Ironstream for Splunk Enterprise Security

Delivering real-time mainframe data for enterprise-wide security

What it is

Splunk Enterprise Security (ES) is a premium solution offered on the Splunk platform to enable security teams to use all data to gain organization-wide visibility and security intelligence. Regardless of deployment model, Splunk ES can be used for continuous monitoring, incident response, running a security operations center, or for providing executives a window into business risk.

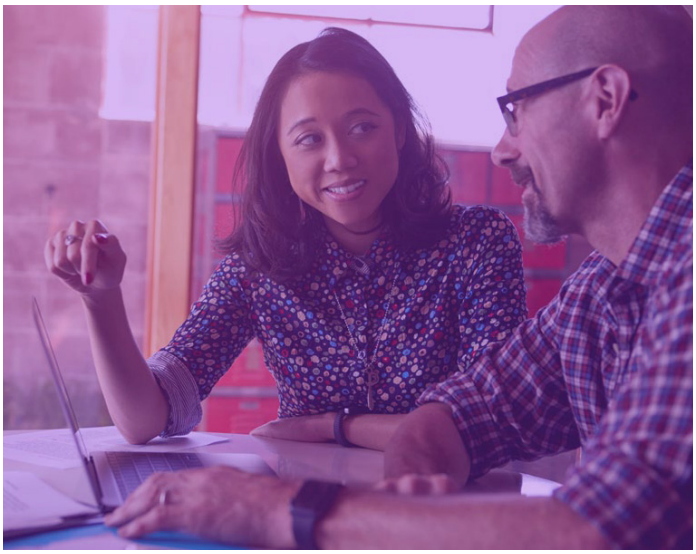
The Splunk platform, however, does not natively support mainframe log data -- which means your enterprise-wide security view has a significant blind spot.

Precisely Ironstream, the industry-leading product for forwarding mainframe log data to Splunk, directly maps z/OS security events and information into Splunk ES dashboards.

What it does

The Splunk ES application provides insights into all manner of potential threat indicators generated by networks and endpoints across the enterprise. It delivers those insights through alerts, reports, and visualizations, including dozens of customizable dashboards. It streamlines all aspects of security operations and is suitable as the basis of a security operations center for organizations of all sizes and levels of expertise. Splunk ES is built around a variety of data models, which define consistent relationships in machine data and which standardize data coming from different sources. Ironstream, for its part, normalizes and streams z/OS log data (i.e., Syslog, SyslogD, SMF, RMF, Log4j, SYSOUT) to the Splunk Enterprise platform for correlation, analytics and visualization.

Ironstream additionally takes the incoming z/OS security information and maps it to the Splunk ES Common Information Model (CIM). The result is a true enterprise-wide view of security activity, threats, and intrusions.



With Ironstream for Splunk ES:

- TSO logon tracking is obtained from SMF Type 30 Records
- TSO account activity (create, update, delete, lockout) is obtained from SMF Type 80 Records
- z/OS Traffic Regulation Management Daemon (TRMD) and SyslogD are analyzed for intrusion detection
- 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

Using Ironstream for Splunk enables you to get total visibility into:

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

In other words, you get a comprehensive view of your security environment from a single pane of glass!

Value Provided

Ironstream was developed in conjunction with Splunk specifically because of the many challenges associated with getting real-time access to the z/OS data required to make Splunk Enterprise the ultimate tool for the many organizations with mainframes in their enterprise.

For security information, the need to continuously divert specialty mainframe staff hours and acquire additional tools was just not a viable solution.

Ironstream removes that daily mainframe skills burden and enables the security, compliance, and SIEM experts to do their jobs.

The combination of Ironstream and Splunk ES can enable security teams to respond quickly to attacks, work proactively to identify threats, and have the assurance that all critical systems across the enterprise are covered.