

# GETTING STARTED WITH SPLUNK FOR MONITORING AND DIAGNOSTICS

A guide to gaining real-time insights into industrial operations

## Introduction

Managing industrial processes and systems means you're likely working with SCADA and other industrial control systems (ICS), process historians, and alarm and event sensors. These diverse operational technologies (OT) make it challenging to gain a unified view into the availability and performance of your industrial environment.

By collecting, analyzing and visualizing time-series sensor data, alarms and events, and other machine data generated by your OT and IT systems, you can gain this unified view—and a competitive edge. This guide outlines how you can use this data and Splunk software to better monitor your industrial assets, applications and infrastructure, and quickly diagnose issues in your industrial operations and processes.

## Benefits of Better Monitoring and Diagnostics

Gaining a real-time and unified view into the health, availability and performance of highly distributed industrial assets and complex control systems is an uphill battle. These systems often use proprietary protocols and data-access interfaces that frequently

operate in silos in your environment. With limited visibility, decision-makers can fall into the trap of making decisions based on intuition rather than data.

Unifying and analyzing the machine data generated in industrial environments can help you to:

- Ensure equipment is operating as intended
- Monitor, track and avoid unplanned asset downtime
- Rapidly perform root-cause analysis and pinpoint costly operational issues
- Understand the cause of failures and improve efficiency and availability

## Getting Started

Many organizations already use Splunk software to gain a consolidated view across their IT systems to improve performance and availability. You can use the same platform to gain a unified view into OT systems as well. Additionally, Splunk software is already integrated with leading IoT platforms, including AWS IoT, Xively by LogMeIn, and Citrix Octoblu, which enable fast time-to-value for developers and end users.

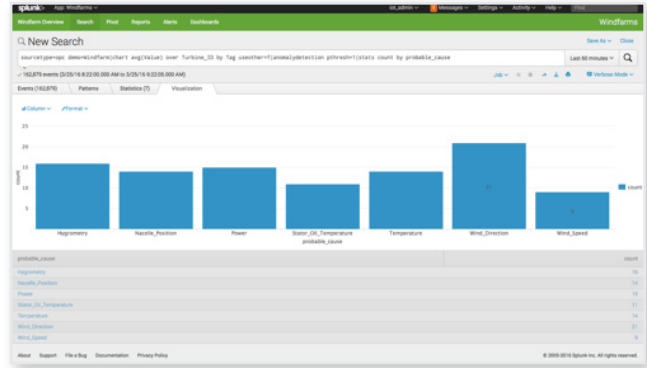
## Data Sources Table

Data Type	Where to Find It	What It Can Tell You
Sensor data and other metrics	Historian databases, OPC, Kepware Industrial Data Forwarder for Splunk, HTTP event collector, MQTT, AMQP, COAP, JMS	Asset performance, anomaly detection, predictive maintenance, set point monitoring
Alarms and events	OPC, alarm and event servers, databases, log files	Root-cause analysis, failure forensics, nuisance alarm reduction, capacity planning
Application logs	Local log files, log4j, log4net, Weblogic, WebSphere, JBoss, .NET	Operator activity, application performance
Infrastructure data	Switches, routers, servers, desktops, HMIs	Networking and communications troubleshooting, cybersecurity



#### 4) Identify Anomalies in Sensor Data

- **What to look for:** Anomalies in individual sensor readings or anomalies against a body of historical data from a group of assets
- **Why?** Using advanced analytics such as anomaly detection or machine learning can quickly identify outliers and patterns
- **Example search:** ... sourcetype=opc demo=Windfarm | chart avg(Value) over Turbine\_ID by Tag useother=f | anomalydetection pthresh=1 | stats count by probable\_cause



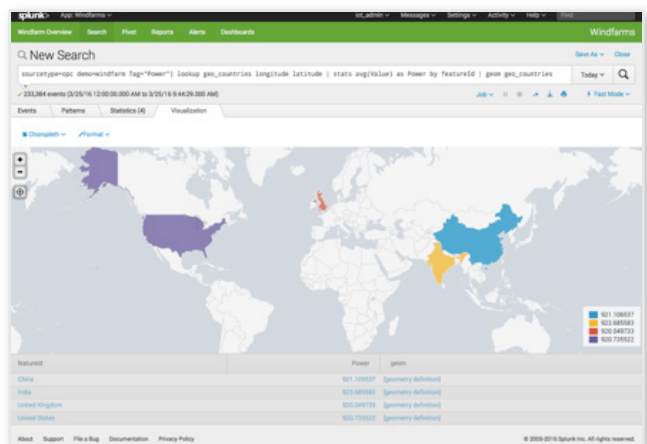
#### 5) Enrich Operational Data With Data From Work Order, Asset and Other External Systems

- **What to look for:** Patterns in metrics related to activities not stored with your sensor data
- **Why?** Activities affecting your sensor data might not be stored in your tag historian or operational database. Find subtle root causes of operational problems by mashing up data from all of your operational data sources
- **Example search:** ... | lookup workorder\_lookup Asset\_ID AS Asset\_ID OUTPUTNEW Last\_Maintenance\_Date AS Last\_Maintenance\_Date | stats min(Power) by Last\_Maintenance\_Technician, Last\_Maintenance\_Date, Asset\_ID | sort min(Power) | head 5

Last_Maintenance_Technician	Last_Maintenance_Date	Asset_ID	min(Power)
19824	1/10/18	OWF-07	423.581598
19824	3/26/18	AWF-08	423.581598
19824	6/10/18	OWF-08	423.581598
19824	9/3/18	OWF-08	423.581598
98772	9/20/18	OWF-08	423.581598

#### 6) Enrich Operational Data With Geolocation Data to Gain a Global View of Operations

- **What to look for:** Patterns in data related to geographic or other location-based groupings
- **Why?** The physical nature of industrial environments means that cause and effect may be related to proximity. Automatically group data on-the-fly using any location-based borders—as big as a country or as small as a production line—to monitor metrics and KPIs
- **Example search:** ... demo=windfarm Tag="Power" | lookup geo\_countries longitude latitude | stats avg(Value) as Power by featureid | geom geo\_countries



## Connecting Splunk to Industrial Data and the IoT

### **Keeware Industrial Data Forwarder for Splunk**

Get real-time data collection from over 150 open and proprietary industrial data protocols common in energy, manufacturing, and oil and gas environments.

### **Modular Inputs**

There are many free apps and add-ons that simplify the connection and collection of data from industrial systems. Use MQTT, COAP, AMQP, JMS and other modular inputs for Splunk to quickly and easily configure connectivity to these message brokers and protocols. For a complete list, go to our [website](#).

### **HTTP Event Collector**

Use a standard API and token-based authentication to enable applications and devices to send millions of events per second directly to Splunk Enterprise or Splunk Cloud for analysis.

## Summary

Managing complex industrial operations isn't easy, but getting full visibility of your operations can help. With this guide and data sources you may already be analyzing, you can move from being reactive to proactive, while maximizing your operations performance, security and availability.

[Try Splunk Cloud or Splunk Enterprise for free](#) or learn more about [IoT and industrial data](#).

Already have Splunk? [Download Splunk Apps](#) on Splunkbase.



 [sales@splunk.com](mailto:sales@splunk.com)

 [www.splunk.com](http://www.splunk.com)