precisely

Case Study:

# Agency Meets Audit/Information Security Needs

Ironstream and Splunk Help Federal Law Enforcement

## Challenge

A federal law-enforcement agency faced a big challenge. It had to respond to ever-changing reporting requests from its auditors in order to prove compliance with information-security requirements. For that it would need to collect and analyze operational log data from all of its many IT systems.

That intelligence would have to encompass the history as well as the current status of enterprise security information. The agency had previously chosen Splunk® Enterprise as its log management and analytics platform, so it already had the ability to acquire the necessary log data from its distributed, multi-vendor, open-source environment.

But an important source of log data was still missing. That source was (and is) the agency's mainframe systems, which possessed extremely sensitive authentication information, as well as enterprise-wide details on password changes, log-in successes and failures, and accounts being locked out of the mainframe systems. All of that detail, however, was beyond the reach of Splunk.

## Solution

An extensive search brought up one product that offered the best solution — Ironstream from Precisely.

Ironstream for Splunk® was created specifically for the purpose of collecting log data from the System Management Facility of IBM z/OS, transforming it to generic machine language, and forwarding it in real time to the Splunk platform.

That was all the federal group needed to know, and they moved quickly to adopt.

## Results

The customer for the first time now has full visibility, in real time, into the most sensitive authentication procedures and data across their IT environment. They now have enterprise-wide visibility into:

- Failed authentication attempts
- Attempts at accessing resources that are denied by the access control mechanism
- Privileged user actions
- Activities that require privilege
- All attempted accesses of security-related resources, whether successful or not
- Creation or deletion of users
- Changes to user security information or access rights
- Changes to system security configuration
- Changes to system software
- Attempts at escalation of privileges
- All log-in activity
- Password changes

The agency is now able to audit for unusual activity at the individual user levels, helping them detect security exposures such as:

- Access from an unusual location, unusual network zone, or unusual time of day
- Changes to user privileges and rights
- Excessive data transmissions
- Unusual movement of data

Ironstream for Splunk collects z/OS log data from IBM mainframes, transforms it to generic machine language, and forwards it securely to Splunk Enterprise, Splunk Enterprise Security, or Splunk Cloud™. That way, mainframe log data can be merged on the Splunk platform with all other machine data from distributed systems across the enterprise. Users are thus able to have a true 360-degree view of the entire enterprise IT infrastructure.