National Insider Threat Special Interest Group (NITSIG)

Insider Threat Information Sharing & Analysis Center

Insider Threat Detection For Computer Systems / Networks

NITSIG PROPRIETARY INFORMATION - NOT FOR PUBLIC RELEASE

Background On
Insider Threat Detection Tools Workshop

On June 5, 2019, the National Insider Threat Special Interest Group (NITSIG), in partnership with the University of Maryland's Applied Research Laboratory for Intelligence and Security (ARLIS) held a workshop on Insider Threat Detection Tools (ITDT'S). This is the first of a series of workshops to be held on this subject.

The workshop was held at the Johns Hopkins University - Applied Physics Laboratory, in Laurel, Maryland.

The idea behind the workshop was driven from inputs from Insider Threat Defense Group clients and NITSIG Members.

Recurring Questions & Concerns Were;

- How Does My Organization Detect Insider Threats On Computer Systems / Networks?
- Can I Use Existing Network Security / Open Source Tools?
- What Is The Best ITDT To Purchase?
- How Do I Evaluate ITDT'S?
- What Are The Pro's / Con's Of Operational ITDT'S

The NITSIG did extensive research before holding this workshop, and spoke with a large number of Insider Threat Program (ITP) Managers. The consensus was that vendors seem to be telling organizations what they need, why they need their tool, and why their tool is the best.

ITP Managers stated that more in-depth (Unbiased) education is needed on evaluating ITDT'S, but agreed that this education will not likely come from the vendors.

Workshop Attendees

15 individuals from the Insider Threat Community (U.S. Government / Private Sector) attended the workshop and contributed to the consensus of the set of key challenges related to Insider Threat Detection (IDT) and ITDT'S.

All attendees have a role in managing or supporting ITP's, have served as an Insider Threat Analyst of ITDT output, or have experience in some combination of these functions. Participants represented U.S. government agencies and the private sector businesses.

There is no attribution of contributions to individual participants or to the agencies / organizations they represent. The output from workshop attendees is based on their **real world experiences** related to the procurement and use of ITDT'S.

Vendors were excluded from the workshop. This allowed open discussion of user experiences with their current ITD capabilities and vendor purchased ITDT’S.

The workshop was intended to go beyond traditional evaluation methods from Gartner, Forrester Research and other organizations that produce high level expensive reports that must be purchased.

The NITSIG is not aware of any extensive in-depth method / bake off / lab testing of the current ITDT’S on the market. (ITDT’S Consumer Reports, ITDT’S Expo)

A report was written by the UMD ARLIS capturing the outputs from the workshop. These outputs greatly contributed to this presentation.

ITDT'S
Behind The Marketing / Sales Pitches

DoD PERSEREC 2018 Report - A Strategic Plan To Leverage The Social & Behavioral Sciences To Counter the Insider Threat

Insider Threat Detection Tools: High Price Tags / Steep Learning Curves (Page 14)

The sheer size of the past and present DoD workforce, along with the mandate to monitor all activity on classified networks, has motivated a number of technological innovations.

Today's user activity monitoring (UAM) and user entity behavioral analytics (UEBA) products can: ingest multiple data sets, to include free text; automatically anonymize data and link datasets; baseline behavior against individual and peer group norms; identify anomalies; assign risk scores; and present actionable results on easy-to-navigate dashboards. Faster processing times and cheaper storage enable agencies to simultaneously gather, organize, and analyze disparate data sets and respond to potential threats in near real-time.

Key Findings

1) UAM and UEBA tools are expensive, and critics have begun to ask whether the value-add sufficiently exceeds the price tag, especially when these tools have steep learning curves.

2) According to several SMEs, many tools were not designed with end-users in mind (Analyst), cannot be quickly deployed "out of the box", and / or require maintenance that causes lengthy outages.

3) In the absence of comprehensive and free market surveys, consumers have begun to educate themselves on open source solutions that could meet their needs without the corresponding high cost.

Source:
www.dhra.mil/Portals/52/Documents/perserec/reports/TR-18-16-Strategic-Plan.pdf

U.S. Government Agency:

- Purchased tool, never deployed it.

Hospital:

- Did not define real world use cases for hospital, before purchasing tool. Used general use cases.
- Tool not detecting policy violations, observed / actual indicators of concern.
- May need to purchase additional software to import / ingest additional data from other sources.
- May need to purchase additional vendor support to tweak tool.

Bank:

- Purchased tool because CISO used to work for tool company.
- Tool is Insider Threat Analyst's dream, Network Engineer's nightmare.
- Discounted use of tool. Now using another tool.

Healthcare Organization #1:

- Purchased tool. Found out it was venture capital funded by China. Discontinued use of tool.

Vendor Problems / Concerns

- Vendor moving tool to cloud. Customer loosing features they liked / used
- Vendor tool software development done outside of U.S. (Source Code Review)
- Marketing hype using Insider Threat Surveys (We Know There Is A Problem)
- We detect and mitigate Insider Threats (What Activities?)
- Not giving real world examples of what your tool can detect (Case Studies)
- Once tool is purchased, licensing terms subject to change
- Some tool pricing is based off of volume of data used-analyzed. If additional data is imported (From Other Tools) into tool, costs will increase
- Vendor Award claims (Just An Award Vs. In-depth Tool Evaluation)
- Vendor professional services for support can cost $50,000+ year

Or

Hire a Data Scientist and build your own tool from scratch, or contract for services. (You’re In Control)

Key Workshop Findings
Major Issues Related To ITD / ITDT'S

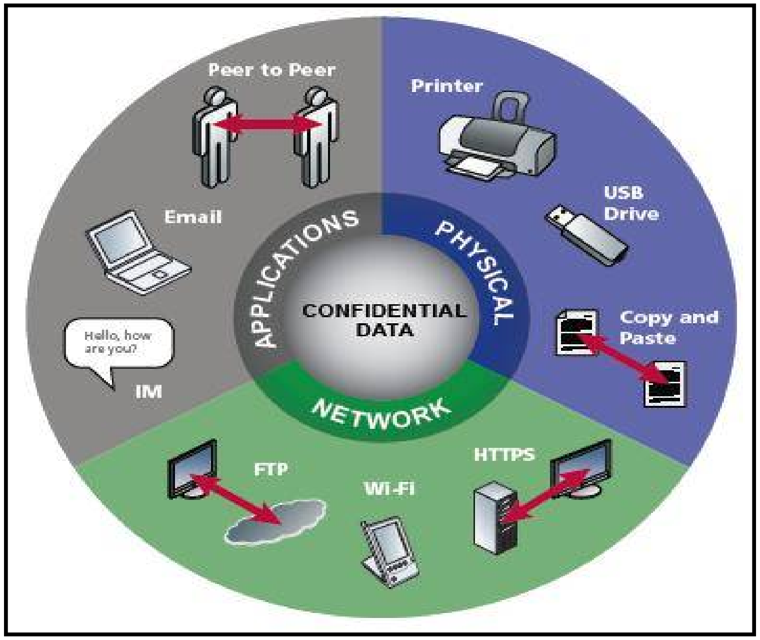
Conducting A Data Inventory
What data is stored on the organizations computers, networks, mobile devices? (Crown Jewels)

Defining The Organizations Requirements For Employee Monitoring
This is the first step that is **extremely important** before evaluating or purchasing an ITDT.

Example Use Cases (Is Tool Pre-Configured With Use Cases?)

- ☐ Employee Performance / Productivity
- ☐ Employee Time Fraud (Raytheon: Employee Pleads Guilty To Illegally Retaining Classified Information)
- ☐ Employee Satisfaction (Disgruntled After Negative Performance Review)
- ☐ Employee Flight Risk (Job Searching, Job Jumping)
- ☐ Management Problems (Treatment Of Employees)
- ☐ 13 Adjudicative Guidelines For Security Clearance Holders
- ☐ Separation From Employer (Resigned, Terminated, Mass Layoffs)
- ☐ Careless / Malicious Employees (Violations Of Security Policies, USB Devices, Cloud Storage, E-Mail /Web Mail Usage, Internet Usage, Etc.)

- ☐ Data Access / Usage, Data Theft / Exfiltration
  - o Computer / Network
  - o Remote Access / Activities
  - o Database Access / Activities
  - o Mobile Devices (Storage, Usage)
- ☐ Sentiment / Keyword Analysis Of Text For E-Mail / Instant Messaging (Keyword Lists)
- ☐ Unauthorized Use / Installation Of Software Applications (Self Running – No Install Required Applications: Steganography, Remote Access, Etc.)
- ☐ Compromised Employee Network Credentials
- ☐ Monitoring Activities Of Privileged Users (Network / IT Staff)
- ☐ Computer & Network Sabotage / Data Destruction
- ☐ Cyber Criminal – Insider Threat Collusion
- ☐ Dark Web Research / Use (Onion Router / Tor)
- ☐ Workplace Safety / Workplace Violence
- ☐ Criminal Activities



Computer - Network Activities
Indicators Of Concern

- ☐ Login / Logoff Of User Accounts (General & Privileged Users)
- ☐ File Events (Computer / Network Access - Add, Copy, Move, Modify, Rename, Delete)
- ☐ File Activity / High Volume Copying Of Files From Network To Computer
- ☐ USB / DVD-CD Usage
- ☐ E- Mail / Web Mail Usage
- ☐ Network Print Events (Large Print Jobs)
- ☐ Printing To Local Printer (Bypass Network Printer Monitoring)
- ☐ Software Application Usage (To Include Installs, Self Running Executables)
- ☐ Operating System Changes (Processes, Services)
- ☐ Network Bandwidth Usage (Large File Transfers)
- ☐ Internet Usage (Websites Visited, Searches, Uploads, Downloads, Social Networking Usage, Cloud Storage, Etc.)
- ☐ Web Browser Plug-Ins (Screen Sharing, VPN, Etc.)
- ☐ Web Browser Incognito / Private Browsing Mode
- ☐ VPN / FTP Usage
- ☐ Use Of Virtual Machines (File Uploads)
- ☐ Facebook Messenger, Go To Meeting, Skype (File Uploads)
- ☐ Local Network Use Vs. Wifi Access (Mobile Hotspot Use For Data Exfil.)

Other Items Of Concern

- ☐ Using Web File Sharing Services To Upload Large Files (Bypass N/W Security Tools)
- ☐ Copier Usage / Fax Usage
- ☐ Multi-Function Device Usage (Printer, Fax, E-Mail, Scan)
- ☐ Charging Cell Phones / MP3 Players W/ Computer (Use As Storage Device)
- ☐ Phone PBX Systems
- ☐ Facility Access Systems

ITDT Vendors Use Various Names When Marketing Their Tools

- ☐ User Activity Monitoring (UAM)
- ☐ User Entity Behavior Analytics (UEBA)
- ☐ User Behavioral Analytical (UBA)
- ☐ Data Loss Prevention (DLP)
- ☐ Digital Rights Management (DRM)
- ☐ Network Endpoint Protection (NEP)
- ☐ Security Information Event Management (SEIM)
- ☐ Privileged Access Management (PAM)
- ☐ Etc.

Which ITDT Tool Address Insider Threats The Best? - Not An Easy Answer

- ☐ How does your organization define Insider Threat? (Going Beyond NITP, NCC2 Regulations) The definition can be different for each organization.
- ☐ What behaviors / activities are you trying to detect / mitigate? (Define Your Requirements Before Beginning Evaluations Of ITDT'S)
- ☐ Do any of your existing network security tools meet some of your requirements? (Conduct Network Security Tool(s) Inventory)

Understanding Various ITDT'S Capabilities

What Does The Organization Want The ITDT To Do?

- ☐ Report On Observed Behaviors / Activities (Policy Violations)
- ☐ Report On Deviations Of Normal Behaviors / Activities
- ☐ Report On Predictive Behaviors / Activities
- ☐ Prevent / Block Activities Of Concerns (Data Exfil)
- ☐ Be Interactive (Display Warning Message To Employees)
- ☐ Employee Threat Risk Scoring
- ☐ Keystroke Logging
- ☐ Video Recording Of Employee Activities On Computer

Advanced Features

- ☐ Import / Use Of External Data Sources (TransUnion, TR-Clear, Etx.)
- ☐ Machine Learning / Artificial Intelligence

What Tool Capabilities Are Need For Your Organization?

Don't Purchase Tool Just Based On External CIO / ITPM Recommendations

ITDT Evaluation Concerns

ITDT Compatibility Problems

- ☐ Interoperability With Operating Systems, Software Applications, Network Security Tools
- ☐ ITDT'S Agent Installed On Computers
- ☐ Test & Evaluation Of ITDT'S Before Purchasing (Try Before Buy – Pilot)

ITDT Management

- ☐ Role Based Access (Administrator (Full Control), Insider Threat Analyst)
- ☐ Data Anonymization (Hide Identity Of Individual Being Monitored)

ITDT User Interface

- ☐ Ease Of Use, Learning Curve, Training Required (Training Provided / Costs)

ITDT Installation, Configuration, Deployment

- ☐ Scalability (# Of Computers / Networks)
- ☐ Bandwidth Requirements / Usage
- ☐ Endpoint Data Throttling To Server
- ☐ Silent Agent Install (Agent Hidden From Operating System)
- ☐ Installation: Plug & Play (Plug & Pray), Ease Of Configuration / Customization (Vendor Help Provided? / Costs?)
- ☐ Default Rule Sets / Custom Rule Sets (Vendor Support Creating? / Costs?)

Integration / Interoperability With Other Network Security Tools

- ☐ Importing Of Data Supported From Other Network Security Tools (Additional Plug-in Costs?)
- ☐ Data Mining, Correlation, Analysis
- ☐ External Data Ingestion (Badge Systems, Human Resources, Public Data Endera, TransUnion, Etc))

ITDT Data Storage

- ☐ Organization Data Storage Retention Requirements (How Many Years?)
- ☐ Data Retention Access (Real Time, Cold Storage)
- ☐ On Site Or Vendor Cloud
- ☐ Data Ownership (Organization, Vendor)
- ☐ Charges From Vendor Based On Amount Of Data Collected (Cost?)
- ☐ Type Of Database Required For Storage (Cost?)
- ☐ Database Storage Requirements

Detection, Prevention & Alerting / Reporting

- ☐ Managing / Analyzing The Extensive Amounts Of Data Generated by ITDT'S.
- ☐ Event / Alert Overload Problems With ITDT Server
- ☐ # Of Insider Threat Analysts Required

ITDT Support For

- ☐ Operating Systems
- ☐ Desktop
- ☐ Laptops
- ☐ Smart Phones
- ☐ Tablets
- ☐ Virtual Machines

Purchasing Questions / Licensing Options

- ☐ License Per User / Per Endpoint
- ☐ Perpetual License (One Time Charge / Indefinite Use, Cost Upgrades?)
- ☐ Subscription (Commitment?)
- ☐ Hardware Requirements (Who Supplies?)

ITDT Installation / Support / Upgrades

- ☐ Can The Organization Provide IT Support For Problems With Tool?
- ☐ Vendor Provided Support (Costs?)
  - o Installation
  - o On-Site Support / Troubleshooting
  - o Web Based / Remote Access Support
  - o Telephone Support
  - o E-Mail Support

Vendor support to the tool and teaching the company techs is critical when there is a problem with the tool.

When a tool has issues it can affect hundreds or thousands of systems at once, causing a massive denial of service condition or work stoppage.

Company Information

- ☐ U.S. Based Company
- ☐ Defense Contractors FOCI Concerns (Foreign Ownership, Control / Influence)
- ☐ # Years In Business
- ☐ Venture Capital Funded
- ☐ Acquisition Of Other Vendor Tools / Integration Into Existing Tool
- ☐ Acquisition Potential Or Pending By Another Company (ObserveIT-Proofpoint)
- ☐ Product Development (In House / Outsourced Outside U.S.)
- ☐ NIST / FIPS / FISMA / FEDRAMP Accreditation
- ☐ Current Customer Base
- ☐ Customer References Available

There are several ITDT's available that are under active development by companies in countries hostile to U.S. interests.

These tools are a perfect in-road to a company's crown jewels and spotting assessing personnel for later recruitment.

UMD ARLIS ITDT Workshop Summary

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

- Identifying a suitable Insider Threat Detection Tool (ITDT) is an overarching problem. More education is needed. Vendors need to understand an organizations detection and mitigation requirements first.

- Incompatibility issues with an ITDT and computer systems, other software applications and networks. (Endpoint Agent Requirement)

- ITDT manpower requirements and costs associated with an ITDT can be very high.

- Insider Threat detection capability gaps exist with some tools, because specialized triggers need to be configured, which may require internal IT or vendor support.

- An ITDT can produce an extremely high number of events, causing data analysis overload.

- The problem with risk ranking and false positives. Feels like you are playing "Whack A Mole".

- The lack of integration of employee data sources such as Human Resources data and other important data sources such as Access Control Systems.

- The problem of focusing on actual employee policy violations vs. behavioral predictions.

Questions ?

Contact Information

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