Insider Threat Detection (ITD) In The Enterprise - Capabilities and Services

ASSESS | DETER | DENY | DEFEND | DEFEAT | EVOLVE

Insider Threat Assessment & Program Development

- **Characterize, Assess, Evaluate, Recommend**
- **Policy Development & Implementation**
  - •CI/IT Program Initiation & Guidance
  - Senior Executive Policy & Directives
  - CI/IT Strategy
  - Policy Maintenance
  - Impact Considerations
    - Tangible: - Intangible:
- **ITD Program Plan, Processes & Procedures**
  - Master Process
  - Identify Scope of Assessment
  - Conduct survey of customer's existing program
  - Standard Operating Procedures
  - Alignment with NIST, ICD, Policies
- **Assessments & Initial Analysis**
  - Identify Organization's IP, Goals & key business processes
  - Prioritization of Business Functions
  - Identify Scope of Assessment
  - Conduct survey of customer's existing program
    - Provide a comparison against benchmark programs
  - Review customer's authorities, policies, and requirements
    - Ensure compliance with applicable federal and state laws
  - Gain insight of key organization operations
    - Complete interviews
    - Identify "crown jewel" digital equities
  - Survey existing network security posture
    - Configuration management review
    - Vulnerability Scanning
    - Web traffic analysis
    - Review of auditing capabilities
  - System administrator review and analysis
- **Reports & Recommendations**
  - Reports on Findings
  - Recommendations
  - Vulnerabilities
  - Next Steps

Secure ITD Environment

- **Design, Deploy, Customize, Monitor**
- **Investigator Network Design & Build**
  - Assess current hardware and software deployment and controls
  - Virtualization vs. Physical Impacts
  - Accreditation status & requirements
  - Implementation of Digital Case Management System
- **Deployment of ITD Investigator Network**
  - Data Storage
  - Network Infrastructure Impact, Analysis, Monitoring
  - Core Servers for ITD Control and Surveillance
  - Desktop Delivery, monitoring
  - Testing & System Accreditation
  - Software & Hardware customization and tailoring
- **Shadow Networks & Enclaves**
  - Operations & Maintenance
  - Maintain patch levels
  - Hardware health monitoring
  - System Accreditation
  - Maintenance
  - Continuous Monitoring
- **Cross Domain Design**
  - UNCLASSIFIED
  - CLASSIFIED
  - Cross Domain
- **Unattributed System Design**

ITD Data Identification & Collection

- **Create, Collect, Tune, Extract**
- **Insider Threat Data**
  - Create Data Collection Mechanism
  - Establish data warehouse
  - Execute cross- domain solutions
- **ITD Data Collection**
  - Host based data collection
  - System Log Collection
  - User behavior data
  - Disparate data set collection
  - Data integrity & availability needs
- **Tune ITD Data**
  - Alignment of disparate data sets
  - data set categorization
  - custom policy design & creation
- **Extract, Transform, Load (ETL)**

Extract

- Coordination with data owners
- Design / engineering of data set delivery to secure enclave
- Data set categorization
- Custom policy design & creation

Transform

- Determination of data subset inclusion
- Application of threat specific filters
- Data cleanup processes & procedures
- Data de-duplication actions
- Automation

Load

- Database loading and scheduling
- Load performance monitoring

Data Analysis & Lead Development

- **Engineer, Model, Analytics, Leads**
- **Engineering Analysis**
  - Analysis platform creation
  - Personnel Behavior Dashboard
    - Dashboard creation & tailoring based on customer specifics
    - Key information & situational awareness based display
- **Behavior Modeling**
  - Behavior modeling analytics
  - Identification of high risk personnel
  - Anomalous activity determination
- **Data Analytics**
  - Analysis platform toolsets
  - Data anomalies triage
  - All-source data analysis
- **Develop & Use Metrics**
  - Baseline Configurations
  - Review & Refine
  - Determine Effectiveness
  - Reporting
  - Types of Metrics

Incidents | Violations | C & A Process Participation & Analysis|

- **Lead Development**
  - Identification of potential Investigative leads
  - Elevation of leads for assessment
  - Written reports of findings
  - Advanced analytical and collection methodologies

Investigations

- **Assess, Interview, Report**
- **Investigative Assessment**
  - Criminal Behavior Assessment
  - Identification of Policy violations
  - SOURCE / SUBJECT Interviews
  - Elevate to appropriate authority for criminal or concerning behavior
- **Digital Forensics / Media**
  - Conduct Forensics review
  - Media exploitation analysis
  - Removable media analysis
  - Reverse Engineering

For more information, contact:
General Dynamics –Mission Systems

Elaine Forgo; (703) 263-2833, Elaine.Forgo@gd-ms.com
Mark Hutnan; (571) 271-4284, Mark.Hutnan@gd-ms.com
Steve Marker; (202) 510-7153, Stephen.Marker@gd-ms.com

ITD Program Enhancement

- **Learn, Adapt, Evolve**
- **Organizational Integration**
  - Supporting Groups within the organization
  - Capability integration
  - Personnel Security
  - Physical Security
  - Human Resources
- **ITD Program Depth**
  - Program "Hub" for all ITD activities
  - Review
  - Improvement of overall security within an organization
- **Lessons Learned**
  - Documented
  - Tracked
  - Collaborative
  - Continuous Improvement
  - Improved TTP's

Training & Awareness

- **Incident Response Training**
  - Security Officer Training
  - Reporting requirements
  - Evidence preservation
  - Triage
- **Awareness Campaigns**
  - Briefings
  - Lessons Learned
  - Current Threats
  - Best Practices
  - Case Studies
  - Concenring behavior and methods of reporting
- **Delivery Methods**
  - Classroom
  - Web-Based
  - CBT
  - Signage & Posters
  - Summary Materials
  - Marketing Collateral
- **Conduct Awareness Training**
  - Three Tiers
    1. General Population
    2. ISSM's, ISSO's, CIPO's, COOP POC's
    3. Senior Executives