SECURE YOUR LOGS DOWN TO THE ROOT

QuintessenceAnx

APPDYNAMICS

Before I Get Started

There will be some text heavy slides.

😱📚

There is a link to my slides & resources at the end.

DON'T PANIC

Let's Dive In.

Quick Overview of Terms and Concepts*

*Not an exhaustive list.

Hash: obscuring data (one-way)

Pinch of salt

🧂

Encrypt:
obscuring data (reversibly)

Try to avoid bloating the term "security"

Different Security Objectives*

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Non-repudiation

*Also not an exhaustive list.

Always be aware of your objective(s).

Oh, and what do I not mean by security?

Security Through Obscurity

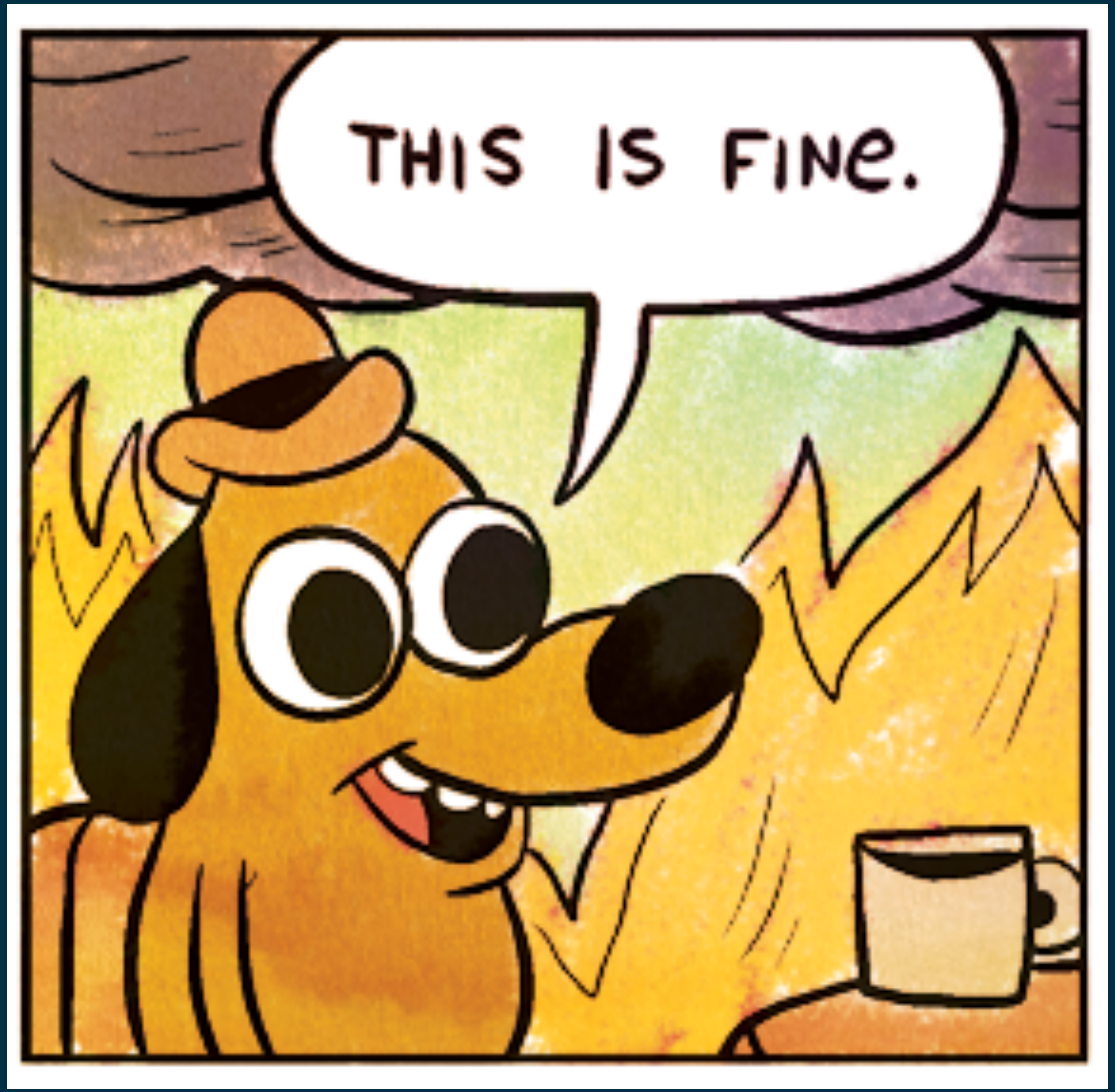
No.

Do not do this.

'cause consequences

e.g. "They don't know where ${X} is, right?"

Who needs consistent naming conventions anyway?


THIS IS FINE.

e.g. "Key management is hard, let's share."

This isn't your housemate.

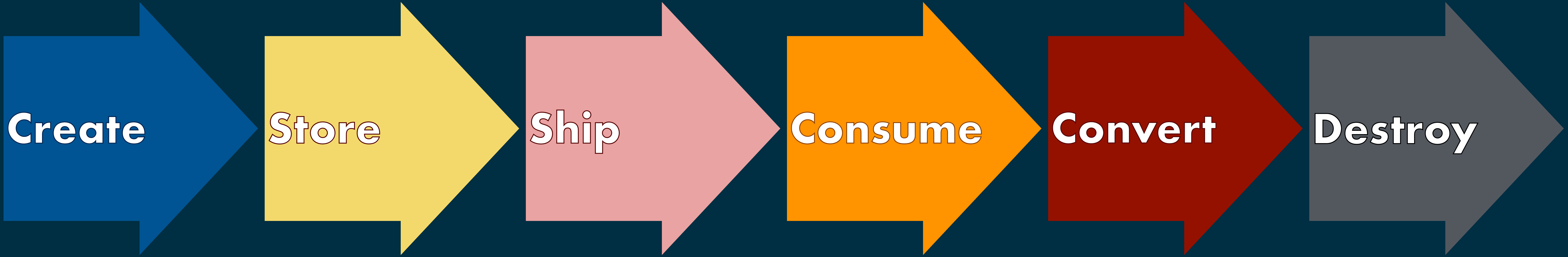
I'M OKAY WITH THE events THAT ARE UNFOLDING CURRENTLY.

There are more, but I think you grok me.

☺️

The main event: how does this apply to logs? 🤔

Log Lifecycle



Create

Store

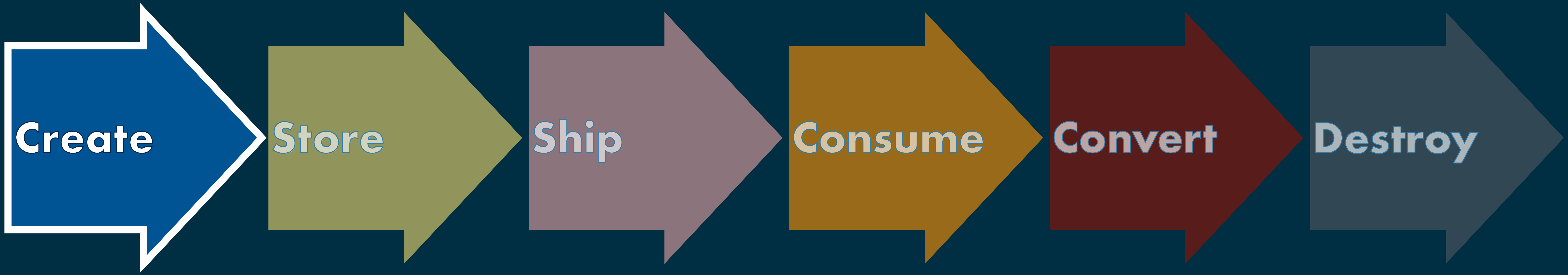
Ship

Consume

Convert

Destroy

Create



Create

Store

Ship

Consume

Convert

Destroy

Do not write sensitive data to your logs

Do not. write. sensitive data. to your logs.

Sensitive data, e.g.:

- Personally identifying information (PII)
  - SSNs are high cardinality, right? 😂
- Credentials, including passwords and keys
  - e.g. ever version control your dotfiles?
- Keystrokes
- Matching results by either percent (e.g. X% match on FaceID or fingerprint) or pass/fail
- Financial or health data
- Internal endpoints and/or IP addresses
- Database queries
- The list goes on.

Essentially, log only what you need.

"What if I really need that sensitive data", you ask?

Food for thought, this is CWE-532.

So it comes up.

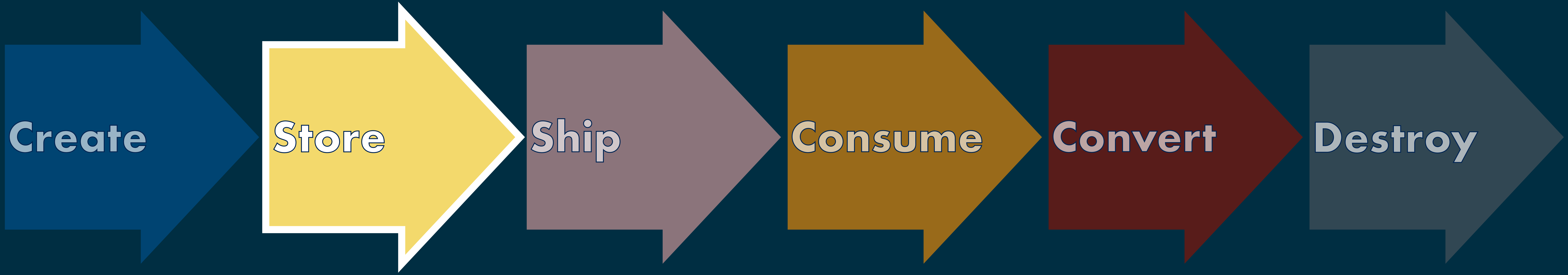
Don't ship it - log around it, e.g.:

- Use a token that references the data
- Use a salted or low-sodium hash
- Encrypt the log and/or your data
- Redact data as needed
- Remember to adhere to any regulatory compliance requirements
  - e.g. PCI, HIPAA

Now what to do with these logs?

☺️

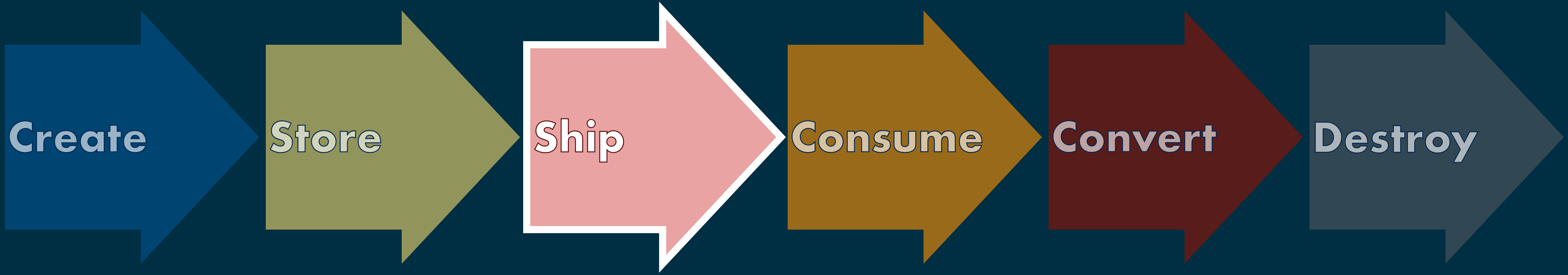
Store



Batten Down the Hatches

- Limit access to the log files
- Limit access to the storage volume(s) they reside on
- Log files should be append only
- Encrypt where possible
- Take a look at forward secure sealing (FSS) if you're encrypting your logs
  - i.e. how to prevent past manipulation with current keys
- Rotate your log files regularly

Ship



Create

Store

Ship

Consume

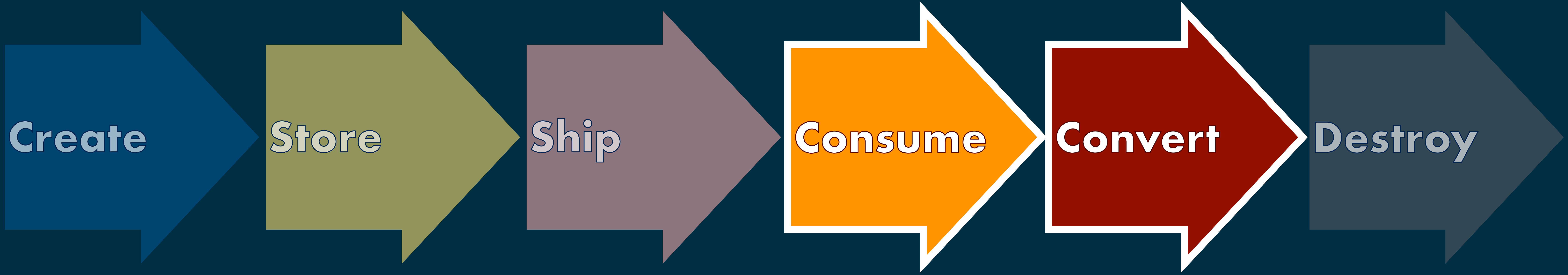
Convert

Destroy

Actually shipping it this time

- If you are using a 3rd party / SaaS solution:
  - Make sure your provider supports shippers that allow you to ship securely, e.g. over TLS / SSL via rsyslog.
- If using an on prem solution:
  - Secure your network
  - Ship encrypted
  - Limit key access to central log server

Consume & Convert



Create

Store

Ship

Consume

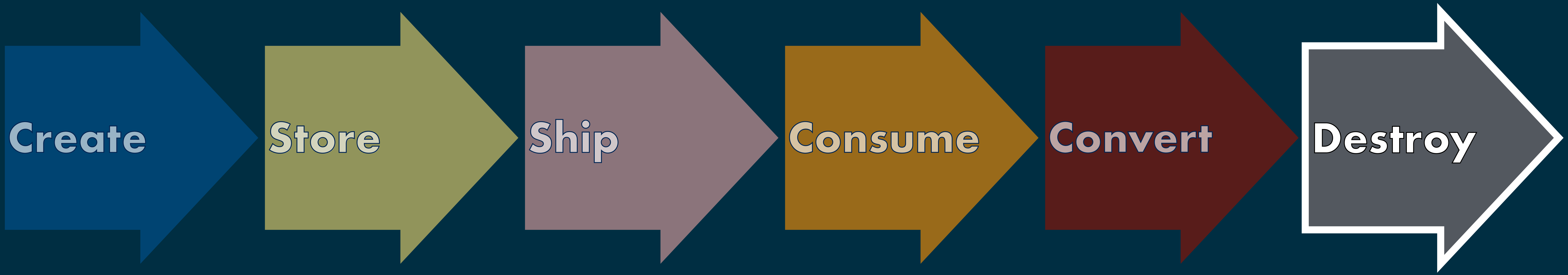
Convert

Destroy

Safe Data Use

- For a SaaS solution: ensure they provide access control
- For an on prem solution: ensure you have access control
  - Also: limit access to the log server itself
- Limit / deny malformed or malicious queries
  - e.g. Elastic has a handy 2014 blog post (back in its youth) that explains a few ways to crash the then-current version of Elasticsearch (to help you start thinking about this topic).

Destroy



Create

Store

Ship

Consume

Convert

Destroy

Secure Destruction

- This also comes up often (CWE-117)
- Ensure that locally and remotely (if using a SaaS) that data is destroy according to relevant industry standards
  - e.g. CESG CPA, Crypt Erase, NIST
  - This may mean anything from wiping data to shredding physical storage, depending on your industry.
- Do you need to delete or wipe? Know the difference. Use the difference.

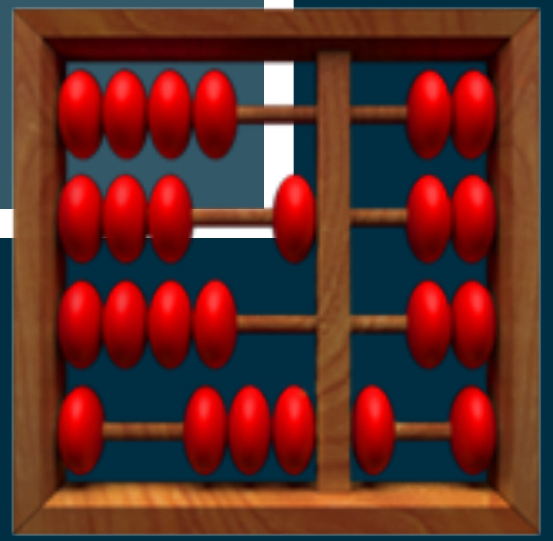
Closing Tips

Tip # 1: Know your data

Tip # 2: Know your infrastructure

👀

Tip # 3: Know your risks



Tip # 4: Don't apply what doesn't apply

🤔

Tip # 5: Trust, but verify

👌

Tip # 6: Use your metrics

Tip # 7: Protect & utilize your audit trail

Tip # 8: Use well designed alerts judiciously

🚨

Tip # 9: Don't be a target - find help as needed

Tip # 10: Prevention is the difference between This Is a Problem and This Is a Disaster.

🤔 🥺

Slides, References, & Reading Available on Notist

https://noti.st/quintessence

Thank you!

QuintessenceAnx

Technical Evangelist 🥑

@

APPDYNAMICS