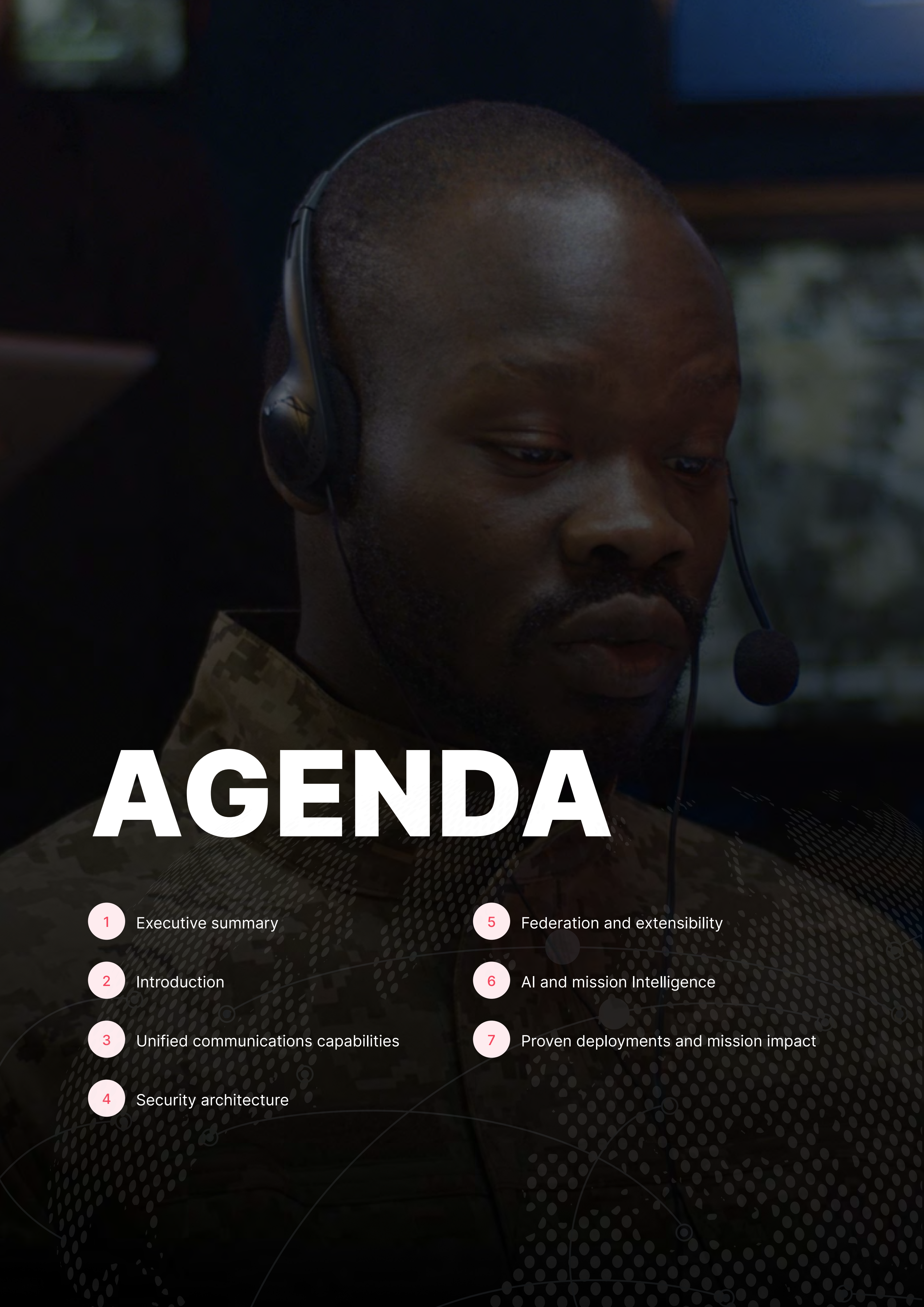
Rocket.Chat Secure CommsOS™ for U.S. Mission-Critical Communications



AGENDA

1. Executive summary
2. Introduction
3. Unified communications capabilities
4. Security architecture
5. Federation and extensibility
6. AI and mission Intelligence
7. Proven deployments and mission impact

Executive Summary

Modern defense and intelligence operations depend on secure, adaptable communication systems that perform reliably across classified, coalition, and disconnected networks.

This white paper outlines how Rocket.Chat supports the operational and security needs of the Department of Defense, the Intelligence Community, and federal system integrators. It highlights the platform's core communication capabilities, its defense-grade security model, and its integration of on-premises AI for mission automation and knowledge management.

Readers will gain an understanding of how Rocket.Chat enables unified, policy-controlled collaboration across enclaves—improving situational awareness, accelerating information flow, and strengthening command decision advantage.

> This paper was written to help agencies and integrators rethink what secure communication means in modern operations. It's about achieving mission assurance—enabling organizations to innovate without ever compromising control.
>
> Christopher Skelly, CPO, Rocket.Chat

Introduction

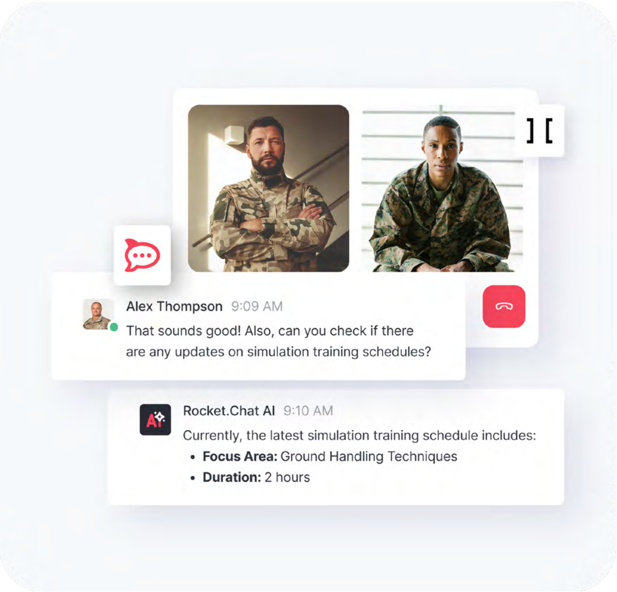
Rocket.Chat Secure CommsOS™ delivers a **unified, extensible communication and collaboration environment optimized for mission-critical operations.** It provides secure messaging, voice, video, and AI capabilities that operate seamlessly within air-gapped or federated network topologies. Workspaces can be interconnected across missions using secure federation to maintain coordination without compromising enclave boundaries.

Built on an open-source foundation under the MIT licence, with enterprise capabilities available under a commercial licence, Rocket.Chat provides full transparency, code auditability, and integration flexibility. All server, mobile, and desktop components are open-source and available for independent security review.

The platform's AppsEngine toolkit allows developers to create encapsulated mission extensions and automated workflows that can be safely deployed across enclaves.

Identity and access management integrate natively with existing Zero-Trust infrastructures through RBAC, ABAC, and enterprise SSO models.

Deployments are supported across major operating systems via a variety of manual deployment paths or the company's LaunchPad CLI.



Alex Thompson 9:09 AM
That sounds good! Also, can you check if there are any updates on simulation training schedules?

Rocket.Chat AI 9:10 AM
Currently, the latest simulation training schedule includes:
- **Focus Area:** Ground Handling Techniques
- **Duration:** 2 hours

AI capabilities—including on-premises large-language and retrieval-augmented generation (RAG) models—are deployable entirely within secure environments to meet operational and classification requirements.

Communication and collaboration

Rocket.Chat supports multiple modalities of secure collaboration:

Messaging

Asynchronous and real-time communication is supported through direct messages (DMs), multi-party DMs, team channels, and topic-specific discussion rooms. Each room supports text messages, file attachments, audio and video messages, reactions, and read receipts—maintaining persistent operational context across shifts and missions.

Voice

Secure, streaming person-to-person voice calls are managed through WebRTC for internal workspace communications. For external PSTN calling and PBX integration a SIP switch can be enabled.

Video conferencing, screenshare, whiteboards

The platform's conferencing connectors allow workspace owners to enable video conferencing through pre-built integrations with conferencing systems, initiating video calls and whiteboard sessions directly from the Rocket.Chat interface.

Native screenshare with voice calls and native video conferencing are under development to further enhance real-time collaboration.

Intelligent workflows

Automated actions within messaging rooms are powered by Rocket.Chat's AppsEngine toolkit, allowing integration with external systems and data stores.

Typical mission workflows include posting critical data to operational teams and triggering actions in external systems.

Security architecture

The platform provides a comprehensive suite of security capabilities to support defined mission security parameters.

Air-gapped operation

Rocket.Chat can be deployed in fully air-gapped or classified enclaves, supporting complete network isolation and compliance with DoD cybersecurity standards.

The platform is trusted across the federal stack with **DoD ATO up to IL6** and is deployed across **NIPR, SIPR, and JWICS** environments.

ABAC and RBAC enforcement

Aligned with the Zero-Trust principle—"never trust, always verify"—the platform implements both role-based (RBAC) and attribute-based (ABAC) access control models. RBAC supports custom role creation using more than 200 configurable permissions, while ABAC leverages an internal Policy Decision Point (PDP) mechanism that evaluates user attributes to determine room-level access decisions.

External PDP integration is under development for systems such as Sentris and Virtu, allowing externalized access decisions without exposing user attributes.

End-to-end encryption (E2EE)

Rocket.Chat supports optional end-to-end encryption (E2EE) for direct messages and private rooms using client-side cryptography. Each protected room is assigned a randomly generated symmetric "room key," created on the user's device. Messages and file uploads are encrypted locally using an authenticated cipher with unique nonces, and only ciphertext plus integrity tags are stored on the server. The room key is delivered to each participant by encrypting it with their device's public key (asymmetric key exchange) and is re-keyed whenever membership or device keys change. Encryption keys reside exclusively on the client within a local vault, which is unlocked using the user's E2EE passphrase.

Identity management and authentication

Rocket.Chat integrates with enterprise identity systems through LDAP, Active Directory, and SSO protocols such as SAML and OAuth 2.0. LDAP/SAML groups can map directly to channels and roles to streamline provisioning. Multi-factor authentication (MFA) is supported, with phishing-resistant FIDO2/WebAuthn authentication in development.

Iron Bank

Rocket.Chat leverages the Department of Defense's Iron Bank project to provide customers and users with secure, hardened container images that meet strict cybersecurity and compliance standards. By using Iron Bank, Rocket.Chat ensures all releases undergo rigorous security scanning and validation.

Federation and extensibility

Rocket.Chat is designed for secure connectivity and modular adaptability across diverse mission environments. Its architecture enables cross-enclave communication where appropriate and supports flexible extension to meet evolving operational requirements.

Native federation

Rocket.Chat workspaces can be federated via the Matrix protocol, enabling communication between selected users and rooms across authorised workspaces. Bridges are also available for integration with messaging systems based on XMPP and proprietary platforms such as Microsoft Teams.

A native XMPP translator is under development to simplify integration with NATO systems and legacy mission networks that rely on XMPP-based messaging.

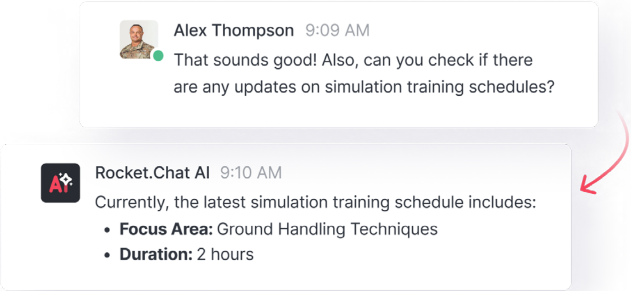
AppsEngine extensibility

The Rocket.Chat's AppsEngine toolkit enables developers to build secure, modular applications ("apps") deployable across any workspace. These apps automate workflows, integrate data streams, and extend Rocket.Chat functionality without altering core code—preserving accreditation integrity.

Future enhancements will extend AppsEngine to support apps that act as MCP clients to standardize AI integrations.

John Simon 9:09 AM
Initiate Operation Stealth Raptor at 0400 hours. Deploy assets to grid 17.

Joe 9:10 AM
Acknowledged. Alpha and Bravo teams will mobilize at 0330 hours. Coordinates confirmed.



Alex Thompson 9:09 AM
That sounds good! Also, can you check if there are any updates on simulation training schedules?

Rocket.Chat AI 9:10 AM
Currently, the latest simulation training schedule includes:

- **Focus Area:** Ground Handling Techniques
- **Duration:** 2 hours

AI and mission intelligence

Rocket.Chat delivers a proprietary architecture for integrating secure, on-premises AI assets designed to meet mission needs.

Intelligent search

Specific rooms or categories of rooms can be designated for secure indexing and semantic retrieval. All indexed data is stored in the vector search repository, with encryption levels segregated according to message classification attributes. Natural-language search requests are parsed to extract filter criteria, and retrieval is scoped according to user room access and ABAC policy enforcement.

Secure knowledge base (RAG architecture)

Rocket.Chat's on-premises RAG pipeline is used to ingest natural language content which is stored as vector embeddings. All data is stored with segregated encryption by classification level and users can interact with stored knowledge via Rocket.Chat's augmented retrieval which includes comprehensive guardrails when retrieving data and synthesizing replies.

Summarisation and translation

Messages and conversations can be summarised by RAI based on the content of a thread or within a specified chronological range of messages. Translations can also be performed on demand, supporting any source and target languages available through the large language model (LLM) selected by the organisation.

These capabilities enable U.S. government and defense organizations to maintain full control over information and eliminate dependence on external or non-accredited AI services.

Proven deployments and mission impact

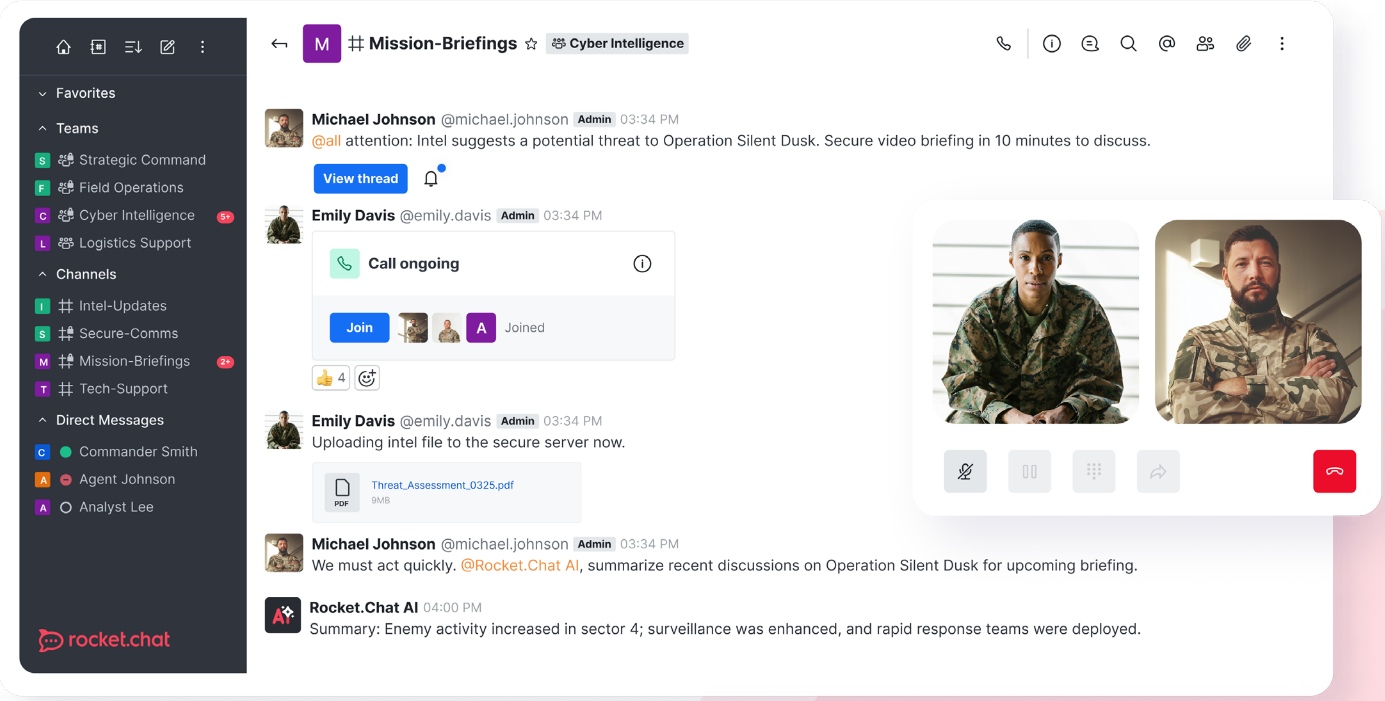
Rocket.Chat Secure CommsOS™ is a trusted communications platform deployed across U.S. defense, intelligence, federal civilian organizations, and major federal system integrators operating in classified, air-gapped, and high-assurance network environments. It supports a wide range of national and joint mission programs, providing secure messaging, voice, video, and workflow automation for multi-domain operations, command and control, and interagency coordination.

Across these deployments, Rocket.Chat has demonstrated the ability to operate securely within air-gapped and classified networks while maintaining the agility and interoperability required for joint, coalition, and multi-domain operations. Its deployment success underscores its readiness for sustained mission use under the most demanding security and performance conditions.

Rocket.Chat provides a proven, extensible, and Zero-Trust-compliant foundation for unified mission communications. Its open architecture, hardened deployment model, and AI-enabled automation deliver operational agility, situational awareness, and assured information integrity across the full spectrum of defense and intelligence operations—empowering warfighters, analysts, and decision-makers to collaborate securely and effectively in any environment.

Confidentiality Notice:

Rocket.Chat upholds strict standards of discretion and operational security. Due to the sensitive nature of defense, intelligence, and federal programs, external disclosure of specific customers, deployments, or environments is prohibited. Any references in this document are provided solely for internal use by cleared personnel and authorized partner organizations with a legitimate need to know.



Michael Johnson @michael.johnson Admin 03:34 PM
@all attention: Intel suggests a potential threat to Operation Silent Dusk. Secure video briefing in 10 minutes to discuss.

Emily Davis @emily.davis Admin 03:34 PM
Call ongoing

Emily Davis @emily.davis Admin 03:34 PM
Uploading intel file to the secure server now.

Michael Johnson @michael.johnson Admin 03:34 PM
We must act quickly. @Rocket.Chat AI, summarize recent discussions on Operation Silent Dusk for upcoming briefing.

Rocket.Chat AI 04:00 PM
Summary: Enemy activity increased in sector 4; surveillance was enhanced, and rapid response teams were deployed.

Connect with our Federal Solutions team

Contact us

rocket.chat