Comprehensive Security Policy Document

📌 Section 1: Security Rules and Guidelines

To prevent, detect, and respond to cyber threats, the organization implements the following foundational rules:

1. Data Classification & Access Control

- Confidential data (e.g., football playbooks) must be classified and protected with role-based access controls.
- Access to critical data is granted only to authorized personnel and reviewed quarterly.

2. Mandatory Security Awareness Training

- All staff must complete quarterly cybersecurity training with a focus on phishing, ransomware, and insider threats.
- High-risk users (e.g., coaches, analysts) must complete an additional phishing simulation quarterly.

3. Backup & Recovery Protocol

- Backups must be taken daily, stored offline and tested weekly.
- Backups must be immutable (read-only) for at least 30 days.
- No system restoration is allowed from a potentially infected environment.

⚠️ Section 2: Incident Response Plan (Crypto Ransomware)

1. Incident Overview

- **Type:** Crypto Ransomware Attack (likely CryptoLocker variant)
- **Target:** Confidential Football Playbook Files
- **Impact:** Encrypted Files, Locked Systems
- **Ransom Demand:** $100M in Bitcoin
- **Risk Level:** Critical

---

2. Detection: SIEM-Based Threat Monitoring

- **Log Aggregation** from endpoints and servers
- **Anomaly Detection**: Rapid file renames, encrypted extensions
- **Correlation Rules**: Unusual folder access, external IP connections
- **Alert**: Triggered on ransomware indicators

---

3. Containment Strategy

- **Immediate Isolation** of affected host (LAN, VPN, Wi-Fi)
- **Account Lockout** for compromised users
- **Block Known IPs** and command & control domains
- **Preserve** forensic image for legal and audit use
- **Extended Steps:** Audit logs, restrict remote access, notify stakeholders

---

4. Eradication

- **Identify Strain** (CryptoLocker variant) via ransom note

- **Remove Executables** using EDR/AV
- **Patch Entry Point** (RDP, vulnerabilities)
- **Reset Passwords**, search for backdoors
- **Threat Hunt** using Indicators of Compromise (IoCs)

5. Recovery

- **Restore** from offline, clean backup
- **Rebuild OS**, reinstall software, validate data integrity
- **Monitor** restored systems for 48 hours
- **Notify Stakeholders & Law Enforcement**
- **Communicate** breach impact appropriately

6. Post-Incident Actions

- **Conduct Post-Mortem** and documentation
- **Update** SIEM rules and detection systems
- **Run Refresher Trainings**
- **Improve Backup Strategy**
- **Share Intelligence** with ISACs and law enforcement

🔐 Section 3: CIA Triad Alignment

CIA Element	Policy/Procedure Alignment

Confidentiality	Data access is restricted to authorized users only. Playbooks and other IP are encrypted and stored securely.
Integrity	Only validated, clean backups are restored. Systems are rebuilt from trusted sources to avoid corruption.
Availability	Backups ensure continuity. Recovery procedures restore operations within defined RTO/RPO timelines.

⚖️ Section 4: Legal & Ethical Compliance

📜 Relevant Laws & Regulations

1. **Computer Fraud and Abuse Act (CFAA)** – Addresses unauthorized access to protected systems. Our IRP ensures compromised access is immediately revoked and investigated.

2. **General Data Protection Regulation (GDPR)** or **State Data Breach Laws (e.g., CCPA)** – Requires prompt breach notification and secure handling of personal or sensitive data.

🤝 Ethical Considerations

- **Do Not Pay Ransom**: Unless all legal and recovery avenues are exhausted, paying ransom is discouraged as it may fund criminal enterprises.

- **Transparency with Stakeholders**: Ethical responsibility to notify affected individuals and partners of breaches in a timely, honest, and respectful manner.

✅ How the IRP Upholds These:

- Logs and forensic images are preserved for legal investigation.

- Law enforcement is notified of critical ransom demands.

- Public and internal communication aligns with legal and ethical standards of breach disclosure.

- User training helps prevent social engineering exploits, fostering ethical responsibility among staff.

✅ Final Notes

This Security Policy and Incident Response Plan are designed to:

- Safeguard confidential data
- Respond effectively to ransomware attacks
- Align with legal mandates and ethical values
- Maintain the integrity of operations under stress

Would you like this exported as a downloadable Word or PDF document?

You said:
break down CIA TRIAD ALIGNMENT , in what steps would it be breached and steps to fix the breach

ChatGPT said:

Here's a breakdown of the **CIA Triad Alignment** specifically for your ransomware scenario. It explains:

- **How each element of the CIA Triad (Confidentiality, Integrity, Availability) could be breached**
- **What steps in your Incident Response Plan address and fix each breach**

🔐 CIA TRIAD BREAKDOWN: BREACH & RESPONSE

🔒 1. Confidentiality

Definition: Ensuring that sensitive information is accessed only by authorized users.

🔻 **How It's Breached in the Attack:**

- The attacker **gained unauthorized access** to the confidential football playbook.
- Files may be **exfiltrated** before encryption.
- **Phishing or RDP exploit** was used to access internal systems.

🔧 **Steps to Fix Confidentiality Breach:**

1. **Containment**
    - Disable compromised user accounts.
    - Block command-and-control IPs to stop data exfiltration.
2. **Eradication**
    - Patch the entry point (RDP vulnerability or phishing vector).
    - Remove persistence mechanisms (e.g., scheduled tasks, registry keys).
3. **Post-Incident**
    - Rotate all access credentials.
    - Implement stricter access control and MFA.
    - Conduct phishing training refreshers.

✅ 2. Integrity

Definition: Ensuring that data is accurate, unaltered, and trustworthy.

🔻 **How It's Breached in the Attack:**

- Ransomware **encrypts files**, rendering them altered and unreadable.

- There’s a risk of **file tampering or injection of malicious code** before or after encryption.

🔧 Steps to Fix Integrity Breach:

1. **Detection**
    - SIEM flags unauthorized encryption or data manipulation.
2. **Recovery**
    - Validate and restore files from **pre-infection backups**.
    - Rebuild systems from **trusted, clean OS images**.
3. **Post-Incident**
    - Monitor restored systems for anomalies to confirm data integrity.
    - Run endpoint detection and vulnerability scans.
    - Improve backup testing and implement file integrity monitoring tools.

🟢 3. Availability

Definition: Ensuring systems and data are accessible to authorized users when needed.

🔻 How It’s Breached in the Attack:

- Systems are **locked down** or **crashed** by the ransomware.
- Users **cannot access** critical files or applications during the attack.

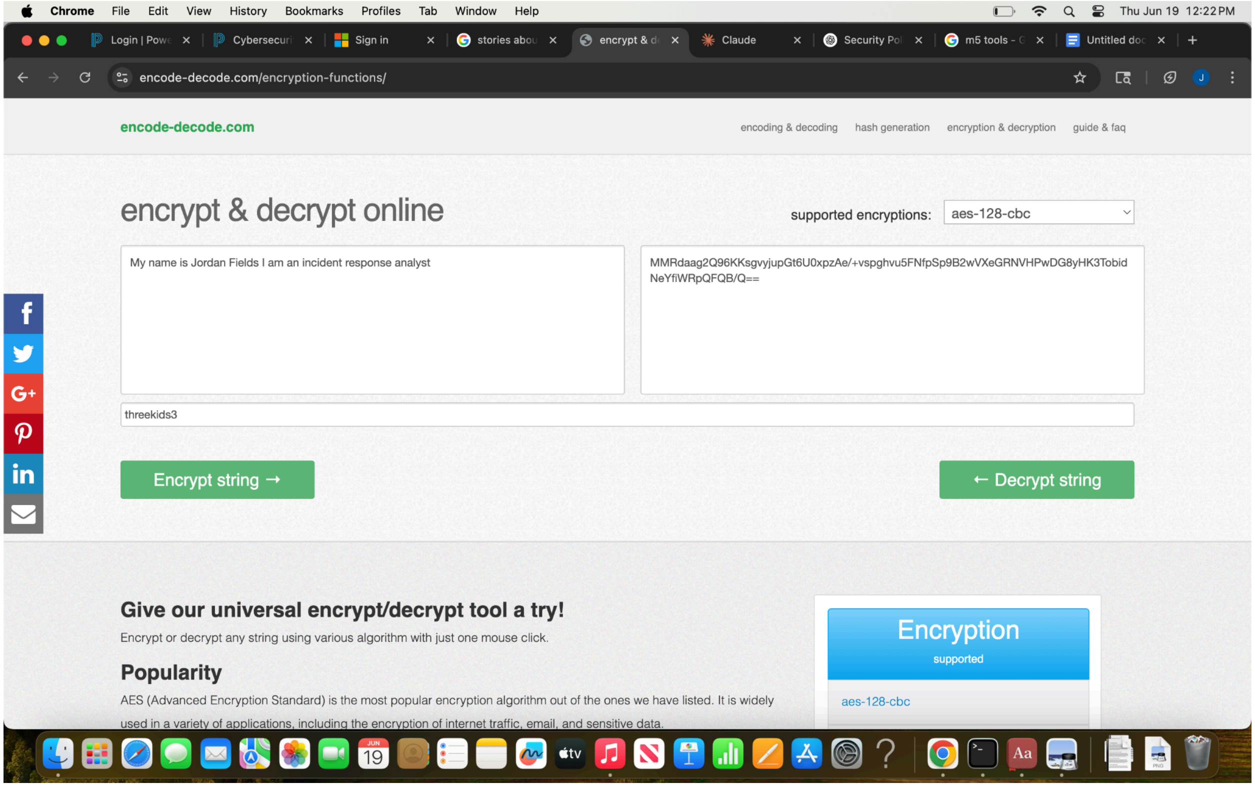
🔧 Steps to Fix Availability Breach:

1. **Containment**
    - Isolate infected systems to prevent ransomware from spreading further.

2. **Recovery**
    - Restore affected machines from **offline, clean backups**.
    - Rebuild entire environments from scratch if needed.
3. **Post-Incident**
    - Strengthen backup systems with **offsite and immutable backups**.
    - Conduct disaster recovery drills to improve RTO (Recovery Time Objective).

🧩 Summary Matrix

CIA Element	How It Was Breached	Fixing Steps
Confidentiality	Unauthorized access to playbooks, possible data theft	Disable accounts, block C2 traffic, patch entry, rotate creds
Integrity	Files encrypted and potentially modified	Restore from clean backups, rebuild system, scan for tampering
Availability	Systems and data rendered inaccessible	Isolate systems, restore backups, rebuild OS, test resilience



encrypt & decrypt online

supported encryptions: aes-128-cbc

My name is Jordan Fields I am an incident response analyst

MMRdaag2Q96KKsgvyjupGt6U0xpzAe/+vspghvu5FNfpSp9B2wVXeGRNVHPwDG8yHK3TobidNeYfiWRpQFQB/Q==

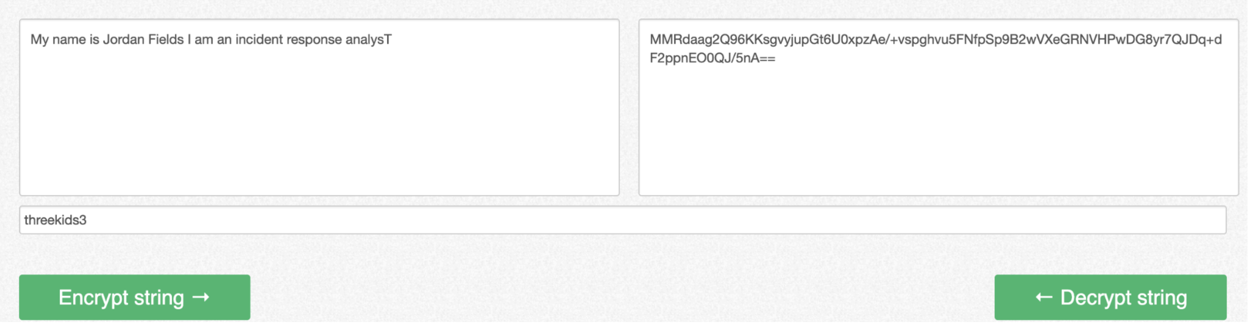
threekids3

Give our universal encrypt/decrypt tool a try!

Encrypt or decrypt any string using various algorithm with just one mouse click.

Popularity

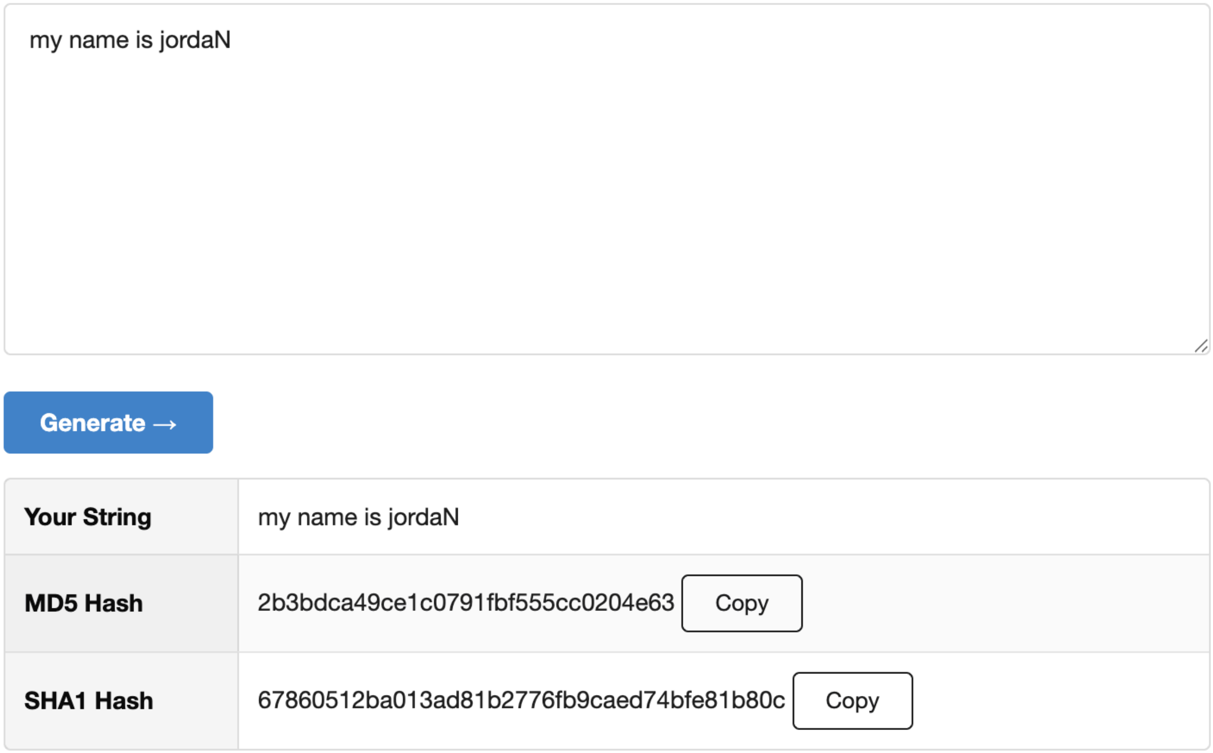
AES (Advanced Encryption Standard) is the most popular encryption algorithm out of the ones we have listed. It is widely used in a variety of applications, including the encryption of internet traffic, email, and sensitive data.



My name is Jordan Fields I am an incident response analysT

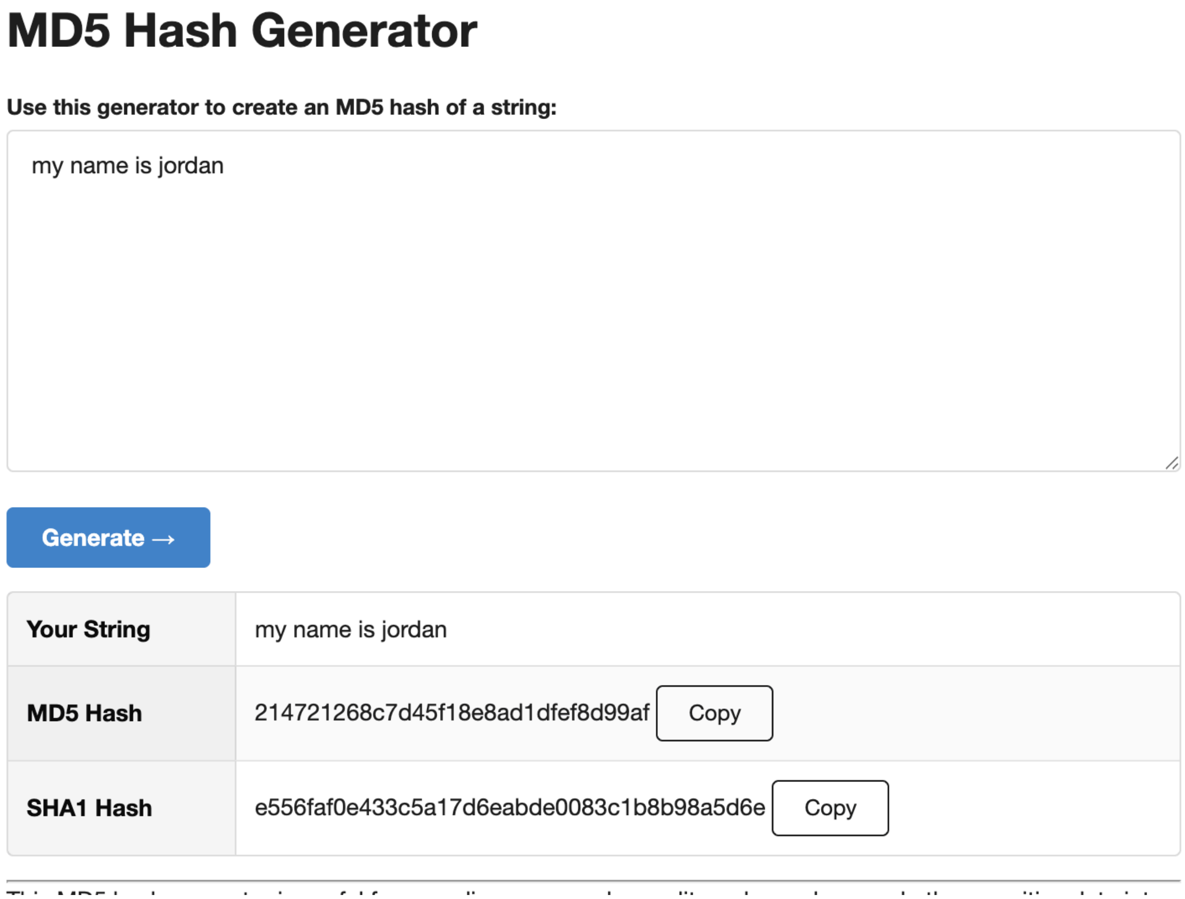
MMRdaag2Q96KKsgvyjupGt6U0xpzAe/+vspghvu5FNfpSp9B2wVXeGRNVHPwDG8yr7QJDq+dF2ppnEO0QJ/5nA==

threekids3



my name is jordaN

Your String	my name is jordaN
MD5 Hash	2b3bdca49ce1c0791fbf555cc0204e63
SHA1 Hash	67860512ba013ad81b2776fb9caed74bfe81b80c



MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

my name is jordan

Your String	my name is jordan
MD5 Hash	214721268c7d45f18e8ad1dfef8d99af
SHA1 Hash	e556faf0e433c5a17d6eabde0083c1b8b98a5d6e