INSIDER RISK MANAGEMENT PROGRAM & AI SECURITY CONTROLS TRAINING COURSE™

REDUCE INSIDER RISK & DATA BREACHES

STRENGTHEN AI SECURITY CONTROLS

ENHANCE CROSS-FUNCTIONAL COLLABORATION

IMPROVE COMPLIANCE & GOVERNANCE

PROTECT ASSETS, REPUTATION & VALUE

www.insiderthreatdefensegroup.com

INSIDER THREAT DEFENSE GROUP ™

Insider Risk Management Program Experts

INSIDER RISK MANAGEMENT PROGRAM & AI SECURITY CONTROLS TRAINING COURSE ™

Insider Risk Program Manager W/ AI Security Controls Certificate / Credential ™

TRAINING COURSE OVERVIEW

This highly sought after 2 day training course is designed for anyone managing or supporting an Insider Risk Management (IRM) Program (IRMP): Insider Threat Analyst, FSO, CSO, CISO, Human Resources, CIO – IT, Network Security, Governance, Risk & Compliance Professionals, Counterintelligence Investigators, Mental Health / Behavioral Science Professionals, Legal Etc.),

The training provides comprehensive guidance from A to Z for an IRMP: Implementation, Management, Investigations, Evaluation & Optimization and AI Security Controls. The training is structured to provide value whether participants are building a new program or looking to mature an established program.

This training provide students with a handbook and an abundance of training materials, educational resources, templates and checklists needed for an IRMP.

This training also provides a variety of templates and checklists that are needed when implementing or enhancing an AI system and performing an AI systems security controls assessment.

No need to take 2 different courses that would cost substantially more, when you can take this course and get the benefits of both. **The training is presented in both classroom and virtual formats.**

IRMP OVERVIEW

This training focuses on transforming a new or existing IRMP from a **REACTIVE** program, into a shared **PROACTIVE** organizational responsibility. This will ensure key stakeholders are **universally aligned** from an enterprise / holistic perspective to identify, respond to, investigate, prevent and mitigate employee risks / threats. This collaborative approach to IRM will enhance the security controls (Non-Technical, Technical) for an organization to prevent operational disruptions and downtime, financial loss, theft of assets, compliance fines, workplace violence, legal exposure and more.

This training course will provide students with the critical thinking skills and in-depth knowledge that is needed for conducting investigations, and for collecting, correlating and analyzing various employee data sources to generate accurate employee risk and threat profiles to identify potential or actual Insider Threats, using proven analytic principles and methodologies.

The training will cover conducting a comprehensive Insider Threat Vulnerability & Security Controls Assessment to help identify gaps and weaknesses in the security foundations of the organization.

AI SECURITY CONTROLS & FRAMEWORK OVERVIEW

While an individual managing an IRMP may not be responsible for AI system design and implementation, they should still have a in-depth understanding of the necessary security controls that should be implemented to ensure their organization is being properly protected from the unintentional or intentional misuse of an AI system by employees and AI agents. This knowledge will also be helpful if there is an AI systems incident.

Whether you're implementing an AI system or are looking to enhance the security of an existing system, you will greatly benefit from this training.

AI Risk Management Frameworks from NIST and ISO/IEC 42001 are some of the leading guides for developing secure AI systems. Unfortunately these frameworks do not provide in-depth guidance on the many operational security controls that are needed for employee and AI agent visibility, and the controls that are needed to alert and block unintentional and intentional actions by employees and AI agents. Just because an organization has achieved ISO/IEC 42001 certification does not mean their AI system is secure.

Most major AI platforms provide some security controls. But this varies depending on the whether the organization purchased a business version or enterprise version. The key is **to evaluate**, **not assume** if the security controls exist in the platform your organization is using or considering.

To properly evaluate if an AI system has the necessary security controls, will involve performing a gap analysis. You can't just rely on a vendor of an AI model telling you security's is built in. You must define your AI system security requirements to ensure your organizations existing or new AI system is properly designed and configured to protected against the many threats that can be caused by employees and AI agents.

This training will **1)** Provide guidance on the AI system operational security controls that are necessary for organizations to obtain **enhanced visibility** and **control** of their employees and AI agents actions. **2)** Deep dive into the many critical questions that need to be addressed for comprehensive AI system security.

A demonstration will be provided by Witness AI of their industry recognized and very comprehensive AI Systems Security Monitoring, Alerting and Blocking platform. This demonstration will allow organizations to benchmark their out of the box AI systems security controls to determine if improvements are needed.

Recent research from numerous sources on AI systems incidents is indicating the financial impacts are costing organizations from $1 Million to $15 Million or more. If the proper security controls are implemented and monitored, this can prevent or mitigate the impacts from an AI security related event, and cut overall breach recovery costs by an average of nearly $2 million.

This training is aligned with established frameworks such as the NIST AI Risk Management Framework and the ISO/IEC 42001 and provides more in-depth guidance on operational security controls.

KEY TOPICS COVERED

MODULE 1: INTRODUCTION TO INSIDER THREATS

- ✓ What Is Insider Threats?
- ✓ Who Can Be An Insider Threat?
- ✓ Going Beyond Typical Definitions (Real World Examples & The Severe Impacts To Organizations)
- ✓ Insider Threats Overview, Damages & Impacts / Review Of Monthly Reports Produced By The National Insider Threat Interest Group (Eye Opening View Of The Severity Of Insider Threats)

MODULE 2: INSIDER THREAT MOTIVATIONS / BEHAVIORAL INDICATORS

- ✓ Employee Behavioral Indicator(s) Warning Signs / Risk & Threat Profile Generation (Non-Technical, Technical) (**Checklists Provided**)
- ✓ Contributing Organizational Risk Factors / Recognizing The Employer - Employee Trust Relationship Breakdown Indicators
- ✓ Understanding The Importance Of Going Beyond Background Investigations To Identify Employee Problems / Concerns Using Employee Continuous Monitoring And Reporting (Post Hire, Case Studies, Solutions)

MODULE 3: SECURITY FOUNDATIONS & CRITICAL SECURITY CONTROLS REQUIRED TO PROTECTING AN ORGANIZATION ASSETS

- ✓ Security Policies And Procedures That Are Critical For Protecting An Organizations Assets (**Templates Provided**)
- ✓ Identifying Key Information Assets (Data Inventory) And The Protection Strategies Required To Safeguard The Information (**Template Provided**)
- ✓ Conducting An Insider Threat Vulnerability / Security Controls Risk Assessment To Evaluate Gaps & Weaknesses In Organizational Security Foundations (Non-Technical, Technical) (**Checklists Provided**)
- ✓ Employment Separation And Termination Procedures (**Checklist Provided**)

MODULE 4: IRM PROGAM (IRMP)

- ✓ How To Define The Business Use Case And Scope For An IRMP
- ✓ How To Gain Support And Buy In For The IRMP / Discussions With CEO, Board Of Directors, Executive Management (**Template Provided**)
- ✓ Understating The Rational For Alternate Names For An ITP / IRMP
- ✓ What Are The Costs Related To Creating & Managing An IRMP? (Personnel, Budgeting, Resources Needed)
- ✓ IRM / IRMP Compliance Regulations / Understanding The Limitations And Risks Of Just Checking The Box
- ✓ Understanding The IRMP Legal Considerations
- ✓ Understanding The Employee Lifecycle And Key Stakeholder Responsibilities For IRM
- ✓ Creating An IRMP Governance Structure: Critical Roles, Responsibilities & Collaboration Required By Key Stakeholders For Employee Risk & Threat Information Sharing
- ✓ Creating A Comprehensive IRMP Framework From A To Z
- ✓ Essential Documentation Required For An IRMP (**Templates Provided**)
- ✓ Essential Data Sources For Insider Threat Detection / Investigations (Internal, External)
- ✓ IRMP Optimization (Risk Assessments, Gap Analysis & Strategic Planning)
- ✓ Providing IRMP Metrics To CEO / Board / Senior Management For Resources (Budget, Personnel) To Optimize The IRMP (**Template Provided**)

MODULE 5: INSIDER THREAT AWARENSS, REPORTING, INCIDENT RESPONSE & INVESTIAGTIONS

- ✓ Creating A Workforce Culture Of See Something, Say Something (**Insider Threat Awareness Training Materials Provided**)
- ✓ The Legal And Privacy Considerations On The Collection, Use And Sharing Of Employee Information
- ✓ The Legal And Privacy Aspects Of Workplace Employee Monitoring (Computers, Mobile Devices, Etc.)
- ✓ Creating The Procedures And Framework For Insider Threat Reporting, Conducting Investigations & Case Management (**Templates Provided**)
- ✓ Identifying, Collecting, Correlating And Analyzing Employee Data Sources To Support Insider Threat Investigations

MODULE 6: INSIDER THREAT MONITORING FOR COMPUTER SYSTEMS & NETWORKS

- ✓ Detecting Activity Indicative Of Insider Threat Behavior Using Network Security Tools (NST's) / User Activity Monitoring (UAM) Tools (UAMT's) (**Checklists Provided**)
- ✓ Performing A Gap Analysis To Evaluate The Strengths And Weaknesses Of Existing UAM Software) (**Checklists Provided**)
- ✓ Detailed Guidance Into The Various Capabilities & Features To Consider And Questions To Ask When Comparing Different Vendor UAM Solutions (**Checklists Provided**)
- ✓ Eye Opening Demonstrations Of The Malicious Insider Threat Playbook Of Tactics For Stealing Information And Data As Easy As 1, 2, 3 (What Your NST's, UAMT's Might Not Detect)

MODULE 7: AI SECURITY CONTROLS & FRAMEWORK

- ✓ AI Risk Management Framework Limitations
- ✓ Creating A Comprehensive AI Systems Employee Acceptable Use Policy (**Templates Provided**)
- ✓ Critical Questions That Need To Be Addressed For Comprehensive AI Systems Security (**Checklist Provided)**
- ✓ Understanding AI Systems And The Underlying Sub Components That Require Monitoring, Traceability, Alerting & Blocking Controls To Prevent The Unintentional Or Intentional Misuse Of An AI System By Employees, AI Agents
- ✓ Guidance On Performing A Security Controls Gap Analysis For AI Systems (**Checklist Provided**)

CONTINUING PROFESSIONAL EDUCATION (CPE) CREDITS

Students attending this training will earn **16 CPE Credits** towards CPE requirements for security certifications they have obtained.

TRAINING RECOGNITION / STUDENT SATISFACTION & COMMENTS

Over **1000+** students have attended our training courses and endorsed them as the most affordable, next generation and value packed training for IRM, that are taught from a real world, practical, strategic, operational and tactical perspective.

Our very high levels of student and client satisfaction are the result of the ITDG being experts at building IRMP's, as we do more than just provide training. We also provide consulting services and incorporate lessons learned from our consulting engagements. **Our student and client satisfaction levels are in the EXCEPTIONAL range**. You are encourage you to read the feedback from our students on this link.

COMPANY RECOGNITION

The ITDG Has Provided IRMP Training / Consulting Services To An Impressive List Of 700+ Clients:

White House, U.S. Government Agencies, Department Of Homeland Security, TSA, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines) Intelligence Community (DIA, NSA, NGA) FBI, U.S. Secret Service, DEA, Law Enforcement, Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines, ExxonMobil, Royal Canadian Mounted Police and many more. (Full Client Listing)

ABOUT THE ITDG / TRAINING COURSE INSTRUCTOR BACKGROUND

All ITDG training courses are based on our Insider Risk Management (IRM) Program 360 Framework & Assessment Methodology (IRMP360FAM™). The IRMP Framework encompasses 11 critical domains for IRM and an IRMP and **EXCEEDS** all compliance regulations. Our methodology is practical, real world, cost effective, proven and addresses Insider risks and threats from an enterprise cross functional perspective, and from a non-technical and technical perspective.

IRM is comprised of many different security disciplines that encompass, but are not limited to physical security, information / data security, cyber security, computer / network monitoring, digital forensics and other areas. The instructor for this training (Mr. Jim Henderson) is an industry recognized IRMP Subject Matter Expert, that has **20+** years of experience, has protected classified information up to the TS-SCI level, has a broad background in many security disciplines listed above, has received specialized training, holds numerous security certifications and received numerous awards for his contributions to the security field.

Mr. Henderson is also the Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG). The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center (ISAC), as no such ISAC existed.

Combining NITSG meetings and events and ITDG training courses / consulting services, the NITSIG and ITDG have provided IRM guidance and training to **3,400+** individuals. (More Information)

Please contact the ITDG with any questions you may have about this training.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
IRMP Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Risk - Threat Vulnerability Assessor
FBI InfraGard Member
561-809-6800
www.insiderthreatdefensegroup.com
james.henderson@insiderthreatdefense.us