



Readiness by Design

Systems Engineering for Defense Supply Chain Resilience

**Department of the Air Force
Information Technology and
Cyberpower Training and
Education Event (DAFITC)**

Track 2: Securing the Lifeline:
Supply Chain Risk Management for
Mission-Critical IT and Warfighter
Communications Systems

August 25-27, 2025



Agenda

The Challenge: Fragility in Mission-Critical Supply Chains	3
The Solution: Engineering Supply Chain Resilience	4
Operationalizing Resilience: Supply Chain Program Maturity	5
Deloitte in Action: Securing the Supply Chain	
• Hardware Assurance: CentralSight™ • Software Assurance: Cyber-Supply Chain Risk Management (C-SCRM) • Scenario Modeling: FutureScape™ • Analysis as a Service: Dynamic Adversary Intelligence (DAI)	6
How to Get to Us	11



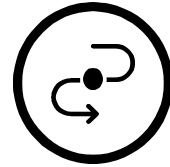
The Challenge: Fragility in Mission-Critical Supply Chains

In an era marked by persistent and sophisticated threats, the resilience of defense supply chains is paramount to sustaining warfighter readiness. Adversaries are increasingly targeting mission-critical IT and communications systems, challenging acquisition leaders to deliver secure, resilient capabilities at speed and scale.



Cost

Budget overruns can strain financial resources, **hindering ability to efficiently manage and sustain** vital programs



Schedule

Project delays **disrupt timely** acquisition and deployment of critical systems to support **operational demands**



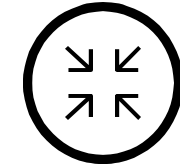
Performance

Variability in supplier performance compromises the effectiveness of systems, **challenging ability to deliver reliable warfighter capability**



Security

Security risks jeopardize sensitive data and operational integrity, **threatening commitment to safeguarding vital assets** to national security



Resilience

Limited ability to prevent or recover from disruptions **threatens mission survivability and scalability—reducing global competitive edge**

Core Challenges

Contributing Factors

- *Limited Vendor Base*
- *Supplier Financial Stability*
- *Lack of Supply Chain Visibility*
- *+6 More...*

- *Workforce Shortages*
- *Production Bottlenecks*
- *Part Shortages*
- *+9 More...*

- *Part Quality Variability*
- *Supplier Responsiveness*
- *Interoperability Challenges*
- *+7 More...*

- *Cybersecurity Threats*
- *Counterfeit Parts*
- *Part Tampering*
- *+8 More...*

- *Foreign Dependence*
- *Obsolescence*
- *Limited Infrastructure*
- *+5 More...*

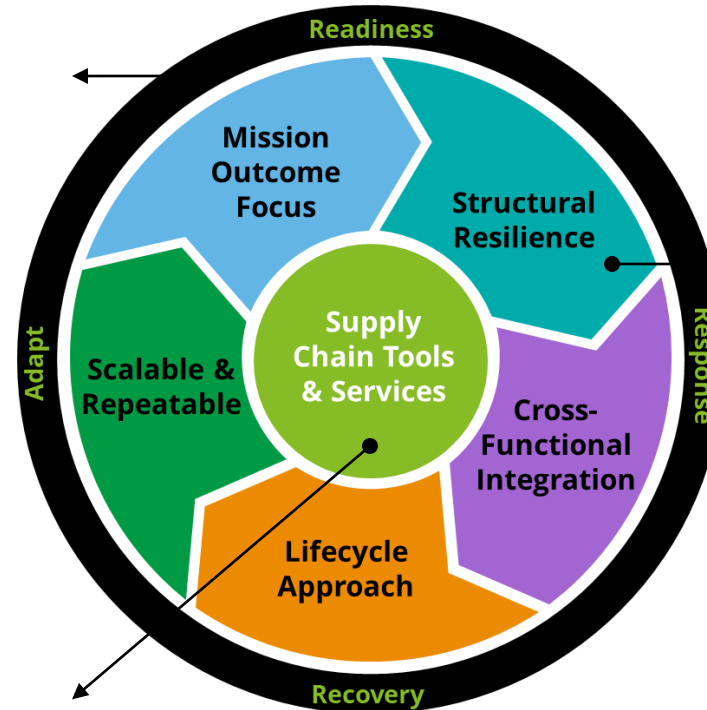
There are over 50 contributing factors that influence the overall health and performance of the Defense Industrial Base—each of which can significantly affect acquisition, sustainment, and modernization efforts

The Solution: Engineering Supply Chain Resilience

A supply chain is not a single function or workflow—it's a **complex, interconnected system** made up of **people, processes, and technologies** working together to deliver a product. Because these elements are deeply interdependent, changes in one area ripple across the entire system. That's why a **systems engineering (SE) approach** is vital—it treats the supply chain as a whole, not an isolated collection of parts or suppliers.

Operational Phases

- **Readiness:** Proactively prepare for disruptions by identifying risks, planning ahead, and building resilient capabilities
- **Response:** Act quickly to contain and mitigate disruptions using real-time visibility and coordinated execution
- **Recovery:** Restore operations and stabilize performance to return to normal functionality
- **Adapt:** Learn from disruptions to improve systems and enhance future readiness



SE Principles for Supply Chain Resilience

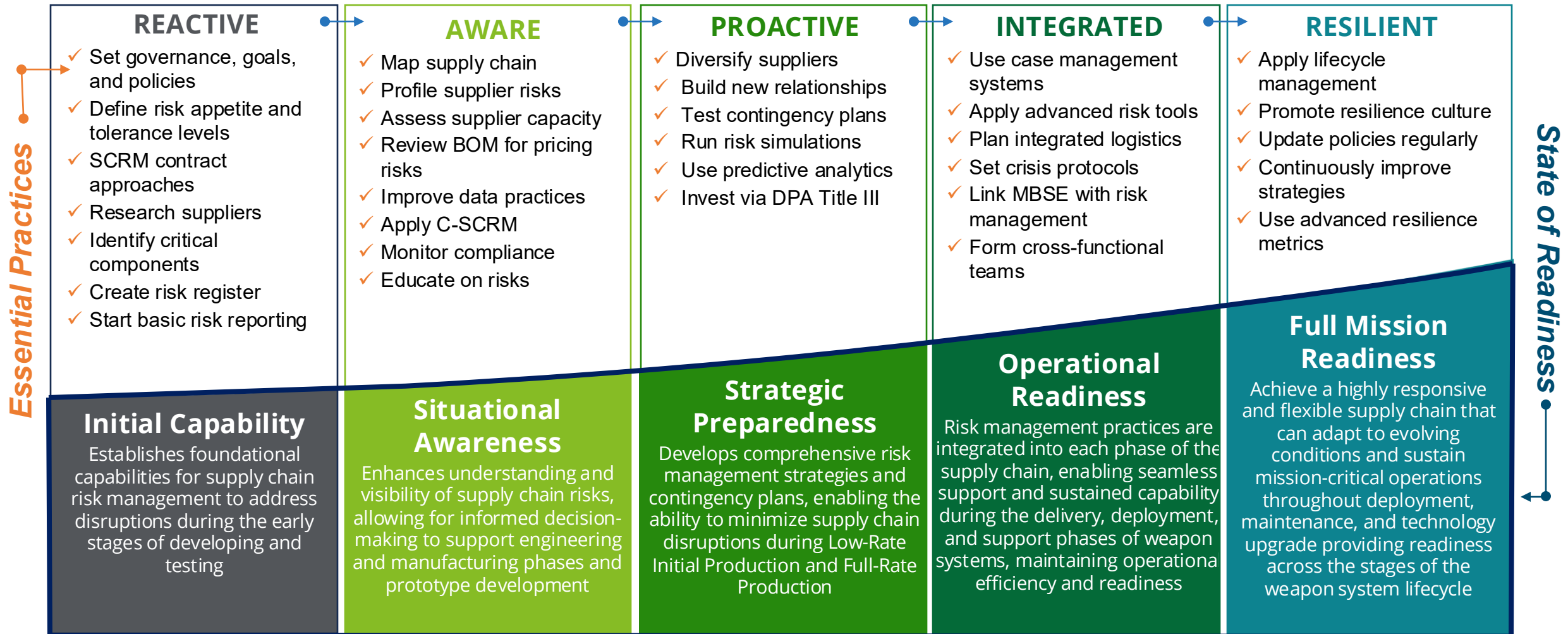
- **Mission Outcome Focus:** Align supply chain capabilities with mission-critical goals, ensuring secure, timely, and cost-effective delivery
- **Structural Resilience:** Embed flexibility, redundancy, and agility into supply chain design to maintain continuity
- **Cross-Functional Integration:** Break down silos by coordinating across procurement, logistics, cyber, and intelligence functions
- **Lifecycle Approach:** Maintain resilience throughout the entire system lifecycle via continuous risk assessment and adaptation
- **Scalable and Repeatable Frameworks:** Use structured, repeatable methods to ensure supply chains can scale and respond effectively across operations

Supply Chain & Network Operations (SCNO)



Operationalizing Resilience: Supply Chain Program Maturity

The architecture below demonstrates how resilience—the ability to maintain operations despite disruptions—can be integrated into a DoD supply chain program. As the organization advances and refines its processes, resilience is further strengthened. Each essential practice builds upon the previous one, steadily enhancing the supply chain’s readiness. This continuous improvement approach enables the supply chain remains capable of supporting critical missions, even as risks and challenges evolve.



Deloitte in Action: Securing the Lifeline

Deloitte offers a unique perspective, and the capabilities needed to bring these proficiencies to your supply chain. We serve as advisors to government clients on end-to-end digital transformation, providing insights through cognitive solutions, real-time data visibility, and delivering advanced technology solutions including Internet of Things (IoT) and Blockchain.

Focus Areas / Offerings

Digital Supply Chain Strategy

- Use AI, IoT, blockchain for full visibility
- Enable real-time, data-driven decisions

Synchronized Planning & Fulfillment

- Optimize inventory, warehouse, and transport
- Use tech to streamline goods flow

Smart Manufacturing, Operations, and Repairs

- Boost productivity with smart systems
- Improve asset use and operational efficiency

Supply Management & Digital Procurement

- Digitize Source-to-Pay processes
- Enhance transparency and speed

Energy, Climate, and Natural Resources

- Support sustainable energy/resource policies
- Drive operational reform for climate goals

WHY DELOITTE?

Functional Experience

Technical Advisors

Ecosystems & Alliances

Value-Focused Mindset

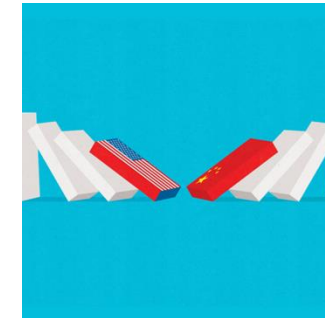
Tools & Accelerators

Organization & Change Management

OUR THOUGHT LEADERSHIP



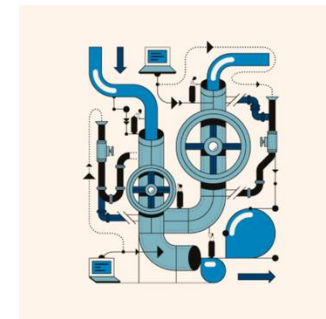
[Restructuring the supply base: Prioritizing a resilient, yet efficient supply chain](#)



[Supply chain resilience in the face of geopolitical risks](#)



[Enhancing supply chain resilience in a new era of policy](#)



[Meeting the challenge of supply chain disruption](#)

Hardware Assurance: CentralSight™

A Software as a Service (SaaS) platform that operationalizes advanced analytics, structured methodologies, and leverages subject matter experience to help clients map supplier relationships, trace risk impacts, and continuously monitor supply chain integrity. Supported by Deloitte's experienced supply chain professionals, the solution delivers comprehensive risk assessments and provides tailored mitigation strategies, including real-time monitoring and alerting through 12 supervised AI/ML models that publish risk events for user review.

Our Approach



Supply Chain
Illumination

Risk Triage

Prescriptive Risk
Mitigation

Monitoring &
Alerting

Managed Service

A single platform to manage risks within your supply chains, supported by experienced supply chain professionals



Users are able to:

- 1 Visualize supplier networks to nth tier
- 2 Assess risks and access mitigation strategies
- 3 Proactively monitor news for risk events
- 4 Access company reports and insights

Assessments

Companies



Supplier Networks



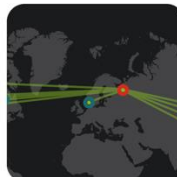
Industrial Base



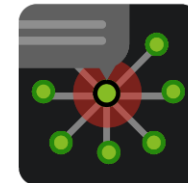
Key Capabilities



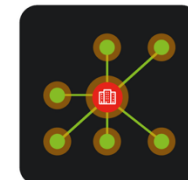
*Explore
Relationships*



*Extract
Insights*



*Identify
Vulnerabilities*



*Maintain
Compliance*



*Actionable
Mitigations*



*Stay
Informed*

CentralSight™ Video



Software Assurance: Cyber-Supply Chain Risk Management (C-SCRM)

A systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. C-SCRM involves identifying, measuring, and mitigating the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains. Deloitte's C-SCRM approach involves advising, implementing, and operating comprehensive strategies to manage cybersecurity risks throughout the supply chain.

1 ADVISE

- ❑ **Current State Assessment:** Diagnose C-SCRM capabilities and understand the cyber-supply chain and software inventory
- ❑ **Gap Assessment:** Evaluate the current state against the desired future state to inform program implementation
- ❑ **Strategy and Implementation Plan:** Create a blueprint for the C-SCRM program and set organizational risk contexts
- ❑ **Software Bill of Materials (SBOM) Strategy:** Design methodologies for collection, storage, and analysis to strengthen software supply chain security



2 IMPLEMENT

- ❑ **C-SCRM Program Establishment:** Set up governance and oversight structures to foster a positive risk culture through information-sharing, cross-functional collaboration, and defined policies and procedures
- ❑ **Risk Appetite Definition:** Set thresholds for risk tolerance and align risk management with strategic goals
- ❑ **SBOM Strategy Execution:** Enhance software transparency through secure storage, ingestion, and analysis to proactively identify vulnerabilities
- ❑ **NIST SP 800-161 Controls:** Implement controls to secure the cyber-supply chain

3 OPERATE

- ❑ **Ongoing Risk Assessments:** Conduct continuous assessments to enhance security and address key risk decisions.
- ❑ **SBOM Ingestion and Analysis:** Illuminate the software inventory to identify and manage vulnerabilities.
- ❑ **Cyber-Supply Chain Illumination:** Use vendor tools and technologies to identify and action potential risks.
- ❑ **NIST RMF Execution:** Strengthen system integrity through secure supply chain practices.

What can SBOMs reveal?

- | | | |
|---|---------------------------------------|--------------------------------|
| Software Vulnerabilities | Bugs and Open Issues | Software Dependencies |
| Malware / Malicious Packages | Open-Source Package End of Life Risks | Software License Risk |
| Foreign Ownership, Control, or Influence (FOCI) | Code Quality Indicators | Regulation and Compliance Gaps |

■ Cybersecurity
 ■ Software Engineering
 ■ Governance

"Software is at the core of every weapon and supporting system we field to remain the strongest, most lethal fighting force in the world."

-SECDEF Memo, Directing Modern Software Acquisition to Maximize Lethality Memorandum, 6 Mar 25

Scenario Modeling: FutureScape™

Our simulation platform provides a digital testbed to quantitatively evaluate the impact of potential disruptions on your network and help you harden your supply chain before these disruptions occur. Once your supplier and buyer relationships are illuminated through CentralSight™, FutureScape™ then models the complexities of your supply chain to simulate various disruptive events.

FutureScape™ for **Supply Chain** is designed to:

- Simulate the movement of goods across multiple networks
- Run simulations rapidly to assess the impact of disruptions early and often
- Test combinations of changes to optimize supply chain networks

“What-if” levers you can pull

- Transit Time
- Production Capacity
- Trade Implications

“What-if” metrics you can explore

- Bottleneck Count
- Production Capacity Recovery
- Critical Production Capacity



Agent-Based: Simulates individual responses to disruptions, showing ripple effects of large-scale changes



Cloud-Native: Runs massive, complex simulations in the cloud for speed and scalability



Patented Engine: Enables fast, high-fidelity simulations across many cloud computers for rapid, simultaneous scenarios.

Is FutureScape™ right for you?

I need to make the most of my limited time, money, and resources.

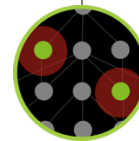
Optimize Resources



With FutureScape™ you can identify where to focus your supply chain efforts for the greatest impact. FutureScape™ pairs supply chain illumination data and with its library of simulations to measure the impact of future events on multi-tier supply chain networks.

I do not know how to answer my “what-if” questions.

Data Quantity & Quality



FutureScape™ models your current supplier network as a baseline, and then runs additional models to simulate the potential impact of disruptions on your current environment. The simulation-aided analysis fills in data gaps, providing you with insights into what could happen as disruptions arise with your supply chain network

I do not even know what disruptions to look for.

Decision Advantage



Clients can configure different scenario types, such as sanctions, natural disasters, and geo-political events, for simulation to measure their potential impact on your supply chain. FutureScape™ —technology and team—helps you iteratively test potential disruptions to design mitigation strategies that harden against your risk.

Analysis as a Service: Dynamic Adversary Intelligence (DAI)

Deloitte's DAI Managed Service helps unmask the person behind the keyboard using a sophisticated, full-spectrum investigative and intelligence team, extensive data sources, custom tools, and agile analysis. Our goal is to identify cyber actors and methods to facilitate recovery, takedowns, arrests, targeting, tracking, and intelligence reporting. DAI flips the script on antagonists, allowing organizations to take decisive action in record time while understanding threats in exact technical, organizational, and persona-level detail

DAI decreases time-to-target with increased confidence and **brings enhanced understanding of the adversary's technical, financial, and enabling networks** based on custom analytics. The analytic outputs, tools, applications, and intelligence reporting produced by DAI are **focused on the most critical portions of the adversary's persona, logical & physical layers, and associated networks**—resulting in actionable intelligence and tailored information for use in investigative operations.

22+

Custom Splunk Integrations

120+

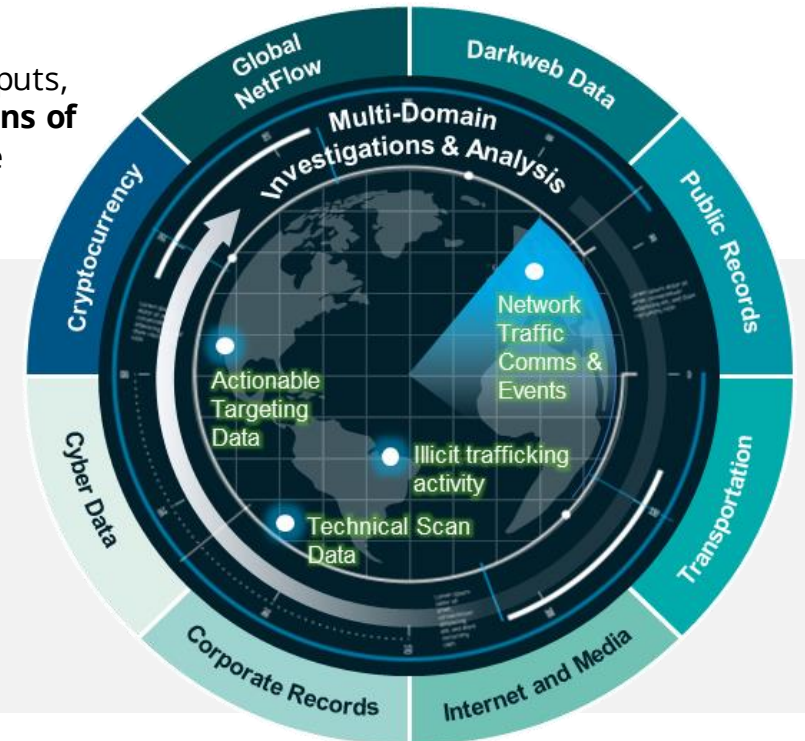
Analytics Dashboard

19

Unique Data Source

Intelligence & Investigative Support

- Cyber Technical Enumeration
- Dark Web Markets
- Financial Fraud
- Maritime & Transportation Tracking
- Corporate/Business Records
- Critical Infrastructure & NetFlow



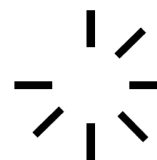
Expansive Data Access

Reduced data acquisition and subscription costs concentrate years of tradecraft and development experience to be accessible on Day 1



Custom Ingestion (ETL) and Retention

No sensors needed – conduct technical collection and analysis without revealing investigative processes



Real-Time Results

Speed up investigations to get analytical results and actionable intelligence in real-time



Custom Dashboards & Development

In-house development team customizes dashboards and develops purpose-built tools for enhanced analysis

How to Get to Us

Deloitte offers multiple avenues for new clients to engage our services through a variety of contract vehicles. These vehicles provide a streamlined experience for both the client agency and Deloitte, facilitating efficient collaboration and strengthening the working relationship among all parties involved.



Questions?

For more information, please contact:

Janie Keating

Air Force Account Leader
Partner
Deloitte & Touche LLP
+ 1 571 882 7960
jkeating@deloitte.com

Suzanne Woerl

Air Force Material Command
Managing Director
Deloitte & Touche LLP
+ 937 258 4801
swoerl@deloitte.com

Ben Sprague

Air Education Command
Principal
Deloitte & Touche LLP
+ 1 571 814 6818
benrsprague@deloitte.com

Diane Ashley

Space Force & SPACECOM
Managing Director
Deloitte & Touche LLP
+ 1 703 944 1355
diashley@deloitte.com

Julie Hrushka

Space System Command
Principal
Deloitte & Touche LLP
+ 1 571 882 7187
jhrushka@deloitte.com

Ray Briggs

Air Mobility & TRANSCOM
Principal
Deloitte & Touche LLP
+ 1 202-213-1742
rabriggs@deloitte.com

Chris Duve

Air Combat Command
Managing Director
Deloitte & Touche LLP
+ 1 303 298 6715
cduve@deloitte.com

Mike Ornelaz

Presenter
Manager
Deloitte & Touche LLP
+ 1 937 581 1320
mornelaz@gps.deloitte.com

Michelle Steele

Space Operations Command
Managing Director
Deloitte & Touche LLP
+ 1 303 305 7714
msteele@deloitte.com

Keith Watts

Space HQ & Training and
Readiness command
Managing Director
Deloitte & Touche LLP
+ 1 303 298 6758
kewatts@deloitte.com

About Deloitte & Touche / Deloitte Consulting

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte Consulting LLP and Deloitte & Touche LLP, which are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting. Use or disclosure of information contained on this page is subject to the restriction noted on this slide.

Copyright © 2025 Deloitte Development LLC. All rights reserved