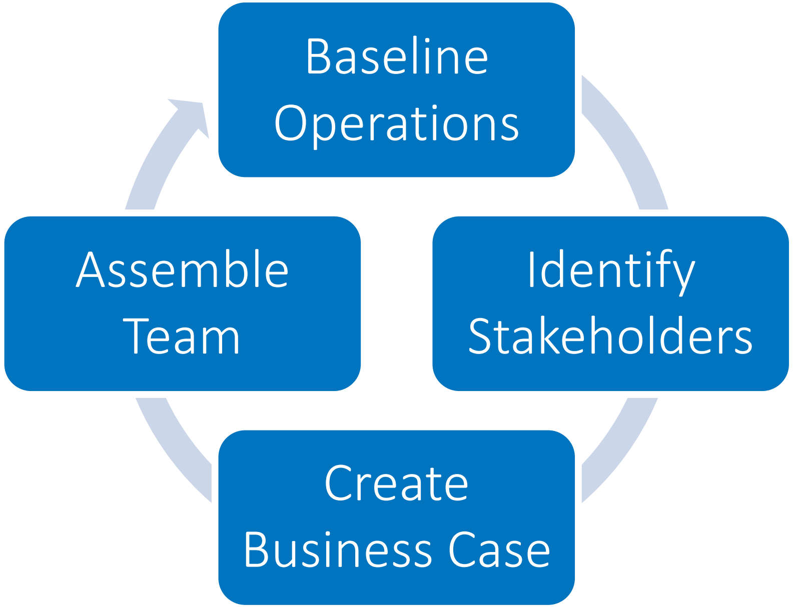
- Perform Risk Assessment
- Develop Action Plan
- Develop Operating Framework
- Obtain Employee Support

Implement (4 Weeks)

- Analyze Data & Solutions*
- Develop Response Capability
- Oversight & Compliance



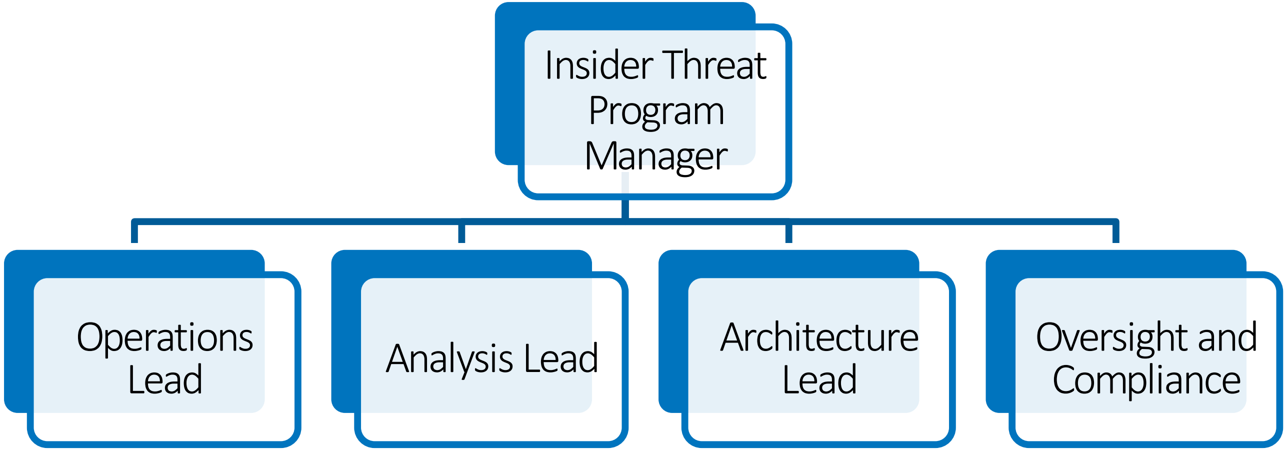
Initiation Phase (4 Weeks)



1. **Baseline Current Operations** (1 Week)
   - What components are already in place? Maturity level?
   - Use interviews; not surveys
2. **Identify Stakeholders** (1 Week)
   - Don't forget informal leaders
   - Legal, HR, IT, Communications, etc.
   - Create **Insider Threat Advisory Council**
3. **Create Business Case** (1 Week)
   - Don't forget unintentional threats
   - Focus on how business will benefit
   - What are risks of inaction?
4. **Assemble the Team** (1 Week)
   - Determine work roles
   - Align resources with roles
   - Hire as needed

Sample Insider Threat Management Team

These Do Not Need to Be Full Time Roles



Insider Threat Program Manager

Operations Lead

Analysis Lead

Architecture Lead

Oversight and Compliance

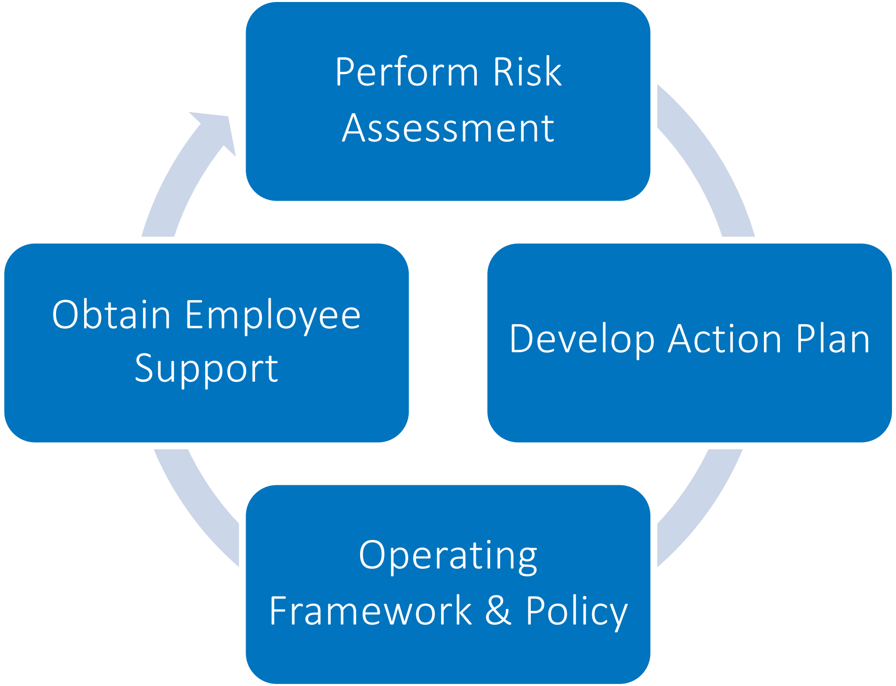
Operations Lead: Investigations & Incident Response

Analysis Lead: Monitors alerts, drafts reports, lead generation

Architecture Lead: Tool management, optimization, data ingestion

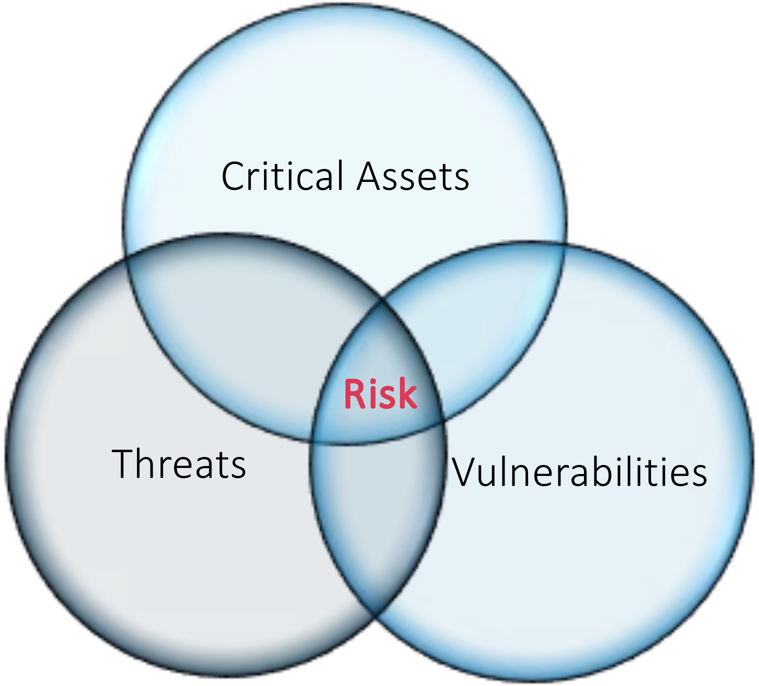
Oversight and Compliance: Performance measurement, policies and procedure adherence

Initiation Phase (8 Weeks)



1. **Perform Risk Assessment** (3 Weeks)
   - ID and **prioritize** critical assets, threats and vulnerabilities
   - Document/quantify risk(s)*
   - ID countermeasures and **tradeoffs**
2. **Develop Action Plan** (2 Weeks)
   - What are you protecting? How will it be mitigated? Resources needed? Solutions/tools? Timeframe?
3. **Develop Governance** (1.5 Weeks)
   - Documented policies, procedures and strategic plan to support Action Plan
   - Engagement mechanism with senior leadership?
4. **Employee Support** (1.5 Weeks)
   - Comms plan (email, flyers, etc.)
   - Deliver message

Sample Risk Assessment Approach



ID Risk and Loss Impact:

- **Asset**: Audit cases
- **Undesirable event**: Inappropriate adjustments (or lack of) to audit cases due to bribery or extortion of auditor
- **Consequence of loss**: Financial; reputational; legal

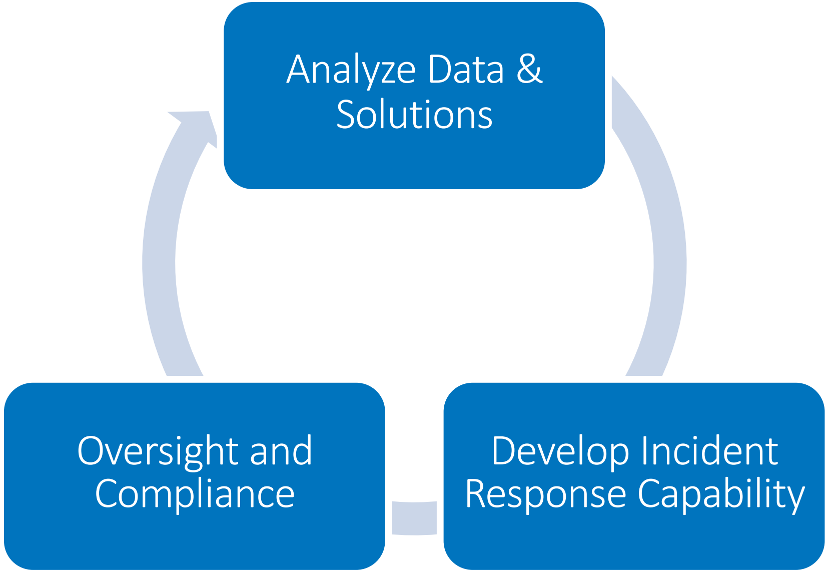
ID and Characterize the Threat

- **Motivation**: Financial; retaliation
- **Capability**: High; no sep of duties; not monitored
- **Frequency**: Med to high; several prior occurrences
- **Likelihood**: Med to high
- **Org Tolerance**: Extremely low
- **Taxpayer Tolerance**: Extremely low
- **Legal Impacts:** Extremely high

Identify Countermeasures and Costs:

- Separation of duties – low cost (Priority 1)
- UBA monitoring – moderate cost (Priority 2)

Implementation Phase (4 Weeks)



1. **Analyze Data and Solutions** (2 Weeks)
   - What data is available? Internal; external?
   - Data sharing agreements
   - Understand form and shape of data
   - Evaluate analytic solutions
   - Do you have proper expertise? Hire or outsource as needed
2. **Develop Response Capability** (1 Week)
   - Different responses depending on event
   - Proper legal / investigative support
   - Draft investigative workflows (tabletop exercises)
3. **Oversight and Compliance** (1 Week)
   - "**Watch the watchers**"; outside core Insider Team
   - Reporting mechanisms and metrics
   - Feedback loops

Watching the Watchers

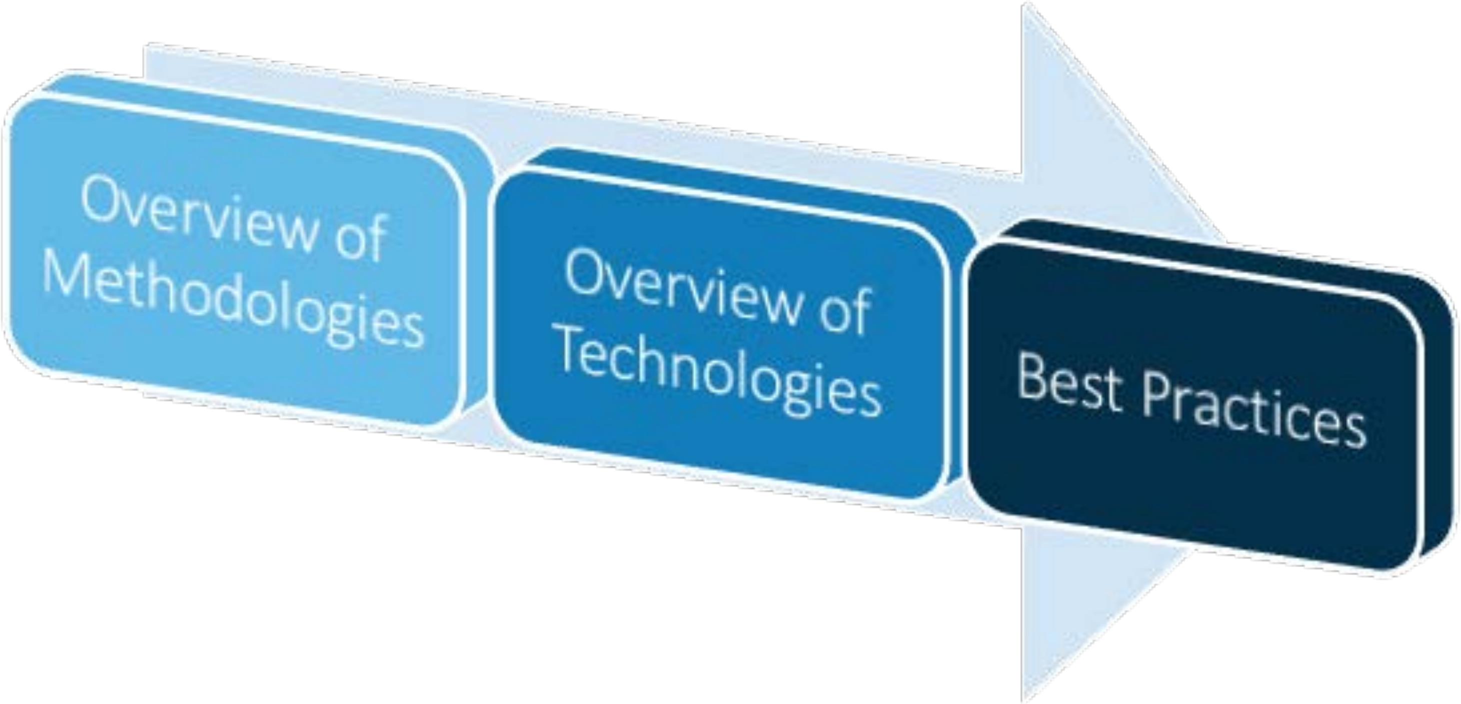
Who Should Build It?

- Could they be a threat?
- Core competency?
- Experience?
- Competing priorities?

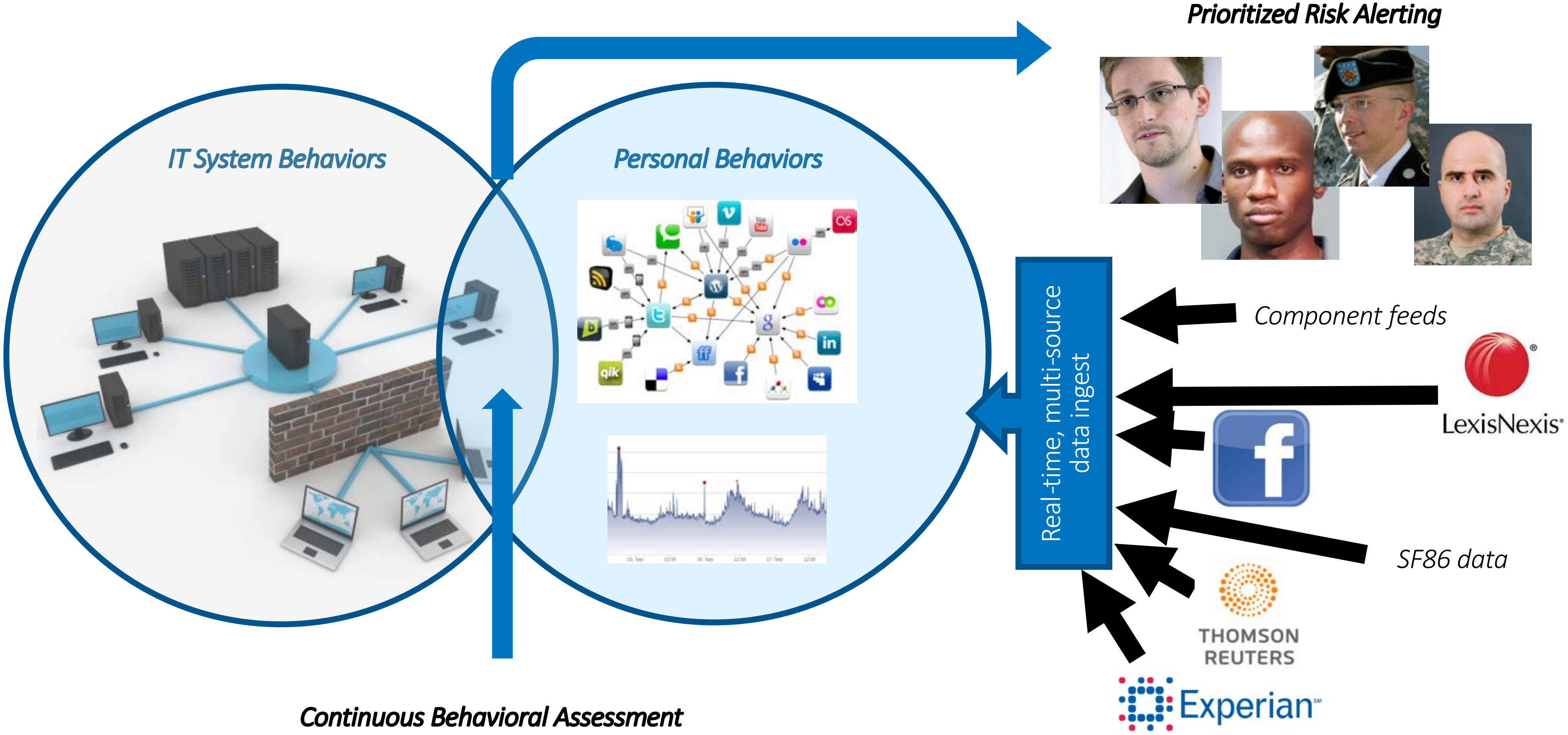
Where the Rubber Meets the Road

The Technical Implementation

Analytic Platforms, Hybrid Analytics and Best Practices



The Insider Threat Spectrum



Prioritized Risk Alerting

IT System Behaviors

Personal Behaviors

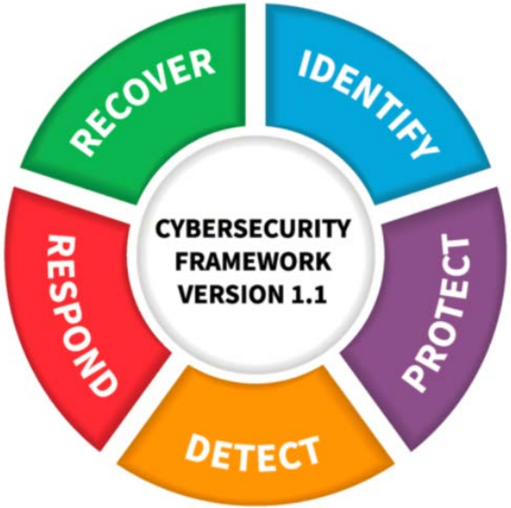
Real-time, multi-source data ingest

Component feeds

SF86 data

Continuous Behavioral Assessment

SAS Approach: NIST based CONOPS and SOAPA Architecture

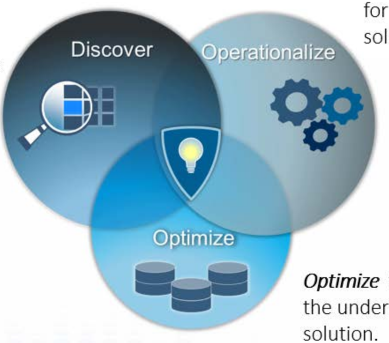


Credit: N. Hanacek/NIST

Security Intelligence Meta Life Cycle

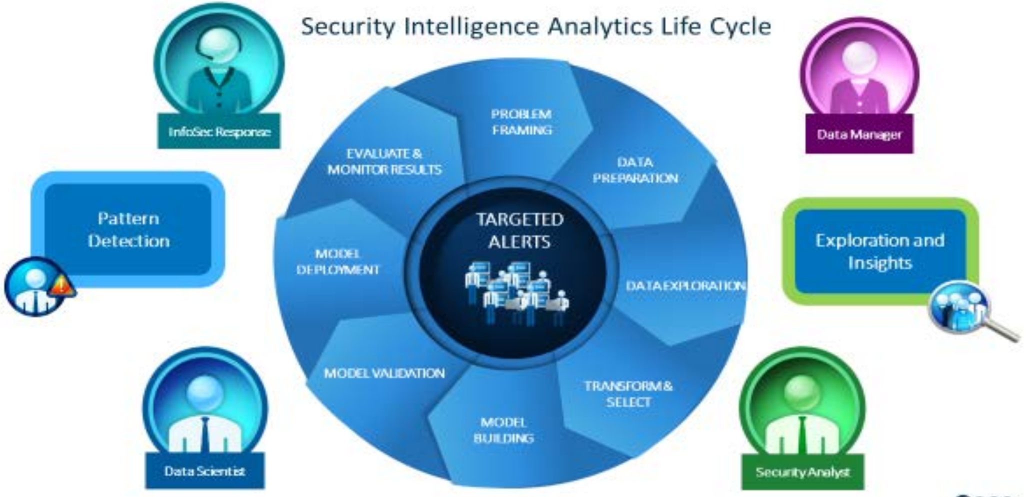
Concept of Operations (CONOPs) Framework

Discover events needing "targeting" and investigation using SAS and Open Source analytic tools and techniques

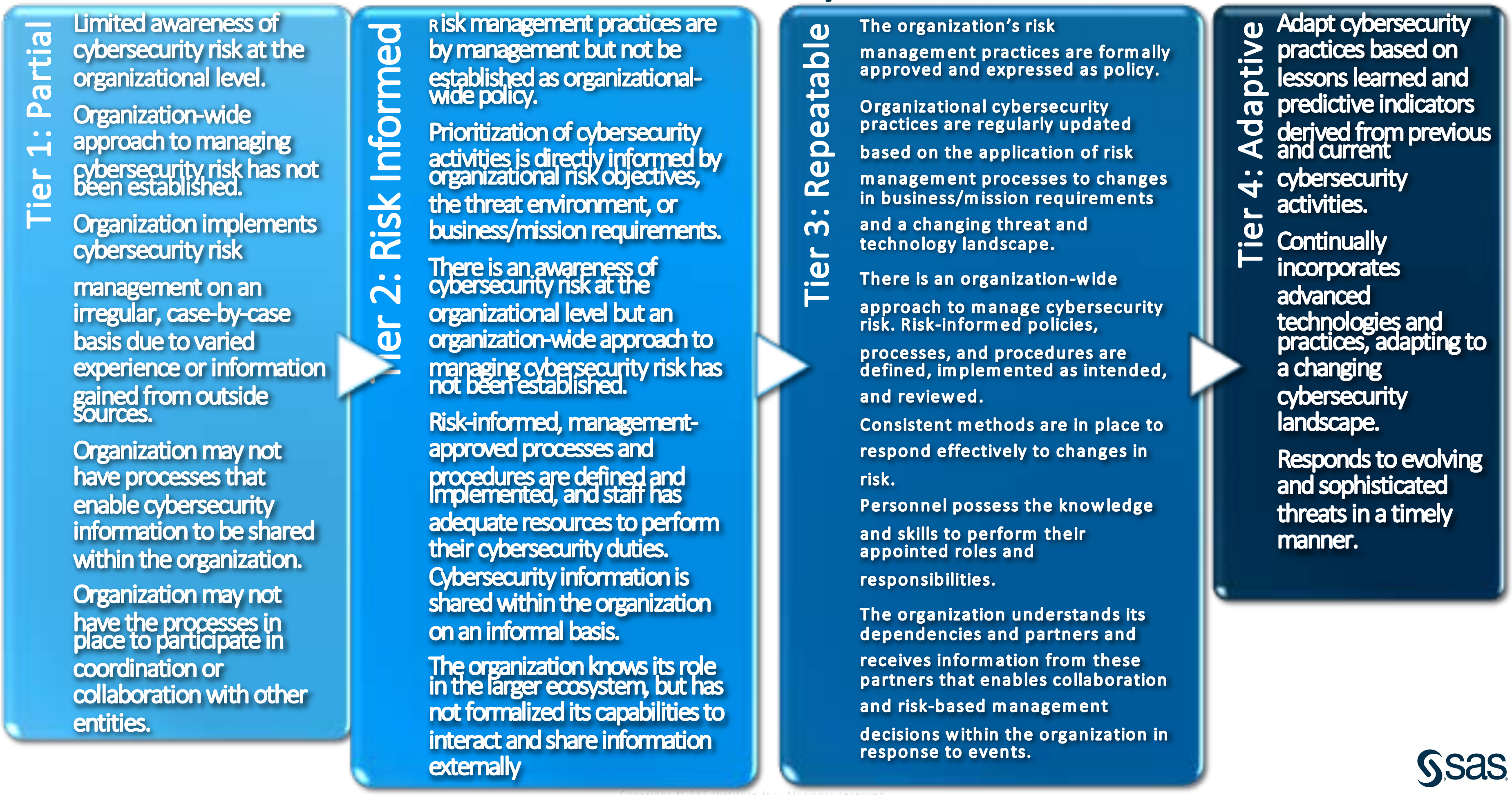


Operationalize the resultant discoveries for investigation/dispositioning using solution capabilities.

Optimize the process continuously using the underling data derived from the solution.



NIST Maturity Levels



Tier 1: Partial

- Limited awareness of cybersecurity risk at the organizational level.
- Organization-wide approach to managing cybersecurity risk has not been established.
- Organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources.
- Organization may not have processes that enable cybersecurity information to be shared within the organization.
- Organization may not have the processes in place to participate in coordination or collaboration with other entities.

Tier 2: Risk Informed

- Risk management practices are by management but not be established as organizational-wide policy.
- Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established.
- Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties.
- Cybersecurity information is shared within the organization on an informal basis.
- The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally

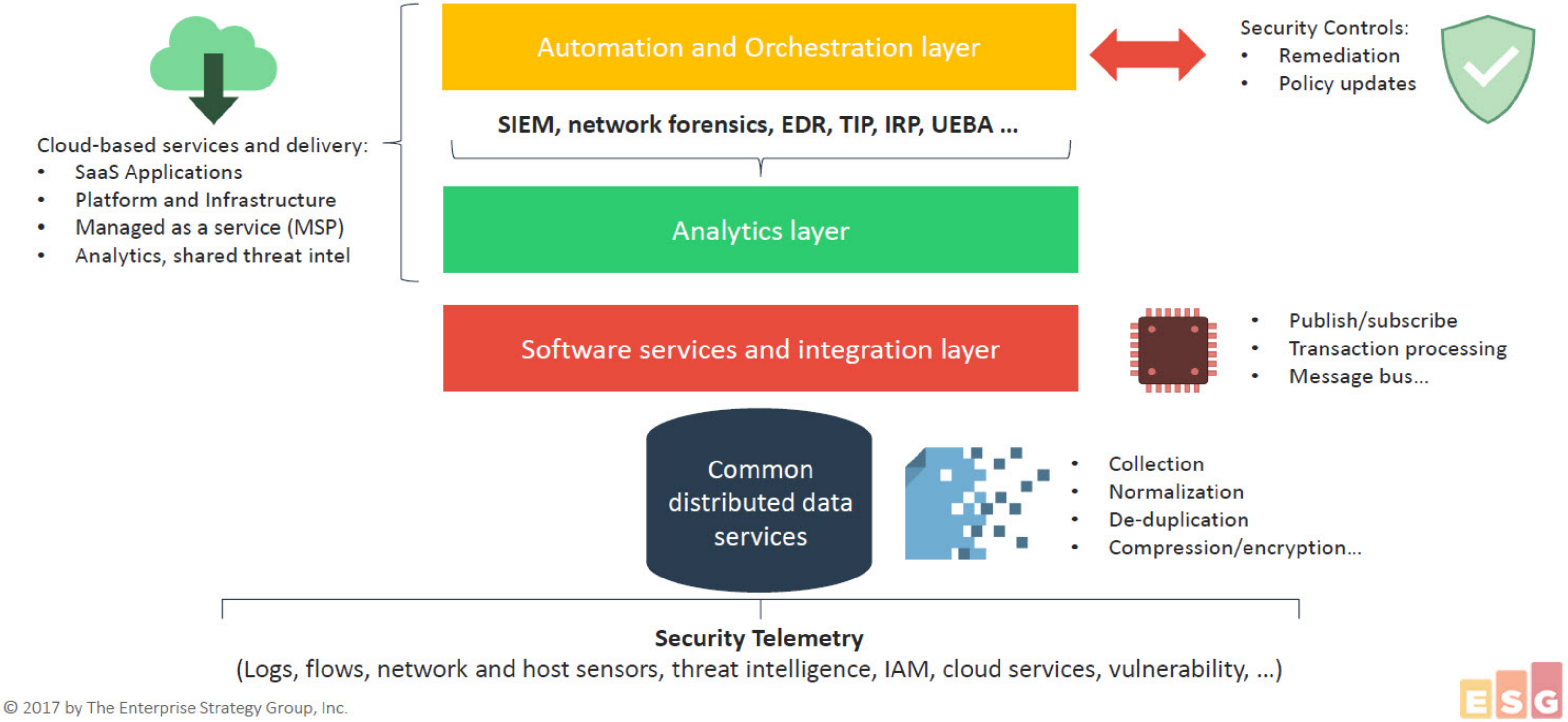
Tier 3: Repeatable

- The organization's risk management practices are formally approved and expressed as policy.
- Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.
- Consistent methods are in place to respond effectively to changes in risk.
- Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

Tier 4: Adaptive

- Adapt cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.
- Continually incorporates advanced technologies and practices, adapting to a changing cybersecurity landscape.
- Responds to evolving and sophisticated threats in a timely manner.

SOAPA: Security Operations and Analytics Platform Architecture



Cloud-based services and delivery:

- SaaS Applications
- Platform and Infrastructure
- Managed as a service (MSP)
- Analytics, shared threat intel

Automation and Orchestration layer

SIEM, network forensics, EDR, TIP, IRP, UEBA …

Analytics layer

Software services and integration layer

Common distributed data services

Security Controls:

- Remediation
- Policy updates

- Publish/subscribe
- Transaction processing
- Message bus…

- Collection
- Normalization
- De-duplication
- Compression/encryption…

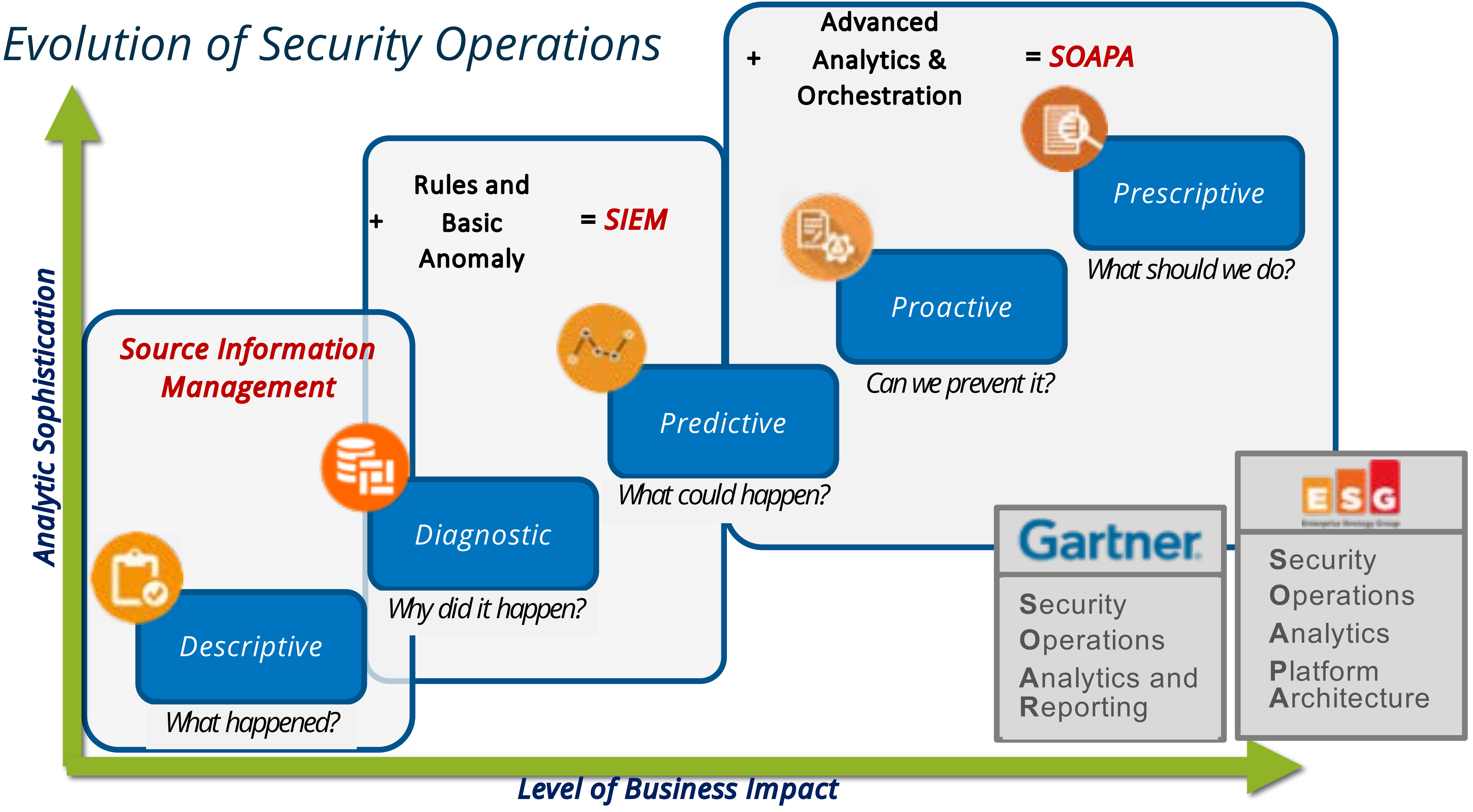
Security Telemetry

(Logs, flows, network and host sensors, threat intelligence, IAM, cloud services, vulnerability, …)

Oltsik,Jon, (2017, January 3) Security data growth drives SOAPA. CSO, p. Security Section

Aldorisio , Jeff, (2018, February 21) WHAT IS SECURITY OPERATIONS AND ANALYTICS PLATFORM ARCHITECTURE? A DEFINITION OF SOAPA, HOW IT WORKS, BENEFITS, AND MORE. Digital Guardian, p. Data Insider Blog

Evolution of Security Operations



Analytic Sophistication

Level of Business Impact

Source Information Management

Descriptive

What happened?

Diagnostic

Why did it happen?

+ Rules and Basic Anomaly = SIEM

Predictive

What could happen?

+ Advanced Analytics & Orchestration = SOAPA

Proactive

Can we prevent it?

Prescriptive

What should we do?

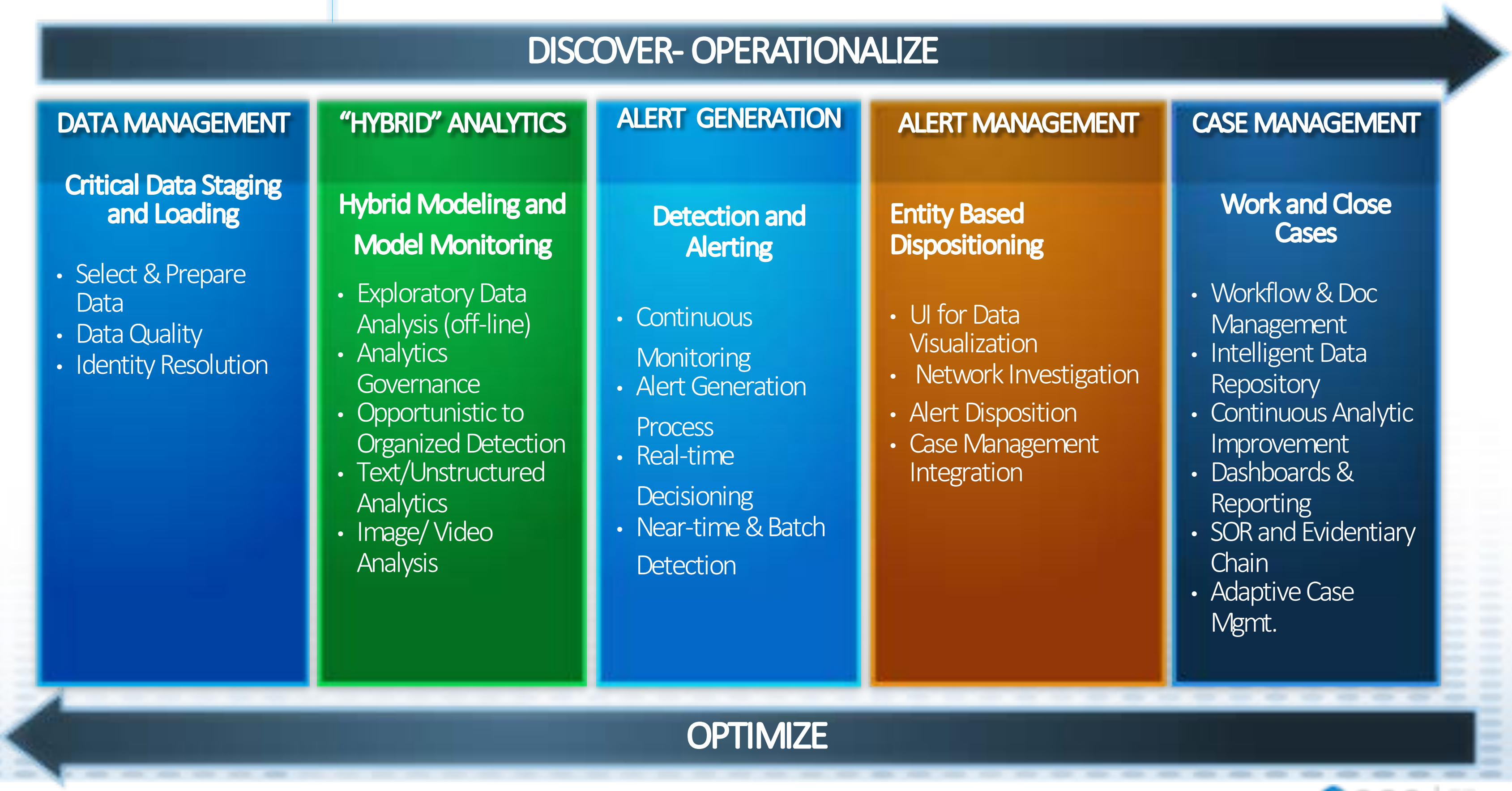
Gartner

Security Operations Analytics and Reporting

ESG

Security Operations Analytics Platform Architecture

Components of and Insider Threat Focused Analytics Platform



DISCOVER- OPERATIONALIZE

DATA MANAGEMENT

Critical Data Staging and Loading

- Select & Prepare Data
- Data Quality
- Identity Resolution

"HYBRID" ANALYTICS

Hybrid Modeling and Model Monitoring

- Exploratory Data Analysis (off-line)
- Analytics Governance
- Opportunistic to Organized Detection
- Text/Unstructured Analytics
- Image/ Video Analysis

ALERT GENERATION

Detection and Alerting

- Continuous Monitoring
- Alert Generation Process
- Real-time Decisioning
- Near-time & Batch Detection

ALERT MANAGEMENT

Entity Based Dispositioning

- UI for Data Visualization
- Network Investigation
- Alert Disposition
- Case Management Integration

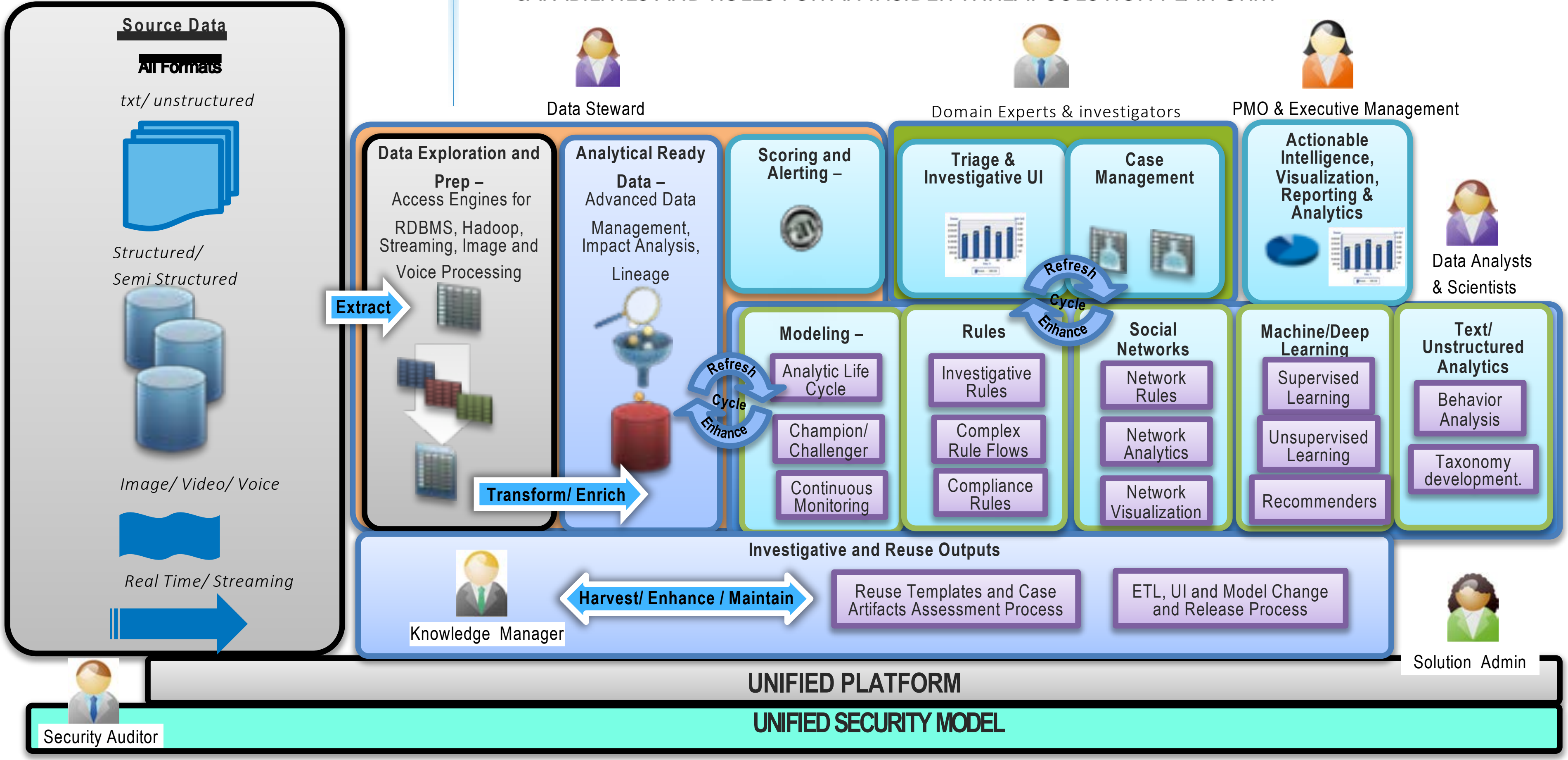
CASE MANAGEMENT

Work and Close Cases

- Workflow & Doc Management
- Intelligent Data Repository
- Continuous Analytic Improvement
- Dashboards & Reporting
- SOR and Evidentiary Chain
- Adaptive Case Mgmt.

OPTIMIZE

CAPABILITIES AND ROLES FOR AN INSIDER THREAT SOLUTION PLATFORM



Source Data

All Formats

txt/ unstructured

Structured/ Semi Structured

Image/ Video/ Voice

Real Time/ Streaming

Extract

Data Steward

Domain Experts & investigators

PMO & Executive Management

Data Exploration and Prep – Access Engines for RDBMS, Hadoop, Streaming, Image and Voice Processing

Analytical Ready Data – Advanced Data Management, Impact Analysis, Lineage

Scoring and Alerting –

Triage & Investigative UI

Case Management

Actionable Intelligence, Visualization, Reporting & Analytics

Data Analysts & Scientists

Refresh Cycle Enhance

Transform/ Enrich

Modeling –

- Analytic Life Cycle
- Champion/ Challenger
- Continuous Monitoring

Rules

- Investigative Rules
- Complex Rule Flows
- Compliance Rules

Social Networks

- Network Rules
- Network Analytics
- Network Visualization

Machine/Deep Learning

- Supervised Learning
- Unsupervised Learning
- Recommenders

Text/ Unstructured Analytics

- Behavior Analysis
- Taxonomy development.

Investigative and Reuse Outputs

Knowledge Manager

Harvest/ Enhance / Maintain

Reuse Templates and Case Artifacts Assessment Process

ETL, UI and Model Change and Release Process

Solution Admin

UNIFIED PLATFORM

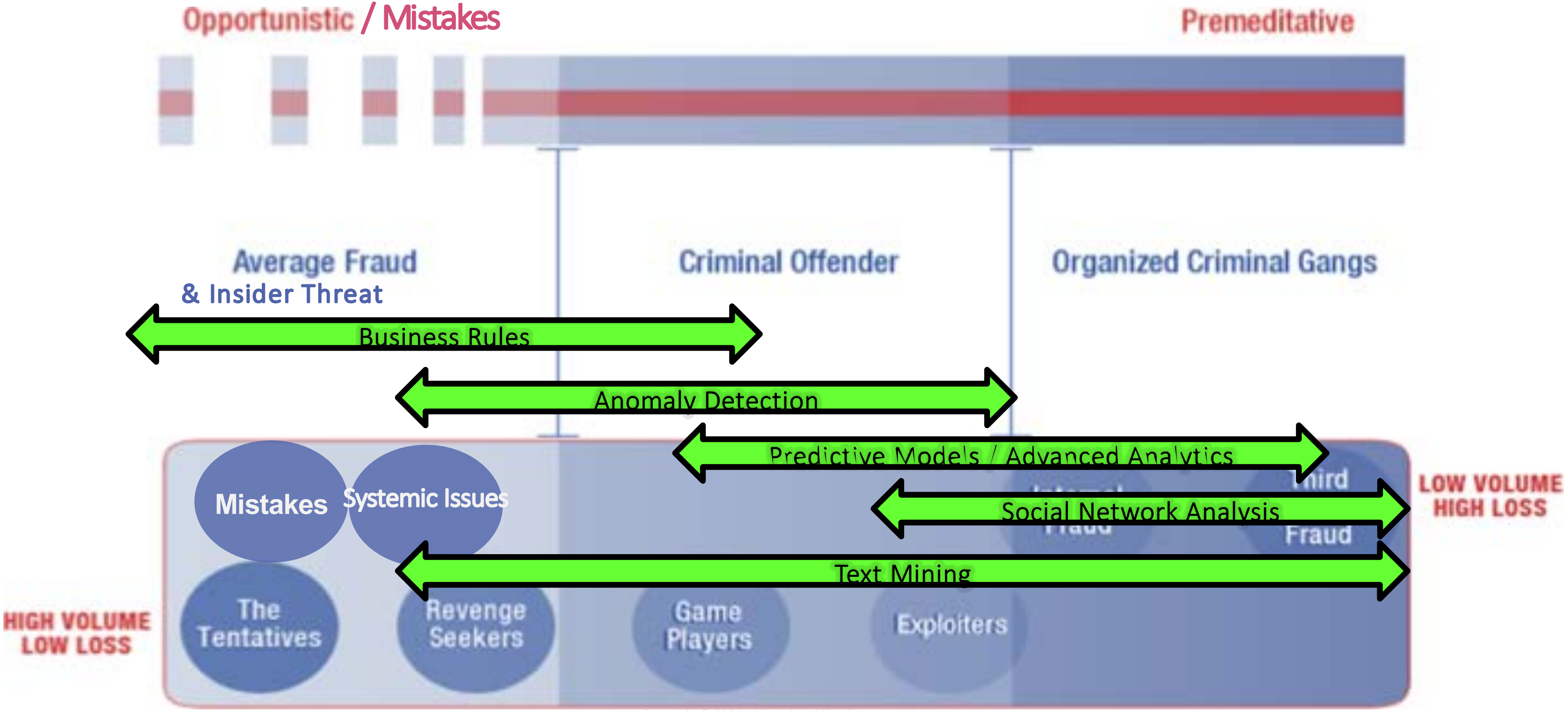
Security Auditor

UNIFIED SECURITY MODEL

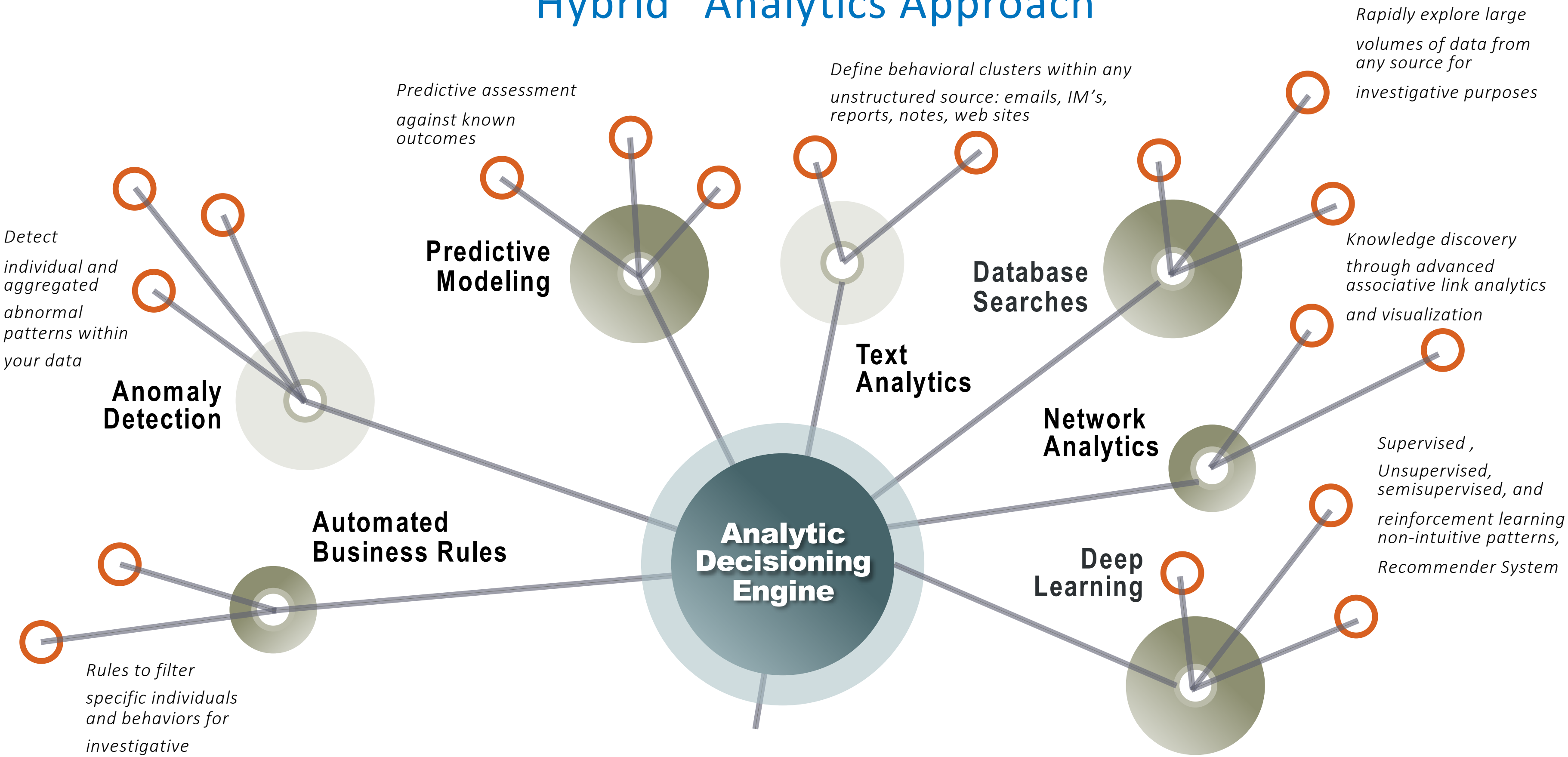
sas

Spectrum of Insider Threat

Hybrid Analytic Detection Methodology



“Hybrid” Analytics Approach



Analytic Decisioning Engine

Anomaly Detection

Detect individual and aggregated abnormal patterns within your data

Predictive Modeling

Predictive assessment against known outcomes

Text Analytics

Define behavioral clusters within any unstructured source: emails, IM’s, reports, notes, web sites

Database Searches

Rapidly explore large volumes of data from any source for investigative purposes

Network Analytics

Knowledge discovery through advanced associative link analytics and visualization

Deep Learning

Supervised , Unsupervised, semisupervised, and reinforcement learning non-intuitive patterns, Recommender System

Automated Business Rules

Rules to filter specific individuals and behaviors for investigative criteria

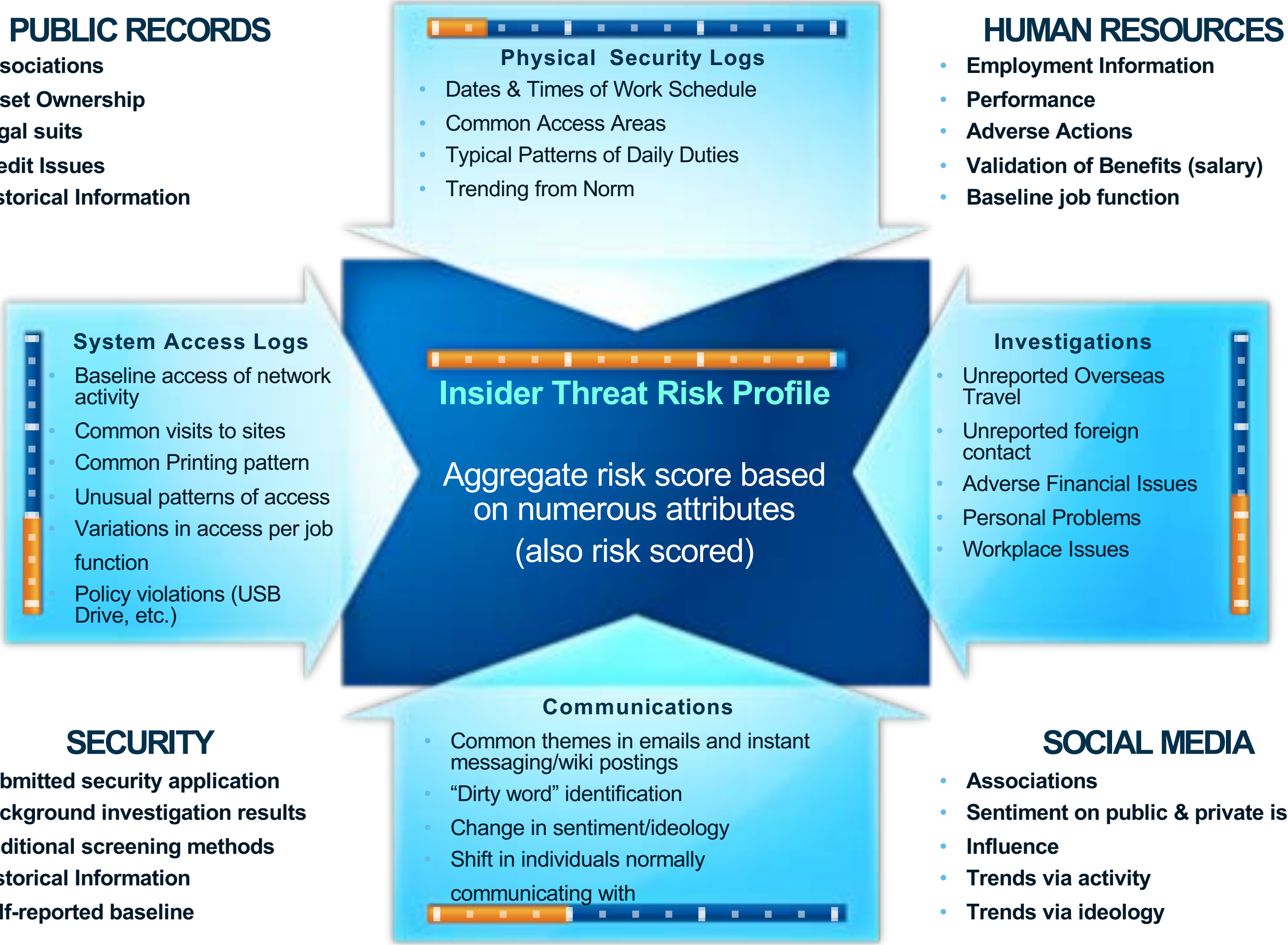
LEVERAGING NUMEROUS ADVANCED ANALYTICS TECHNIQUES

PUBLIC RECORDS

- Associations
- Asset Ownership
- Legal suits
- Credit Issues
- Historical Information

HUMAN RESOURCES

- Employment Information
- Performance
- Adverse Actions
- Validation of Benefits (salary)
- Baseline job function



Physical Security Logs

- Dates & Times of Work Schedule
- Common Access Areas
- Typical Patterns of Daily Duties
- Trending from Norm

System Access Logs

- Baseline access of network activity
- Common visits to sites
- Common Printing pattern
- Unusual patterns of access
- Variations in access per job function
- Policy violations (USB Drive, etc.)

Insider Threat Risk Profile

Aggregate risk score based on numerous attributes

(also risk scored)

Investigations

- Unreported Overseas Travel
- Unreported foreign contact
- Adverse Financial Issues
- Personal Problems
- Workplace Issues

Communications

- Common themes in emails and instant messaging/wiki postings
- “Dirty word” identification
- Change in sentiment/ideology
- Shift in individuals normally communicating with

SECURITY

- Submitted security application
- Background investigation results
- Additional screening methods
- Historical Information
- Self-reported baseline

SOCIAL MEDIA

- Associations
- Sentiment on public & private issues
- Influence
- Trends via activity
- Trends via ideology

Analytics Platform for Insider Threat

Without a robust platform effective threat response is hindered

Analytics Platform*: An analytics platform is a unified and proper solution designed to address the demands of users, especially large data-driven companies, on the inadequacy of relational database management systems (RDBMS) in providing contextual analyzed data out of all the stored information.

*Techopedia https://www.techopedia.com/definition/29493/analytics-platform

Types of Analytics Platforms *:

Everyone Says they have a Platform

- **Code Based** (Primarily Open Source) – Platform is Custom Coded
- **Application Based** (Open Source, Commercial and Combination thereof) – Platform is custom coded and integrated with one or more applications (COTS and/or Open Source) typically using a custom coded SOA methods
- **Solution Based** - (Primarily Commercial) –Platform is COTS and maintained and supported by a vendor. Integration API's are provided for Open Source and third party applications.

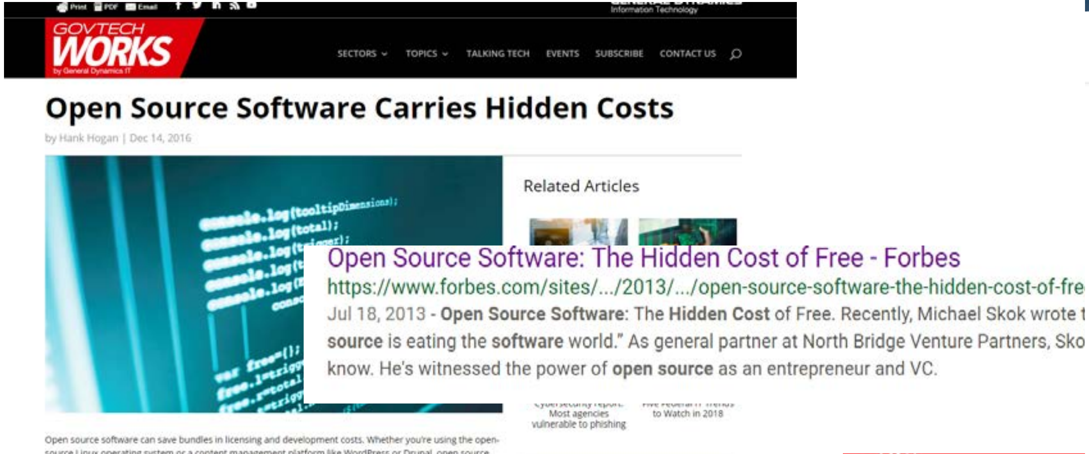
*Techopedia https://www.techopedia.com/definition/29493/analytics-platform

Qualitative Benefit Matrix of Analytic Platform Types

Platform	COTS	Application	Code
Development Effort	Small	Moderate	High
Maintenance Effort	Small/Moderate	Moderate	High
Auditability Effort	Low/Moderate	Moderate	High
Integration Costs	Low	High	High
Liability	Low	Moderate	High
Software License Cost	Yes	Yes and/or No	Yes and/or No
Data Management Effort	Low	Moderate	High
Flexibility	Moderate	Moderate/High	High
Latest Technologies	Low/Moderate	Moderate/High	High

What is the right approach?

Many Opinions on the topic


Print PDF Email
GOVTECH WORKS by General Dynamics IT
Information Technology
SECTORS TOPICS TALKING TECH EVENTS SUBSCRIBE CONTACT US

Open Source Software Carries Hidden Costs

by Hank Hogan | Dec 14, 2016

Related Articles

Most agencies vulnerable to phishing

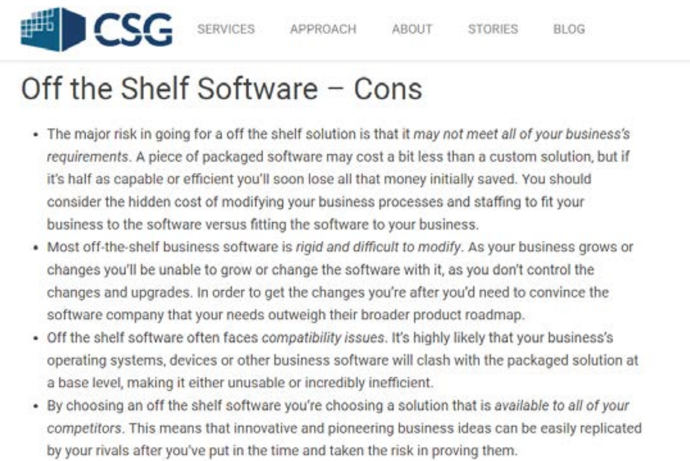
to Watch in 2018

Open source software can save bundles in licensing and development costs. Whether you're using the open-source Linux operating system or a content management platform like WordPress or Drupal, open source

Open Source Software: The Hidden Cost of Free - Forbes

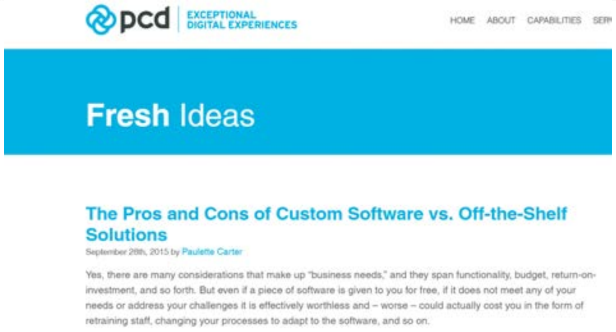
https://www.forbes.com/sites/.../2013/.../open-source-software-the-hidden-cost-of-fre

Jul 18, 2013 - **Open Source Software:** The **Hidden Cost** of Free. Recently, Michael Skok wrote t **source** is eating the **software** world." As general partner at North Bridge Venture Partners, Sko know. He's witnessed the power of **open source** as an entrepreneur and VC.



Off the Shelf Software – Cons

- The major risk in going for a off the shelf solution is that it *may not meet all of your business's requirements*. A piece of packaged software may cost a bit less than a custom solution, but if it's half as capable or efficient you'll soon lose all that money initially saved. You should consider the hidden cost of modifying your business processes and staffing to fit your business to the software versus fitting the software to your business.
- Most off-the-shelf business software is *rigid and difficult to modify*. As your business grows or changes you'll be unable to grow or change the software with it, as you don't control the changes and upgrades. In order to get the changes you're after you'd need to convince the software company that your needs outweigh their broader product roadmap.
- Off the shelf software often faces *compatibility issues*. It's highly likely that your business's operating systems, devices or other business software will clash with the packaged solution at a base level, making it either unusable or incredibly inefficient.
- By choosing an off the shelf software you're choosing a solution that is *available to all of your competitors*. This means that innovative and pioneering business ideas can be easily replicated by your rivals after you've put in the time and taken the risk in proving them.


pcd EXCEPTIONAL DIGITAL EXPERIENCES
HOME ABOUT CAPABILITIES SER
Fresh Ideas

The Pros and Cons of Custom Software vs. Off-the-Shelf Solutions

September 28th, 2015 by Paulette Carter

Yes, there are many considerations that make up "business needs," and they span functionality, budget, return-on-investment, and so forth. But even if a piece of software is given to you for free, if it does not meet any of your needs or address your challenges it is effectively worthless and – worse – could actually cost you in the form of retraining staff, changing your processes to adapt to the software, and so on.

BEST-FIT ENTERPRISE SOFTWARE

By Chris Doig, Advisor, CIO | NOV 19, 2015 5:30 AM PT

Opinions expressed by ICN authors are their own.

OPINION

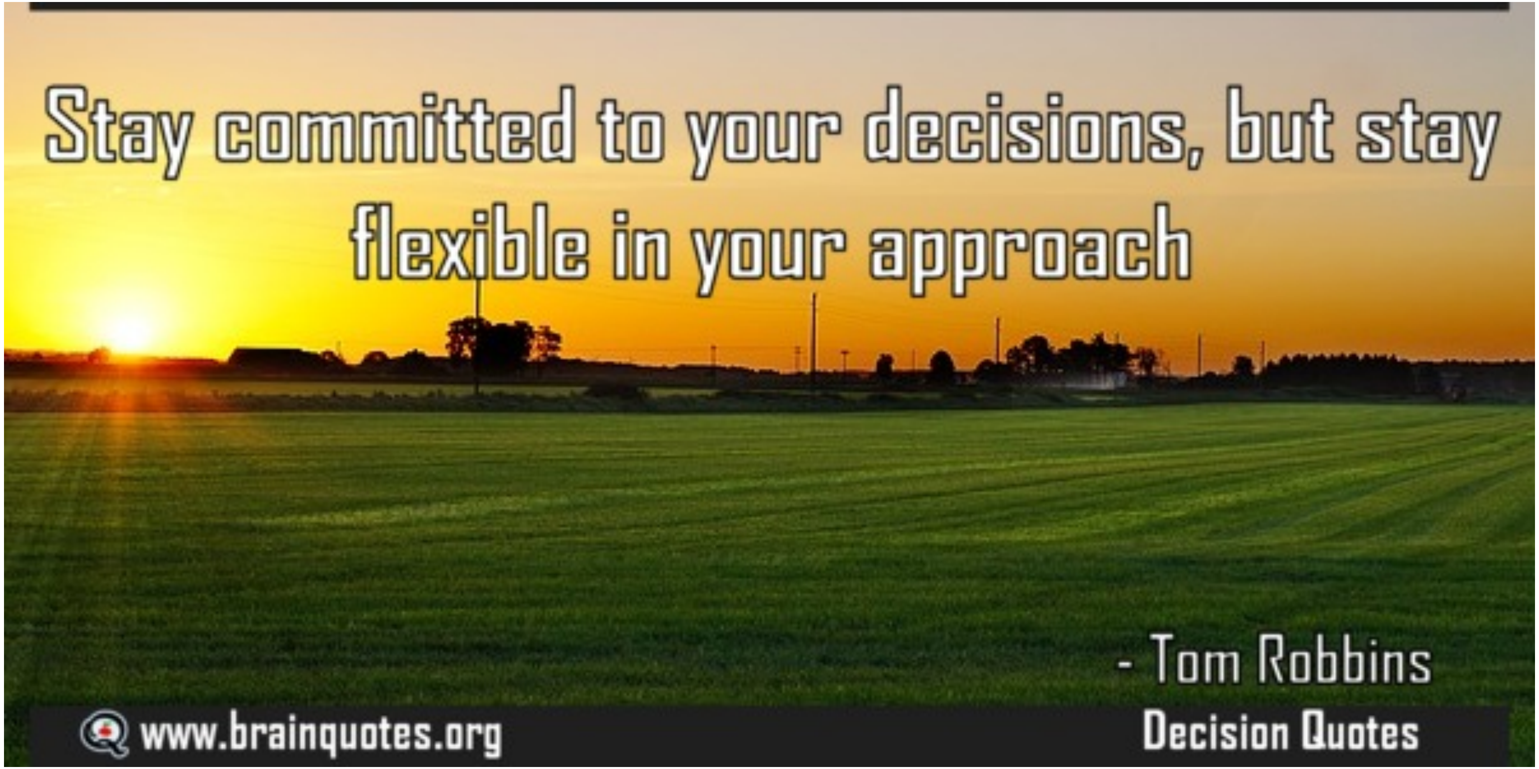
Calculating the total cost of ownership for enterprise software

The TCO is a vital part of the ROI calculation for enterprise software, yet too often it is ignored or underestimated. See what should be in the TCO estimate, and use that to make better software selection decisions based on the ROI.

Some Thoughts on Deciding on a Platform

Look at all options in relation to your Agency’s unique needs

- Do you have an existing Insider Threat Group?
  - If So, what are their skill sets?
  - What is the budget of you Agency for combating Insider Threat?
- Do you have an executive mandate, priorities and timeline for Insider Threat?
- What is your agency risk profile for Insider Threat?
- What are your Agency skill sets in relation to a Insider Threat Implementation (Analytics, Application/ System Development, Business Process Analysis) ?
- What is the current maturity of your IT Group or Agency in new Technologies especially using Big Data and Analytics?
- Create a “Criteria for Success” Document and evaluate platform approaches to the definition you create.
- Consider leveraging a combination of COTS and Open Source levering the strengths of both.
- Ensure the Platform has robust Data Management and Data Cleansing Capabilities.
- What are your organizations security and audit requirements?


Stay committed to your decisions, but stay flexible in your approach
- Tom Robbins
www.brainquotes.org
Decision Quotes

A Hybrid Analytical Approach

4 essential Capabilities for Combatting Insider Threat

- **A holistic, behavior-based view of "normal,"** to more accurately detect suspicious behavior .

- **Cross-channel visibility**, to detect complex patterns of behavior that may involve multiple layers across channels, products and accounts .

- **Alert management of Threat events**, to automate decisions and score risk before the investigation process .

- **Integration with workforce, anti-fraud and cyber sytems,** to improve efficiency and effectiveness in fighting Insider Threat while reducing the cost and effort .

Hybrid Detection in Detail

True detection relies on understanding behavior in broader context, as well as being able to detect new patterns . Analytics is required to properly group customers and accounts that should behave **similarly** . A hybrid approach supplements rules by applying multiple flavors of analytics, such as:

- Predictive modeling. Neural networks, decision trees, generalized linear models, econometric models and gradient boosting can unearth new cases and patterns based on the previous disposition of alerts and cases .
- Text Analytics. Extract meaningful information from vast stores of unstructured (text) data, such as reports, staff notes, social media and websites .
- Anomaly detection. Techniques such as mean, standard deviation, percentiles, univariate and multivariate regression, clustering, sequence analysis and peer group analysis can be applied to identify abnormal patterns in the data .

- Automated business rules. Transactions can be filtered on sophisticated rules that reflect behavioral patterns/factors associated with suspicious behavior . For example, automated rules could flag transactions made by the same employee in multiple time zones in a short period of time .
- Database searches. Supplement detection and investigation processes with data from internal and external sources, such as from Lexis Nexis, CIS, DowJones, Websearch, Dunn/Bradstreet and OFAC .
- Entity Based network analysis. Identify links between people, businesses, documents, devices or transactions that could reveal organized crime activities

Real World Examples of Platform Analytics Benefits

Government Customer Examples

- **Reduction of False Positives**
  - Reduction of approximately 32% investigative cases using advanced text analytics applied to case notes for reducing false positives. This was quickly achieved within the first 6 months of production roll out.
- **Data Quality Issues**
  - Estimate to correct source data quality issues for alert generation using existing agency coding methods 2 months
  - Use of existing COTS Data cleansing algorithm 2 Days
- **Federal Information Security Management Act (FISMA) Audit Requirements**
  - Need to interface with a legacy agency mainframe authorization service for User Access Validation and Audit
  - Because of existing COTS metadata structure for user, roles and groups across all system applications (Data Management, Hybrid Analytics, Alert Generation, Alert Management, Case Management) implementation was completed on time with single developer with a minimum of complexity.
- **Implementation of an Agile Dev Opps Environment**
  - Initial requirements were need to be adapted quickly to the reality of the production environment it terms of UI and workflow.
  - Allows end users and developers to quickly collaborate and deliver fully validated critical solution enhancements into production every 3 weeks using Agile Sprints. Enhancements included UI's adapted for the investigators as they determine better approaches, more efficient workflow processes to investigate and close cases, summary and detailed status reports for management and better alerting models for case generation.
- **Improved Investigative efficiency**
  - Automated checks have resulted in a saving of 400 staff years across operational teams
- **Consolidated Risk Profile for all employees**
  - Created a consolidate insider threat risk profiles by individual in a complicated organization with a global footprint and approximately 30,000 employees and contractor staff.

To the Next Level

New and Growing Technologies

- AI Augmentation - The Limits of Human Cognition
  - Augment the Investigator
  - Augment the System
  - Non-Intuitive Associations
- Bio Metrics
- From Passive to Active Approaches
  - Analytic Designed Honey Pots
  - Workforce Analytics – Remove the evolving threat
  - Appling Triggers and Measuring responses
- Virtual Reality
  - Streaming Data
  - Immersive Data Environment
  - Team Collaboration

Key Take Aways

1. Don’t let perfection get in the way of good.
2. Begin your 100 day plan on Thursday.
3. Work with the resources you have – prioritize, start small and grow over time.
4. Lean into organizations who have done this before for strategic guidance and enablement.
5. Involve your stakeholders (employees, unions, legal, etc).
6. Move the needle. Leave a legacy.

sas.com