INSIDER THREAT PROGRAM TRAINING COURSE
INSIDER THREAT RISK MITIGATION SERVICES

Insider Threat Defense

- Insider Threat Defense is currently assisting U.S. Government agencies, Defense Industrial Base contractors and businesses in mitigating the risks posed by malicious insiders, through Insider Threat Program Training and Insider Threat Risk Mitigation Services.
- Insider Threat Defense offers an Insider Instructor Led and Web Based Insider Threat Program Training Course. The Insider Threat Program Training Course was developed in accordance with Executive Order (EO) 13587, National Insider Threat Policy (NITP), NISPOM Conforming Change 2- Insider Threat Draft and other supporting regulations.
- The Insider Threat Program Training Course provides organizations with a proven and comprehensive Insider Threat Program Risk Management Framework for detecting and mitigating Insider Threats. The course goes beyond compliance with Insider Threat Program requirements, and is the reason Insider Threat Defense is fast becoming the leader in Insider Threat Program Training / Insider Threat Risk Mitigation Services.
- Insider Threat Defense is excited to announce that the following organizations / individuals have attended the Insider Threat Program (ITP) Training Course;

<table>
<thead>
<tr>
<th>Social Security Administration (6-2014)</th>
<th>US Army Enterprise NetOps (6-2014)</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Nuclear Security Administration (10-2014)</td>
<td>Marine Corps Intelligence Activity (8-2014)</td>
</tr>
<tr>
<td>FBI (1-2015)</td>
<td>White House National Security Council (10-2014)</td>
</tr>
<tr>
<td>Centers For Disease Control &amp; Prevention (3-2015), (6-2015)</td>
<td>Ernst &amp; Young (1-2015)</td>
</tr>
</tbody>
</table>

Insider Threat Defense Contact Info
Founder / Chairman Of The National Insider Threat Special Interest Group
Cyber Security -Insider Threat Program Training Course Instructor
Cyber Threat-Insider Threat Risk Analyst / Risk Mitigation Specialist
888-363-7241 / 561-809-6800
www.insiderthreatdefense.com
jimhenderson@insiderthreatdefense.com
INSIDER THREAT USER ACTIVITY MONITORING TOOLS
INSIDER THREAT BEHAVIORAL ANALYSIS TOOLS

Tanager, Inc. – Insider Threat Risk Mitigation Experts
Tanager is a Women Owned Small Business (WOSB) with core capabilities in Cyber Security and Insider Threat. Tanager provides insider threat mission support services to the IC, DOD, Federal agencies and the commercial sector. Tanager performs insider threat services in the following areas: Insider Threat program implementation; requirements analysis, risk assessments and gap analysis; identifying critical data sets for data correlation; insider threat IT solutions implementation; data analysis, inquiries and investigations; legal and HR privacy concerns; develop charter, SOP’s and CONOPS. NCIX Insider Threat Program of the Year award 2012; DIA Director’s Award 2010, 2012.

Tanager is a Valued Added Re-Seller (VAR) for the following) Insider Threat Detection-User Activity Monitoring Tools, and Insider Threat Analytics Tools. (Digital Guardian, Raytheon Sureview, SecuroniX and Red Owl Analytics.

www.tanagerinc.com

Digital Guardian - Insider Threat User Activity Monitoring / Data Loss Prevention Tool
Digital Guardian is security’s most advanced endpoint agent, providing transformative data visibility and control where you’re most vulnerable. It’s the only patented data protection platform trusted on millions of endpoints to secure against insider and outsider threats. And it’s been proven to run silently for the world’s top IP holders, with zero impact on even the most performance-sensitive devices.

www.digitalguardian.com

Raytheon Sureview - Insider Threat User Activity Monitoring Tool
Raytheon’s integrated solution can effectively help you monitor your entire enterprise ecosystem without disrupting business continuity. The policy platform pulls it all together and displays all enterprise activity in an intuitive visual dashboard. If a clear violation is detected, you can target specific events or individual users for investigation. Raytheon provides you all the details, insight, and complete context in the form of video replay to immediately assess the severity of the threat, fix the problem, and build the policies to prevent it from happening in the future.

www.raytheon.com/capabilities/products/sureview

SecuroniX - Insider Threat Behavioral Analysis Monitoring Tool
The SecuroniX solution is built to address these challenges by delivering these capabilities in an out-of-the-box solution that does not require a long-term data analytics and discovery project. Using purpose-built data mining, correlation, enrichment, and analytics, the SecuroniX solution detects not only users with high risk identity profiles but also high-risk activity, access, and events in your organization associated with insider threats. Simply put SecuroniX produces Insider Risk Intelligence. It does this by mining and analyzing a diverse set of user, system, application, security event, physical access, and even telephone activity to identify abnormal behavior associated with data theft/misuse, fraud, or IT sabotage. Beyond detection, SecuroniX performs continuous monitoring, scoring, reporting, and advanced investigative capabilities. The solution provides the advanced technology needed for a complete insider threat management program that leverages your existing security programs/investments.

www.securoniX.com/solution/insider-threat-detection

Red Owl Analytics - Insider Threat Behavioral Analysis Monitoring Tool
Using cutting edge inferential algorithms, social networking theory and easy-to-understand visualizations, RedOwl's Reveal software use today's enormous data trails to answer the same questions managers have been asking since the days of slide rules. Reveal turns the data trail into meaningful answers to plain language questions, providing the ultimate in digital situational awareness.

www.redowlanalytics.com
Symantec – User Activity Monitoring / Data Loss Prevention Tool
Discover, monitor, protect and manage your confidential data wherever it’s stored and used – across endpoints, mobile devices, network and storage systems - with the market-leading data loss prevention solution from Symantec.
www.symantec.com/data-loss-prevention

McAfee - User Activity Monitoring / Data Loss Prevention Tool
McAfee Total Protection for Data Loss Prevention (DLP) safeguards intellectual property and ensures compliance by protecting sensitive data wherever it lives — on premise, in the cloud, or at the endpoints. McAfee DLP is delivered through low-maintenance appliances (physical or virtual) and McAfee ePolicy Orchestrator (ePO) platform, for streamlined deployment, management, updates, and reports.

Spectorsoft - User Activity Monitoring Tool
Spector 360 is a comprehensive user activity monitoring solution that enables companies to log, retain, review and report on employee activity. Spector 360 creates a definitive record of an employee’s digital behavior, and in doing so provides organizations with the ability to see the context of user actions.
www.spectorsoft.com/solutions/insider-threats.html

Spectorsoft Contact Info
Kurt Abrahams
kabrahams@spectorsoft.com
561-209-1269

InterGuard - Insider Threat Protection In The Cloud
- Employee Monitoring - Monitor & control all computer activity, including both program and internet usage.
- Web Filtering - Monitor & control all internet activity, including social, email, IM and gaming websites.
- Data Loss Prevention - Prevent Data In Motion and Data At Rest leakage at the end-point.
- Laptop Theft Recovery - Prevent the loss of confidential information and valuable company resources.
www.interguardsoftware.com/jump_interguard.html

Microsoft Active Directory Rights Management Services (AD RMS)
- AD RMS can be used to augment the security strategy for your organization by protecting documents using information rights management (IRM).
- AD RMS allows individuals and administrators through IRM policies to specify access permissions to documents, workbooks, and presentations. This helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people. After permission for a file has been restricted by using IRM, the access and usage restrictions are enforced no matter where the information is, because the permission to a file is stored in the document file itself.
- AD RMS and IRM help individuals enforce their personal preferences concerning the transmission of personal or private information. They also help organizations enforce corporate policy governing the control and dissemination of confidential or proprietary information.
Insider Spyder - Insider Threat Behavioral Analysis Monitoring Tool

- Insider Spyder software looks at past and present actions to identify people who, while otherwise appearing to stay within their normal duties, are putting confidential information at risk.
- Based on a tested model, the software analyzes whether actions may represent possible security breaches. This stands in contrast to the normal approach in the marketplace: inflexible rules-based endpoint software which tries to flag specific activities that violate established organizational policy and makes it relatively easy for an insider to circumvent existing rules without detection.
- Our solution reduces the false positives inherent in competing approaches, achieving this with minimal impact on legitimate users. Insider Spyder is not a content analysis or Data Leakage Protection (DLP) tool and focuses instead on anomalies in user behavior.

www.insiderspyder.com/products.html

Insider Spyder Contact Information
Scott Gorvett
Office: 703-774-9000
scott.gorvett@insiderspyder.com

Personam - Insider Threat Behavioral Analysis Monitoring Tool

Personam has developed advanced technology to address the insider threat problem using the only viable means – behavioral analysis. Our technology monitors individual and device activity to build robust organizational and personal behavior models, and uses the insight to identify threats within an otherwise productive organization. Our methods are successful at identifying threats without undue breaches in employee privacy, leaving the important trust relationships intact.

www.personaminc.com

Personam Contact Info
John“Chris”Kauffman
Office: 571-297-9371 / Cell: 301-807-8022
ckaufman@personaminc.com

Interset - Insider Threat Behavioral Analysis Monitoring Tool

Statistically, human decision-making processes can be observed, measured, and even predicted if tracked according to each person’s unique decision-making patterns and risk-tolerance levels. The Interset E2A Engine uses sophisticated models to do exactly that. The solution identifies that a pattern of behavior has deviated from its norm, but also quantitatively measures the probability that an observed behavior is risky. User Anomalies Are Detected By:

- Comparing individuals, files and machines against their historic behavior.
- Determining like user patterns across the enterprise and comparing behavioral patterns between any two.
- Detecting dissimilar patterns between members of the same group or job role.
- Comparing individuals against the entire organization.

www.www.interset.com

Interset Contact Info
Mike Dilascio
Cell: 781-354-7663
mdilascio@interset.com
DeviceLock Endpoint DLP Suite

- DeviceLock Endpoint DLP provides port/device/printer/clipboard/printscreen controls, key logger protection, file shadowing, and enterprise DLP for “data-in-motion” and “data-in-use” on Windows endpoints. The Suite is comprised of DeviceLock core, ContentLock, NetworkLock, and the DeviceLock Search Server.

- DeviceLock Endpoint DLP is an Active Directory Group Policy MMC snap-in management solution and super-light architecture for quickly applying granular, contextual, and content-based controls for user access, activity auditing, data shadowing, event-based SMTP/SNMP alerting, and key-logger protection to prevent sensitive data leakage through peripheral ports, devices, printers, and network applications/protocols for both mobile and in-network endpoints.

- DeviceLock Discovery provides “data-at-rest” eDiscovery DLP for any Windows-based or SMB-based nodes on the network. Discovery provides a “point-and-shoot” server-based platform for eDiscovery, instant data remediation, and protection of sensitive data based on its content.

- DeviceLock for Mac provides port/device security, auditing, and file shadowing controls for the Apple OS Macintosh platform.

- Virtual DLP DeviceLock is the most advanced DLP solution for virtualized and hosted Windows and Macintosh OS systems using Citrix, VMWare, Microsoft, and other “terminal services” virtualization tools to solve data security issues in VDI, VPN, BYOD, and DaaS scenarios.

DeviceLock Contact Info
925-231-440
us.sales@devicelock.com
www.devicelock.com

PRIVILEGED USER ACTIVITY MONITORING TOOLS

Privileged User Session Auditing On Windows, Linux And UNIX Systems From Centrify

Privileged Session Manager For Servers From Cyber-Ark Software

Privileged User Monitoring - User Activity Video Reporter From Netwrix
www.netwrix.com/privileged_user_monitoring.html

ObserveIT Record And Replay All Remote User Sessions On Your Network Servers
www.observeit-sys.com

Xceedium Xsuite Privileged User Activiting Monitoring Tool
Xceedium Xsuite combines access control, privileged password management, and privileged user monitoring and session recording in an integrated platform that improves security and addresses auditor requirements. This integrated approach ensures you know who exactly is using privileged accounts, enables continuous monitoring of privileged sessions, and provides the mechanisms to automatically respond in real time.
www.xceedium.com/solutions/privileged-identity-management
NETWORK ANALYSIS TOOLS

Lancope’s Network Analysis Tool: StealthWatch
Lancope, Inc. is a leading provider of context-aware security for real-time insider threat detection, incident response and forensic investigations. As part of Cisco’s Cyber Threat Defense solution, Lancope’s StealthWatch System transforms the network into a virtual sensor grid for obtaining continuous network visibility and security intelligence to reduce enterprise risk. Armed with pervasive network insight, agencies can better protect against APTs, DDoS, zero-day malware and insider threats while assisting in compliance for HIPPA, FIPS, CDM, FISMA/NIST, NERC, PCI DSS, SCADA and SOX/COBIT. Lancope’s security capabilities are continuously enhanced with cutting-edge research from StealthWatch Labs.
For More Information, visit www.lancope.com

Lancope Contact Info
Randy Martin
Federal Account Manager
301-524-0068
rmartin@lancope.com

DATABASE SECURITY TOOLS

Oracle Database Vault
Oracle Database Vault reduces the risk of insider and outsider threats and addresses common compliance requirements by:
- Preventing privileged users (DBA) from accessing sensitive application data.
- Preventing compromised privileged users accounts from being used to steal sensitive data or make unauthorized changes to databases and applications.
- Providing strong controls inside the database over who can do what and controls over when and how applications, data and databases can be accessed.
- Providing privilege analysis for all users and applications inside the database to help achieve least privilege model and make the databases and applications more secure.

E-MAIL INBOX SEARCH TOOLS

Digiscope Search Tool For Microsoft Exchange Server
Digiscope's intuitive Microsoft Outlook-like interface allows you to Search, Export, or Recover Mailboxes, Folders, or Individual Items within an Exchange Offline EDB, PST file, or Live Production Exchange Server.
www.lucid8.com/product/digiscope.asp

Multi-Mailbox Search In Exchange Server 2010 (Could Enable Discovery Of Investigation)
DATA BREACH DISCOVERY TOOL
Tiversa - Peer To Peer Networks (P2P) / Data Loss Repository
Documents that have been found and are regularly found on P2P networks include; Tax Returns, Credit Reports, Confidential Business Documents, Classified Government Documents, WikiLeaks Documents, SF86 Questionnaire for National Security Positions, First Lady’s Safe House Location, Details On Presidential Motorcade, Strike Fighter Jet Data, Blueprints Of Obama's Marine One Helicopter, Medical Records / Health Care Data, etc.

Tiversa
• Tiversa monitors peer to peer file sharing networks for data that should not be there, but is.
• Tiversa provides P2P Intelligence and Security services to corporations, global law enforcement, government agencies, individuals and LifeLock Identity Theft.
• Tiversa monitors over 550 million users issuing 1.8 billion searches a day on P2P network in real time.
• Tiversa can locate exposed files, provide copies, determine file sources and assist in remediation and risk mitigation.

www.tiversa.com

Tiversa Contact Info
J. Andy Tormasi
Office: 724-940-9030
jtormasi@tiversa.com

STEGANOGRAPHY DETECTION TOOL
StegAlyzerRTS - Steganography Analyzer Real-Time Scanner
• Sensitive data leakage is of utmost concern to corporate management. Data Loss Prevention (DLP) solution providers offer products with a wide range of functionality and capability. However, none of these products detect insider use of steganography.
• StegAlyzerRTS is the world’s first commercially available network security appliance capable of detecting digital steganography applications and the use of those applications in real-time. StegAlyzerRTS offers a “drop-in, turn-key” capability that will not affect network throughput.
• StegAlyzerRTS detects insiders downloading steganography applications by comparing the file fingerprints, or hash values, to a database of known file, or artifact, hash values associated with over 1,225 steganography applications.
• StegAlyzerRTS also detects insider use of steganography applications by scanning files entering and leaving the network for known signatures of over 55 steganography applications. StegAlyzerRTS detects insider theft of sensitive information hidden inside other seemingly innocuous files which are sent to an external recipient as an e-mail attachment or posted on a publicly accessible web site.

www.sarc-wv.com/products/stegalyzerrts/learn_more.aspx

Steganography Analysis & Research Center Contact Info
Chad Davis
chad.davis@backbonesecurity.com
877-560-7272
E-MAIL / WEB CONTENT FILTERING TOOLS
Barracuda offers a wide variety of security tools. (E-Mail Content Filtering, Web Content Filtering, Web Application Security, Firewall, VPN, etc.
[www.barracuda.com/products/emailsecurityservice](http://www.barracuda.com/products/emailsecurityservice)

Barracuda Contact Info
Steve Gehris
Office: 610-384-6823
Cell: 484-437-4700
sgehris@barracuda.com

Clearswift Secure E-Mail Gateway
[www.mimesweeper.com/products/clearswift-secure-email-gateway](http://www.mimesweeper.com/products/clearswift-secure-email-gateway)

SECURITY EVENT INFORMATION MANAGER (SEIM) TOOLS

Splunk SEIM Tool
- Splunk Enterprise makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results.
- By monitoring and analyzing everything from customer clickstreams and transactions to security events and network activity, Splunk Enterprise helps you gain valuable Operational Intelligence from your machine-generated data.
- And with a full range of powerful search, visualization and pre-packaged content for use-cases, any user can quickly discover and share insights. Just point your raw data at Splunk Enterprise and start analyzing your world.

Splunk Contact Info
703-206-6400
gov@splunk.com

QRadar SEIM Tool
IBM QRadar Security Intelligence Platform products deliver:
- A single architecture for analyzing log, flow, vulnerability, user and asset data.
- Near real-time correlation and behavioral anomaly detection to identify high-risk threats.
- High-priority incident detection among billions of data points.
- Full visibility into network, application and user activity.
- Automated regulatory compliance with collection, correlation and reporting capabilities.

ArcSight SEIM Tool
The ArcSight Insider Threat package offers integrated case management that includes case-specific features for collaboration, incident annotation, real-time dashboards and reports. This allows you to effectively and efficiently limit the information users can access. Also included is an integrated knowledge base that can house contact information, policies, procedures and other pertinent information that is necessary when investigating insiders. The entire process from detection through response, and the general management of the incident is audited. This audit information can be made available in a report to outline the chronology of the investigation.
INSIDER THREAT DATA ANALYSIS TOOLS

Palantir Technologies – Insider Threat Data Analysis Tool
- With Palantir, you can protect your organization’s sensitive information and intellectual property from theft, misuse, and abuse. Whether employees are maliciously exfiltrating data or unintentionally violating data use policies, our technology allows you to proactively and efficiently identify and respond to threats.
- With Palantir's data integration capabilities you get a holistic view of employee behavior. Palantir can incorporate data commonly used for information security, including email records, web access, removable media, travel records, badge reader logs, VPN logins, alert streams from traditional data loss prevention (DLP) products, and more, alongside employee activity from proprietary databases, trading systems, customer relationship management (CRM) tools, and other core business data sources.
- Your existing investments in data required for regulatory compliance or corporate retention policies can now be used to strengthen defenses against insider threats.

www.palantir.com/solutions/insider-threat

EMPLOYEE BACKGROUND CHECKS – CONTINUOUS EVALUATION SERVICES

Experian Public Sector Services
Experian Public Sector is a trusted provider of superior data and analytics that enable government agencies to make the right decisions. Experian’s extensive data assets, unique analytical offerings, and proven track record of adhering to the highest standards in data security and regulatory compliance allow agencies to make mission-critical decisions in a timely and cost-effective manner.

Eligibility Assurance Framework
- Protect the integrity of your program and grant access of benefits to only those individuals who truly qualify. Experian’s Eligibility Assurance Framework offers government agencies decisioning support across the entire eligibility life cycle.
- Designed with the utmost flexibility in its components, the product supports a full range of agency needs: Verify: Leverage vast data sources to validate applicant information upon system entry.


Experian Public Sector Services Contact Info
Neli Coleman
Director, Product Management - Public
Sector Office: 703-765-0355
neli.coleman@experian.com

TLOXP - Investigative And Risk Management Tool
TLOxp is used by the largest global corporations, major financial institutions, insurance carriers and tens of thousands of law enforcement agencies to investigate and research people, locations and companies for due diligence, risk assessment, fraud detection, identity authentication and more.

People Search Tool
Names, Addresses, Aliases, SSN'S, Bankruptcies, Foreclosures, Liens, Judgments, Criminal History, Phone Numbers, Relatives, Neighbors, Associates Assets Including Property, Vehicles and more.

TLOXP Contact Info
Scott Kiersten
Transunion Specialized Risk
Division Phone: 561-226-9662
skierst@TransUnion.com
**Thomas Reuters Special Services (TRSS)**
TRSS delivers a comprehensive portfolio of Threat Intelligence Solutions that help our clients with strategic initiatives focused on:
- Continuous Monitoring and Evaluation of Security Clearance Holders
- Insider Threat Detection
- Threat Analysis


Please contact me with any suggestions to be added to this list.

**Jim Henderson, CISSP, CCISO**
Founder / Chairman Of The National Insider Threat Special Interest Group
Counterespionage-Insider Threat Program Training Course Instructor
Cyber Security-Information System Security Program Management Training Course Instructor
Cyber Threat-Insider Threat Risk Analyst / Risk Mitigation Specialist
888-363-7241 / 561-809-6800
Connect With Me On LinkedIn:
[www.linkedin.com/in/isspm](http://www.linkedin.com/in/isspm)

**Websites / E-Mail Addresses:**
[www.insiderthreatdefense.com](http://www.insiderthreatdefense.com)
[jimhenderson@insiderthreatdefense.com](mailto:jimhenderson@insiderthreatdefense.com)
[www.nationalinsiderthreatsig.org](http://www.nationalinsiderthreatsig.org)
[jimhenderson@nationalinsiderthreatsig.org](mailto:jimhenderson@nationalinsiderthreatsig.org)

Lasted Updated: 3-23-15