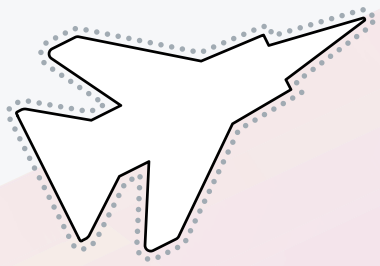
The Essential Guide to JADC2

Achieving Joint All-Domain Command and Control



splunk>

turn data into doing™

Table of Contents

What is JADC2?

JADC2, or Joint All-Domain Command and Control, is the emerging term senior DoD officials are using to describe linking the correct data to all warfighters for the best decisions and outcomes.

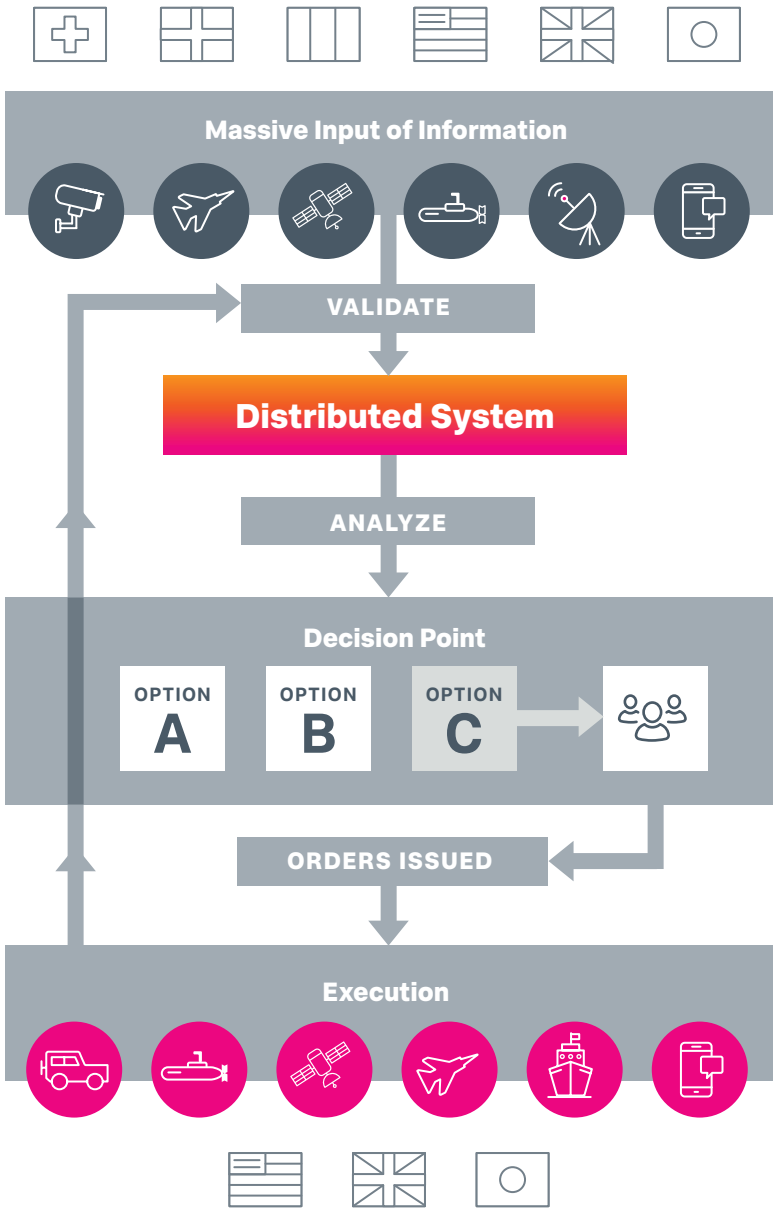
For the first time, it's realistic to imagine a scenario where highly advanced sensors deployed in ships, planes and tanks continually feed critical, real-time information back to headquarters. Then, using state-of-the-art AI and machine learning (ML) tools, commanders analyze the avalanche of incoming intelligence and make better decisions, faster.

This technology is already benefiting spaces like human assistance in disaster relief (HAIDR), which often involves pulling data from disparate sources to make optimal decisions in real time. And, with advancements in cloud, connectivity and sensor technology, using data as a key asset has gone beyond the proving ground. It's now possible to optimize operations on a global scale. A fully operational JADC2 environment will leverage AI and ML to accelerate decisions to machine speed across air, sea, undersea, land, space and cyberspace — automating processes and empowering actions at speeds missions demand.

"We see JADC2 is absolutely core to the way we're gonna defend the homeland."

— General Terrance O'Shaughnessy

The Vision: Future of Joint Warfare



The Challenges to Successful JADC2

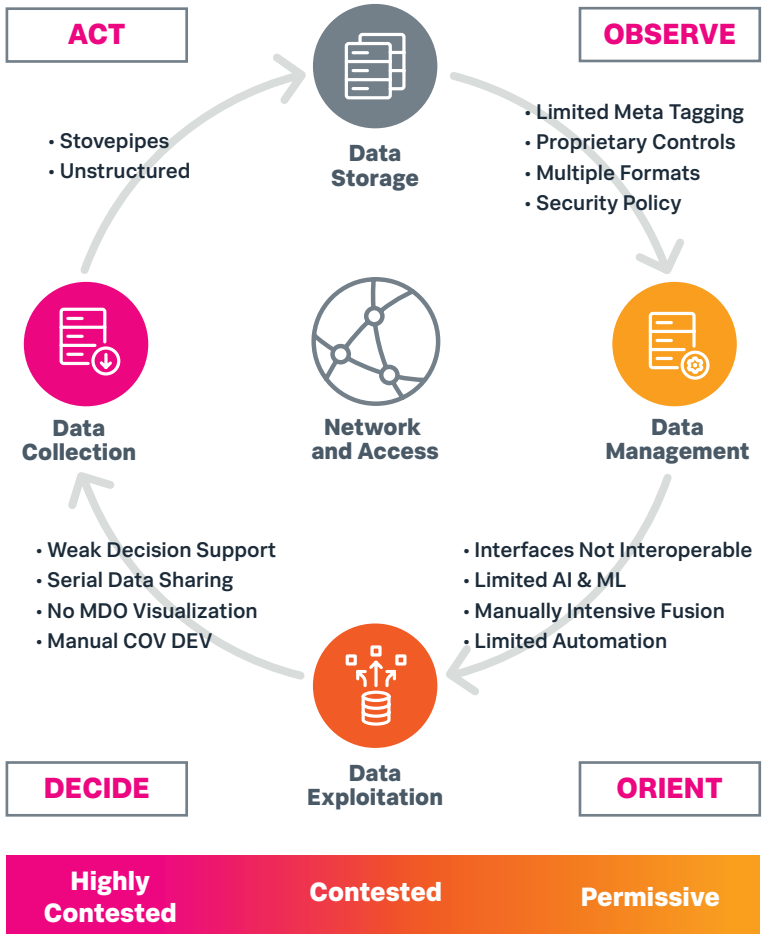
JADC2 provides a necessary evolution for the armed forces because it operationalizes all battlefield data while enabling more confident and rapid decision making by our nation's warfighters. But it's not without challenges. Compressing the OODA (short for observe, orient, decide, act) Loop requires a more holistic approach to solve the emerging spectrum of challenges.

It's no longer enough to take a snapshot of all your systems at a point-in-time, and then create a data model based on that static snapshot. Examples of challenges decision makers face at each stage of the OODA loop include:

Observe	Orient	Decide	Act
Limited Meta-tagging	Limited AI and ML	No MDO Visualization	Stovepipes
Unstructured Data	Limited Automation	Manual COA/DEV	Interface Not Interoperable
Multiple Formats Security Policy	Manually Intensive Fusion	Serial Data Sharing	Proprietary Controls

Challenges to Compressing the OODA Loop

The OODA Loop: Observe, Orient, Decide, Act



Compress the OODA Loop?

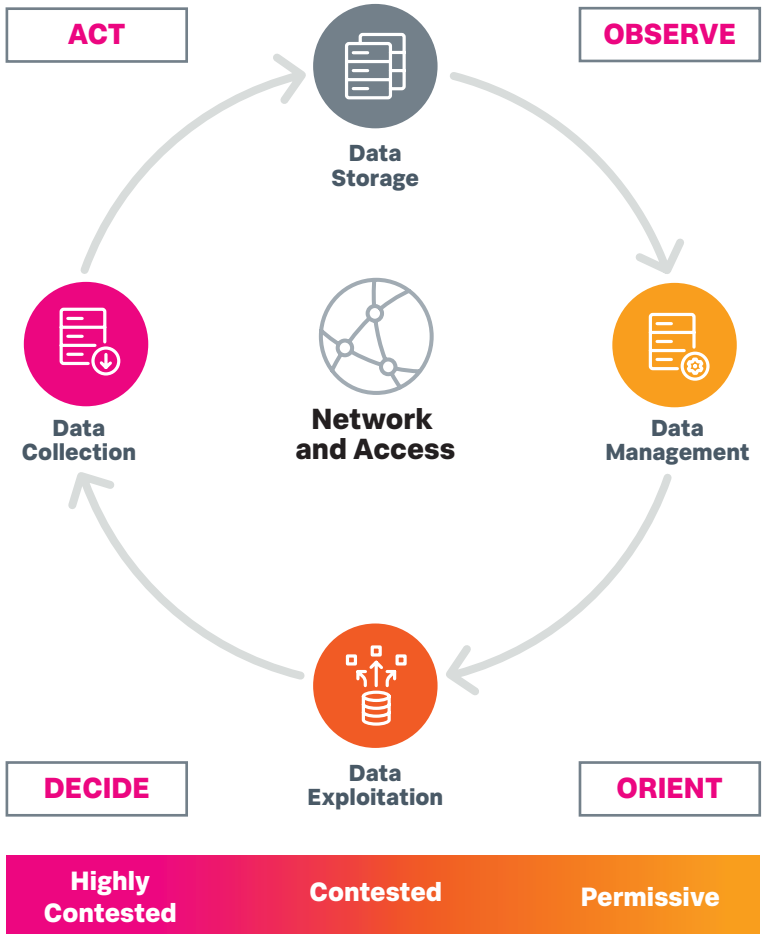
The best way to compress the OODA Loop is to optimize the flow of data. Using a traditional approach, Combatant Commands may need to manually pull data points from disparate, disconnected systems, manually created data in formats like Excel or from legacy databases. This solution works as long as you have plenty of time to wait for all of the relevant information. But on the battlefield, there is no time to waste.

Without a centralized platform to consolidate data, Combatant Commands must make life and death decisions without the best available tactical information. In today's world, traditional approaches don't fit.

This is where Splunk comes in, bringing data to every decision to effectively compress the OODA Loop.

Challenges to Compressing the OODA Loop

The OODA Loop: Observe, Orient, Decide, Act



Five pillars of a successful JADC2

A JADC2 environment should be as easy to use as any consumer app. And that can be done with Splunk, as it takes a massive amount of disparate information (most of which is likely already available) and condenses it into actionable intelligence. For example, IoT sensors on warfighters can provide a holistic view of the battlefield when fed directly into Splunk.

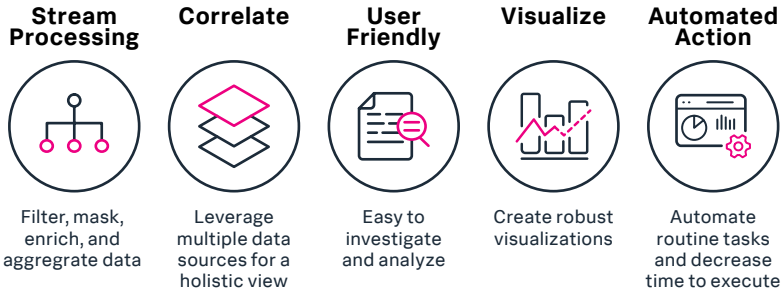
But fusing the data sources that are already at hand is just the beginning. As you break down stovepipes and siloes, previously disconnected systems will be able to communicate the most up-to-date information available. Decision makers can answer questions such as:

- Who is available?
- What effects (Kinetic, Non-Kinetic, or Cyber) are available?
- How long will it take to get there?
- What is the likelihood of success?
- What are the collateral effects?

Data is displayed in an easy-to-use format — similar to a rideshare or delivery app. Combatant Commands will execute their operations with the best possible data available, and they will be able to adapt and change strategies as adversaries adapt and new challenges arise — using a single interface to collate structured and unstructured data. A JADC2 environment improves coordination and increases interoperability among the branches of the U.S. military by leveraging technology and real-time data.

There are strong examples from both the public and private sector of how Splunk's AI /ML capabilities can help accomplish the above through anomaly detection, predictive analytics and clustering. Regardless of whether the mission is routing supplies, medical assistance, or deploying forces to ensure mission success, rapid information flow and decision support is critical.

Operational Advantage



> "We cannot deter what we cannot defeat, and we cannot defeat that which we cannot detect."
>
> — General Terrance O'Shaughnessy

See it in practice

HAIDR missions often involve pulling data from disparate sources to make optimal decisions in real time. The data used to make these decisions might come from weather alerts and forecasts, social media messaging, email or state department reports. This is just one example of how customers are already using Splunk to gain an operational advantage. School districts, firefighters, city planners and the Department of Energy's National Ignition Facility (NIF) are among the growing number of customers relying on Splunk to streamline operations.

Use cases

City of Los Angeles enables real-time security intelligence across 40+ agencies

To protect its digital infrastructure, the City of Los Angeles requires threat intelligence and situational awareness of its security posture. Previously, the city's more than 40 agencies had disparate security measures that complicated data analysis. Los Angeles turned to Splunk to assess citywide risks, gain visibility into suspicious activities and proactively mitigate threats.

Business impact:

- Created an integrated citywide security operations center (SOC)
- Increased protection for digital assets, infrastructure and public services
- Enabled threat intelligence and real-time, 24/7 network surveillance across the city

The city now uses Splunk to ingest raw logs and other data from its more than 40 departments. Splunk then integrates this information into an integrated SOC where the team can analyze and visualize the data in easy-to-use dashboards. With this unified view, executives and analysts can monitor malware, identify top attackers and their targets, and have always-available situational awareness of security events to make the city a safer place for its citizens.

Saving lives with Splunk and Royal Flying Doctor Service

The Royal Flying Doctor Service of Australia (RFDS) is one of the largest and most comprehensive aeromedical organizations in the world. This nonprofit organization provides emergency and primary healthcare services for those living in rural, remote areas of Australia — people who cannot access a hospital or general practice due to the vast distances of the Outback.

Business impact:

- Centralized data analytics and monitoring to deliver critical care to 290,000 patients annually
- Enabled real-time alerts on the temperature of refrigerated vaccines and medicines, which has optimized medicine delivery and reduced waste
- Delivers detailed information to donors, communicating life-saving missions performed in their sponsored region

RFDS's fleet of 63 aircraft — which makes them Australia's third-largest airline — produces large volumes of avionics and location data as it covers its "waiting room," which spans four-thousand square miles. Splunk® dashboards provide real-time visibility into the status and movements of the fleet, equipping RFDS with the information it needs to efficiently deliver critical health services in circumstances where every second counts.

National Ignition Facility unlocks the potential of clean energy and safeguards the U.S. nuclear stockpile

The National Ignition Facility (NIF), located at California's Lawrence Livermore National Laboratory, is the world's largest laser. To support the NIF's core missions, including nuclear stockpile stewardship and scientific discovery, scientists and engineers require a secure, reliable IT infrastructure. Splunk® Enterprise and Splunk® IT Service Intelligence (ITSI) now sit at the heart of the NIF's control system, which manages more than 66,000 control points to power NIF's massive laser facility.

Business impact:

- Maximized system uptime and performance
- Improved control systems reliability, enabling the team to maintain the necessary systems to double the number of laser shot experiments from 200 to 400 annually
- Ensures the health of more than 66,000 Internet of Things (IoT) devices, in addition to the IT infrastructure

After bringing network, authentication and host data into Splunk to solve security challenges, the team aggregated this data with a variety of other sources to gain real-time visibility across the facility. The lab's engineers can now take action on events based on everything from application data to sensor data like laser voltage, temperature and pressure.

Splunk brings data solutions to real-world problems

The above examples are a product of the effective use of these Splunk solutions. Fusing AI and ML with automation and adaptive response capabilities can lead to effective critical operations and contribute to mission success.

Deploy Splunk Data Stream Processor to:

- Turn raw data into high-value information
- Take action on the data in motion
- Protect sensitive data
- Distribute data to multiple destinations

Deploy Splunk Enterprise to:

- Monitor every aspect of a mission
- Monitor complex systems
- Provide complete operating picture
- Reduce downtime

Deploy Splunk Phantom for:

- Automated dispatch
- Multi-sensor notifications
- Predictive response

Operations Improvements

Unlike legacy data platforms and siloed monitoring tools, Splunk offers a cost-effective, extensible and massively scalable analytics platform that delivers enterprise-wide visibility across cloud, on-premises and hybrid system deployments, enabling agencies to reuse data to overcome challenges across discrete programs and mission objectives. Splunk empowers teams to turn data into action through:

Automation
An operational JADC2 provides a significant advantage — automatically collecting and correlating data from disparate sources into complete services, increasing the speed and accuracy of identifying necessary relationships. Once an organization has a good handle on correlating and analyzing data streams, the next step is to automate responses to abnormal conditions.

Anomaly detection
Use historical data to alert on unexpected behavior for one or multiple events. Patterns are continuously updated in real time.

Intelligent event management
Collect and enrich events from multiple sources into a single alerting framework. Real-time, automated event correlation triggers alerts as data enters the system, using out-of-the-box (OOTB) machine learning policies for immediate noise reduction. Incidents are automatically prioritized by service score and impact.

Predictive analytics
Predict future incidents 30 minutes in advance using machine learning algorithms and historical service health scores. The top five contributing service metrics are displayed to guide troubleshooting.

SOC Automation
Phantom enables teams to work smarter by executing automated actions across their security infrastructure in seconds, versus hours or more if performed manually. Teams can codify workflows into Phantom's automated playbooks using the visual editor (no coding required) or the integrated Python development environment. By offloading these repetitive tasks, teams can focus their attention on making the most mission-critical decisions.

Orchestration
Phantom is the connective tissue that lets existing security tools work better together. By connecting and coordinating complex workflows across the SOC's team and tools, Phantom ensures that each part of the SOC's layered defense is actively participating in a unified defense strategy. Powerful abstraction allows teams to focus on what they need to accomplish, while the platform translates that into tool-specific actions.

Incident response
Phantom helps security teams investigate and respond to threats faster. Using Phantom's automated detection, investigation and response capabilities, teams can execute response actions at machine speed, reduce malware dwell time and lower their overall mean time to resolve (MTTR). And now with Phantom on Splunk® Mobile, analysts can use their mobile device to respond to security incidents while on-the-go. Phantom's event and case management functionality can further streamline security operations. Case-related data and activity are easily accessible from one central repository. It's easy to chat with other team members about an event or case, and assign events and tasks to the appropriate team member.

Splunk — The Future of JADC2

The time it takes to get intelligence from the places where soldiers, sailors and airmen are operating up to the highest level of authority is critical. A fully operational JADC2 environment will give Combatant Commands the tools to observe, orient, decide and act in near real time. Splunk will allow the DoD to fully or partially automate the Decision and Action portion of the OODA Loop, allowing decisions at the speed of relevance.

It all points to JADC2 becoming the cornerstone for modern battlefield operations and deterrence, at a time when civilian technologies — like apps to locate the nearest gas station or where you left your phone — set the pace for the degree of connectivity and intuitive use that battlefield commanders should expect.

Gaining an operational advantage over adversaries is key to mission success. With access to artificial intelligence, machine learning, and high-quality data streaming, the military service branches can now set a higher standard for communication and information-sharing.

Learn **More.**

Ready to learn more about how the Data-to-Everything™ Platform can contribute to a successful JADC2? Speak with a Splunk expert to discuss your environment and assess your requirements.

Speak to an Expert

splunk>

20-19256-SPLK-Essential-Guide-to-JADC2-105