RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: HUM-T10

TURNING YOUR SECURITY STRATEGY INSIDE OUT – MANAGING INSIDER THREAT

James Christiansen

Chief Information Security Officer (CISO)
Teradata

TERADATA

Gary Harbison

Chief Information Security Officer (CISO)
Monsanto Information Security Office

MONSANTO

The Perfect Storm

Business Performance

Threat and Attack Sophistication

Churn of Infrastructure

Limited Resources

Regulations and Compliance

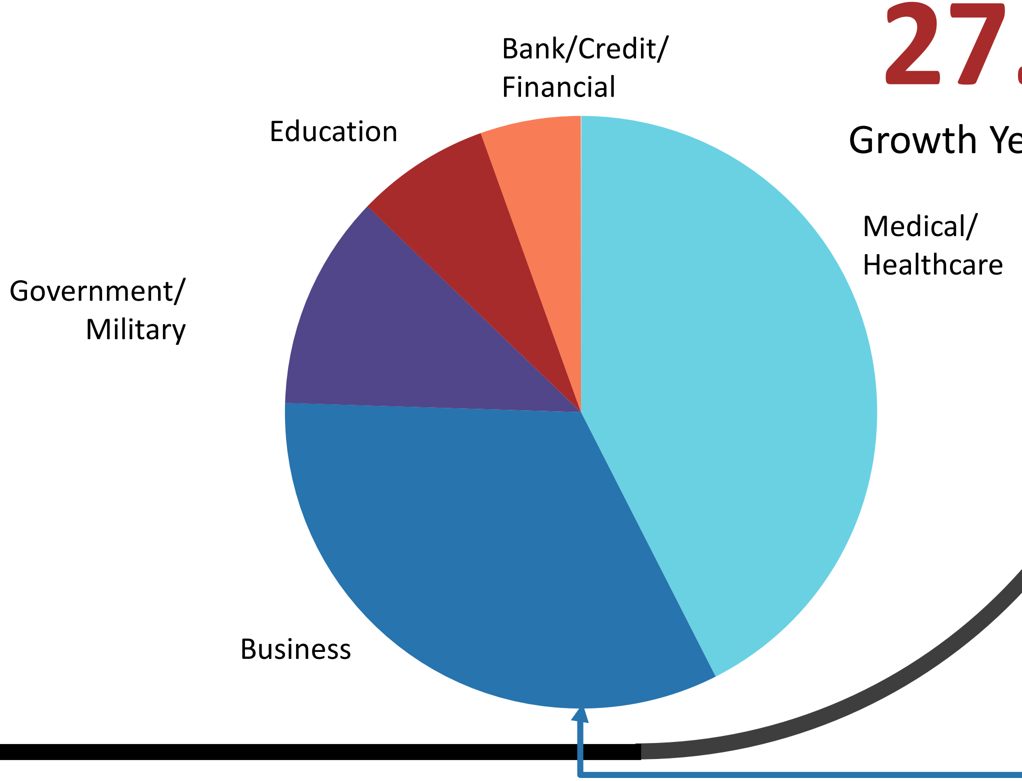
Massive Volumes of Data

Transformation of Access and Endpoint

Data Access vs. Security

Bad and Getting Worse

#RSAC



27.5%

Growth Year over Year

52.5%

Security Incidents attributed to Insider Threat*

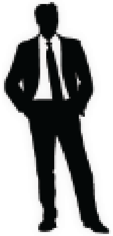
783

Identified and Reported Breaches

Source: Identity Theft Resource Center * Infosec Magazine

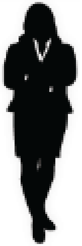
Every Company will be a Technology Company

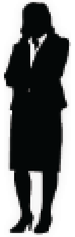
Malicious Insiders



Disgruntled Quitter Saboteur

“Huge fight with boss; quit and deployed a time bomb that corrupted our HR system and inserted randomly false transactions in a client back-end system”





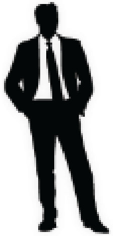
Entitled Individual Client PII Thief

Recruited out and took everything with her – client lists, structured product ideas, internal working documents – everything she’d ever been a part of.”

Planted Insider State Sponsored / Organized Crime

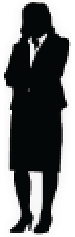
A contract resource is brought into develop a sensitive program. “Spent the next two years passing information to one of our competitors.”

Non-Malicious Insiders



Inadvertent Insider

Needed to get personnel information to insurance provider. Sent email with entire company personnel information. “I didn’t know anyone would see it!”

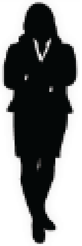


M&A Leader Sensitive Information

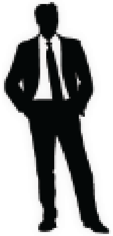
Working on the details of a significant acquisition. “Fat fingered” the email address. “Can I recall the email?”

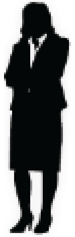
Executive Leader Wrong distribution

While discussing a sensitive management issue the executive sends information to the wrong distribution list. Causing extreme reputation damage “Why do we have distribution lists?”



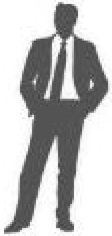
Outside In

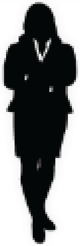




External Attacker Masquerades as Insider

Advanced Persistent Threat: In the typical APT attack once the attacker has successfully gained access to the systems (often through phishing attack) they escalate privileges to gain administrative rights and then go lateral through the system. Best – Disguise traffic as normal.





Insider Threat – More Difficult Than Others

- Already Bypassed Primary Controls
  - The insider has physical and logical access
  - They understand internal processes and "lingo"
- Hard to Distinguish Right from Wrong
  - Are they accessing the information as part of their normal work or malicious?
- Able to Cover Their Actions
  - The insider knows the detection controls and can often cover up what they have been doing
- Requires Maturity in Data Governance and Access Control

Insider Threat – More Difficult Than Others

- Can go Undetected for Years
  - Because insider knows internal processes and controls they can more easily advert detection
  - Insider breaches are often more expensive – go longer undetected and precise in their attack
- Hard to Convict
  - Need a solid case to get law enforcement Interested
  - Unless required by law it is often not in the best interest of the company
  - The insider can say “oops” my mistake

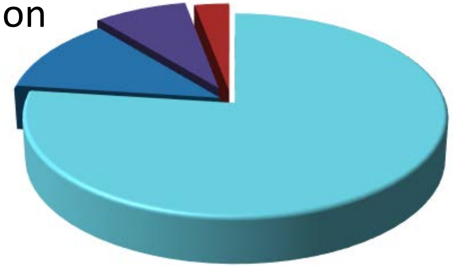
How Insiders are Handled (Unregulated Data)

How are insiders handled?

- The far majority of the time they are dismissed without legal or law enforcement action
- Civil action is taken to recover losses
- Law enforcement notified
- Law enforcement and legal action
- Emerging laws are enabling increased protection

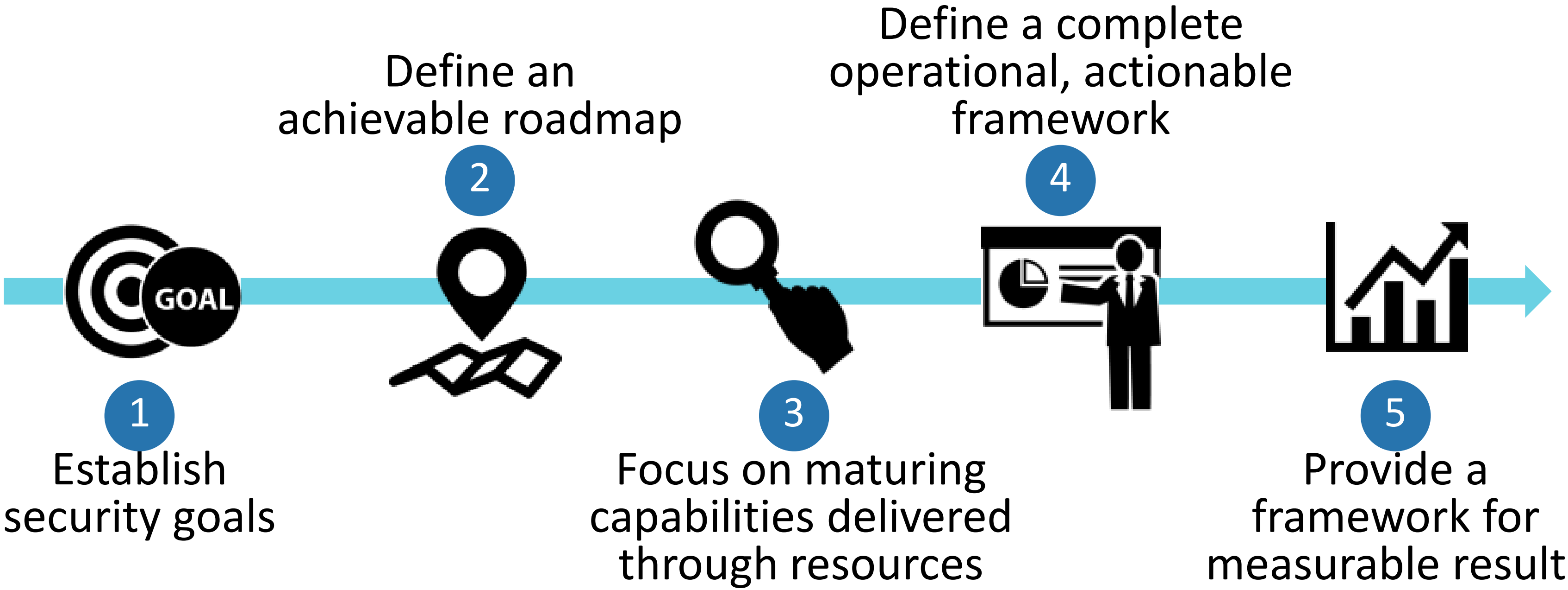
Leading reasons not reported to law enforcement

- Damage level insufficient to warrant prosecution
- Lack of evidence to prosecute
- Concerns about negative publicity
- Concerns about liability
- Concerns competitors will use incident to their advantage



Insider Threat – Program Solution

Five Goals of the Insider Threat Program



1 Establish security goals

2 Define an achievable roadmap

3 Focus on maturing capabilities delivered through resources

4 Define a complete operational, actionable framework

5 Provide a framework for measurable results

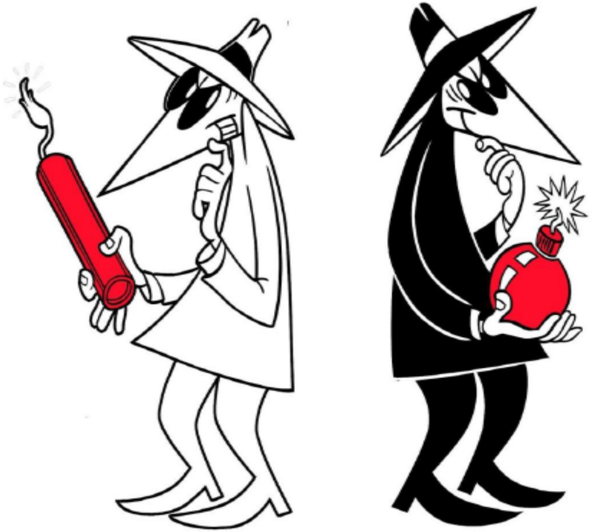
Phase I – Establishing Insider Threat Program

- Executive sponsorship
  - Educate the executive staff on the importance of an insider threat program.
  - Ensure there is sponsorship and governance of the program at the Executive Team Level
- Establish a set of strong policies and processes
  - Hiring policies and background checks
  - Consistent training and awareness. Repeatable processes can help take the emotion out of the process and ensure decision making is streamlined and consistent
- Factor in privacy requirements
- Consider other groups across the company
  - Legal, Human Resources, Physical silo your approach
  - Create a cross functional steering team and investigations team to ensure a holistic approach

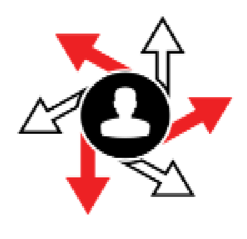
Know Your Enemy

- Who would be targeting your organization?
- Who would they target in your organization?
- Who are the high risk individuals in your organizations?
- What high-value assets would they go after?

Tip: Never underestimate the power of human intuition in detection of an insider threat



Insider Threat Modeling [1]



TURNING POINT

Technology:
- Security Intelligence

RECON

Technology:
- Security Intelligence

Technology:
- Behavioral Analysis

Process:
- Rights Management

Process:
- On/Off Boarding

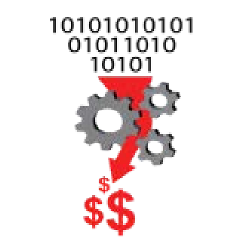
PACKING

Technology:
- DLP

Technology:
- Behavioral Analysis

Process:
- Incident Response

Process:
- Forensics



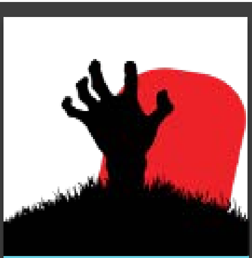
DATA THEFT

Technology:
- DLP

Technology:
- Behavioral Analysis

Process:
- Incident Response

Process:
- Forensics



RESURRECTION

Process:
- Incident Response

Process:
- Forensics

[1] Source: James Robinson, Optiv Security

Insider Threat Capabilities Maturity Model [1]

Base Capabilities

- Have ownership and support for program
- Have resource(s) that can run the program
- Have resource(s) that can perform analysis and investigations
- Be able to determine critical data
- Be able to determine users that have access to critical data
- Be able to proactively identify how insiders will attack.

Level 1 Capabilities

- Have a program steering committee for directions and updates
- Have a policy
- Execute an education and communication plan for organization
- Have a source of leads (internal)
- Have tooling to support base response capabilities
- Have internal incident response process

Level 2 Capacities

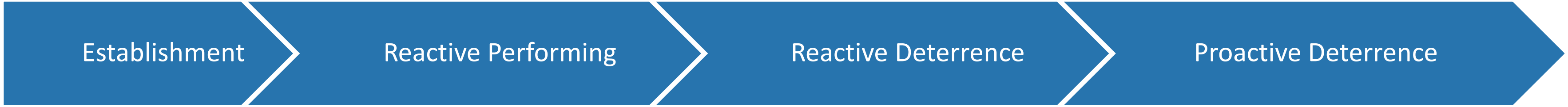
- Evaluation of program for additional capabilities and tooling
- Have external IR flows (legal council, law enforcement engagement, Public Relations)
- Track training delivery to org.
- Be able to identify users in higher risk situations
- Test incident response process and update

Level 3 Capabilities

- Have training for higher risk personnel (briefing and debriefing)
- Be able to get leads from external sources
- Have contractual obligations for 3rd parties
- Include insider threat modifications for mergers and acquisitions
- Be able to track trends of incidents and attacks

Level 4 Capabilities

- Optimize and adjust program based on trends
- Have 3rd parties participate in intelligence, response, and other program activities
- Provide business intelligence



Establishment

Reactive Performing

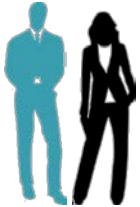
Reactive Deterrence

Proactive Deterrence

[1] Source: James Robinson, Optiv Security

Calculating the Insider Risk [1]

The average job tenure is 4.4 years [2] which means for a 1000 person company 227 will leave each year (23%)



Of those people leave 14% [3] or **32 per year** say they will take your data.

Risk Based Approach

- Define the number of critical assets
- Factor in the number of employees that have access to the assets
- For example if there are ten critical assets and 10% of staff members have access results in 23 staff per year leave and 14% taking your critical assets (3) would result in **30 critical assets per year** taken

((((Turnover rate * # of staff) * % with access) * % that will take data) # of critical assets) = Critical assets taken per year

[] edition.cnn.com/2012/08/07/business/stealing-information-work/

[3] forbes.com/sites/jeannemeister/2012/08/14/job-hopping-is-the-new-normal-for-millennials-three-ways-to-prevent-a-human-resource-nightmare/

2

[1] Source: James Robinson, Optiv Security

Insider Threat Focus Areas

- Privileged Users
  - Malicious and non-malicious threat. They are in a trusted role and can misuse their access and are targets for credential attacks
- Third Parties
  - Outsourcers, contractors, third-party vendors, maintenance vendors and partners have access to your systems and your staff
- Terminated and Departing Employees
  - Employees can take data with them when terminated. May plant malware, time bombs or backdoors
- Employees Facing Uncertainty
  - During an acquisition or restructuring employees facing uncertainty are more vulnerable to manipulation

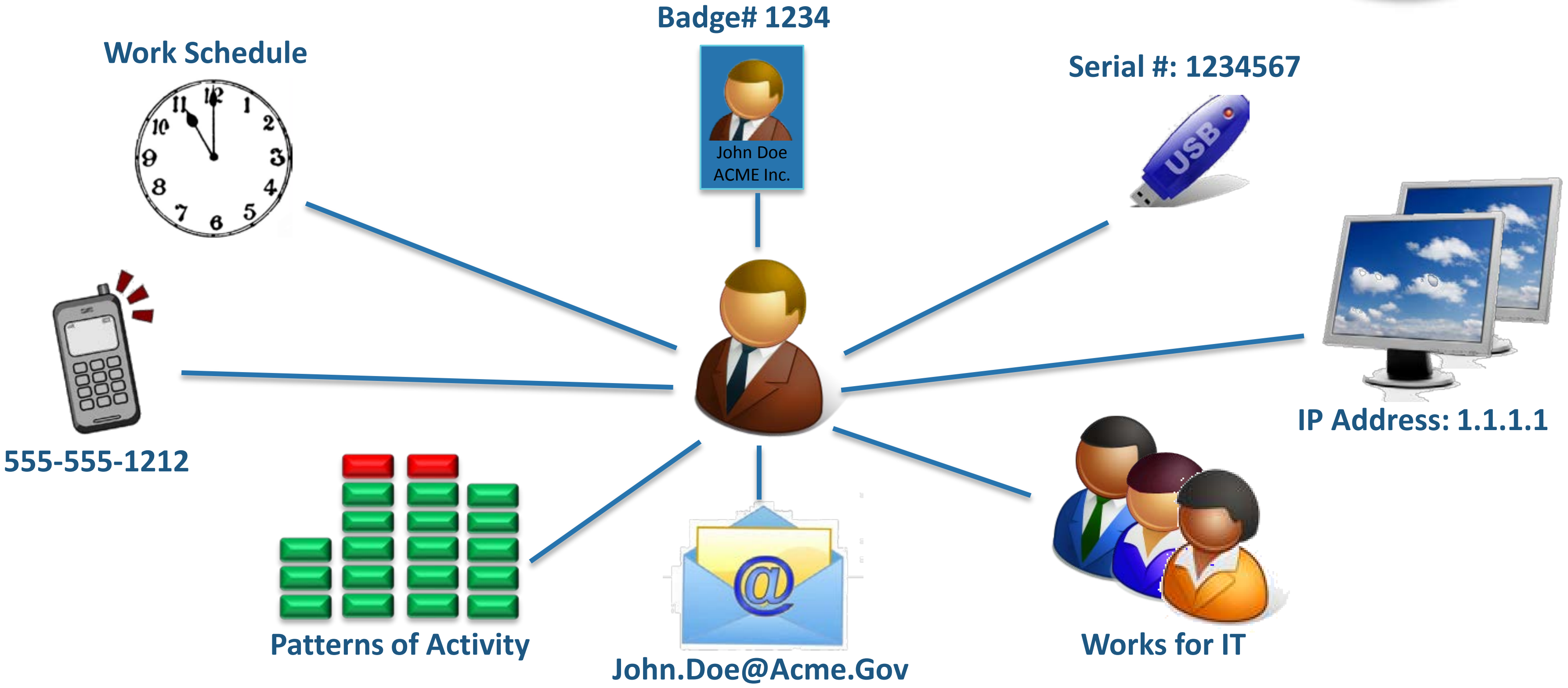
Phase II – Reactive Controls & Processes

- Initial skeleton of insider threat program
  - Some visibility of insider threat, but largely reactive to insider incidents
- Establish a standard processes for investigations
  - Engage HR and Legal
  - Drive consistency through documented processes… remove emotion
- Alerts from DLP and SIEM tools
  - Overwhelmed with volume
  - No context to alerts and data at risk
  - Business context is key… analytics is the future
- Use product coaching
  - "Sure you want to send?"– Real time awareness is the most effective
  - Awareness programs to educate

Phase III – Operational Controls

- Dedicated resources (depending on size and complexity of company)
  - Teamwork – more than an information security problem
  - Build a virtual/cross functional team to handle the issue and operate the program
- Processes to scale program from reactive operational mode
- Behavioral modification
  - Create a culture of ownership whereby staff feel comfortable reporting "Something doesn't look right". It is no longer socially acceptable to break rules
- Tune monitoring tools
  - Become more intelligent about alert handling
  - Add initial analytics to alerts to provide context
- Formal and meaningful entitlement and access reviews

What is Normal?



Badge# 1234

Work Schedule

Serial #: 1234567

555-555-1212

IP Address: 1.1.1.1

Patterns of Activity

John.Doe@Acme.Gov

Works for IT

Phase IV – Purposeful Operations

- Monitor changes in the environment
  - Merger & Acquisition, Strategic Changes
  - Staff Moral
- Upgrade Existing Tools (like DLP or SIEM)
  - Require too much care and don't "really" detect insider activity effectively
  - Implement dedicated analytics tools
- Profiling behaviors of specific groups
  - What is normal behavior?
- Monitoring against defined potential insider activity
  - Both technical and physical
- Metrics used to adjust analytics and track progress

Because We all Like Tools!

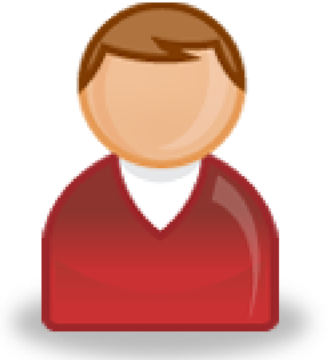
- Maturing a Program
  - Each of the phases has a People, Process and Technology Component. The implementation of higher levels of technology should be done in conjunction of maturing the people and process components.
- Enabling Technology Solutions
  - Data Encryption
  - Network Segmentation
  - Predictive Artificial Intelligence / Behavioral Analytics
  - SIEM
  - DLP
  - Identity and Privileged Access Management
  - User Activity Monitoring

Phase V – Strategic Business Focus

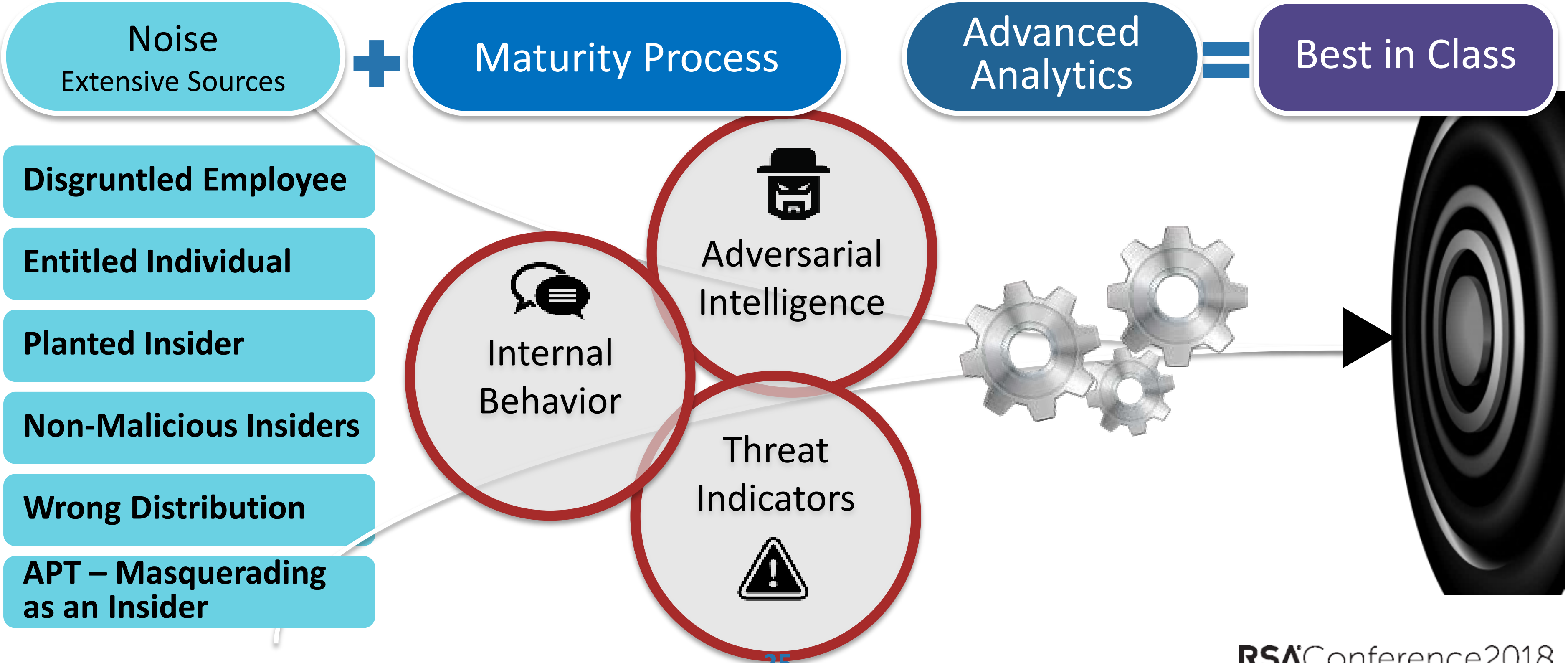
- Business Focus
  - Continually work with the business leaders on the threat level and how to manage as part of a strategic partnership
  - Building programs around corporate events (e.g. acquisition, layoffs, organizational changes, incentive modification, etc.)
- Fusion Center – Cyber Threat – Internal Intelligence Organization
  - The power of analytics will help with detection of sophisticated adversaries, and insider threats
- Disciplined Hiring
  - Psychological testing for those access to sensitive information
  - Extensive background checking
  - Check for ties relating to Cyber Espionage actors

Insider Investigations

- Have documented, consistent and repeatable investigation approaches
  - This will have an emotional aspect
  - Never make assumptions of guilt or innocence
  - Let the data and observations be your guide
- Engage Legal and HR immediately in an insider investigation
  - Present the alerts and gain approval to proceed
  - Cases that may result in legal action should be performed at the direction of counsel
- Have a good case management system
- Improved detection will result in more cases.
  Make sure you can manage and track them well



Insider Threat – Best in Class



Noise
Extensive Sources

+

Maturity Process

Advanced Analytics

=

Best in Class

Disgruntled Employee

Entitled Individual

Planted Insider

Non-Malicious Insiders

Wrong Distribution

APT – Masquerading as an Insider

Internal Behavior

Adversarial Intelligence

Threat Indicators

How to Apply What You Have Learned

Within three months, you should:

90 Days

✓ *Review your current insider threat program maturity level*

✓ *Don’t forget the fundamentals: Training, DLP, adversary analysis, privilege access, culture*

✓ *Establish a plan to move to next maturity level*

Beyond three months, you should:

+ 90 Days

✓ *Obtain specific support for the appropriate level of insider threat maturity level*

✓ *Establish a plan with specific milestones for moving your insider threat program to desired maturity level*

✓ *Maintain a record of Wins, Focus the value of the program to meeting the strategic corporate goals*

James Christiansen

Chief Information Security Officer (CISO)
Teradata

TERADATA

Gary Harbison

Chief Information Security Officer (CISO)
Monsanto Information Security Office

MONSANTO