Mattermost

Mattermost for Cyberdefense Operations

Sovereign Response When Seconds Count

Mattermost provides a sovereign collaboration backbone for cyber defenders that supports everyday vigilance, trusted intel sharing and resilient incident response.

Strengthen security through everyday operational readiness

Cyber resilience is built in the everyday work of security teams—sharing insights, assessing anomalies, coordinating updates, and refining response playbooks. These ongoing interactions are where strong defense takes shape.

Mattermost enhances this foundation with purpose-built collaboration designed to fit the needs of SOC, CERT/CSIRT, MSSPs, and other cyberdefense teams, ensuring secure communication channels for routine operations and strategic planning alike. It empowers security organizations to stay connected, aligned, and effective—long before threats escalate.

Built for Security Operations

Battle-tested in real-world incidents across financial services, critical infrastructure, and government agencies globally, Mattermost provides genuine independence from primary infrastructure—deployed on separate networks, servers, and authentication systems for truly resilient collaboration

Built from inception for high-security environments with granular access controls, encryption-in-transit and at-rest, and support for air-gapped deployment. Mattermost supports NIS2, GDPR, HIPAA, PCI DSS, and government security requirements through flexible deployment and comprehensive audit capabilities.

Ransomware Response

When ransomware encrypts corporate systems including email and collaboration tools, security teams coordinate investigation and remediation through Mattermost, maintaining operational tempo while primary systems remain offline.

Data Breach Containment

Cross-functional response teams (security, legal, communications, IT) collaborate in real-time through automated playbooks, ensuring coordinated action, stakeholder notification, and regulatory compliance during breach response.

SOC Operations

Security analysts triage alerts, share threat intelligence, and escalate incidents through Mattermost channels integrated with the security stack to reduce alert fatigue and accelerate threat response.

Cyber Readiness Coordination

Red teams and blue teams coordinate complex exercises through secure, isolated Mattermost environments for more realistic training scenarios without compromising production systems.

Mattermost for Cyberdefense Operations

Key Platform Capabilities

Forensic Readiness

- Comprehensive audit logs preserving all incident-related communications
- eDiscovery and legal hold capabilities for regulatory compliance
- Timestamped conversation history for post-incident analysis
- Secure archiving with configurable retention policies

Out-of-Band Incident Response

- Deploy completely separate from primary infrastructure for guaranteed availability
- Maintain secure coordination when email, chat, and internal systems are compromised
- Self-hosted on isolated networks or sovereign cloud infrastructure
- Zero dependency on external services or third-party platforms

Integrated Security Operations

- Connect SIEM platforms (Splunk, Sentinel, QRadar) for centralized threat intelligence
- Integrate ticketing systems (ServiceNow, Jira) for automated case management
- Surface alerts from monitoring tools (Prometheus, Grafana, Datadog) in real-time
- Custom integrations with proprietary security tools and forensic platforms

Automated Incident Workflows

- Pre-configured playbooks for common incident types (ransomware, data breach, DDoS)
- Automated task assignment with clear ownership and escalation paths
- Structured communication ensuring nothing falls through during high-pressure events
- Built-in metrics tracking MTTA (Mean Time to Acknowledgment) and MTTR

> Because we are the CERT for critical infrastructure, one of the requirements for people to feel at ease with sharing information was that it was kept within our country. So we needed something that could be hosted locally and wasn't being controlled by another entity and started looking for a Slack alternative.
>
> — **CEO of Nonprofit CERT**

Keep Your Defenders at the Ready with Mattermost

When cyber incidents strike, your response team needs guaranteed communication. Discover how Mattermost ensures operational continuity when primary systems fail. Contact us to discuss deployment options for your security operations. **mattermost.com**

Mattermost