



Intellinx

Get Proactive about Insider Threat (Case Study)

DELJIS The Delaware Criminal Justice System Keeping Sensitive Information Protected from Misuse by Authorised Users

Introduction

Delaware was the first US state to implement an integrated Criminal Justice Information System ICJIS that supports electronic sharing of criminal justice information within the criminal justice community. While the Delaware CJIS has been in existence since 1990, it is constantly changing to meet the needs of system participants - State and local police, the Attorney General's Office, the Public Defender's Office, the Courts, and the Department of Corrections.

CJIS facilitates the electronic sharing of information among all participating agencies. Specifically, case information, from initial contact to case-closing events, is available to CJIS participants. For example, warrant and incarceration information is available to CJIS participants instantly; court dispositions are electronically transmitted to the State Bureau of Identification [SBI]; and Protection From Abuse Orders, created on-line in Family Court, are available to all CJIS participants in real-time. Users are able to determine the status of a case instantly, which greatly enhances the ability to process criminal cases efficiently. Law enforcement's instant access to criminal history, warrant and protection order information has been a critical component of system success. Public safety has been greatly enhanced by the efficient exchange of such background information.

CJIS is based on a central mainframe system which provides several types of user interfaces. These include secured web access to law enforcement officers enabling them to access the system from their patrol cars. Access to CJIS is protected by standard security tools which grant access only to authorised end-users. However, these tools do not monitor how end users utilise their authorised access and cannot detect or prevent misuse by authorised end-users.

The Challenges

CJIS serves over 7,000 end-users. Various types of authorised end-users may pose a potential threat:

- A disgruntled employee that has easy access to confidential data
- An employee who is "just looking" and then "telling" something which is protected information
- An employee looking to "harm" another person by disclosing information
- An employee looking for financial gain by selling sensitive information

Various types of data may be leaked:

- Arrest data
- Complaint/ Incident data
- Crime data
- Motor vehicle and license data

As the information maintained by CJIS is highly sensitive and there are many cases that require the ability to reconstruct user actions in order to find what specific data was accessed by which user. In addition it is needed to know beyond a "reasonable doubt" that no one else had accessed the same information within the relevant timeframe. Like other systems, CJIS maintains log files stored on tapes. However, these logs were not intended to be used as an audit trail and are not "easily" readable.

Feedback

"The Intellinx results were overwhelmingly jaw dropping successful. The logging system performed fantastically better than expected. Turnaround time with the Intellinx system was fabulous.

Breach investigation time decreased by more than 90%.

Potential threats to officer and public safety are reduced.

The implementation did not require any changes to our application code and does not impact system performance."

**Ms Peggy Bell
Executive Director
Delaware Criminal
Justice Information
System (DELJIS)
The State of Delaware**



Prior to implementing Intellinx, investigators needed to plough through mountains of paper logs. Depending on the type of search requested, one second's activity could be represented by one box full of paper.

The old investigation process had significant shortcomings:

- Labour intensive [pulling and mounting tapes]
- Risk of error [missing or damaged tapes]
- Printing and reviewing logs and screens was tedious and prone to errors
- Very long turnaround time for investigations. For example, reviewing 6 months of data took 2½ months!

As a result, requests for investigating activity logs were honoured only for "major crime", not for other suspicious cases.

The Goals in Searching for a New Solution

The Secretary of the Department of Technology and Information and CIO for the State of Delaware, Thomas Jarrett, recognised the critical situation DELJIS was facing and searched for a solution. The desired solution was supposed to meet the following goals:

- Reduce the time associated with investigations
- Have potentially "real time" answers to questions of "Who? Did What? When?"
- Enforce state laws
- Ensure "public and police safety" by reducing the number of threats
- Assist Law Enforcement with criminal investigations of homicides and burglaries
- Provide a log of vehicle or license information that may have been accessed on a recent traffic stop to be used in the search for a missing or wanted person
- Set alerts on names, license, identifying number, case number, complaint number, warrant number to see if anyone accesses information

The Intellinx Solution

Intellinx reconstructs end-user sessions and allows investigators to quickly search for user sessions based on any field value that appears in any user screen. Investigators can visually replay user sessions, screen by screen. The Intellinx patented technology tracks user behaviour patterns at the application screen level and builds profiles of users and user groups. The Intellinx Analytic Engine generates alerts on suspicious events in real time. An event may be considered suspicious if the current activity of an end-user is different from their normal behaviour or if behaviour is different from peers in the same department.

The Results

The Intellinx solution was installed for evaluation in late 2006 and quickly demonstrated that the State would be able to meet its objectives. Within a few hours the system was up and running and started to record the activity of all end users connected to the mainframe.

The Intellinx solution dramatically reduced the duration of internal investigations by more than 90%. For example, investigating 6 months of data now takes 20 minutes using Intellinx, where it took 2½ months previously. It enables DELJIS to investigate every request from law enforcement agencies, not only major crimes as before. For example, in one of the cases an agency requested to check if any user had accessed specific warrant information. A quick investigation using Intellinx revealed that a specific user had accessed information on this warrant and disseminated it to an unauthorised person. This case resulted in one user arrest, one user dismissed, and one user reprimanded and losing access to the system. As Intellinx encrypts and digitally signs recorded data, information from investigations has been accepted as forensic evidence in cases in both Federal and State Courts.

The Intellinx Benefits

- **Deters users just by knowing that all their actions are recorded**
- **Improves the effectiveness by advising of suspicious behaviour**
- **Provides full visibility to user actions**
- **Enhances the State's ability to enforce Delaware laws relating to access and dissemination of records**
- **Real time alerts enforcing security policies by detecting security breaches immediately and enhancing officer safety**
- **Recorded data is encrypted and digitally signed so it can be used as forensic evidence.**
- **Totally non invasive and does not have any performance impact**