



National Insider Threat Special Interest Group (NITSIG)

Using External Data Sources For Insider Threat Detection & Mitigation



External Data Sources

Gathering and analyzing **Internal** data sources is very important for Insider Threat detection and mitigation.

Equally important is knowing what **External** data sources are also available to create the **Big Picture** of an employee who may pose a threat to a company.

Most companies currently perform background screening on employees **Once** at the **Pre-Hire Stage**. This screening is a **Point In Time Snapshot**.

According to Gartner, 80% of Insider Threats can be stopped by monitoring employees' pressures and behaviors outside of work. Unfortunately, most organizations lack the capability and resources to effectively take on such a massive undertaking.

To be more proactive in detecting and mitigating Insider Threats, many companies are using **Post-Hire** solutions that allow the employer to **Continuously Monitor** an employee for **Indicators of Concern**.

These solutions can monitor **External** data sources of criminal and civil information, then **Alert** a company about an employee who has problems (Criminal, Financial) outside of work.

Examples Of External Data Sources



CRIMINAL RECORDS

- Wants & Warrants
- Booking & Arrests
- Criminal History
- Sex Offender Registrations



FINANCIAL ACTIVITY

- Bankruptcy & Foreclosures
- Liens & Judgements
- Lawsuits
- Large Purchases



LICENSES & PERMITS

- Professional Licenses
- Driver's Licenses
- Healthcare Licenses
- Expirations



SANCTIONS

- Healthcare Sanctions
- OFAC Sanctions
- Terrorist Watch Lists
- Criminal Watch Lists

Source

13 Personnel Security Adjudicative Guidelines For Security Clearance Holders

Adjudicative Guidelines

Allegiance to the US

Foreign influence

Foreign preference

Sexual behavior

Personal conduct

Financial considerations

Alcohol consumption

Drug involvement

Emotional, mental, personality disorders

Criminal conduct

Security violations

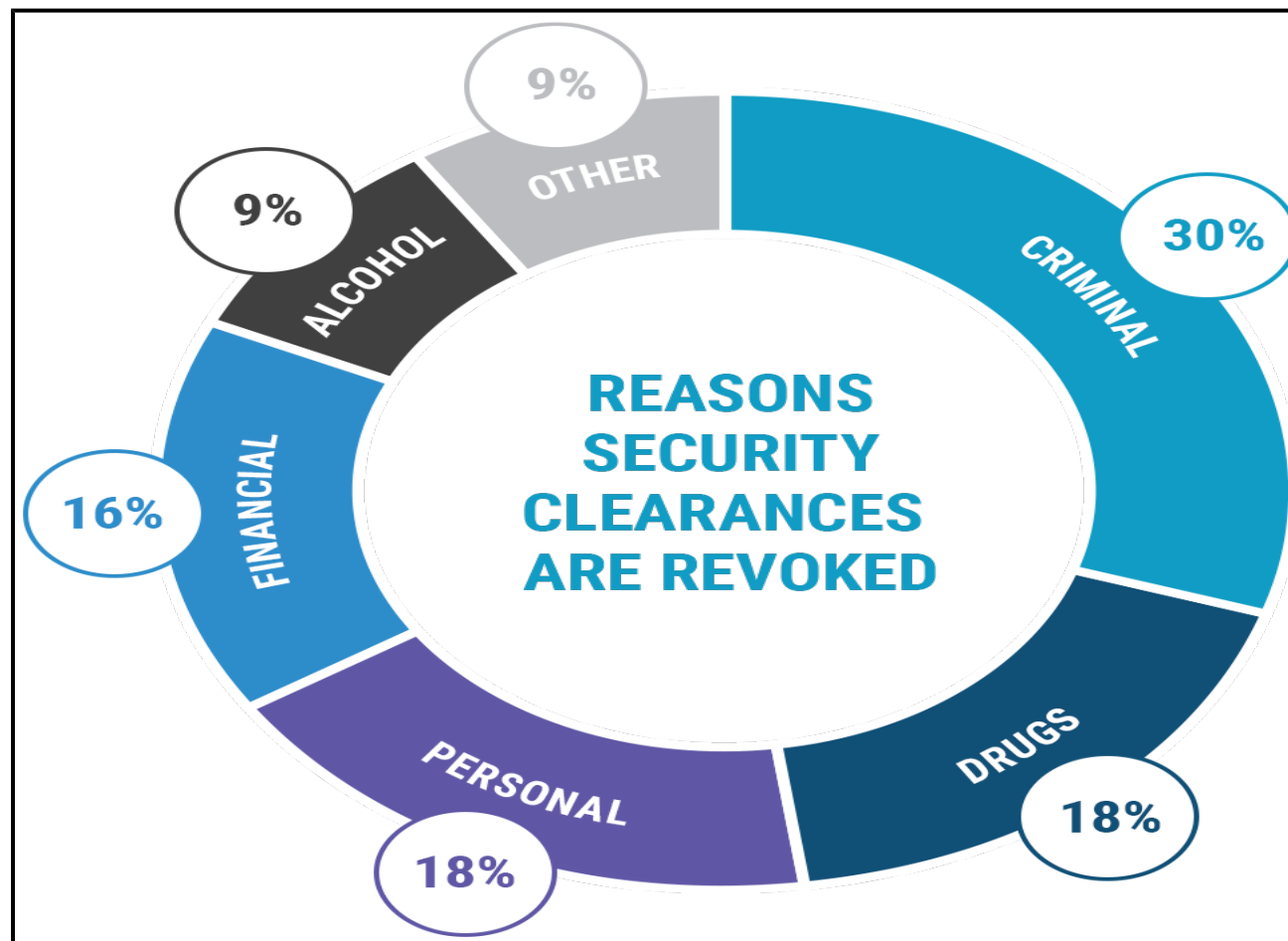
Outside activities

Misuse of IT systems

Why Are Security Clearances Revoked?

In 2013, the Government Accounting Office conducted an in-depth analysis of all people with security clearances. It's hard to imagine a more reputable and better vetted population of people.

The report summarizes all the reasons that security clearances had been revoked. **In more than 90% of the cases, issues typically originated outside of the work environment.**



Employee Continuous Monitoring & Reporting Examples

Example #1:

- ❑ **Enrolled 60,000 Employees** (Global Airline)
- ❑ Monitored Thousand Of Data Sources
- ❑ Detected 11,000 Events In 120 Days
- ❑ 1,771 Events Were Defined As Critical
- ❑ **55 Bookings And Arrest Alerts**

[Source](#)



ALERTS

BOOKINGS/ARRESTS

- Felony theft
- Burglary, intent to commit a felony
- Drug possession, intent to distribute
- False imprisonment
- Second degree assault
- Criminal damage to property
- Receiving stolen property
- Assault and battery
- Simple battery to a child/ cruelty to children
- Felony domestic assault by strangulation
- Failure to appear

CRIMINAL CHARGES

- Criminal felony, rape, assault
- Theft, burglary
- Property crimes
- Drug violation, DUI
- Felony narcotics possession
- False impersonation, forgery

DEATH RECORDS

- 14 recorded deaths

Employee Continuous Monitoring & Reporting Examples

Example #2:

- ❑ **Enrolled 30,000 Employees** (U.S. Government Secure Workers Program For Critical Infrastructure)
- ❑ Workers are responsible for maintaining critical infrastructure and regional facilities, such as airports, rail and bus terminals, bridges and tunnels.
- ❑ Monitored Thousand Of Data Sources
- ❑ Detected 800 Events In 90 Days
- ❑ **Disqualified 24 Employee From Their Jobs**

Example #2 disqualifications were related to Department of Homeland Security and Transportation Administration lists of Disqualifying Criminal Offenses.

[Source](#)



Example #2 Events Detected

Count	Alert Category	Location	Alert Description
1	Bookings/Arrest	Waynes County, NY	Criminal possession, with intent to sell 10 pounds of marijuana
1	Booking/Arrest	Orange County, NY	Drug related, intent to sell
1	Booking/Arrest	Orange County, NY	Unknown offense
1	Booking/Arrest	Loudon County, VA	Unknown offense
1	Booking/Arrest	Alaska Department of Corrections	Felony DUI
1	Criminal-State	Passaic County, NJ	Aggravated manslaughter
1	Criminal-State	Passaic County, NJ	Assault by auto/vessel
1	Criminal-State	Burlington County, NJ	Endanger welfare of a child
1	Criminal-State	Morris, NJ	Possession controlled substance, 3 rd degree
1	Criminal-State	Nassau County, NY	Criminal possession of stolen property
1	Criminal-State	Kings County, NY	Criminal possession of controlled substance
1	Criminal-State	Kings County, NY	Criminal possession of a weapon
1	Criminal-State	Kings County, NY	Robbery 2 nd degree
1	Criminal-State	NY, NY	Assault 1 st degree
1	Criminal-State	Connecticut	Injury/risk of injury to minor – sexual nature
1	Criminal-State	Missouri	Felony possession of controlled substance
1	Criminal-State	Montgomery County, PA	Receiving stolen property
1	Criminal-State	Lancaster County, PA	Receiving stolen property
1	Criminal-State	Essex County, NJ	Endangered welfare of a child; photo sexual act
9	Recorded Death	N/A	Death
2	Sanctions	NJ, Dept. of Labor and Workforce Development	Prohibition from working on NJ Government Contracts
2	Sanctions	NY, Dept. of Treasury	Prohibition from working on NJ Government Contracts
1	Sanctions	PA, Dept. of Human Services	Office of Medical Assistance Program, Medichex List
4	Sex Offender	NY, Division of Criminal Justice	Multiple sexual offenses

Workplace Violence Incident

Jury Awards Over \$1 Million In Negligent Hiring Lawsuit Involving Workplace Violence - November 15, 2016

A jury in Texas has awarded more than \$1 million in a negligent hiring lawsuit filed against a company on behalf of an employee and war hero who was killed in 2015, while on the job, by a co-worker.

Steven Damien Young shot and killed co-worker Jacob Matthew Cadriel with a 38-caliber handgun. Young was arrested and charged with murder. He is currently serving a 45 year sentence.

In 2008, Young was “arrested, charged and convicted in Harris County of the offense of carrying an illegal weapon on the jobsite.” In 2014, he was “arrested and charged in Harris County with the offense of making a terroristic threat.” He was out on bond awaiting trial when he murdered Cadriel.

The negligent hiring lawsuit claimed that Woven Metal Products, who owned the facility where both Young and Cadriel worked, failed to “conduct comprehensive employment background checks and criminal record searches on their employees. This negligence provided an unsafe workplace for employees.

The company was negligent because it “failed listen to numerous workers at the facility who repeatedly told them about the erratic and unstable behavior of Young” and also “failed to provide any training or education on identifying and handling this type of violence behavior in the workplace.” ([Source](#))

Internal / External Data Sources

An organization that only gathers and reviews **Internal** data sources, may not get the complete picture on an employee who may pose a threat to the company.

Combining **Internal** and **External** data sources is the best method to get a more accurate and timely / more current risk profile of an employee.



Employee Continuous Monitoring & Reporting / Investigation Solutions

Transunion

www.transunion.com/solution/threat-monitoring-solutions

Clearforce

www.clearforce.com

Endera

www.endera.com

Thomson Reuters

www.legal.thomsonreuters.com/en/products/clear-investigation-software

Lexis Nexis

www.risk.lexisnexis.com

IDI Core

www.ididata.com

Contact Info

Jim Henderson, CISSP, CCISO

CEO Insider Threat Defense

Insider Threat Program Development Training Course Instructor

Insider Threat Vulnerability Assessor & Mitigation Specialist

Founder / Chairman Of The National Insider Threat Special Interest Group

888-363-7241 / 561-809-6800

www.insiderthreatdefense.com

jimhenderson@insiderthreatdefense.com

www.nationalinsiderthreatsig.org

jimhenderson@nationalinsiderthreatsig.org