WHITE PAPER

Getting 20-20 Vision on Enterprise-class Security

With Ironstream® + Splunk Enterprise Security (ES)

syncsort

Introduction

Contrary to industry lore, the mainframe is not "inherently" secure. While it is generally more secure than its distributed counterparts, stricter security measures are nevertheless required for today's compliance needs — not to mention peace of mind.

First, however, comes the recognition that the mainframe no longer runs in splendid isolation, if indeed it ever did. It is a computer, needless to say — a computer connected to a network. It may even be connected directly to the Internet. Plainly, it cannot be seen as a sealed box.

Our world today, moreover, is vastly more connected. Architectures are more open, and most mainframe systems are still running code that was written well before cyber-security became top of mind to all organizations everywhere. Few security considerations that are important now were present during development of many mainframe applications. These are applications that today are still processing large volumes of mission-critical data. And the number of people who have the knowledge and experience to watch over mainframe operations is shrinking.

Of course, many tools are available that help to even the odds against cyber-attackers. There are fire-walls, encryption engines, and software solutions galore. All those pieces must be *configured*. They must be configured *correctly*. Their operations must be *monitored*, and monitored ideally in real time, to ensure they are working against a threat environment that changes constantly. Doing all that is hard, costly, and by no means foolproof. That reality creates a security blind spot for virtually all enterprises that use a mainframe.

This paper discusses one of the latest and more interesting approaches to cybersecurity in large organizations. The idea is to enable organizations to assess their security posture by scanning their various IT environments as an enterprise-wide whole. That is not what happens today, where there are separate and distinct security needs for z/OS environments on one hand and various heterogeneous distributed-systems environments on the other.

It is an integrated, two-part approach. One part is **Splunk® Enterprise**, a widely-used data-integration platform that draws together log data containing both operational and security information from different computing platforms. It indexes all that to be available for correlation and analysis. With Splunk as a foundation, the **Splunk Enterprise Security (ES)** application was created to be the nexus of a security operations center that can do continuous monitoring of security indicators and provide executives with a window into business risks. The second part of the approach is **Ironstream®**, a technology solution from Syncsort Inc.

Ironstream continually collects operational and security log data from a wide range of sources in the IBM z/OS system, transforms it for the open systems environment, and forwards it to the Splunk platform, all of which can happen in near real time. First we'll examine the Splunk half of this combination, then the Ironstream half, and then discuss how they work together.

Splunk ES — Domains and Dashboards

Technologies and products have emerged in the last dozen years that enable an organization of any size, but especially a large, dispersed enterprise, to collect operational intelligence data from every corner of its IT infrastructure. The data is then centralized into a pooled resource from which — by means of analytics and other Big Data techniques — significant new insights can be gleaned.

Splunk Inc. has pioneered key developments in this area. It's flagship offering, Splunk Enterprise, is a platform that ingests machine data that are collected and forwarded, often in real time, from processing and networking devices across the enterprise.

The Splunk Enterprise Security (ES) application, introduced in late 2015, offers a comprehensive approach to organizational security and is capable of providing visibility across any type and number of on-premise systems, cloud, and hybrid environments. Splunk ES is designed around six domains: (1) overall security posture, (2) access control, (3) endpoint protection, (4) network protection, (5) incident response, and (6) audit protection.

Its various subsystems monitor incoming data continuously, looking for security-related correlations. Findings and alerts are communicated through visualizations and pre-configured but customizable dashboards. There are eight primary dashboards, each of which provides for drill-downs to many other dashboards for more detailed information.

One such dashboard — named "Security Posture" — provides the highest organizational view of notable events, those that occur across all domains. This makes it a logical jumping-off point in a security operations center.

Searches for anomalous activity and other potential threats or intrusions are run against either the data models that are defined in Enterprise Security or the data models as defined in the Common Information Model. (Data models define consistent relationships in machine data, and they standardize data coming from different sources.)

Ironstream z/OS Security for Splunk ES

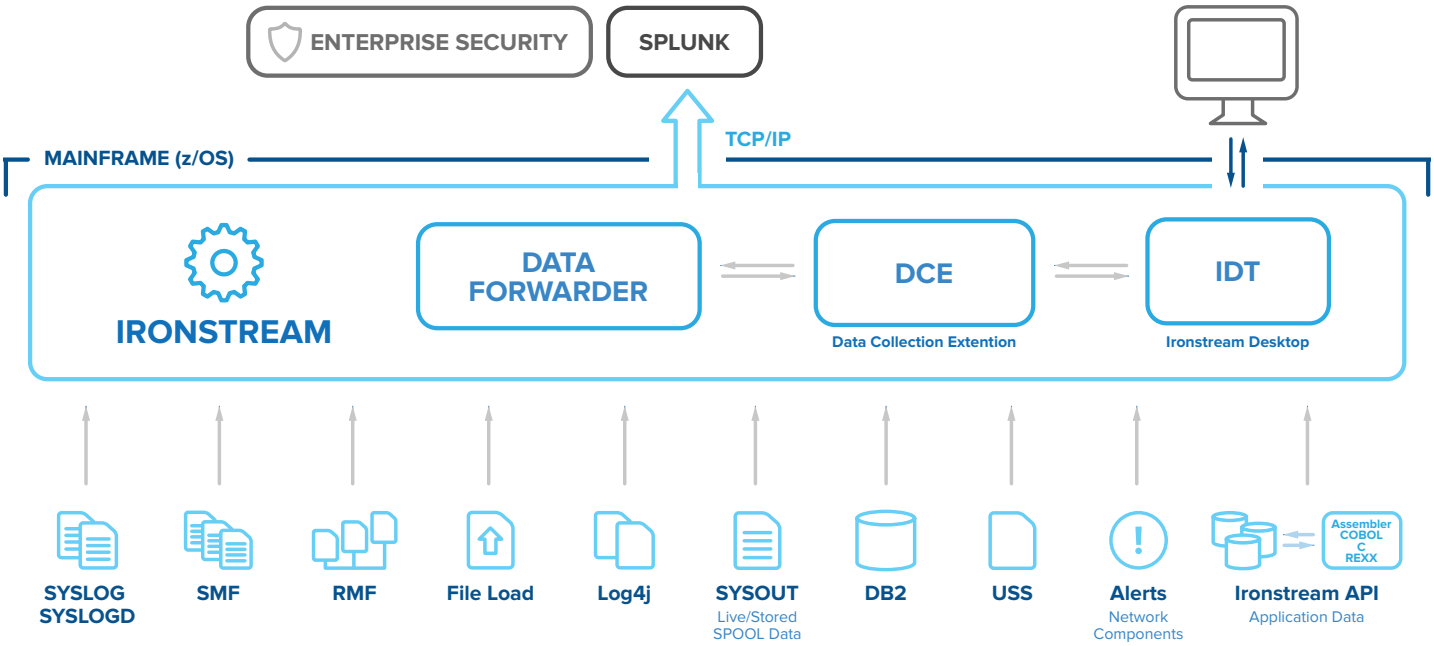
Syncsort Ironstream® is the industry's leading automatic forwarder of z/OS mainframe operational data to the distributed systems world.

Prior to September 2014, when the first version of Ironstream appeared, IT shops needed highly specialized manpower who understood what's involved in extracting data from any of the more than 200 different types of log data produced by a typical mainframe system. In most cases, organizations had to maintain separate and costly systems if they needed to get operational information from z/OS. But with Ironstream, it became easy for Splunk to offer visibility into all systems, and to do so via an ordinary web browser rather than a 3270 "green screen."

Ironstream is actually not one forwarder but several — depending on the particular types of data source that are targeted for forwarding to Splunk. Ironstream can capture information from a variety of z/OS data sources, including Syslog, SyslogD, SMF, RMF Monitor III, Log4j, SYSOUT, DB2 tables, Unix System Services file systems, and standard z/OS datasets. Once in Splunk they can be screened and probed for operational intelligence, with the results conveyed through visualization.

Ironstream contains a Technology Add-on (TA) to Splunk ES. This "Ironstream TA-ES" takes all of the security information and events data that it collects from an IBM z/OS mainframe and maps that information into the Splunk ES Common Information Model (CIM). Ironstream TA-ES populates the Splunk ES dashboards with information and potential correlations in z/OS data alongside data from open-systems devices and networks, giving a true enterprise-wide view of security activity, threats, and intrusions. Ironstream TA-ES collects information from the following sources:

- Port scans, Denial of Service(DoS) attacks, and information about malformed data packets. These data are provided by the z/OS Traffic Regulation Management Daemon (TRMD) and SyslogD, enabling security analysts to perform intrusion detection.
- TSO logon tracking is obtained from SMF Type 30 Records.
- TSO account activity (create, update, delete, lockout) is obtained from SMF Type 80 Records.
- FTP authentications & FTP file analysis (file create, access, update, delete) are obtained from SMF Type 119 Records, along with IP traffic analysis information.
- Network events are obtained from the Ironstream Network Monitoring Component.



Issues and Problems Solved

With the integration of Splunk ES and Ironstream, organizations can overcome the barriers to monitoring z/OS activity by using the same system they use to monitor activity in their non-mainframe IT environments. Doing so is now easy and cost-effective.

Prompt action when suspicious events or anomalies are detected is the essence of sound security measures. A lot of damage can be done to an organization if weeks or months go by before an illicit data breach is noticed. In fact, long lag times are commonplace in organizations that are attacked and that don't have real-time visibility into all of their IT systems. Through access to z/OS security indicators, together with a system that does automatic risk assessments and automatic alerting, Splunk ES + Ironstream can enable quicker reactions. The time between the occurrence of an adverse security event and its discovery can be shortened.

When analytics and other search techniques are applied to the Splunk data repository — which with Ironstream can now easily include z/OS events and operational data — potentially significant correlations between scattered events can be revealed that would be almost impossible to detect absent the Splunk ES + Ironstream integration. The correlation process would, for example, flag for investigation the swipe of an entry card at a building in Miami and a TSO logon by apparently the same person, at roughly the same time, to a z/OS system in Chicago. Again, timely response is the difference between damaging losses and effective prevention.

Some of the most serious security risks in an organization are not external but internal. For example, "Privileged user" activity within the organization requires specialized monitoring that depends on the extraordinarily broad range of events that are logged in real-time in the z/OS environment, where hundreds of distinct categories of events are tracked.

Greater visibility into FTP data movements in the z/OS environment can also be invaluable. Are data volumes off the norm? Is there activity between unknown endpoints? Is data leaving the organization regardless of a ban?

Conclusion

By forwarding key security indicators and events from across the different logging facilities within z/OS and integrating them with open-systems data, Ironstream together with Splunk ES brings to the market an easy, cost-effective way for an organization to get security visibility across its entire IT infrastructure. At the same time — because Ironstream obviates the need for mainframe expertise and mainframe-oriented software solutions — it addresses the growing shortage of mainframe expertise.

With information provided from z/OS by Ironstream-TA, organizations using Splunk ES get total visibility into:

- Authentication and access failures.
- Creation or deletion of users.
- Changes to user security information, passwords, and access rights.
- All TSO log-in activity.
- Excessive data transmissions and unusual movement of data.
- Intrusion detection.

In other words, they get a complete view of their security environment across their entire IT infrastructure from a single pane of glass. They can gain operational efficiencies and better visibility into their enterprise IT infrastructure, including:

- **Clearer, more precise security information.** Alerts and risks affecting key mainframe environments (i.e., CICS, DB2, IMS, MQ, etc.) are as apparent visible as those coming from other systems.

- **Healthier IT operations.** Anomalies in the mainframe environment are just as accessible for analytics and diagnoses as are those anomalies in other systems.

- **Better problem-resolution management.** Mainframe SMF log data is more readily available for analysis and action.

- **Higher operational efficiency.** Information typically provided by legacy silo monitors is more readily correlated with those from other systems in the enterprise.

877.700.0970
www.syncsort.com

ABOUT SYNCSORT

Syncsort is a provider of enterprise software and the global leader in Big Iron to Big Data solutions. As organizations worldwide invest in analytical platforms to power new insights, Syncsort's innovative and high-performance software harnesses valuable data assets while dramatically reducing the cost of mainframe and legacy systems. Thousands of customers in more than 85 countries, including 87 of the Fortune 100, have trusted Syncsort to move and transform mission-critical data and workloads for nearly 50 years. Now these enterprises look to Syncsort to unleash the power of their most valuable data for advanced analytics. Whether on premise or in the cloud, Syncsort's solutions allow customers to chart a path from Big Iron to Big Data. Experience Syncsort at www.syncsort.com.