Ironstream + Microsoft Sentinel

Connect your IBM Z® mainframe and IBM i® systems data to Microsoft Sentinel for comprehensive views for security information and event management or security orchestration, automation and response.

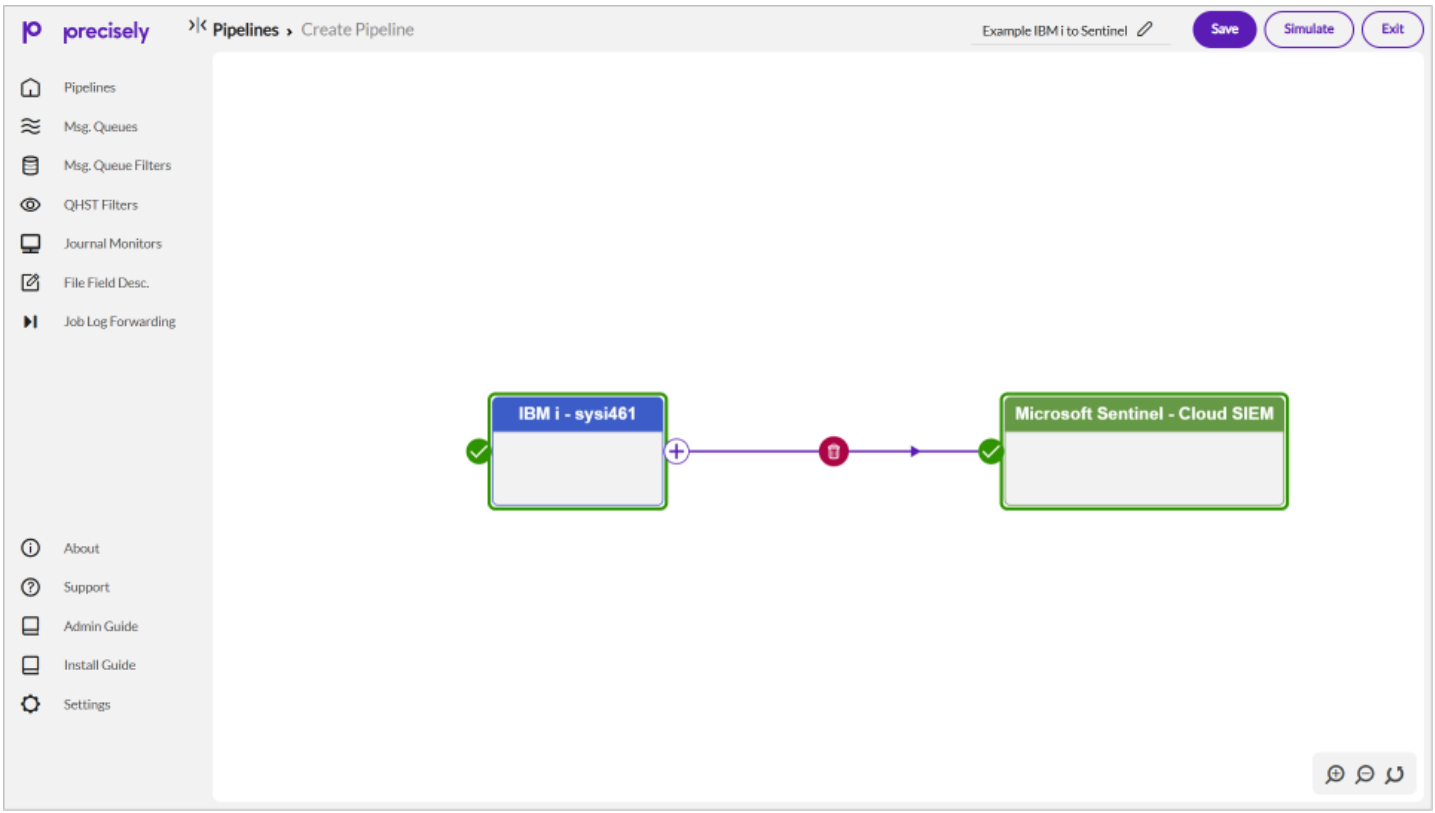
Overview

Organizations struggle to gain full visibility into security threats because critical IBM i and IBM Z data is often siloed from modern security platforms. Without this data, AI-driven threat detection and custom security rules in Microsoft Sentinel lack the complete context needed for accurate analysis and rapid response.

Precisely Ironstream makes it simple to collect, transform and securely stream data from these traditional IBM platforms into Microsoft Sentinel with no need for mainframe or IBM i expertise.

Benefits

- Proactive monitoring, event management, response and resolution with valuable insights from IBM system logs
- Strengthen threat detection by creating custom Microsoft Sentinel rules tailored to IBM system data
- Improve AI-driven analysis by integrating IBM i and IBM Z data into Microsoft Sentinel's built-in AI models for deeper, more accurate threat intelligence
- Seamlessly integrate IBM i and IBM Z data with Microsoft Sentinel to enhance security visibility across Azure Security Center, Azure Defender, and Microsoft 365 Defender



IBM i data support examples

- Journals
- Queues
- Logs
- Application File Journal Data
- Application Message Queues
- Configuration Items
- Collection Services Data
- Job Accounting Data
- History Log (QHST)
- IFS Data
- System Audit Journal (QAUDJRN)
- System Operator Message Queue (QSYSOPR)
- System Summary Performance Data
- Performance Metrics

IBM Z data support examples

- IMS log data
- SMF, LOGREC and Syslog records
- Security information from RACF, ACF2, and Top Secret
- Resource Measurement Facility III data
- UNIX Systems Services (USS) and Log4J files
- Network-performance data

Additional Ironstream Highlights

- **Centralized target management.** Manage multiple targets and pipelines in one place through a unified integration layer with user-friendly UX.
- **Data selection and advanced filtering.** Deliver more focused and relevant IBM machine data flows into IT analytics platforms with advanced filtering capabilities.
- **Multi-target, multi-source support.** Work seamlessly with IT platform discovery processes to include IBM system data alongside all the other systems in the environment.
- **Consumable output.** Get output that is immediately readable by the target system, no legacy data experience required.
- **Pipeline reuse.** No need to refactor pipelines as targets change, keep the same logic for one target as another without the need to redesign or reimplement the pipeline.
- **CPU Impact.** Maintain cost-effective management of IBM system CPU while gaining critical visibility necessary to ensure IT resilience for all systems.