ARMORTEXT

Incident Response Essentials:

Three Requirements for Secure Out of Band Collaboration™

”**ArmorText excels at enabling out-of-band communications…** [and] is a great fit for security operations, incident response communications and collaboration, as well as multi-organization threat intelligence sharing.

The Forrester Wave™: Secure Communications, Q3 2022

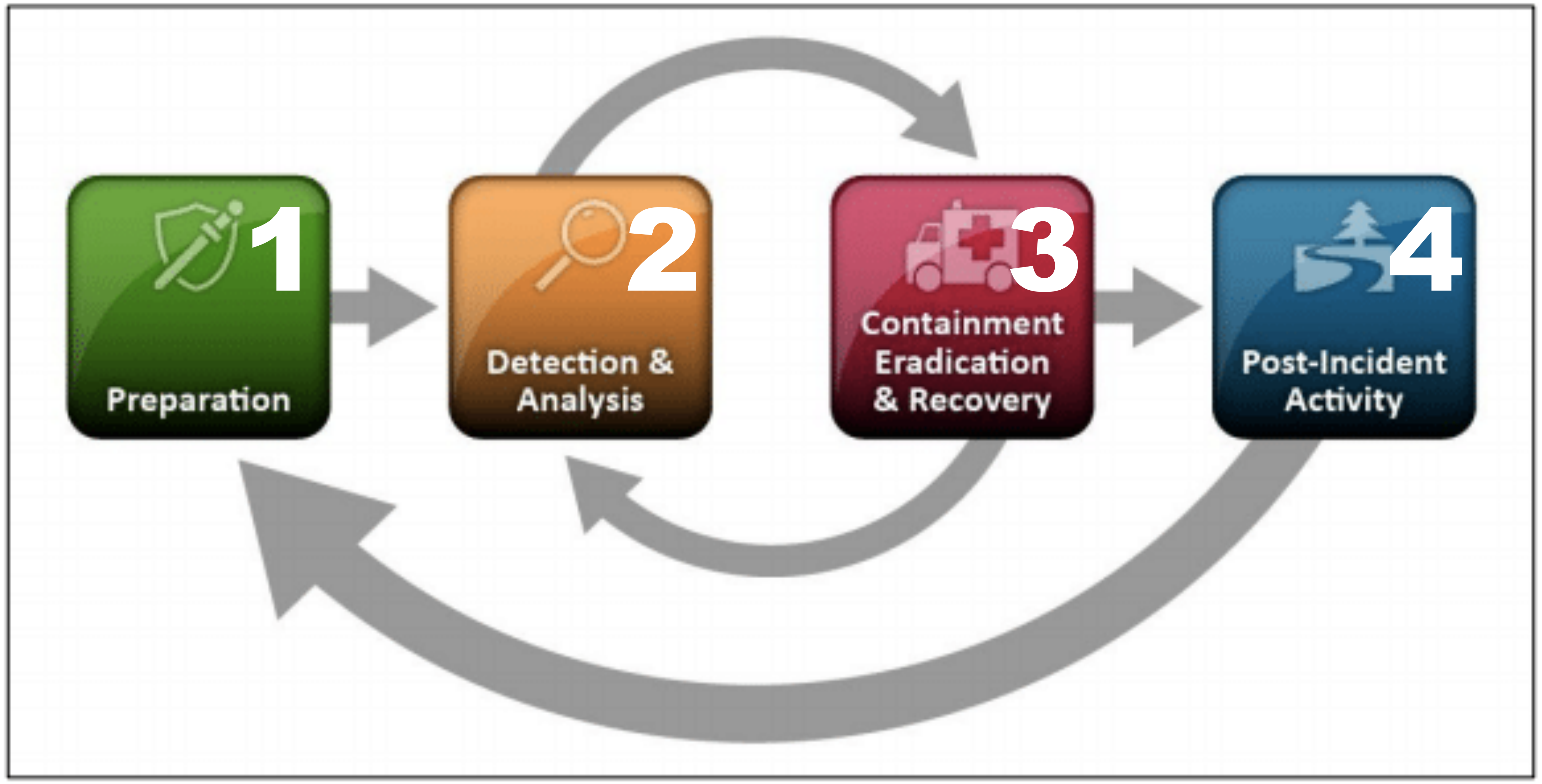
FORRESTER®

ARMORTEXT

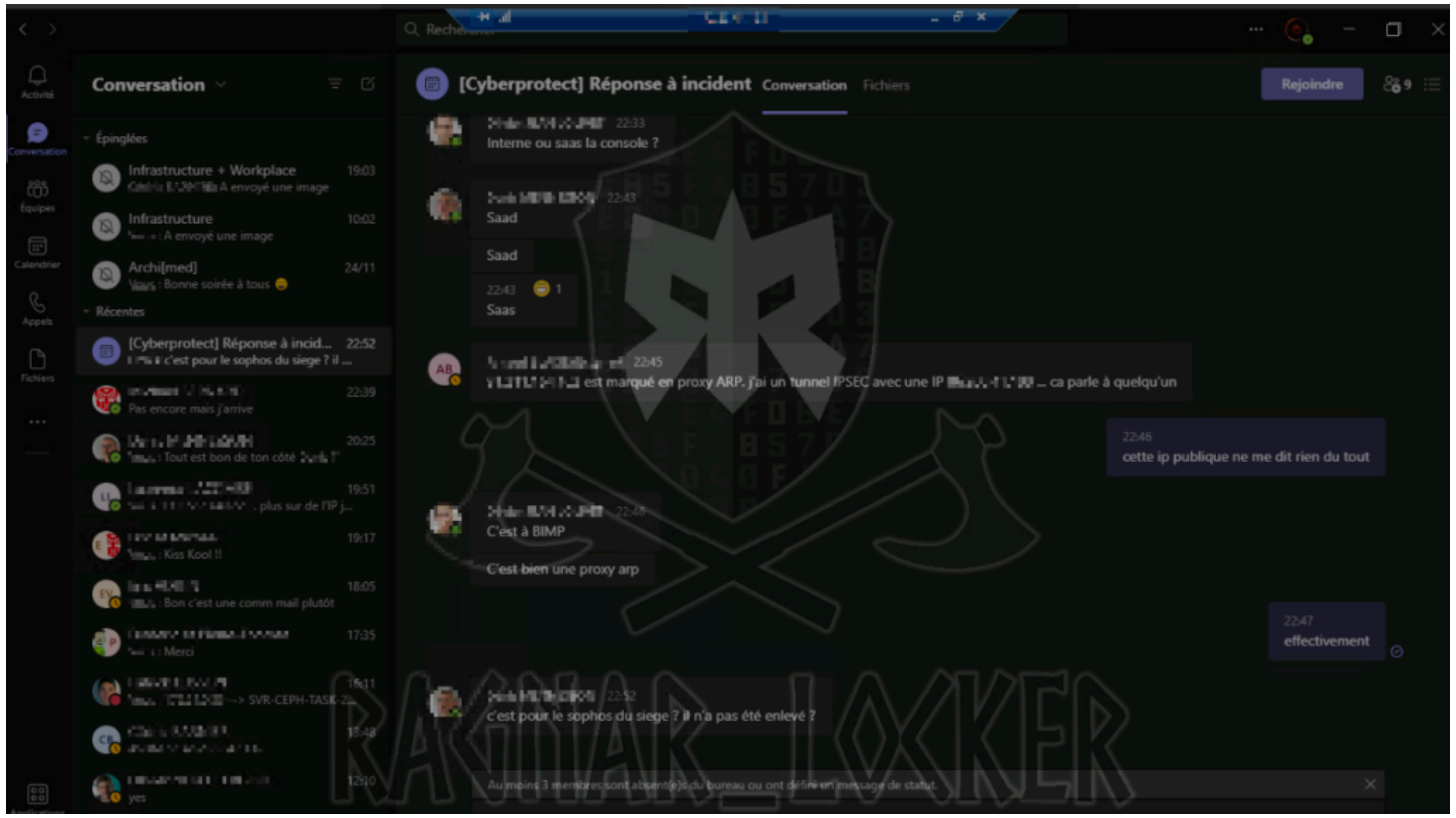
Every Incident Response Plan Is Missing The Same Thing

At each step in any incident response framework, the underlying assumption is responders and mission critical roles can **maintain communications.**

The NIST Incident Response Life Cycle



Microsoft Teams



Épinglées

- Infrastructure + Workplace 19:03 — [redacted] A envoyé une image
- Infrastructure 10:02 — [redacted] : A envoyé une image
- Archi[med] 24/11 — [redacted] : Bonne soirée à tous 😁

Récentes

- [Cyberprotect] Réponse à incid... 22:52 — [redacted] c'est pour le sophos du siege ? il ...
- [redacted] 22:39 — Pas encore mais j'arrive
- [redacted] 20:25 — [redacted] : Tout est bon de ton côté [redacted]
- [redacted] 19:51 — [redacted] . plus sur de l'IP j...
- [redacted] 19:17 — [redacted] : Kiss Kool !!
- [redacted] 18:05 — [redacted] : Bon c'est une comm mail plutôt
- [redacted] 17:35 — [redacted] : Merci
- [redacted] 16:11 — [redacted] --> SVR-CEPH-TASK-2...
- [redacted] 15:48 — [redacted]
- [redacted] 12:10 — yes

[Cyberprotect] Réponse à incident

[redacted] 22:33
Interne ou saas la console ?

[redacted] 22:43
Saad

Saad

22:43 😁 1
Saas

[redacted] 22:45
[redacted] est marqué en proxy ARP. j'ai un tunnel IPSEC avec une IP [redacted] ... ca parle à quelqu'un

22:46
cette ip publique ne me dit rien du tout

[redacted] 22:46
C'est à BIMP

C'est bien une proxy arp

22:47
effectivement

[redacted] 22:52
c'est pour le sophos du siege ? il n'a pas été enlevé ?

Au moins 3 membres sont absent(e)s du bureau ou ont défini un message de statut.

*In December 2021, Ragnar Locker ransomware group breached a French company and released **screenshots** of their **incident response chats** in real-time.*

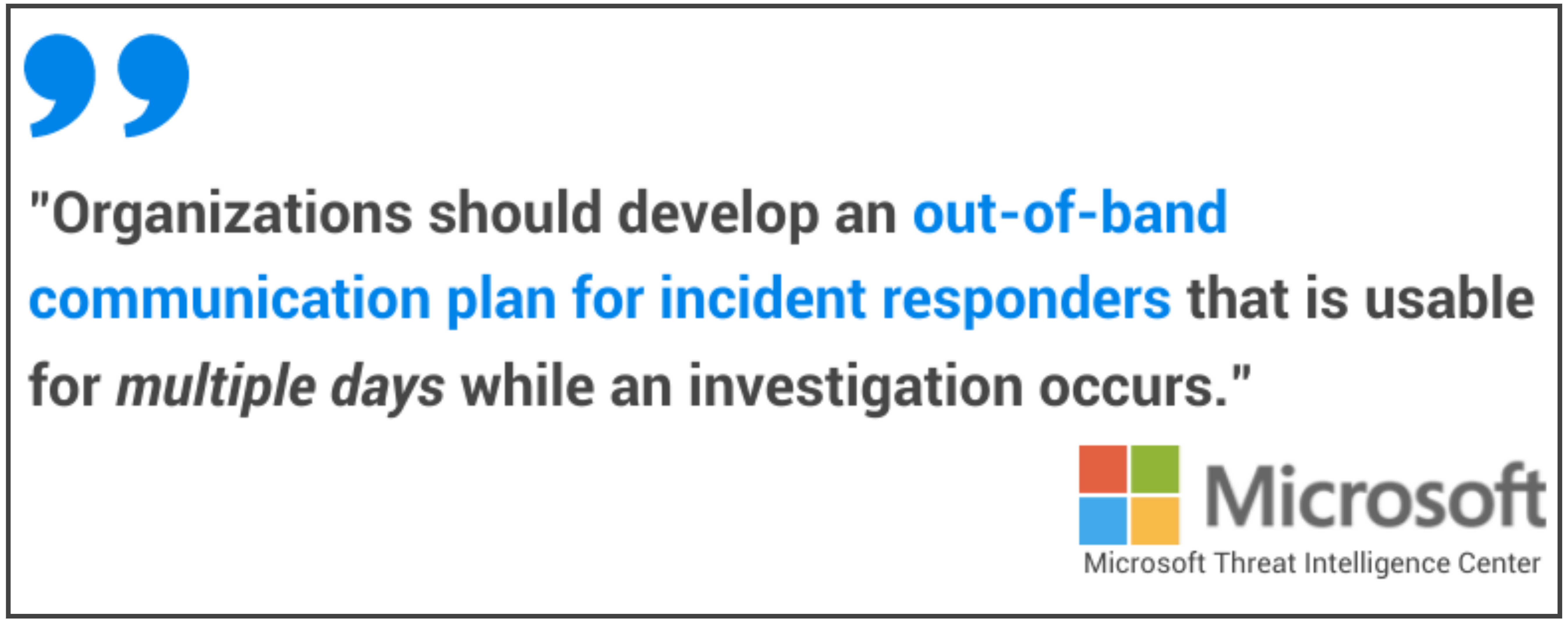
Step Zero: Don't assume your comms tools are safe

With Teams & Slack, the right set of credentials gets you **access to everything**. M&A, financial, legal, security ops, and incident response **emails and chats** are targeted for the intelligence they provide on **internal response efforts**.

ArmorText

Being prepared = Secure Out of Band Collaboration

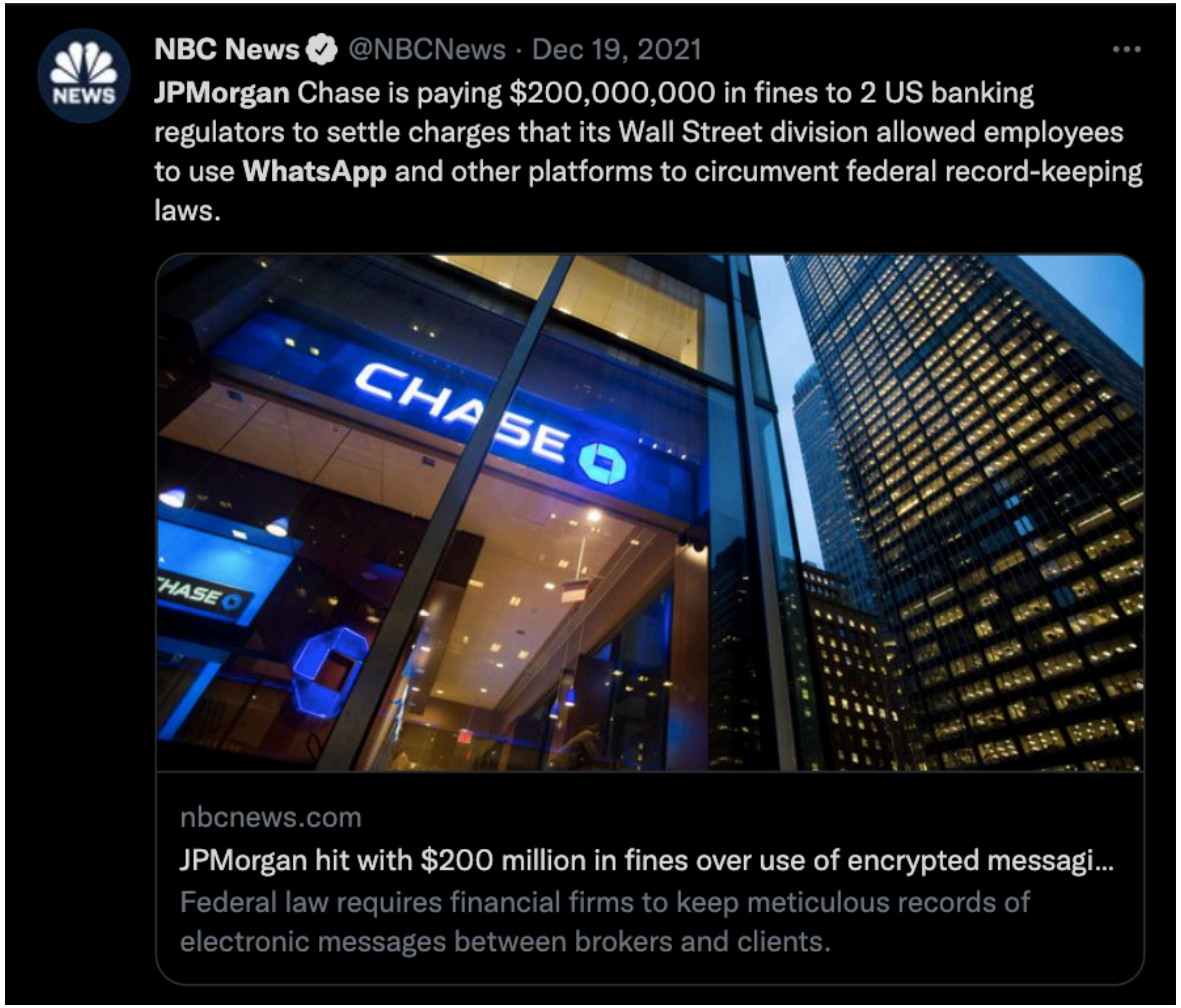
The best laid business continuity and incident response plans will not work when **communications are down** or **can’t be trusted** because a malicious attacker is in the mix.



"Organizations should develop an out-of-band communication plan for incident responders that is usable for *multiple days* while an investigation occurs."

Microsoft

Microsoft Threat Intelligence Center



NBC News @NBCNews · Dec 19, 2021

JPMorgan Chase is paying $200,000,000 in fines to 2 US banking regulators to settle charges that its Wall Street division allowed employees to use **WhatsApp** and other platforms to circumvent federal record-keeping laws.

nbcnews.com

JPMorgan hit with $200 million in fines over use of encrypted messagi...

Federal law requires financial firms to keep meticulous records of electronic messages between brokers and clients.

Signal & WhatsApp can't provide corporate controls

Security is ***more*** than just **end-to-end encryption**. Enterprises require **user management** and **policy enforcement**, and need the ability to **retain** appropriate business **records**.

Privacy Apps just create liability.

ARMORTEXT

Three Requirements for Secure Out of Band Collaboration™

Requirement #1:

It Must Be Standalone

- ❌ A Duplicate of Current Tool
- ❌ Rely on On-premise Component
- ❌ Be Dependent on Network

Requirement #2:

It Must Be More Secure

- ✓ End-to-End Encryption
- ✓ Protect Against Insider Threats
- ✓ Protect Against 3rd-party Breaches

Requirement #3:

It Can’t Sacrifice Controls

- ✓ Maintain User Policy Controls
- ✓ Retained Records Requirements
- ✗ Reintroduce On-prem Dependency

ARMORTEXT

ArmorText = Secure Out of Band Collaboration™

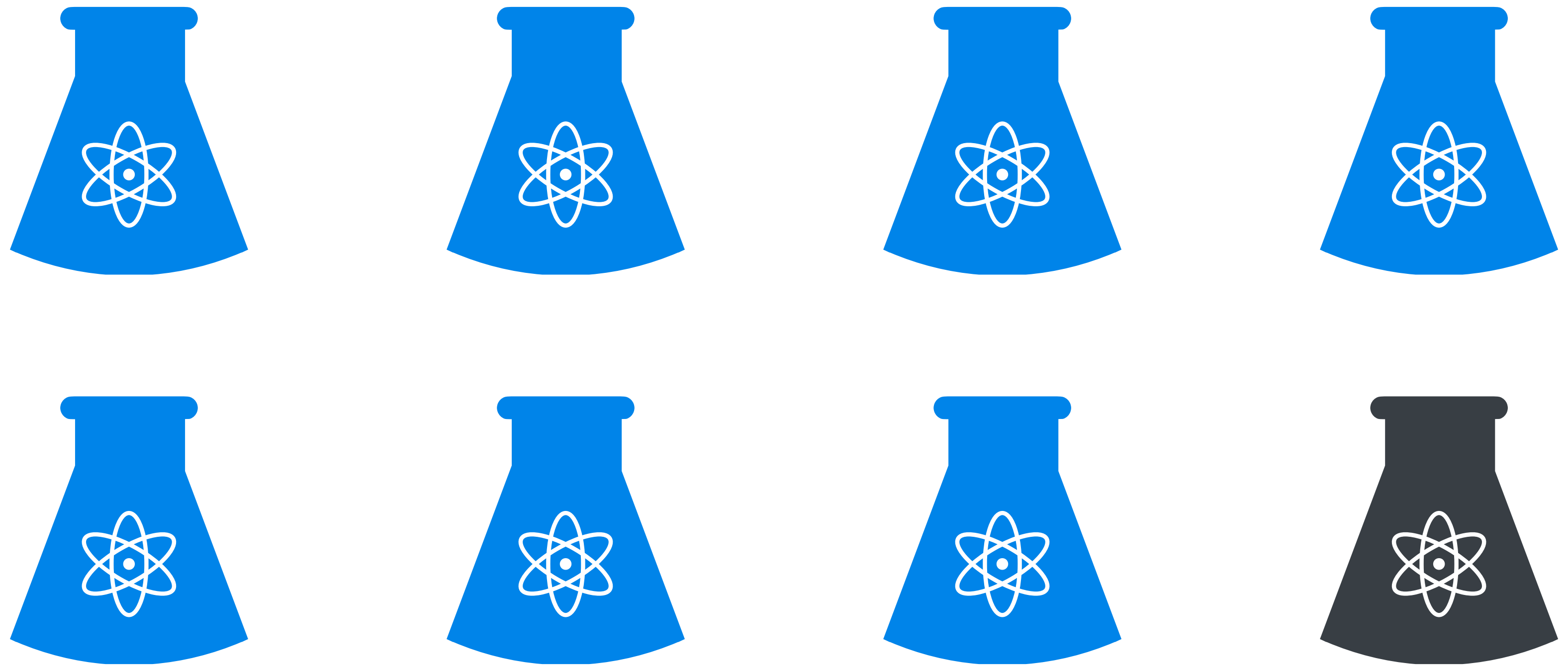
ArmorText is the easiest and most cost effective to deploy because it satisfies **all three requirements** and can be deployed in **under an hour**, providing more security for critical roles & situations **without sacrificing your governance.**

	E2EE Collaboration	User Mgmt, Policy Enfcmt.	Remediation Capabilities	E2EE Audit Trails	No Required Infrastructure	Federation w/ Governance
ARMORTEXT	✓	✓	✓	✓	✓	✓
Enterprise Privacy Apps *(e.g. Wickr, Wire)*	✓	✓	✗	✗	✗	✗
Enterprise Collaboration *(e.g. Teams, Slack, Matttermost)*	✗	✓	✗	✗	✓	✗
Consumer Privacy Apps *(e.g. Signal, WhatsApp)*	✓	✗	✗	✗	✓	✗

ArmorText is a cross-sector leader in **Secure Out of Band Collaboration™**

3 in 5 American Households get power from an **ArmorText** utility

7 out of 8 nuclear reactors are run by an **ArmorText** energy provider



ARMORTEXT

ArmorText provides secure out of band collaboration before, during, and after an incident

ArmorText's security benefits are a result of a unique end-to-end encryption approach that **maintains governance** while reducing risks and **eliminating common attack vectors**.

Exposed Credentials ≠ Exposed Data

Reviewer Access ≠ Access to Everything

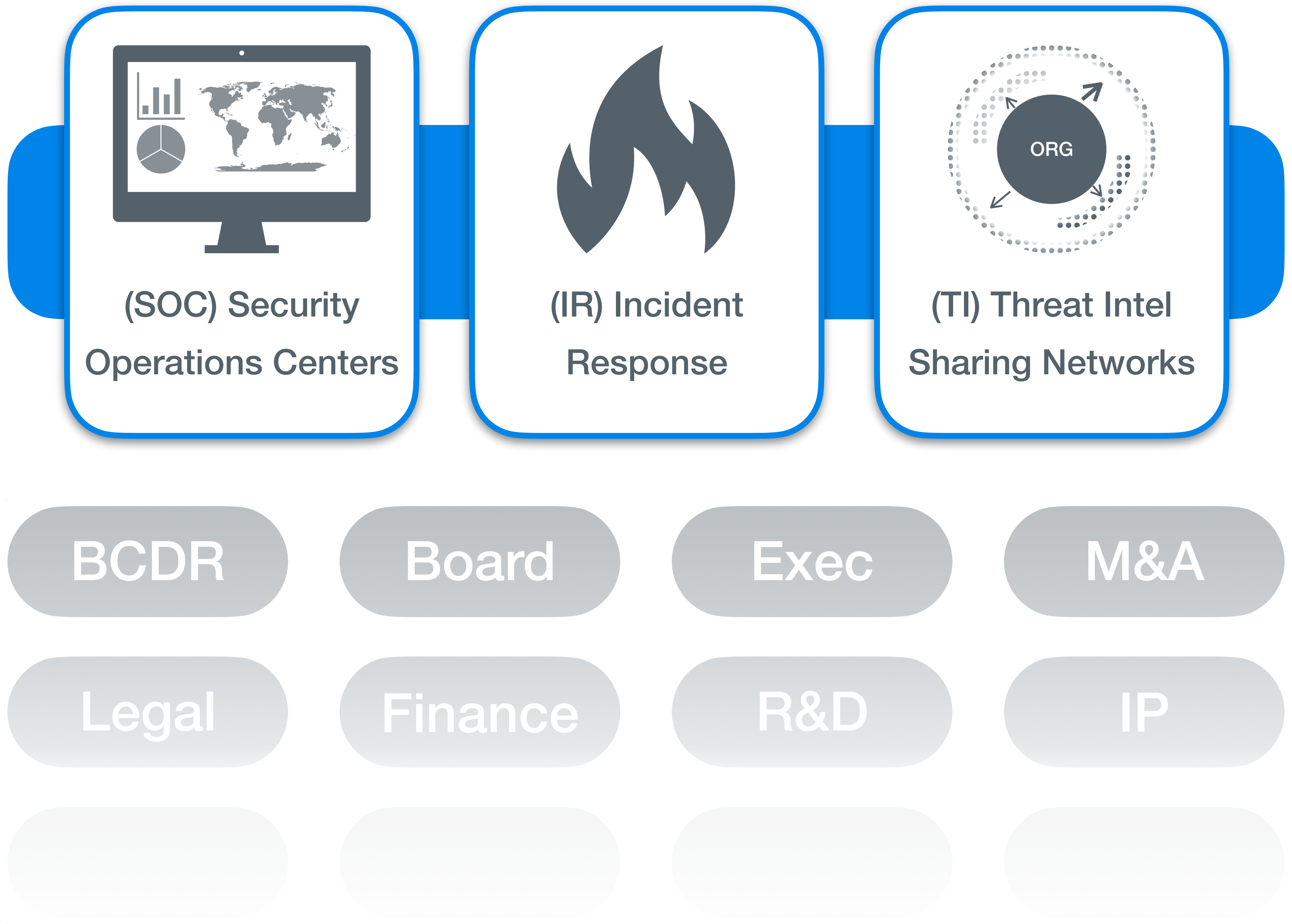
Admin Access ≠ Insider Threat

Compromised Network ≠ Comms Outage

Supply Chain Attack ≠ Data Leaks

Out of Band ≠ Out of Compliance

Initial
Use Cases



(SOC) Security Operations Centers

(IR) Incident Response

(TI) Threat Intel Sharing Networks

BCDR

Board

Exec

M&A

Additional
Use Cases

Legal

Finance

R&D

IP

Start by protecting Security Ops, Incident Response, and Threat Intel

Government and defense utilize distinct channels for secret and top secret comms. Your SOC, IR, and Threat communications deserve that same treatment.

Deploying an Out of band comms tool is easy as it runs alongside your day to day comms and is only used by a select group of critical roles in your org.

ARMORTEXT

Case Study

Energy Sector Incident Response & Collective Defense

> “When events arise, such as SolarWinds, ArmorText is the program's go-to solution to quickly stand up channels with stakeholders, share information, and collaborate in real time.”
>
> *Frank Honkus, Intelligence Programs and CRISP, Associate Director, E-ISAC*

Energy

Utilities are under constant attack from criminal and nation state actors. Portal based intel sharing is too slow for threats moving in real-time and limits active dialogue and exchange of insights.

Problem

How do you improve the quality and speed of information sharing without introducing new weaknesses for hackers to exploit?

Solution

ArmorText’s unique end-to-end encryption approach helps create *Trust* in the network and the identities of the parties sharing while ensuring each party can maintain governance.

Result

More than 80% of all large public & private power in the US leverages ArmorText to protect threat intel sharing and security operations and incident response.

FAQ

01 How does it work?

Leveraging a combination of AES and RSA, NSA approved encryption, messages (and files) shared on ArmorText are uniquely end-to-end encrypted per user per device, whether in 1:1 or group chats. As a result, when users lose devices or they are stolen or compromised, admins can remotely wipe keys and data from affected devices without impacting continuity of conversation across the users' remaining devices.

02 If I can't trust Microsoft, Slack, Cisco, etc, why should I *trust* you?

We can't read your messages. Your users' and reviewers' private keys are never shared with, stored by, or transmit via ArmorText. As a result, we ***cannot*** decrypt our clients' messages.

03 How do we maintain appropriate business records?

As messages are sent, ArmorText automatically end-to-end encrypts them for the reviewers you define. Admins setup distinct scopes-of-review, assigning reviewees to reviewers. These scopes-of-review are optional, but when present can be wholly distinct or overlap as needed.

04 How are admins different from reviewers?

Admins in ArmorText help manage onboarding, information lifecycles, users, security policies, and Trust Relationships with other orgs. Admins also help define scopes-of-review for your designated reviewers. Reviewers have read-only oversight of messages and files sent or received by their reviewees. Admins never see what isn't encrypted for them.

05 Are my comms safe when managed by a partner?

Yes. Admins outside of your organization (*e.g.* an MSSP) can help admin your ArmorText instance, however, they can't be assigned as reviewers over your people. As a result, they can't read your internal communications.

06 Why do hackers target Security Ops, Incident Response, and Threat comms?

SOC, IR, and Threat collaboration includes real-time insight into what's vulnerable and how; ransom negotiation strategies; playbooks for incident response; insights into executive responses, and often involve 3rd-parties.

07 Where else should we leverage ArmorText?

Every organization is different and must draw its own line. Determining which communications can and should take place where is an essential step in defining your Tier & Protect Strategy**™**. For many orgs this will involve internal & external M&A, legal, finance, and IP discussions along with boards whose members often involve 3rd parties.

08 Who else uses ArmorText?

Adopting ArmorText puts you in good company. Over 80% of all large US public and private power leverages ArmorText as do entities providing 3 out of 5 American households their electricity and operating 7 out of 8 nuclear reactors. The IMF, World Bank, DoE, ISACs, the Global Resilience Foundation, and organizations across sectors protect their most sensitive collaboration with ArmorText.

09 Can we connect with other orgs on ArmorText?

Yes. ArmorText Trust Relationships enable your admins to manage which orgs you're connected with and who from your side can be seen by those other orgs. You can use a common setup across Trust Relationships or tailor them uniquely as needed to suite each trusted relationship's needs. We can even help plug you in to threat sharing networks.

10 Will ArmorText run on my existing phone? Tablet? Laptop?

ArmorText clients are available for PC, MAC, Linux, iOS and Android devices.