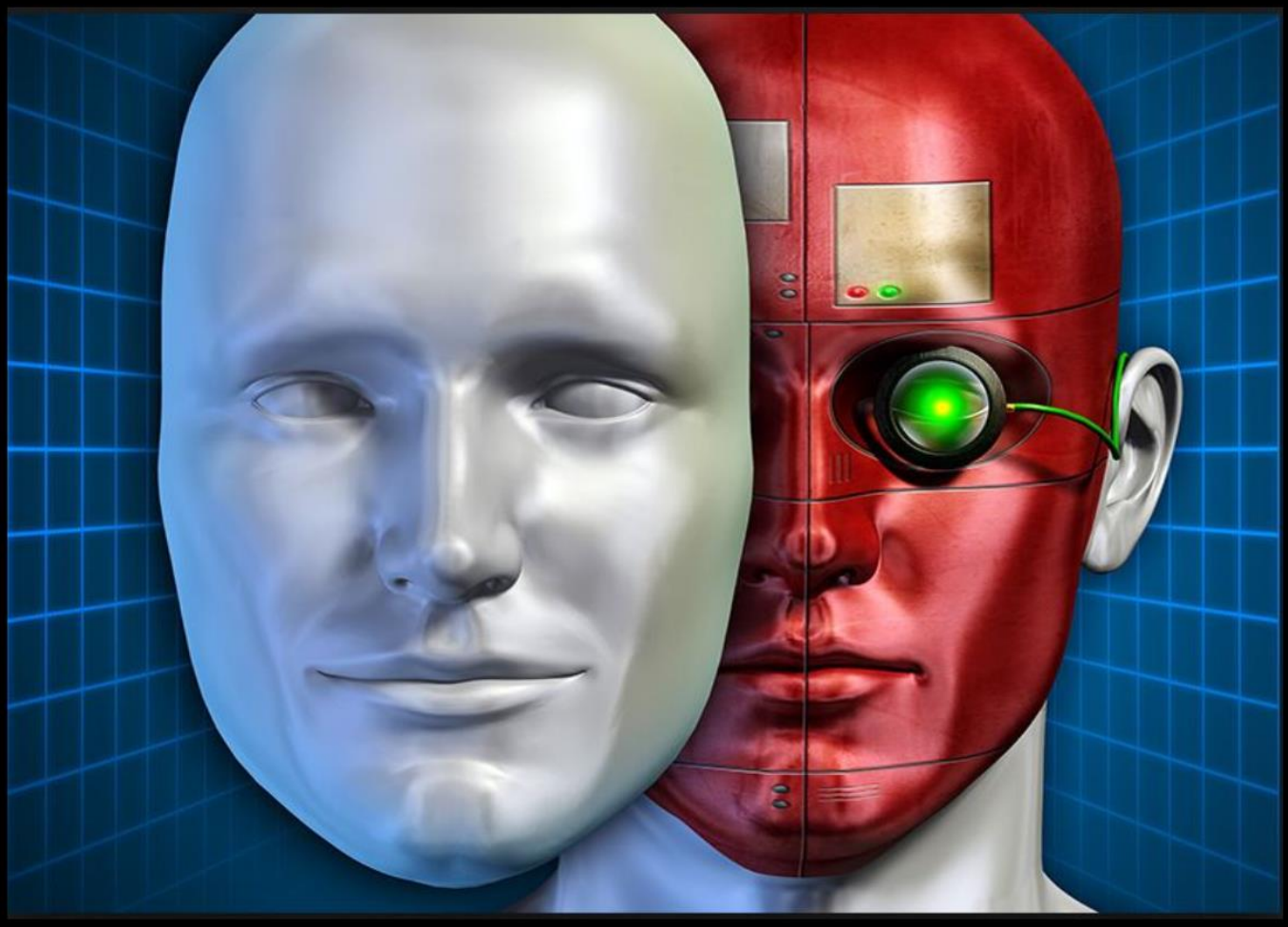
INSIDER THREAT DEFENSE

INSIDER THREAT RISK MANAGEMENT TRAINING & SERVICES CATALOG

Don't Let Appearances Fool You



THE INSIDER THREAT

Is Your Organization At Risk?

www.insiderthreatdefense.us
888-363-7241

INSIDER THREAT DEFENSE

Security Behind The Firewall Is Our Business

Table of Contents

The Insider Threat - How Vulnerable Is Your Organization?

What Is The Insider Threat?

- Disgruntled Employees - Malicious Insiders (Current Or Former Employees, Contractors, Or Other Business Partners)
- Espionage (National Security, Economic, Industrial, Corporate)
- Cyber Criminal-Insider Threat Collusion
- Divided Loyalty Or Allegiance To U.S. / Terrorism
- Financial Threat, Fraud, Bribery, Corruption, Physical Theft
- Data Theft (IP, Trade Secrets, R&D, PII), Data Destruction, Source Code Theft, Network-Information Technology Sabotage, IT Privilege Account Abuse
- Insiders Who Are: Unwitting, Ignorant, Negligent
- Cyber Insider Threat (Malware Infections, Cyber Criminal Social Engineering / E-Mai Phishing)
- Workplace Violence

Insider Threats - A Very Costly And Damaging Problem

- Many companies are only focused on Cyber Criminals penetrating their network perimeter defenses. What lies behind the network perimeter of firewalls and other cyber defense technologies is a very real threat - "The Insider Threat".
- The visibility of the "Insider Threat Problem" has never been greater. The damages that are being caused by an Insider (Witting, Unwitting) have been severe ($ Billions), many times more damaging then an external cyber threat.
- An Insider can change their tactics and techniques to suit their goals, just like malware. The Insider Threat is a human problem, not just an IT or data loss problem, and needs to be addressed with more then just technology, using a holistic enterprise risk management approach.
- In many cases a malicious Insider only needs one vulnerability to achieve their goals, bypassing traditional security controls or non-existent security controls. The end result is that an Insider Threat can seriously damage a organizations network, and can affect the confidentiality of intellectual property, customer loyalty, brand reputation and stock prices.
- The National Insider Threat Special Interest Group has conducted in-depth research and complied some "Eye Opening" reports, surveys and incidents related to the Insider Threat problem.

Could Your Organization Recover From That Damages That An Insider Can Cause?

Insider Incident -1 January 28, 2014

When EnerVest IT Administrator Ricky Joe Mitchell heard that his job with the oil and gas company was on the chopping block, he didn't go quietly. Instead, he reset the company's servers to their original factory settings, disabled cooling equipment for EnerVest's IT systems, along with a data-replication process and deleted PBX system info. As a result, EnerVest was unable to communicate reliably with customers or conduct business operations for a full month and was forced to spend hundreds of thousands of dollars on data recovery efforts. The incident cost the company over $1 million, according to the prosecution. In addition data that the company thought had been backed up, could not be retrieved. Source

Insider Incident -2 December 13, 2006

A 63-year-old, former IT System Administrator that was employed by UBS PaineWebber, a financial services firm, allegedly infected the company's network with malicious code. The malicious code he used is said to have cost UBS $3 million in recovery expenses and thousands of lost man hours. He was apparently irate about a poor salary bonus he received. In retaliation, he wrote a program that would delete files and cause disruptions on the UBS network. His malicious code was executed through a logic bomb which is a program on a timer set to execute at predetermined date and time. The attack impaired trading while impacting over 1,000 servers and 17,000 individual work stations. Source

Insider Threat Collusion - How Many People Could Be Involved In An Insider Threat Incident?
Many times when the Insider Threat is discussed, it is discussed from the perspective of **1** individual being involved. Recent Insider Threat incidents involving collusion with others, to include Cyber Criminals is on the rise. These Insider Threat incidents involving collusion have sometimes involved close to **200** individuals.

Defense Contractor Cheating The Navy's 7th Fleet Is The Largest Corruption Scandal Ever - December 27, 2016
The contractor was Glenn Defense Marine Asia, who provided port security for Navy ships and submarines. This investigation started in 2006. It took the NCIS-Navy 10 years to finally nail this defense contractor. So many Navy people were involved in this scandal. 12 people, including a Navy Admiral, and 9 other Navy personnel have pleaded guilty. 5 people still face charges. Close to **200** other individuals are under scrutiny. Among them are about 30 current of retired Navy Admirals. This incident involved the; Unauthorized disclosure of classified information, politics, bribes, prostitutes, cash, vacations, gifts, parties, insider moles-paid informants, etc.
Source

Maryland Man Sentenced To Prison For Role In Massive Identity Theft And Tax Fraud Scheme - May 3, 2016
Marc A. Bell, 49, a former employee of the District of Columbia's Department of Youth Rehabilitation Services (DYRS), admitted taking part in a massive and sophisticated identity theft and false tax return scheme that involved an extensive network of more than **130** people, many of whom were receiving public assistance. According to court documents, the scheme involved the filing of at least 12,000 fraudulent federal income tax returns that sought refunds of at least $42 million from the U.S. Treasury. The false tax returns sought refunds for tax years 2005 through 2013 and were often filed in the names of people whose identities had been stolen, including the elderly, people in assisted living facilities, drug addicts and incarcerated individuals. Refunds also were sent to people who were willing participants in the scheme. The refunds listed more than 400 "taxpayer" addresses located in the District of Columbia, Maryland and Virginia. Source

FBI Busts Comcast Hacking Suspects - Including Comcast Employee Who Helped Hackers - December 16, 2015.
The FBI has arrested three men on charges that they participated in a hacking and identity theft scheme that attempted to steal personal information for 60 million individuals. The FBI has also accused two of the men of using botnets and hacking corporate email servers to distribute spam on behalf of paying clients, generating illegal profits of more than $2 million. On Aug. 11, 2014, a Comcast Sales Representative provided the Cyber Criminals with access to a remote-administration tool that was running on a computer that had access to the Comcast network, according to the indictment. As a result, it says, the 2 Cyber Criminals were able to access the network and exfiltrate "the names, addresses, phone numbers, and email addresses of potential customers, current customers, and former customers" of Comcast. Source

Software Developer Outsourced Job To China Over VPN - January 16, 2013
In one exemplary illustration of employee negligence, an American software developer outsourced his programming job to a consulting firm in Shenyang, China for approximately $50,000 while he continued to collect a salary of several hundred thousand dollars. Meanwhile, the negligent insider spent his workdays surfing social media and reading emails.

The insider activity was detected when an investigation into anomalous activity discovered that the employee's credentials were being used to remotely access the company systems. The employee had mailed his multi-factor authentication key to the Chinese consultant via Fed-Ex.

For the potential years that the employee outsourced his job, he received excellent marks in his performance reviews and the clean and functional code that he submitted was considered some of the best in the organization. The employee, whom was in his mid-40s, a "family man, inoffensive and quiet. Someone you wouldn't look twice at in an elevator." The evidence even suggested he had the same scam going across multiple companies in the area. Source

Workplace Violence - The Type Of Insider Threat Requiring Much Great Attention

- Unfortunately very disgruntled Insiders have resorted to workplace violence, in some cases resulting in the deaths of innocent coworkers.
- According to the Occupational Safety and Health Administration (OSHA), approximately 2 million employees are victims of workplace violence each year. 18% of violent crimes are committed at the workplace, and roughly 800 workplace homicides occur each year.
- Between January 2009 and July 2015, there were 133 mass shootings in the workplace and shootings account for 78 % of all workplace homicides. Violence in the workplace must be a top concern for employers, as no organization is immune from workplace violence and no organization can completely prevent it. (Source)
- A robust and effective Insider Threat Program will train Security Professionals, Supervisors, Managers and Employees to identify "Behavioral Indicators" that are warning signs for workplace violence. These warning signs include; Employees who do not accept criticism and express anger and blame others for their own poor performance, unexplained increase in absenteeism, increased and severe mood swings and noticeably unstable or emotional responses, frequent loss of temper, personality conflicts with co-workers, increasing dialog about problems at home, including marital, family or financial struggles, increase in unsolicited comments about violence, firearms and violent crimes, increased use of alcohol or illegal drugs, exhibiting signs of depression and withdrawal and experiencing a traumatic event.
- Can your organization take the chance that one of your "Trusted Employees" might commit workplace violence?
- A organization that ignores the warnings signs could face legal action.
  Jury Awards Over $1 Million In Negligent Hiring Lawsuit Involving Workplace Violence
  Family Of Security Guard Killed By Disgruntled Employee, Sues Labor Department For $10 Million

Company Background

- Mr. Henderson is the CEO of Insider Threat Defense (ITD), Inc. He has over 15 years of "**Hands On Experience"** in the development, implementation and management of complex Enterprise Cyber Security-Information Systems Security Programs, Information Assurance Risk Management Programs and Insider Threat Programs, for the Department of Defense (DoD), National Level Intelligence Centers, U.S. Government Agencies, State Governments, large and small businesses. (Bio)

- ITD has become the "**Leader-Go To Company**" for Insider Threat Program (ITP), and Insider Threat Risk Mitigation services. We offer a broad portfolio of training and services to potential clients that will address Insider Threat risks with a cost effective, comprehensive and holistic approach.

- ITD is a pioneer in ITP Management Training. We were one of the first companies to develop and offer comprehensive ITP Development / Management Training ™ to the U.S. Government and defense contractors, who were required to implement ITP's, based of off National Insider Threat Policy, and NISPOM Conforming Change 2 regulations.

- ITD training and services **go beyond** traditional compliance regulations; National Insider Threat Policy, NISPOM Conforming Change 2, Federal Information Security Management Act (FISMA), National Institute of Standards & Technology (NIST), Health Insurance Portability & Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Gramm–Leach–Bliley Act (GLBA), Financial Industry Regulatory Authority (FINRA), Etc.). These compliance regulations are very weak in the area of Insider Threat Risk Mitigation.

- ITD provides consulting services for ITP development, implementation and management, and conduct Insider Threat Risk Assessments.

- Some organizations that provide ITP related training, base their training only off of research. Our training is not just based off of research. We designed our ITP Development / Management Training Course based off of our **10+** years providing "**Hands On**" consulting services to our clients.

- Designing training based off of more then just research, is a primary centerpiece of our training. We incorporate "**Lessons Learned**" based on our analysis of ITP's, and Insider Threat related incidents encountered from working with our clients.

- ITD works with our clients to identify security weaknesses and vulnerabilities. We execute the "Insiders Playbook" of potential breach scenarios, to find holes in the security posture of an organization, **before** a Malicious Insider does.

- ITD training and services are also based upon the **extensive research** we have been conducting since 2009 on the Insider Threat problem. This research has been done in partnership with; U.S. Government Agencies, (Department of Defense, Intelligence Community Agencies), Defense Contractors, Insider Threat Risk Mitigation Vendors, and the FBI Maryland InfraGard Insider Threat Special Interest Group - (Previously Run By Insider Threat Defense CEO).

- The CEO of ITD is the Founder-Chairman of the National Insider Threat Special Interest Group (NITSIG). The NITSIG is a unique and specialized Information Sharing and Analysis Center, focused primarily on Insider Threat Risk Mitigation. The NITSIG Membership is the largest network of Insider Threat Risk Mitigation Security Professionals in the U.S.

- Collectively ITD and the NITSIG have provided ITP related training and awareness to over **1700+** security professionals.

- This extensive collaborative environment of information sharing among our clients and NITSIG Members has provided ITD the unique opportunity to continually enhance our training and services. We provide our clients with the "**Gold Standard**" for successful Insider Threat Risk Mitigation.

Insider Threat Risk Mitigation Services

- ✓ Insider Threat Program Development & Management Training Course ™ (More Info)
- ✓ Insider Threat Program Management With Legal Guidance Training Course ™ (More Info)
- ✓ Insider Threat Program Working Group Training ™
- ✓ Insider Threat Awareness Training / Briefings
- ✓ Insider Threat Training Academy ™ - Web Based Training (More Info)
- ✓ Insider Threat Workshop For CEO's And Board Of Directors ™
- ✓ Insider Threat Program Knowledge And Skills Assessment ™
- ✓ Insider Threat Program Development - Management Guidance / Consulting
- ✓ Insider Threat Risk Assessment And Mitigation Services
- ✓ Insider Threat Data Exfiltration Testing ™
- ✓ Employee Continuous Evaluation, Monitoring & Reporting Service
- ✓ User Activity Monitoring / Behavioral Analytic Tool Guidance / Implementation
- ✓ Agent Surefire Insider Threat Investigation Game
- ✓ E-Mail Phishing Testing / Cyber Threat Awareness Training

Insider Threat Defense Training And Services Offer Our Clients The:

- Ability To Implement Or Enhance An Insider Threat Program
- Ability To Enhance The Workforce Culture Of Security
- Early Detection / Increased Visibility Of Disgruntled And Malicious Employee Threat Indicators
- Ability To Detect Vulnerabilities And Weaknesses, Before A Malicious Insider Does
- Reduction / Likelihood Of Insider Threat Incidents, Legal Problems, Lawsuits
- Protection Of The Company's Intellectual Property, Reputation, Stock Prices, CEO / Shareholder / Investor Confidence

Insider Threat Defense Training And Services Are Trusted By Security Professionals At;

* White House National Security Council
* FBI Headquarters
* FBI Terrorist Explosive Device Analytical Center
* DHS Infrastructure Information Collection Division
* Transportation Security Administration (TSA)
* Department of Defense Inspector General
* Defense Criminal Investigate Service
* Defense Security Service
* National Nuclear Security Administration
* U.S. Cyber Command
* U.S. Army Enterprise NetOps /
* U.S. Army Signal Command
* U.S. Air Force
* Marine Corps Intelligence Activity
* Navy SPAWAR
* OPM – Federal Investigative Services
* Government Accountability Office
* Social Security Administration
* Internal Revenue Service
* Centers For Disease Control & Prevention
* Microsoft Corporation
* BB&T Bank
* American Express
* Equifax
* Home Depot

* Police Executive Research Forum
* Royal Canadian Mounted Police
* National Academy of Sciences
* Association of American Railroads
* Johns Hopkins University Applied Physics Laboratory
* University of Texas @ Austin / ARL
* University of Massachusetts Lowell
* Oklahoma State University
* University of Dayton
* Kansas State University
* Texas A&M University
* Auburn University

* United Parcel Service (UPS)
* FedEx Custom Critical
* JetBlue Airways
* Delta Airlines
* Boeing Integrated Information Systems
* Raytheon / Raytheon BBN Technologies
* General Dynamics Mission Systems
* Northrop Grumman Corporation
* Lockheed Martin, Missiles & Fire Control
* AT&T Government Solutions Security
* Booz Allen Hamilton
* And Many More.....

Insider Threat Defense Client Satisfaction

- In the last few years many companies are popping up with Insider Threat Program Development / Management Training. Some of our students have taken the competitions training and are still confused about how to implement and manage an Insider Threat Program. These students have then taken our training.
- Insider Threat Defense is extremely confident that you'll be happy with our training and services. We can say with confidence our clients are ranking us **#1** compared to the competition. Client comments are stating that our training and services are; comprehensive, structured, holistic, resourceful and affordable.
- Our Insider Threat Risk Mitigation Services have successfully demonstrated to our clients the many vulnerabilities and weaknesses that traditional security approaches fail to mitigate, and will put an organizations assets at risk.

Client Satisfaction Comments

The comments listed below are from student evaluation forms and from e-mails we received after students or clients used our training or services.

The content of the Insider Threat Risk Mitigation Handbook and the compilation of resources both on the Insider Threat Program Training Reference website and in the handbook have been very helpful as we work our way through building a robust Insider Threat Program for CDC.

J. Drew Craig
Lead, Counterintelligence / Insider Threat & SCIF Operations
Public Health Intelligence Office
Office of Safety, Security, and Asset Management
Office of the Chief Operating Officer
Centers for Disease Control and Prevention

The class was awesome and provided a plethora of information. Once again, a pleasure in meeting you and your presentation was on point and very well planned.

Juan Davis
FBI Terrorist Explosive Device Analytical Center (TEDAC)

Thank you for teaching the class—I'm sure this was the most efficient way to get all the information to be compliant with the Insider threat program requirement. The handouts and disc are amazing with incredible reference materials available. I'm sure I'll be able to get this plan in order within the next couple of weeks. Jim, you are an excellent teacher, too. Obviously, you like this field to excel in. We all appreciate your knowledge and your leadership in the class! Pleasure meeting you.

Judith A. Meggitt
President Sound & Sea Technology, Inc.

Good information and a great class. Your class helped to validate where I was going with our Insider Threat Program to meet the NISPOM requirements. After your class I know that there is much more that I can do to make it an effective, meaningful program. I won't be able to implement everything but I certainly have the ammunition to argue for more than just meeting requirements.

Craig Beardsley
Kansas State University Facility Security Officer

Thank you so much for this wealth of information! I'm almost finished with our Insider Threat Program…thanks to your course I had all the reference materials I needed!

Marcie Spalding, CSSO
Next Century Security & Administration Lead, NBP

Thank you so very much for this post class informative email. Even after the class, you are still offering support and providing value! The Insider Threat Program Development class provided everything I hoped for and more!

Dawn Young-Bermudez
President Intelliforce-IT Solutions Group / Intelliforce Technology Partners

---

Just wanted to say I really enjoyed the training last week. Your course provided a great blue print to create my company's Insider Threat Program.

Thomas A. Stearns, CPP
Enterprise Security,
W.L. Gore & Associates, Inc.

Thank you for such a thorough and thought-provoking course. The reference materials alone were well worth the price, and your delivery and personal experience put this class over the top.

Marcie Spalding, CSSO
Security & Administration Lead
Next Century Corporation

I just completed this training and it is AWESOME ! Not like other Insider Threat trainings that I have taken. If you want to do the NISPOM Change 2 correctly, you will take this course. It is packed with a tremendous amount of information and will get you excited about your own plan.

Those who only want to get by with bare minimal requirements may not find it as illuminating as I did. I am competitive by nature, so I like to put my best effort forward. We push ourselves hard to receive a "Superior" DSS rating each year since 2012. This Insider Threat Program Training course will help you do just that. There are 5 agency plans already written and available for your use, just choose one and extract only the parts that you need for your organization. Most of the work is done for you. There are some fascinating 'checklists' that you can include with your Insider Threat Program. Many of them contain things that you may not have thought of. You will receive a training certificate and the Insider Threat Security Special (ITSS) credential. There are 16 CEUs for this training---how can you say NO to something so good that grows YOU as a security professional and strengthens the security posture of YOUR ORGANIZATION... and don't forget the networking opportunities as well.

I highly recommend this course, the benefits are phenomenal. Thank you Jim -- Great course and wonderful presentation

Tammy Breeding
SES Government Solutions (SES GS)
Corporate Security / F.S.O. / I.T.S.S.

Additional Student-Client Comments

Please contact Insider Threat Defense if you would like to speak to security professionals who have used our training and services.

Insider Threat Program Personnel Knowledge And Skills Assessment ™

Cyber Security-Information Systems Security Program Management and Cyber Threat Risk Mitigation is perhaps one of the most important and fastest growing job fields in the country. Another rapidly growing field is Insider Threat Program Management (ITPM) / Insider Threat Risk Mitigation (ITRM).

To reduce the threat from "Malicious Insiders", it is critical that an organization hire individuals (Existing Employees Or New Hires) with the necessary experience and training for ITPM and ITRM positions. There are numerous security certifications that attempt to set baseline knowledge for positions in Cyber Security, Information Assurance, Information Security, Information Systems Security, IT / Networking Security, etc. But none of these certifications address the **core knowledge and skill sets** an individual needs to implement, manage or support an Insider Threat Program.

Contrary to some security professional's opinions, ITPM is a specialized security discipline. ITPM requires a variety of skill sets and a close working relationship with other security disciplines and departments to be robust and effective. (Security, Human Resources, Information Technology, Information Security / Assurance, Legal, Etc.)

Currently there is no government occupational series and pay scale for ITPM and related positions. The National Insider Threat Task Force is exploring whether a new occupational code might be warranted, and stated that it takes more then just the talents one would find in a Counterintelligence Analyst, Human Resources Professional or Information Security Professional.

The purpose of the National Initiative For Cybersecurity Education (NICE) Cybersecurity Workforce Framework, is to provide a fundamental reference of the skill sets needed for individuals working in the many different support functions of Cyber Security. ITPM is a part of Cyber Security. Very little reference is made to the many skills sets required for ITPM in this document.

So with very little guidance being provided on the skill sets required for ITPM / ITRM positions, how can an organization be certain that the individual(s) they are placing in these positions, have the necessary experience, training and knowledge to successfully perform their jobs? In some organizations Human Resource Personnel (HRP) or Recruiters are tasked with validating the skill sets for a candidate. HRP and Recruiters are very knowledgeable in their positions, but are not Insider Threat Subject Matter Experts.

Insider Threat Defense (ITD) offers an Insider Threat Program Support Personnel Knowledge and Skills Assessment (ITPSPKSA) for the individual(s) an organization maybe considering for ITPM / ITRM positions. The ITPSPKSA will ensure that the individual(s) your considering placing in critical positions to protect your organizations assets, have the core knowledge and skill sets required for their positions. If the ITPSPKSA determines that an individual needs additional training, we will recommend what areas need improvement and provide the training.

The ITPSPKSA is based off the training ITD has been providing to our clients on Insider Threat Program development, implementation and management since 2009. We have seen first hand the knowledge and skill sets areas were security professional's need additional training.

Please contact Insider Threat Defense with any questions you may have about our ITPSPKSA service.

Insider Threat Risk Assessment And Mitigation Services

Evaluating Security Behind The Firewall Is Essential

Many organizations are only focused on Cyber Criminals penetrating their network perimeter defenses. According to various reports, IT departments continue to spend large amounts of money on network and endpoint technologies. But Cyber Criminals are still successful in penetrating network defenses of Firewalls, Intrusion Detection Systems (IDS), etc. Why are Cyber Criminals so successful? Because Firewalls are not stopping the Malicious Insider, who is helping the Cyber Criminal in some cases.

According to a report from RedOwl and IntSights, the recruitment of Insiders within the Dark Web is active and growing, with forum discussions and Insider outreach nearly doubling from 2015 to 2016. Sophisticated Cyber Criminals use the Dark Web to find Insiders to help them with their malicious actions and pay them for their services.

A Cyber Criminal is able to arm and weaponize Insiders with the tools and knowledge necessary to help the Cyber Criminal steal data, commit fraud, among other acts, and also to cover any tracks. In one instance, a Cyber Criminal solicited bank Insiders to plant malware directly onto the bank's network. This approach significantly reduces the Cyber Criminals level of effort. The Cyber Criminal doesn't have to conduct e-mail phishing exercises and can raise penetration success rates by bypassing many of the organization technical defenses (Firewalls, IDS, Anti-Virus, Anti-Malware, Malware Sandboxing, Etc.).

The lures for Insiders to assist Cyber Criminals are significant. On one forum, the Cyber Criminal explained the approach to a potential Insider, indicating that he needs direct access to computers that access accounts and handle wire transfers. The Cyber Criminals offered to pay "7 figures on a weekly basis" for continued access.

Michael Theis from the Carnegie Mellon's CERT Insider Threat Center states; "Recently, there's been some research that's shown that criminals on the Dark Web have been reaching out to Insiders to buy their login credentials or get them to sell intellectual property," Theis says. "On the other side, we've seen Insiders looking for extra money going to the Dark Web looking to sell their login credentials."

The Carnegie Mellon University CERT Insider Threat Center characterized the "Malicious Insider" in the 2012 Common Sense Guide To Prevention And Detection Of Insider Threats. The guide stated; **Insiders have a significant advantage over others who might want to harm an organization.** Organizations implement security mechanisms such as firewalls, intrusion detection systems, and electronic building access systems primarily to defend against external threats. Insiders, however, are not only aware of their organization policies, procedures, and technology: they are often also aware of their **vulnerabilities**, such as loosely enforced policies and procedures, or exploitable technical flaws in networks or systems.

Why Should An Organization Perform An Insider Threat Risk Assessment?

Your organization has spent the time and money to implement an Insider Threat Program. Is it robust and effective? Could someone's job be on the line because they ASSUMED the Insider Threat Program was working? Does your organization know what vulnerabilities could ENABLE Malicious Insiders actions to be successful?

Words like qualitative, quantitative, metrics, risk scores, compliance, compliance requirements, security strategy, forecasting, analytics, benchmarks, etc. mean nothing to a determined Malicious Insider. These words also mean nothing when a security professional is briefing the CEO on how the Insider Threat incident happened.

Even if your organization does not have an Insider Threat Program, are you certain a Malicious Insider cannot steal data from your organization with very simple techniques, that will go undetected?

Insider Threat Defense can provide a confidential, independent and unbiased Insider Threat Risk Assessment of your organization, to identify vulnerabilities and weaknesses, and provide effective mitigation strategies.

ITERM 360 - Going Beyond Compliance & Traditional Security Approaches

- At Insider Threat Defense we address Insider Threat Risk Mitigation with a "Real World" approach using an Insider Threat Enterprise Risk Management 360 (**ITERM360** ™) methodology.
- The ITERM360 approach uses a holistic, comprehensive, structured methodology that reviews an organizations governance structure, security policies, security culture, critical business departments, business processes, technical and non-technical security controls for vulnerabilities and weaknesses. This approach also executes the "**Insiders Playbook**" of potential data exfiltration scenarios, to find holes in your security defenses, before an Malicious Insider does.
- Our goal is to give your organization a **complete** prioritized assessment of the risks posed by Malicious and Non-Malicious Insiders.
- Our Insider Threat Risk Assessment includes "Threat Simulation Activities" that test the workforce for susceptibility to social engineering attacks. This is a proven and effective method for changing the behaviors and enhancing the security culture of an organization.
- As part of our assessment we will include E-Mail Phishing Testing (100 Users) and Computer User Activity Monitoring (10 Users) at NO CHARGE. Your organization might be very surprised with the results.
- Our ITERM360 approach has successfully helped our clients identify and mitigate very serious vulnerabilities and weaknesses, that if left unchecked could have had serious consequences. See below comment from one of our clients;

  Mr. Henderson:
  I can't express enough my satisfaction with the insider threat risk assessment that Insider Threat Defense performed for my company. I had no idea of the serious risks my company faced that could enable a malicious insider to steal my company's intellectual property. As you stated to me before the assessment, you would use the "Insiders Playbook" to find vulnerabilities in my company's security defenses, before an Insider did. You did just that. I will definitely be recommending your training and services to other CEO's.

  John Garland / CEO Garland Labs
  Precession Machining / Engineering

About Our Insider Threat Risk Assessment Team

- The Insider Threat Risk Assessment Team is comprised of Insider Threat Subject Matter Experts (ITRME's). Our ITRME's have extensive knowledge of Insider Threat Risks and have conducted assessment for the U.S. Government (DoD, IC), Defense Contractors, large and small businesses.
- The Insider Threat Risk Assessment Team are Certified Information Systems Security Professionals (CISSP), and hold other relevant security certifications.

Protecting The Results Of Insider Threat Risk Assessment Reports

- The Insider Threat Risk Assessment Team will obtain information during a security assessment that will not be shared with anyone, other then the designated point of contact within the organization
- The Insider Threat Risk Assessment Team will sign a Non-Disclosure Agreement (NDA) protecting the confidentiality of the organizations Insider Threat Risk Assessment Report.

Please contact Insider Threat Defense with any questions you may have about our Insider Threat Risk Assessment and Mitigation Services.

Insider Threat Awareness Training / Public Speaking

Insider Threat Awareness Overview

Insiders planning to commit malicious actions against an organization will in most cases exploit an organizations weakest links that give them the greatest chance of success, without being caught. Insiders in most cases know what is checked and not checked, and know when they won't be checked or challenged.

Computer User Activity Monitoring (UAM) tools are important for detecting Insider Threats, but UAM tools will not detect all the technical and non-technical techniques that could be used by an Insider with malicious intentions. A technical savvy malicious Insider, who knows they may be monitored, will likely resort to simple old school techniques to steal data from an organization, bypassing UAM and Behavioral Analytic tools.

Supervisors and Co-Workers have the closest day-to-day contact with employees who may have malicious intent, or who may be dealing with personal and / or professional issues that put them at risk of becoming a threat to the organization.

Mitigating the Insider Threat requires educating employees to become "Human Sensors" to detect and report on disgruntled and behavioral indicators that may indicate a potential or actual Insider Threat. Employees used as sensors are one of the most cost effective ways to identify malicious Insiders. A workforce of educated sensors can create the "Big Picture" of an employee who may pose a threat to an organization.

Insider Threat Awareness Training

- Insider Threat Defense can help your organization create or enhance an Insider Threat Awareness Program. We have helped over 500+ organizations kick start their Insider Threat Awareness Programs with the guidance and educational materials to educate the workforce.

- We can provide Insider Threat Awareness Training to your CEO's, Senior Management, Supervisors, Employees, Insider Threat Program Working Group or at a conference. From the CEO down to the workforce, our training will provide a better understanding of what the Insider Threat Program is about, and not about. This will **reduce the reluctance** of the workforce to report and result in the early detection of Insider Threat concerns.

- What makes our Insider Threat Awareness Training unique, is that it focuses on actual Insider Threat incidents that have been very costly and damaging to organizations. We also think outside the box and provide a eye opening view of the "Insiders Playbook" of potential tactics that could be used against your organization for malicious purposes.

- Our Insider Threat Awareness Training will provide your workforce with the ability to; 1) Recognize disgruntled employees who exhibit behavioral indicators and suspicious activities of concern that must be reported. 2) Identify organizational vulnerabilities, that if left unchecked could be very costly and damaging.

- Our Insider Threat Awareness Training draws on our many years of specialized experience in the areas of Cyber Threats and Insider Threats. We can specifically tailor the training for your audience – pitching it at just the right level to keep people entertained as well as informed.

Please contact Insider Threat Defense with any questions you may have about our Insider Threat Awareness training and briefings services

Insider Threat Defense Has Provided Insider Threat Awareness Briefings / Comments For News Articles, Interviews And Reports To:

National Insider Threat Special Interest Group (NITSIG) (2014-Present) Link

FBI Maryland InfraGard Insider Threat Special Interest Group (2011 To 2014)
FBI Maryland InfraGard Cyber Boot Camp (July 2017)

Navy Strategic Systems Programs Information Technology & Cyber Security Forum (2016)

NCMS Mid-Atlantic Chapter (9-2015)
Insider Threat Program Development Briefing

FBI Pittsburg InfraGard
Insider Threat Concerns & Controls Seminar (10-18-13) Link

Discovery Channel (2-17-13)
Cyber Insider Threat Briefing

National Classification Management Society (NCMS) (10-24-12)
Data Loss Protection And Prevention Briefing

DoD Cyber Security And Information Systems Information Analysis Center (CSIAC) (8-5-13)
CSIAC Insider Threat Workshop Overview
CSIAC Video: Insider Threat Workshop Panel Discussion
CSIAC Insider Threat Workshop Papers And Presentations

WWL New Orleans Radio Station (3-21-14)
Insider Threat Defense On-Air Interview With Tommy Tucker Show Discussing Cyber Threats Link

Maryland Emergency Management Association
Cyber Threat-Insider Threat Risk Mitigation Workshop, Gaithersburg, MD (5-7-14)

Federal News Radio Articles & Interviews With Insider Threat Defense

- Insider Threat Program Implementation Challenges (10-17-16) Link
- 7 Signs Your Co-Worker Is A Potential Insider Threat (10-11-16) Link
- Insider Threat Programs Must Find The Right 'Trust But Verify' Balance (5-20-14) Link
- Insider Threat Program Training Starts With Security 101 (8-5-14) Link

Defense One Website
Government Warms To Continuous Monitoring Of Personnel With Clearances - July 10, 2017

Georgetown University Center For Security Studies (January 2018)
Provided guidance for report being developed on the topic of Insider Threats.

Webinars

- How To Build An Insider Threat Program Link
- Security Week Webinar - Insider Threat Defense & Bay Dynamics: Flavors of Insider Threats & Recipes For Detection Link
- Society For Human Resource Management (SHRM): Employee Threat Identification And Mitigation Link

Employee Continuous Monitoring And Reporting Service

Insider Threat Defense in partnership with Endera is excited to announce an automated, cost effective, proactive solution for identifying and mitigating the risks posed by employees.

Overview Of Background Checks

- Background checks are a point-in-time snapshot of an employees suitability and eligibility for employment.
- Background checks **do not provide** visibility of crimes, financial problems, incidents or personal behaviors that happened **AFTER** the background check was completed.
- Even if the incident happened outside the workplace, it may be of concern to the employer. There may be a concern about an employee within the Human Resources or Security departments, but when it is coupled with an outside incident, the concern may widen and provide additional visibility into the potential threat an employee may pose to an organization.
- Most enterprise security departments have no way of knowing if an employee, on-site contractor or temporary worker poses a threat to an organization, or even employees safety.

Benefits Of Employee Continuous Monitoring And Reporting

- Continuous Workforce Monitoring allows employers to receive **real-time alerts** when an event in an employee's outside life poses a potential threat to the employer, co-workers, and customers.
- Continuous Workforce Monitoring enables organizations to **automatically run continuous checks** on its entire workforce every hour of every day with less effort and cost than a onetime background check.
- Continuous Workforce Monitoring will provide an organization with **visibility and early warning signs** that an employee may pose a threat to an organization.
- A organization that can assure regulatory authorities (Federal-State Government), business partners and customers that its workforce is continually monitored has a clear advantage over one that can't make that promise.

Maintaining A Safe Working Environment

- Unfortunately very disgruntled employees "Insiders" have resorted to workplace violence, in some cases resulting in the deaths of innocent coworkers. A organization that ignores the warnings signs could face legal action.
- According to the Occupational Safety and Health Administration (OSHA), approximately 2 million employees are victims of workplace violence each year. 18% of violent crimes are committed at the workplace, and roughly 800 workplace homicides occur each year. Between January 2009 and July 2015, there were 133 mass shootings in the workplace and shootings account for 78 % of all workplace homicides. (Source)
- The OSHA website states; Workers have a right to a safe workplace. The law requires employers to provide their employees with safe and healthful workplaces. (Source)

Endera Employee Continuous Monitoring And Reporting Solution Overview

- Endera monitors approx. 1000+ sources of information (Federal, State, Local) for information that may be of concern to an organization about their employees.
- Endera actively monitors each employee daily for various types of activities that may have a negative impact on their ability to fulfill their roles in compliance with established regulations, and for information that may indicate that the employee may pose a threat to the organization.
- A organization will receive an alert from within 10 minutes to 24 hours after a new potential negative data source has been discovered about an individual.

Endera Employee Alerts

- **Criminality Activity:** Wants and warrants, bookings and arrests, criminal history and sex offender registrations. (Appriss Booking Database Covering Over 82% Of U.S. Population)
- **Court Records:** Bankruptcy, liens & judgments, lawsuits and foreclosures.
- **Financial Activity:** Bankruptcy, foreclosures, liens, judgments, lawsuits, large purchases.
- **Licenses / Permits:** Professional licenses, drivers licenses, healthcare licenses, concealed weapons permits.
- **Sanctions**: Healthcare sanctions, OFAC sanctions, terrorist watch lists, criminal watch lists.

Endera Customer Case Studies

Large Global Airline

Enrolled 60,000 Employees
Detected Over 1,771 Incidents Of Concern To Employer
55 Bookings And Arrest Alerts That Called For Further Investigation

DHS Secure Worker Program

Enrolled 30,000 Employees
Detected Over 800 Incidents Of Concern To Employer
Disqualified 24 Employees From Working

About Endera

- Endera was originally developed for the federal government to help the FBI screen flight school applicants after 9/11.
- Endera ease of use and low cost makes it one of the most affordable and effective solutions for Continuous Workforce Monitoring available.
- Endera secure, easy-to-use, cloud-based platform, is available as a monthly or yearly subscription service (Per Employee), accessible from any web browser without any software for to install.

Do you know if your employees are exhibiting warning signs that may signal a potential threat to your organization?

Please contact Insider Threat Defense to schedule a demo of the Endera Employee Continuous Monitoring and Reporting Tool.

User Activity Monitoring / Behavioral Analytics Software

Insider Threat Defense in partnership with Veriato (Formerly Known As Spectorsoft), is excited to announce a cost effective solution for employee User Activity Monitoring.

User Activity Monitoring Overview

For an Insider Threat Program (ITP) to be robust and effective requires Communications, Visibility and Sharing of information. The Communication and Sharing pieces require various "Trusted Stakeholders" to share information of concern about employees with the ITP. The Visibility piece requires insight into an employees actions on an organization computer systems, networks and the Internet.

Are Your Employees Stealing Your Data?

Half of employees who left or lost their jobs kept confidential corporate data, according to a global survey from Symantec, and 40% plan to use it in their new jobs. The results show that everyday employees' attitudes and beliefs about intellectual property (IP) theft are at odds with the vast majority of company policies. Employees not only think it is acceptable to take and use IP when they leave a company, but also believe their companies do not care. Only 47% say their organization takes action when employees take sensitive information, contrary to company policy, and 68% say their organization does not take steps to ensure employees do not use confidential competitive information from third parties. Organizations are failing to create an environment and culture that promotes employees' responsibility and accountability in protecting IP.

Research by the Carnegie Mellon University CERT Insider Threat Center shows that most employees who steal IP commit the theft within 30 days before or after leaving the organization.

User Activity Monitoring (UAM) Monitoring Tools Provides The Following Benefits

- The ability to collect, report, and alert on the activity of employees who interact with your data, computer systems, networks and the Internet.
- What data are your employees accessing and when. (Files, Folders)
- What data are your employees sending outside the organization without a valid business reason, or without authorization.
- Insight to overexposed sensitive data on a network, that employees may be accessing, but should not be able to. (File, Folder Permission Problems)
- Insight into concerns about an employees suspicious behaviors via; E-Mail, Internet Surfing, Cloud Storage Usage, Remote Access, VPN, Instant Messaging (Chat, Video), etc.
- Insight into attempted or un-authorized IT (Computer-Network) configuration changes (Downloads & Software Installations)
- Insight into an employees productivity problems.
- Insight into an "Employee Disgruntlement" or indicators of potential workplace violence. (E-Mail Keyword Searches)
- Detect inadvertent and repeated actions by employees that can jeopardize the well being of your organization
- A chronological record of activities, events, screenshots and video screen replay for analysis, reconstruction and examination. (Detect Organization Policy Violations, Criminal Activities, Etc.)
- UAM Tools reduce the reliance on expensive Computer Forensic Tools / Experts.
- UAM Tools will provide e-mail alerts on actions & events.
- Integration with leading Security Information Events Manager (SIEM) Tools like Splunk, Arcsight.
- Termination Decisions (Documentation Of Justification To Head Off Wrongful Termination Claims)
- Detailed Evidence For Legal Actions Against An Employee

Veriato 360 User Activity Monitoring (UAM) Tool Overview

- The Veriatio 360 UAM Tool for desktop and laptop computers enables organizations to log, retain, review and report on employee activity.
- Veriato 360 creates a definitive record of an employee's digital activity, and in doing so provides organization with the ability to see the context of user actions.
- All information can be viewed from the Veriatio 360 Dashboard, which is very easy to navigate. You can monitor employee activity remotely from any web-enabled device, including smartphones, laptops and home computers.

What Can Veriato 360 Monitor?

- Video Screen Snapshots & Video Screen Recording
- File & Document Activity (Files Copied Or Moved: Local Hard Drive, Network)
- DVD / CD, USB Drive Activity (Files Copied Or Moved)
- E-Mail, E-Mail Attachments / Web Mail Activity
- Network Activity
- Print Job Activity
- Web Surfing & Activities
- Web Chat / Instant Messaging
- Web Searches
- Cloud Storage Activity (Files Copied Or Moved To & From Cloud Storage Folders)
- Application Usage
- Keystroke Logging

What Does Veriato 360 Report And Alert On?

- Date & Time Of The Activity
- Computer Where Activity Took Place
- User Logged In / Login Time
- Computer Program Used For The Activity
- File Action Involved: Print, Write, Delete, Create, or Rename
- Device Type Involved: DVD / CD, Cloud, USB Drive
- Network, Printer Device Name & Path (Example: \\SERVER10\LaserJet Printer 2nd Floor)
- Alerts On Websites Visited, Online Searches, Computer Programs Used, File Alerts When Restricted Websites Are Visited, Identified Keywords Are Entered Into A Search Engine Or E-Mails
- Alerts For Excessive Printing, Network Bandwidth, Web Usage / Chat Usage / E-Mail Usage
- Alerts When Copying, Downloading & Uploading Files
- Alert Notice If Data Is Saved To an External Device / USB Drives

Veriato 360 UAM Video Demo

https://youtu.be/N9NDHGsnvV0

Veriato 360 UAM Free Trial

Do know what your employees are doing on your organization computers, network and the Internet? This **FREE TRIAL** is valid for 15 days and comes with FREE SUPPORT and the ability to monitor up to 10 employees. You might be shocked at what your discover about your "Trusted Employees".

Veriato Investigator User Activity Monitoring Tool

- Veriato Investigator is a solution for temporary, focused employee investigations. (60-90 Days)
- Veriato Investigator installs quickly, records detailed information on employee activity, and enables fast, accurate, and efficient exploration and playback of the recorded data.
- Veriato Investigator provides the answers you need so informed decisions get made.
- Veriato Investigator's invisible agent is deployed silently and managed from a remote console, so the target of the investigation is not alerted.

What Can Veriato Investigator Monitor?

- Video Screen Activity
- Website Activity
- E-Mail Activity
- Chat & IM Activity
- File Activity
- Computer Program Activity
- Network Activity
- Website Activity

Veriato Investigator Video Demo

https://www.youtube.com/watch?v=ZD_r6L4-_n4

Veriato Investigator Review - Wins Best Computer Forensics Solution In SC Magazine Awards Europe 2016

http://www.veriato.com/company/press/press-releases/veriato-wins-best-computer-forensics-solution-in-sc-awards-europe-2016

Have Concerns About Employee User Activity Monitoring From A Legal Perspective?

Excellent article by Privacy Right Clearinghouse on employee User Activity Monitoring.
https://www.privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring

Please contact Insider Threat Defense for more information, demo, pricing and a FREE TRIAL of the Veriato 360 User Activity Monitoring Tool, or for more information and pricing for Veriato Investigator. The pricing for Veriato UAM Tools is very affordable compared to the competition.

E-Mail Phishing Testing / Cyber Threat Awareness Training

Insider Threat Defense in partnership with KnowBe4 is excited to announce a cost effective method for reducing Cyber Threats (E-Mail Phishing, Malware, Ransomware, Etc.) to your organization and provide training to the workforce.

Cyber Insider Threat Overview

Malicious Insiders can be very costly and damaging to any organization, because their actions are intentional. Another very costly and damaging problem is the Cyber Insider Threat. The Cyber Insider Threat is not intentional. The Cyber Insider Threat problem clearly stems from the lack of Cyber Threat Awareness Training being provided to the person sitting at the computer keyboard.

Cyber Criminals through social engineering, email phishing, weaponized documents, websites with weaponized links, and various other attack methods, rely on Insiders in most cases for their malicious actions to be successful. These types of attacks are designed to install malware, erase hard drives, steal credentials (Logins, Passwords) to gain access to sensitive data, or install Ransomware to encrypt an organizations data and hold it hostage, until the ransom is paid. With just **one click** of the mouse, an organizations data and networks are compromised in minutes.

According to the Verizon 2016 Data Breach Investigations Report, humans remain the weakest link. The report outlines how Cyber Criminals are **continuing** to exploit human nature, through social engineering, as they rely on familiar attack patterns such as e-mail phishing to exploit the human sitting at the keyboard.

FBI Alert On E-Mail Scams

According to the FBI, Business E-Mail Comprise (BEC) is a serious threat on a global scale," said FBI Special Agent Maxwell Marker, who oversees the Bureau's Transnational Organized Crime–Eastern Hemisphere Section in the Criminal Investigative Division. "It's a prime example of organized crime groups engaging in large-scale, computer-enabled fraud, and the losses are staggering."

"They know how to perpetuate the scam without raising suspicions," Marker said. "They have excellent tradecraft, and they do their homework. They use language specific to the company they are targeting. The days of these e-mails having horrible grammar and being easily identified are largely behind us. (Source)

FBI Alert On Ransomware

Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses - these are just some of the entities impacted recently by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them. The inability to access the important data these kinds of organization keep can be **catastrophic** in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization reputation. **Recent iterations target enterprise end users, making awareness and training a critical preventative measure**. (Source)

Additional statistics compiled by the National Cyber Security Alliance paint a disturbing portrait of small business vulnerability, stating that as much as **60%** of hacked small and medium-sized businesses go out of business after six months. (Source)

The above alerts and statistics clearly show the importance of conducting simulated E-Mail Phishing Attacks, and providing training to the workforce if they fail to recognize attacks.

Building Human Firewalls

Nowadays, networks and computers are configured with security features like firewalls, intrusion detection systems, automated patching, virus and malware software, etc.. Today it has become much harder to compromise networks and computers.

Organization invest so much each year in cyber threat security technologies but still fail to patch the most vulnerable element of all - the Human Operating System (HOS). Despite almost $80 billion spent globally on cyber security, attackers are still getting through organizational network defenses. In almost every publicized case of a breach or network / computer system intrusion, alerts and alarms did go off in the various network monitoring systems, but were ignored since they were buried among tens or hundreds of thousands of alerts.

Cyber intrusions are at an all time high, because many organization have ignored patching the HOS. As a result, the HOS is still stuck in the days of Windows 95. There is no human firewall turned on by default, and the human will click on any web link, or share data with anyone that asks.

KnowBe4 E-Mail Phishing Testing (Free For 100 Users)

Over the last few years, thousands of organization in the U.S have started to phish their own users. IT pros have realized that doing this is urgently needed as an additional security layer. Today, phishing your own users is just as important as having a firewall, antivirus and malware software.

The **FREE** test allows your organization to find out what percentage of your users are susceptible to e-mail phishing attacks. The number is usually much higher than you expect.

Please contact Insider Threat Defense to start your FREE test, and take your first step at protecting your data and networks from being compromised.

KnowBe4 E-Mail Phishing Testing - Cyber Threat Awareness Training Solution

- KnowBe4 offers one of the most cost effective, comprehensive and integrated platforms for simulated e-mail phishing attacks, combined with Cyber Threat Awareness Training.
- KnowBe4's highly effective scheduled E-Mail Phishing Security Tests keep your employees on their toes. Within the Admin Console you are able to schedule regular E-Mail Phishing Security Tests from our large library of known-to-work templates, or choose a template from the community templates section where you can also share phishing templates with your peers.
- KnowBe4's security awareness training specializes in making sure employees understand the mechanisms of e-mail spam, phishing, spear phishing, malware and social engineering. You get high quality web-based interactive training combined with common traps, live demonstration videos, short comprehension tests and scenario-based Danger Zone exercises. When it comes to rolling out training for your users, KnowBe4's Automated Training Campaigns do the heavy lifting for you.
- KnowBe4's robust reporting capabilities allow you to easily access user training completions, workforce phish-prone percentage, compliance reports and more.
- **Ransomware Guarantee**: KnowBe4 is so confident their security awareness training program works, they will pay your ransom if you get hit with ransomware while you are a customer. ($1,000 In Bitcoin)
- Pricing starts at under $20.00 per year, per individual. $20.00 per individual is nothing compared to the cost of a data breach, malware infection, ransomware attack, network downtime, lost productivity and revenue, etc. (Bulk Pricing Available)

Please contact Insider Threat Defense with questions regarding the KnowBe4 E-Mail Phishing Testing / Cyber Threat Awareness Training Solution.

Agent Surefire Insider Threat Investigation Game

Insider Threat Defense Becomes Authorized Dealer For Agent Surefire Insider Threat Investigation Games ™

Insider Threat Defense in partnership with MAVI Interactive is excited to announce state of the art training, skills validation and gaming for security professionals that are looking to reduce "Insider Threat Risks", that can be very costly and damaging.

Agent Surefire Insider Threat Investigation Game Overview

- The Agent Surefire Insider Threat Investigation Game is an immersive Information Assurance / Information Security training simulation (Point & Click), that will raise security professionals awareness on security best practices, and provide the knowledge to implement a defense-in-depth security posture in their organization.
- The game will allow individuals to get the "First Person Perspective" of being an Investigator / Incident Handler to identify and uncover threats and vulnerabilities.
- This unique real-world and interactive approach to training, will execute the "Insiders Playbook" of potential breach scenarios, and educate security professionals on how to find holes in your security defenses, before an Insider does.
- The game is designed to effortlessly bridge daily practices with the most common insider threats, cyber security threats and vulnerabilities. The engaging immersive content delivery allows learning by trial and error, situational awareness, immersed decision making, in a realistic work environment. This learning environment simulates a real-world security breach scenario and engages the trainee to uncover and neutralize the attack.
- This point-and-click adventure game delivers the training in about 1 to 6 hours. 1 hour will identify a minimum number of violations for a passing score. The trainee can continue to practice (For Up to 6 Hours - Practice Makes Perfect) on the exciting storyline, by engaging in the "Catch The Insider" scenario. This additional level of entertaining training increases interest in the subject matter, generating greater repetition resulting in better retention and broader awareness of more complex risks.
- Trainees take on the role of Agent Surefire to scrutinize the work environment, find and categorize security vulnerabilities, gather clues to figure out how the attack has been engineered. The engaging scenario, the multi-sensory experience with varying levels of critical thinking challenges create dozens of "aha!" moments that help the trainee connect with how dangerous insider threat and cyber threats can be.

Agent Sure Insider Threat Investigation Game - Threats and Vulnerabilities Covered

The training / simulation contains more than 120 discoverable cases of information security violations that are categorized under 12 main threat categories.

Agent Surefire Insider Threat Investigation Game - Video

- Office Cabinets And Drawers
- Security
- Improper Handling / Disposal Of Sensitive Documents
- Information Used In Social Engineering
- Using Predictable PINs
- Unauthorized Access
- Malware Infection
- Phishing Messages
- Instant Messaging Abuse
- Insider Abuse Of Internet Access
- Lost Laptop Or Portable Devices
- Theft of Personally Identifiable Information (PII)

Agent Sure Insider Threat Investigation Game Learning Objectives

- Develop Attention To Detail
- Identify And Distinguish Between Threats / Vulnerabilities / Weaknesses
- Develop Critical Thinking Skills & The Ability To Take Proactive Action
- Reduce The Theft Of Intellectual Property / Sensitive Information, Financial Damages, Legal Expenses

CompTlA Security+ Mapping

The Agent Surefire Insider Threat Game maps to the majority of the CompTIA Security+ Certification training content. CompTIA Security+ Domains; Systems Security, Network Infrastructure, Access Control, Assessments & Audits, Cryptography, Organizational Security.

Target Audience

U.S. Government Agencies (Department Of Defense Intelligence Community Agencies), Defense Contractors, Critical Infrastructure Providers, Banking-Financial, Aviation / Airline Security Professionals, large and small businesses.

Target Individuals

Chief Security Officers, Facilities Security Managers / Officers, Chief Information Security Officers, Information Systems Security Managers / Officers, Information Assurance Managers / Officers, IT / Network Security Administrators, Computer Security Incident Responders, Computer Security-Forensics Investigators, Etc.

Benefits

The Agent Surefire Insider Threat Game

- ✓ Is a new, fun and exciting way to promote Insider Threat Awareness.
- ✓ Transforms the learning experience into a rewarding and engaging process for discovering security vulnerabilities and identifying Insider Threats.
- ✓ Simulates high risk stakes and increased competition between participants.
- ✓ Can be used to test security professionals you maybe considering hiring, to evaluate their knowledge, skills and abilities in identifying Insider Threat risks.

Pricing

The Agent Surefire Insider Threat Game is sold on a per user, per game basis. Single Use License: $49.95. Quantity pricing available. (Post Game Insider Threat Risk Mitigation Guidance Provided)

Please contact Insider Threat Defense if you have any questions about the Agent Surefire Insider Threat Game, or if you would like to purchase the game.

National Insider Threat Special Interest Group ™

- The CEO of ITD is the Founder-Chairman of the National Insider Threat Special Interest Group (NITSIG). The NITSIG is a unique and specialized Information Sharing and Analysis Center, focused primarily on Insider Threat Risk Mitigation. The NITSIG Membership is the largest group of Insider Threat Risk Mitigation Security Professionals in the U.S. The NITSIG Board is comprised of Insider Threat Experts.

- The NITSIG provides Security, Education, Training and Awareness (SETA) to individuals (NITSIG Members) working for the U.S. Government, Department of Defense, Intelligence Community Agencies, Defense Contractors, Critical Infrastructure Providers, Banking-Financial Institutions, Aviation Security Professionals / Airports, large and small businesses and organization on; Insider Threat Program Development / Management, Employee Threat Indication And Mitigation, Insider Threat Awareness, Insider Threat Risk Mitigation and Workplace Violence - Active Shooter Response topics.

- The NITSIG provides NITSIG Members with access to a broad network of security professionals to collaborate with on Insider Threat Risk Mitigation.

NITSIG Meetings

The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland, Herndon, Virginia, and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend meetings. (More Info)

NITSIG Insider Threat Symposium And Expo (ITSE) ™

- The NITSIG announced that it will hold a 1 day ITSE on October 19, 2018, at the Johns Hopkins University - Applied Physics Laboratory, in Laurel, Maryland. There is **NO COST** to attend.
- The ITSE is exclusively focused on Insider Threat Program Development / Management, Employee Threat Indication And Mitigation, Insider Threat Awareness, and Insider Threat Risk Mitigation.
- The Symposium will include speakers who are Insider Threat Subject Matter Experts, that work for the U.S. Government, Intelligence Agencies, Defense Contractors and private sector businesses.
- The Symposium will provide attendees with access to a broad network of security professionals to collaborate with on Insider Threat Risk Mitigation.
- The Symposium will feature an Insider Threat Discussion Panel. The panel will be comprised of Insider Threat Subject Matter Experts who will provide attendees with useful information on developing, implementing and managing an Insider Threat Program, the hurdles, challenges, best practices and quick wins for Insider Threat Risk Mitigation.
- The Expo will include vendors that have proven technologies and services (Currently Used By The U.S. Government / Private Sector) for Insider Threat Detection; Insider Threat User Activity Monitoring-Behavioral Analytics Tools, Employee Continuous Monitoring and Reporting Services, Insider Threat Program Development Training / Management Services, etc.
- More Info

NITSIG Insider Threat Reports, Surveys & Incidents

The NITSIG maintains a repository of information related to Insider Threat Reports, Surveys & Incidents. Having a hard time convincing management that the "Insider Threat Problem" can be very damaging and costly to an organization? This is the place to look.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.htm

Insider Threats Incidents - Could These Happen To Your Organization?

This document complied by the NITSIG highlights some "Eye Opening-Insider Threat Incidents".

NITSIG Membership
There is **NO CHARGE** to join the NITSIG.

Once your NITSIG Membership Application is approved, you will be added to the e-mail distribution list and receive meeting announcements and other related information. (NITSIG Membership Application)

NITSIG Hotline
Have a question you need answered about Insider Threat Risk Mitigation? Contact the NITSIG Hotline via e-mail: hotline@nationalinsiderthreatsig.org or toll free #: 888-363-7241.

INSIDER THREAT DEFENSE

Your Trusted Partner For Insider Threat Risk Mitigation

Contact Information

As you can see from our catalog, Insider Threat Defense offers a broad portfolio of training and services to our potential clients.

Please give us a call. One of our Insider Threat Risk Mitigation Experts would be more then happy to answer any questions you may have.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense, Inc.
Insider Threat Program Development / Management Training Course Instructor
Insider Threat Vulnerability Assessor & Mitigation Specialist
Founder / Chairman Of The National Insider Threat Special Interest Group
FBI Maryland InfraGard Member
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us
www.nispomcc2training.com
james. henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org