CISA's IRMPE Self-Assessment an Overview

Michael Theis, CISSP, SAC (retired), CCII
Chief Engineer, Strategic Engagements
Enterprise Threat and Vulnerability Management
CERT Program

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0085

Agenda

CERT Insider Risk Research Overview

IRMPE Overview

IRMPE Improvements in the Self-Assessment Tool

Demonstration of the Self-Assessment Tool

Q&A / Open Discussion

CERT Insider Risk Research


```
Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. *"
| eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name
"@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND
recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip, sender_address,
recipient_address, message_subject, total_bytes'
```

Conducting research, modeling, analysis, and outreach to develop socio-technical solutions to combat insider threats since 2001

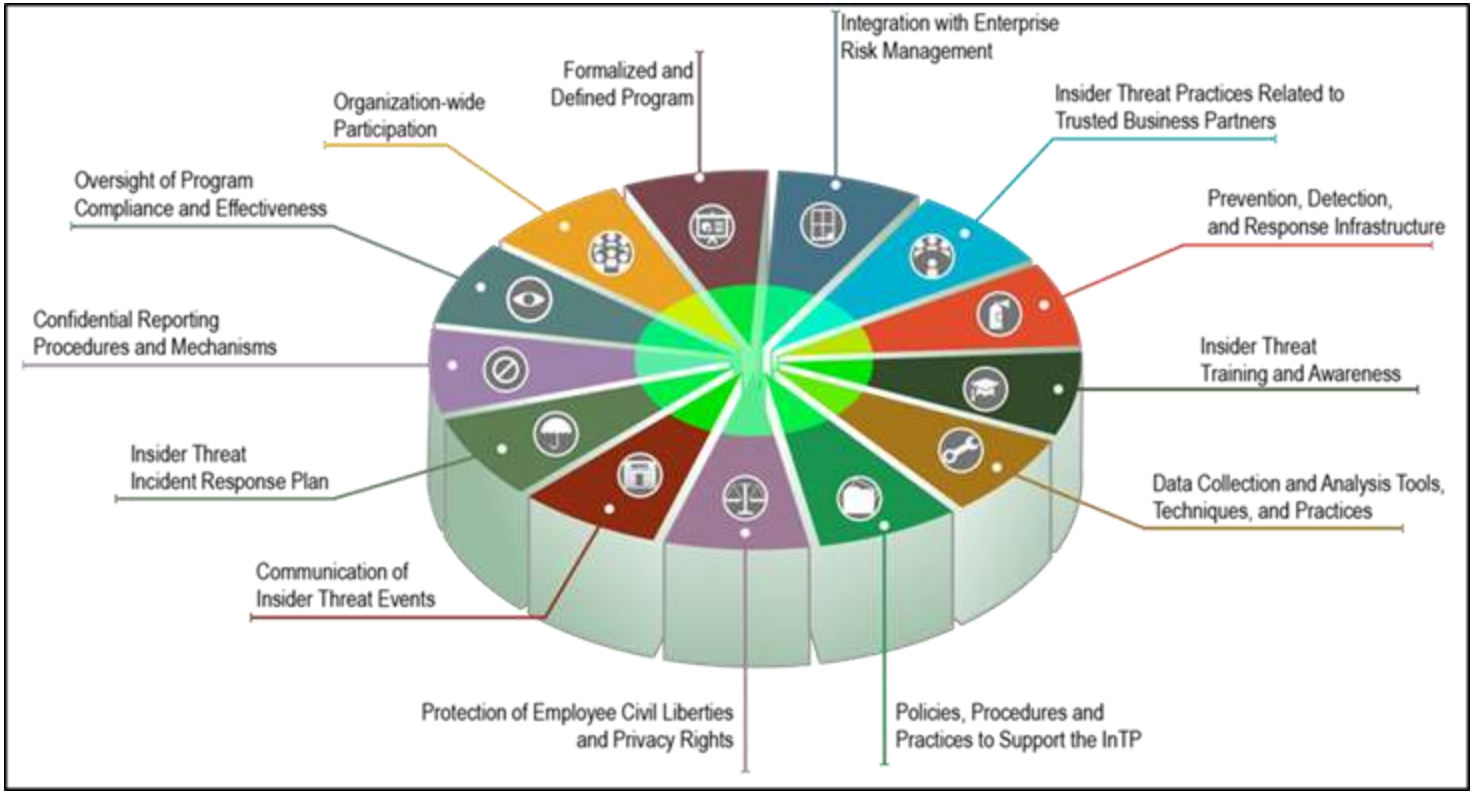
Insider Risk Management Program Evaluation (IRMPE) Overview

- The SEI **measures the effectiveness of insider risk management programs** using its IRMPE capability

- The IRMPE **benchmarks** insider risk programs against a set of recommended best practices derived from the **National Insider Threat Policy and Minimum Standards**, and the SEI's extensive research background in insider risk mitigation

- The **observations** and **recommendations** of the IRMPE help the organization develop a **roadmap** that can be used to establish and maintain a mature and effective insider risk program

IRMPE Focus Areas



IRMPE Capabilities

Program Management	Personnel and Training	Human Resources & Investigations	Data Collection and Analysis
Formalized Program	Organization-wide Participation	Candidate Employee Verification and Hiring	Insider Threat Incident Response
IRMP Policy	IRMP Team Composition	New Employee Onboarding Process	IRMP Access to Information
Internal Risk Incident Response Plan	Awareness Training for the Organization	Employee Behavior	User Activity Monitoring
IRMP Communications Plan	IRMP Team Training	Employee Investigations	Integrated Data Analytic Capability
ERM Integration	Role-based Training for the Organization	Employee Support Programs	
Critical Asset Identification	Manager and Supervisor Training	Employee Separation	
IRMP Governance			
Compliance, Quality, Effectiveness, and Performance of the IRMP			

IRMPE Modifications for the Self-Assessment Tool

- Reduced IRMPE's assessed capabilities to fit 4-hour completion target
- Built-in report generation, including recommendations (Adobe Experience Manager - Forms v6.5)
- Provided longitudinal analysis capability (rudimentary)
- Incorporated the first-ever Maturity Indicator Level (MIL) model for IRMPs (based on CERT-RMM)

A Sampling of CERT-RMM Applications and Derivatives

Insider Risk Mitigation Program Evaluation Overview

- Derived from and developed similarly to the Cyber Resilience Assessment
- 3 Process Areas (Program Management, Personnel & Training, Data Collection & Analysis), 20 goals, 80 specific practices
- Mapped to CERT-RMM, CMMC, National Insider Threat Policy and Minimum Standards, relevant NIST standards, and the CERT Common Sense Guide to Mitigating Insider Threats

Obtaining the Self-Assessment Tool Package

There are five components to the package

- Insider Risk Mitigation Program Evaluation (IRMPE): Assessment Instrument (.pdf, 5.7MB)
- IRMPE Question Set and Guidance (.pdf, 785.13 KB)
- IRMPE Quick Start Guide (.pdf, 1.12 MB)
- IRMPE User Guide (.pdf, 1.02 MB)
- IRMPE One-Pager (.pdf, 607.01 KB)

Entire package is located here

Demonstration of the Self-Assessment Tool

CAVEAT: This is a demonstration of the tool only. I do not represent CISA, or any of its policies, positions, or processes.

Q&A / Open Discussion