Counterintelligence & Insider Threat Detection

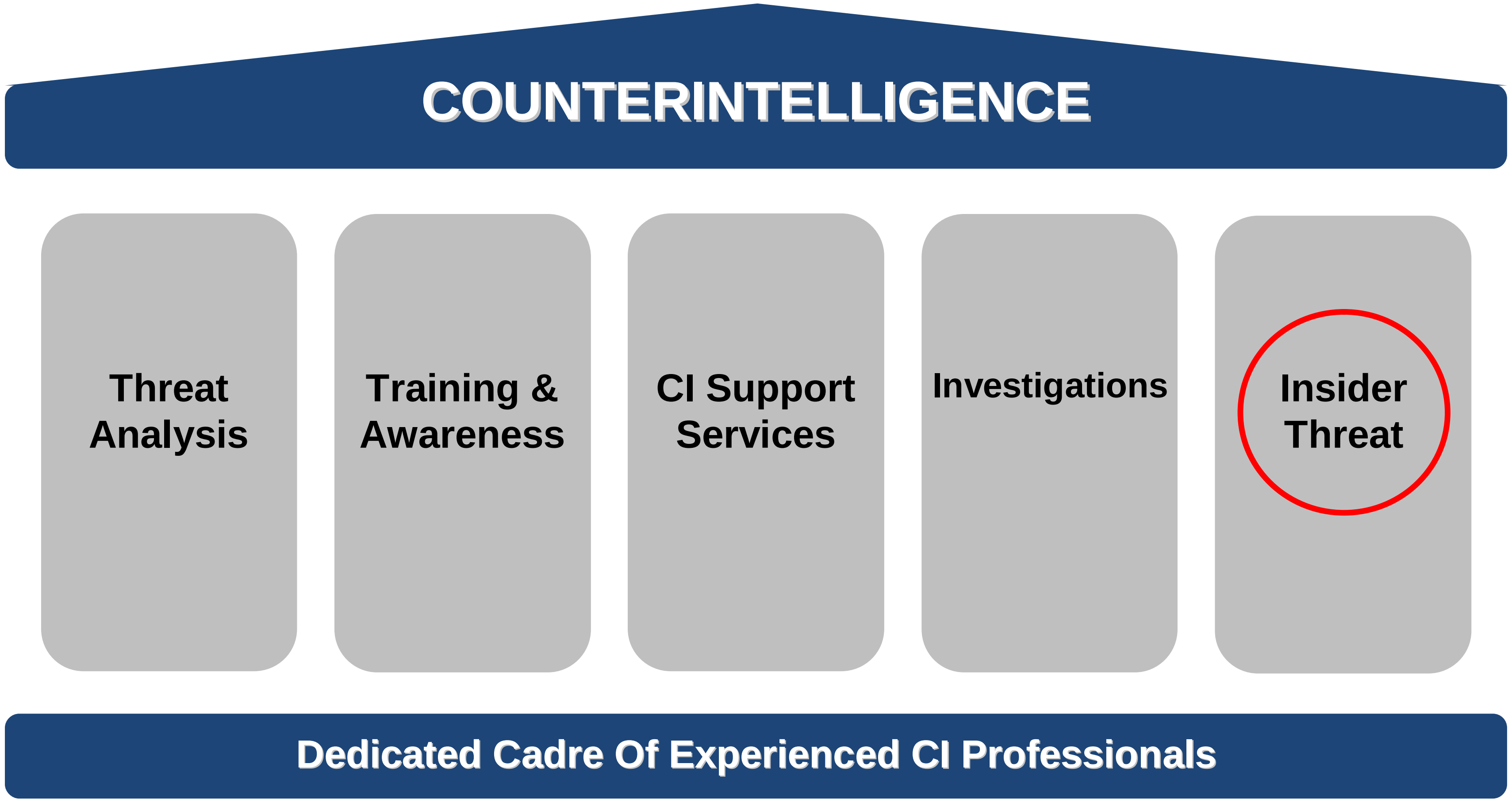
National Insider Threat Special Interest Group

July 18, 2017

LOCKHEED MARTIN

Douglas D. Thomas
Director, Counterintelligence Operations
& Corporate Investigations

Lockheed Martin Counterintelligence



COUNTERINTELLIGENCE

Threat Analysis

Training & Awareness

CI Support Services

Investigations

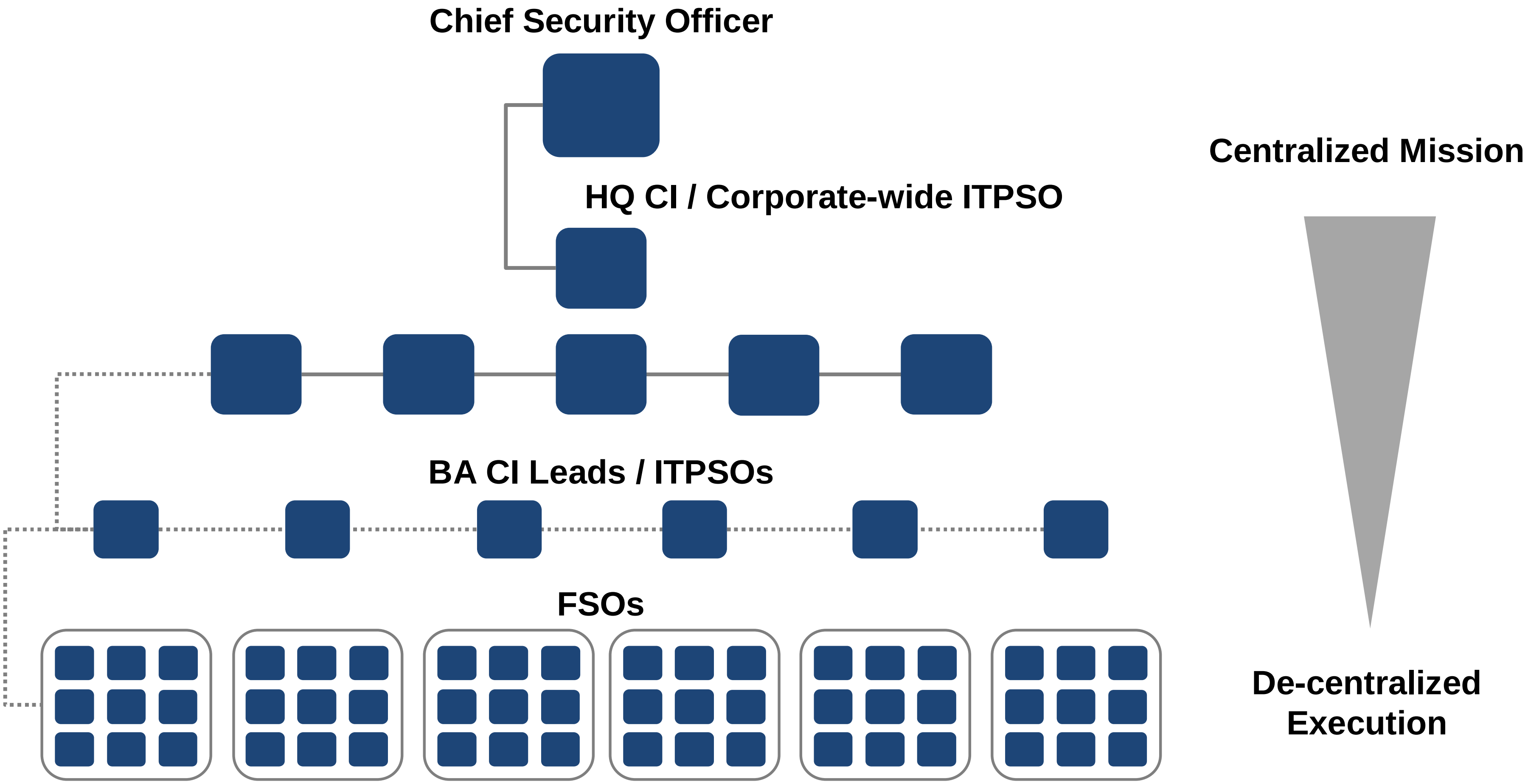
Insider Threat

Dedicated Cadre Of Experienced CI Professionals

Comprehensive Insider Threat Definition

- **Intelligence & National Security Alliance (INSA) definition:**
  - ***"The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits: acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace"***
- **Based Upon Commonly Shared Behaviors Preceding Acts of Workplace Violence, Suicide, and Espionage**
- **A Program Built Around Behavioral Analysis Allows for Applicability for a Variety of Threats**
- **Allows for Education of Employees Based on Broad Observable Behaviors**

Organizational Structure



Chief Security Officer

HQ CI / Corporate-wide ITPSO

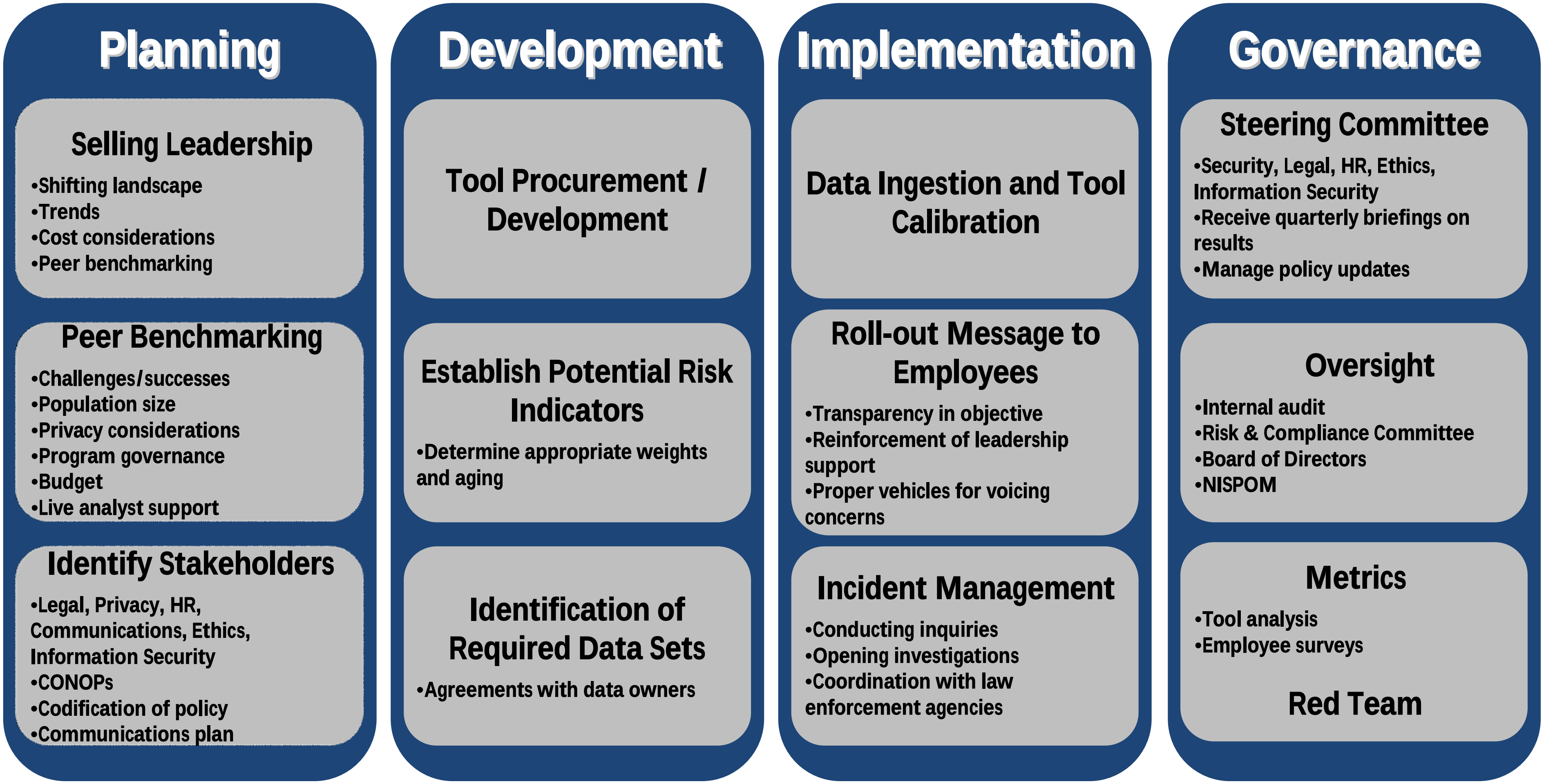
BA CI Leads / ITPSOs

FSOs

Centralized Mission

De-centralized
Execution

Insider Threat Detection Program



Planning

Selling Leadership

- Shifting landscape
- Trends
- Cost considerations
- Peer benchmarking

Peer Benchmarking

- Challenges/successes
- Population size
- Privacy considerations
- Program governance
- Budget
- Live analyst support

Identify Stakeholders

- Legal, Privacy, HR, Communications, Ethics, Information Security
- CONOPs
- Codification of policy
- Communications plan

Development

Tool Procurement / Development

Establish Potential Risk Indicators

- Determine appropriate weights and aging

Identification of Required Data Sets

- Agreements with data owners

Implementation

Data Ingestion and Tool Calibration

Roll-out Message to Employees

- Transparency in objective
- Reinforcement of leadership support
- Proper vehicles for voicing concerns

Incident Management

- Conducting inquiries
- Opening investigations
- Coordination with law enforcement agencies

Governance

Steering Committee

- Security, Legal, HR, Ethics, Information Security
- Receive quarterly briefings on results
- Manage policy updates

Oversight

- Internal audit
- Risk & Compliance Committee
- Board of Directors
- NISPOM

Metrics

- Tool analysis
- Employee surveys

Red Team

Potential Consequences Of Haphazard Approach

- **Failure to Cultivate Leadership Support**
  - **Minimum Allocation of Dedicated Resources**
  - **Difficulty Obtaining Data Sets from Other Company Functional Areas**
  - **Exceedingly Restrictive Governance Apparatus**
- **Failure to Properly Calibrate Program Before Launching Investigations**
  - **Unnecessary Disruption of Employee Productivity**
  - **Loss of Confidence from Company Leadership**
- **Failure to Develop Responsible Employee Messages**
  - **Creation of "Culture Of Snitches"**
  - **Distrust Amongst Employees**

Communication To Employees

- Proper Introduction to Employees – IMPERATIVE!
- “Perception is Reality”
- Absolute Transparency in Purpose and Objective
- Communication of Adherence to Corporate Value Structure
- Reinforcement of Leadership Support
- Joint Strategy Development (Human Resources, Communications, Public Relations)
- Executive Review
- Multi-pronged Approach
- Shared Indicators

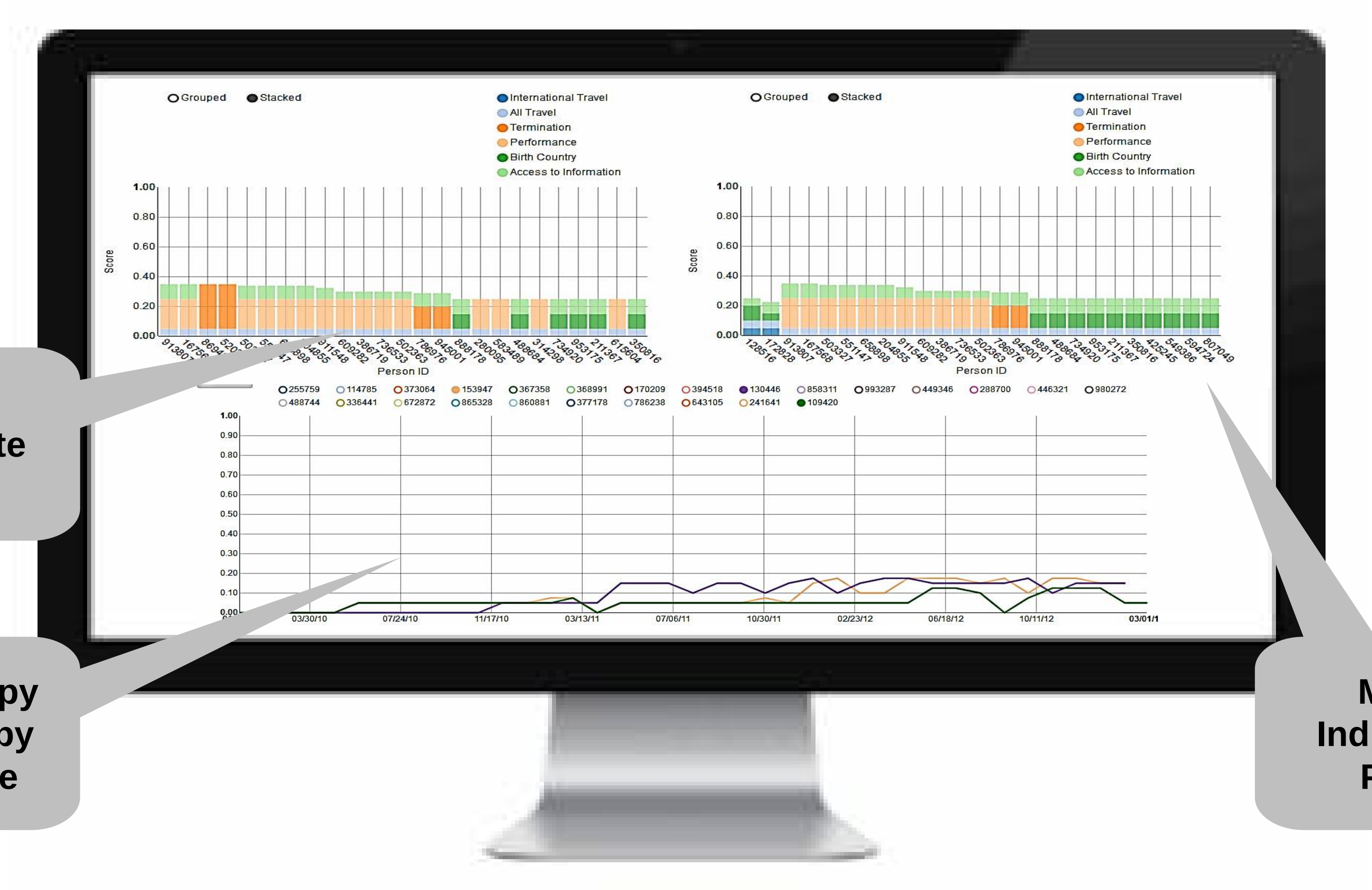
Privacy Considerations

- Address Privacy Considerations in Employee Communications
- Coordination with Corporate Privacy General Counsel
- International Privacy Laws
- Restricted Access to Data
- “Red Team” Detection Systems
- International Association of Privacy Professionals (IAPP)

Risk Analysis & Mitigation System (RAMS)

- Evaluation of Employee Attributes, Behaviors and Actions According to Analyst-defined Models
- Digital and Human Behavioral Baseline
- Lead Generation and Triage from Three Graphical Outputs
- Automated Link Analysis
- Categories and Attributes are Assigned Weights
- Models Run Against an Entire Population or Subsets
- Based on Big Data Technologies (Petabyte+)
- Notifications and Alerts
- Data Encryption
- No Profiling

RAMS Daily Graphical Output



Top Composite Score

Top Entropy Changes by Employee

Most Individual PRIs

2016 Insider Threat Program Metrics

- Employee CI Training & Awareness
- Receipt of Threat Information / Implementation of Mitigation
- Suspicious Contact Reports (SCR) Generating Government Referrals or Intelligence Information Reports (IIR)
- Name Checks
- CI Leads From Insider Threat Tool
- Cases Opened
- Cases Referred to Federal Law Enforcement
- Files Recovered
- Case Disposition

Transition To Risk-Based Approach

- Identify Assets
  - Technology, process, and/or knowledge
  - Personnel assigned to those assets
- Prioritize Assets
- Identify and Analyze Threat, Vulnerability, & Impact
  - Methods of Operation
- Develop & Align Tailored Threat Mitigation Strategies

2017 Initiatives

- First-line leader Insider Threat course
- Protecting the “Middle Way”
- “Off the Grid” Employees
- University engagement
- Standardization of Workplace Violence Protection Plan
- Integration of Open Source Data into Insider Threat Program

Lessons Learned

- Organizational leadership buy-in NOT won and done!
- Long process; funding can be incremental
- Functional area partnerships key to program success
- Cyber, Security, HR, Ethics, Legal, Communications
- Continual coordination with General Counsel
- Internal Audit engagement
- Communications plan
- “Opaque transparency”
- Application in suicide and workplace violence prevention
- FLE referral proof of concept
- Break down “business as usual” mindset

Critical Takeaways

- Corporate Proprietary Information and Intellectual Property → ***HOT*** targets!
- Reporting indicates steady upward trend in targeting
- Threat is real, formidable, and aggressive
- Current business environment exposes us to more vulnerabilities
- Strong partnerships are key (internal and external)
- Automated analysis capability is essential for any large organization
- Data loss prevention tool ≠ insider threat detection capability
- Program transparency → mitigate concern, promote deterrence, garner program support