Secure Your Logs Down to the root

Quintessence Anx, Technical Evangelist
@QuintessenceAnx

Barcelona | January 27-31, 2020

DEVLIT-4020

Agenda

- Introduction
- Quick Concept Review
- Log Management Life Cycle
- Security Implications Over the Cycle
- Best Practices Moving Forward
- Conclusion

Before I Get Started

There will be some text heavy slides 😱📚

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

Let’s Dive In

A Quick Overview of Terms & Concepts

Hash: Obscuring Data

(one directional)

Pinch of salt

Encrypt: Obscuring Data

(bi-directional)

Common Weakness Enumeration (CWE)

Common Vulnerabilities and Exposures (CVE)

Try to avoid bloating the term “security”

Different Security Objectives*

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

*Not an exhaustive list

Always be aware of your objective(s).

Oh, and what do I not mean by security?

Security through obscurity

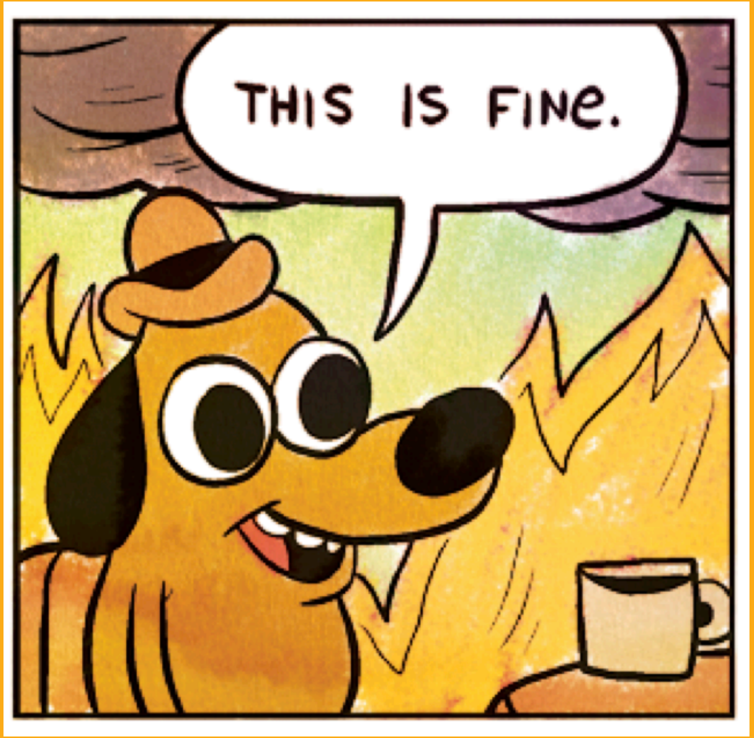
No.

Do not do this.

Because (unintended) consequences

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

(Who needs consistent naming conventions anyway?)


THIS IS FINE.

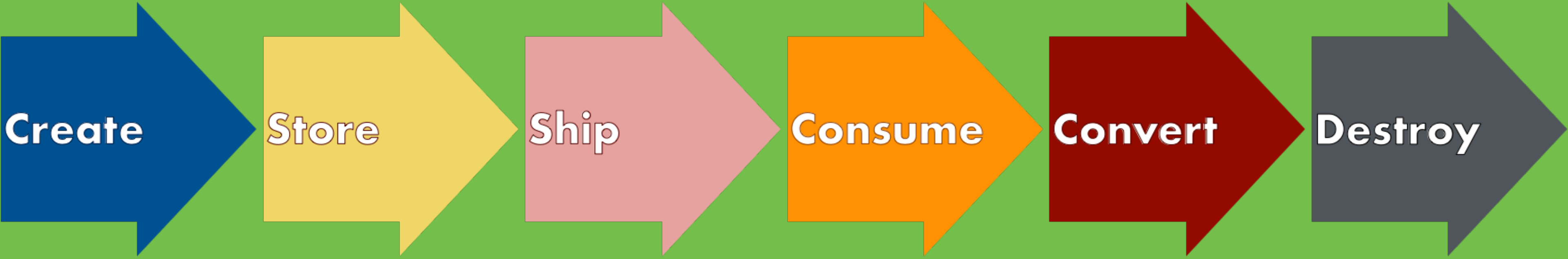
e.g. "Key management is hard, let's share."

(This isn't your housemate.)

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

There are more, but I think you got it.

The main event: how does this apply to logs?



Create

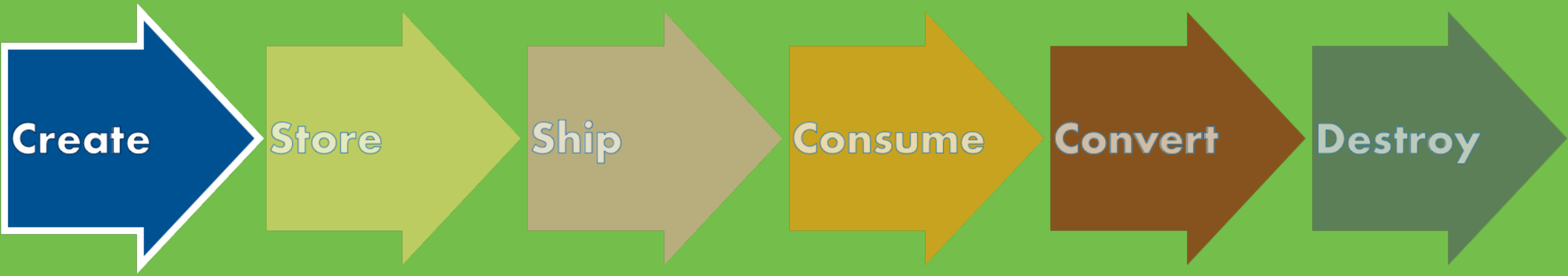
Store

Ship

Consume

Convert

Destroy



Create

Store

Ship

Consume

Convert

Destroy

Do not write sensitive data to your logs

Do not write sensitive data to your logs.

What is sensitive data?

Some Examples of Sensitive Data*

- Personally identifying information (PII)
  - Tax and passport IDs 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

*Not an exhaustive list

Essentially, log only what you need.

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

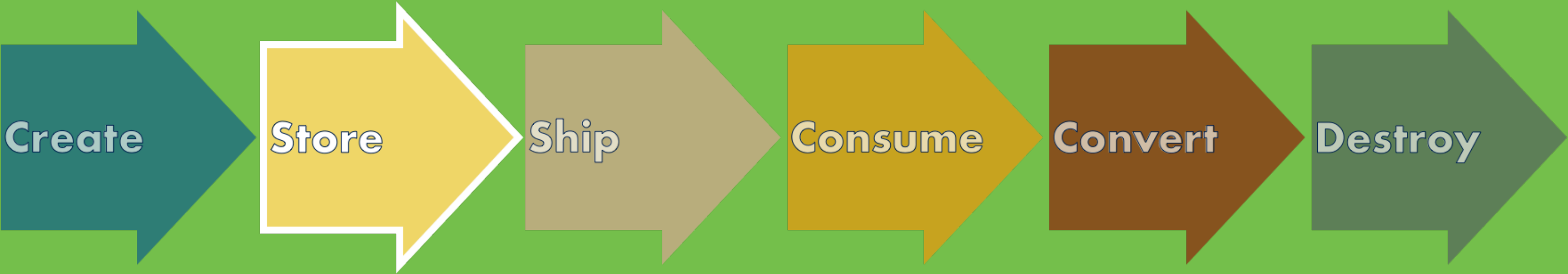
Food for thought, this is CWE-532*.

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. GDPR, CCPA, PCI, HIPAA

Now what to do with these logs?



Create

Store

Ship

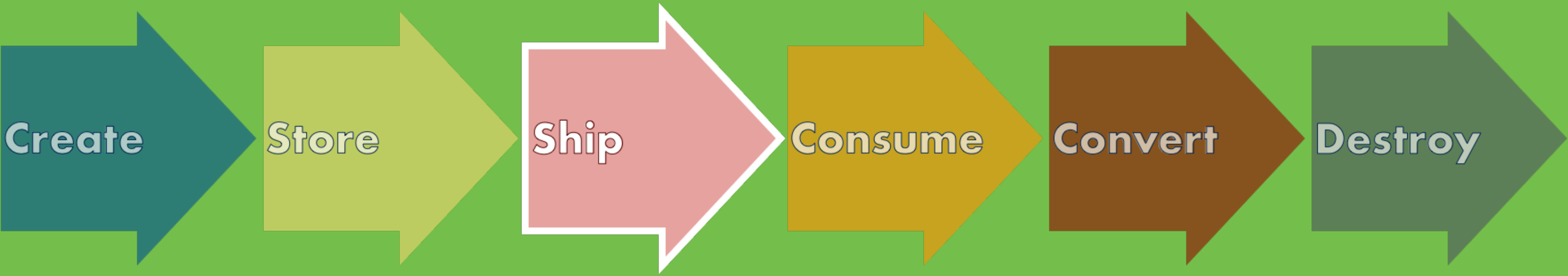
Consume

Convert

Destroy

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



Create

Store

Ship

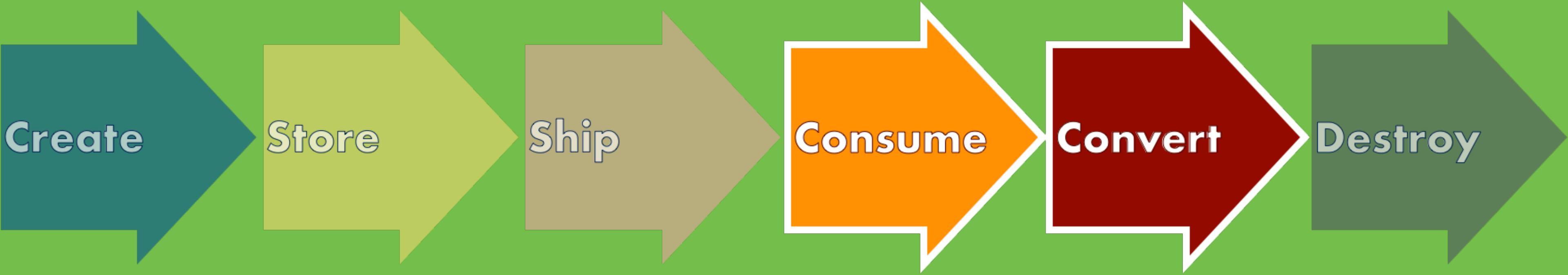
Consume

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



Create

Store

Ship

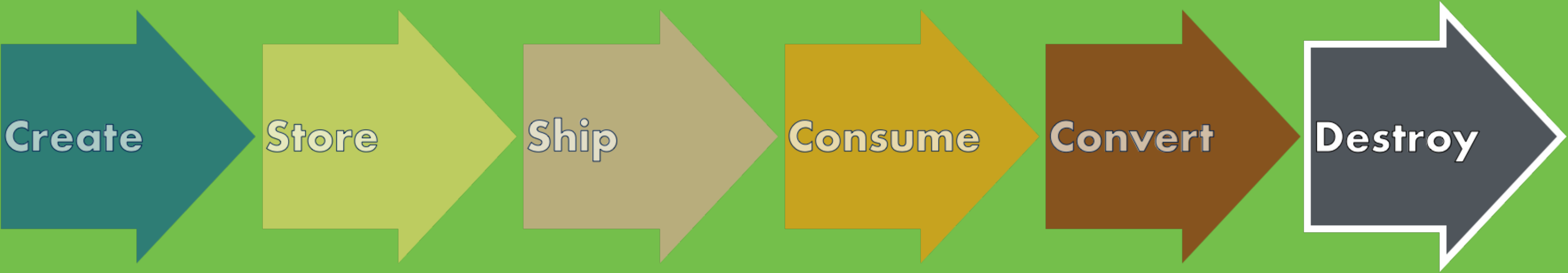
Consume

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).



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 destroyed according to relevant industry standards / procedures
  - e.g. CESG CPA, NIST, Cryptographic Erase
  - 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.

Before you go...

- Security is a broad space with a lot of separate concepts
  - e.g. Authorization, Integrity, Availability, etc.
- Don’t store sensitive data …
  - … but if you do, make sure it’s obscured, e.g. via token, hash, or encryption.
- Know your data and your infrastructure: you need to know what tradeoffs you are making to address them later.

Before you go...

- *Security is a broad space with a lot of separate concepts*
  - *e.g. Authorization, Integrity, Availability, etc.*
- *Don’t store sensitive data ...*
  - *... but if you do, make sure it’s obscured, e.g. via token, hash, or encryption.*
- *Know your data and your infrastructure: you need to know what tradeoffs you are making to address them later.*
- For more questions: please join the WebEx room DEVLIT-4020
- Help me iterate – complete the survey and tell me your thoughts!

Slides, Live Streaming, and Recordings Available on Cisco Live

https://www.ciscolive.com/online

References & Reading Available on Notist

https://noti.st/quintessence

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

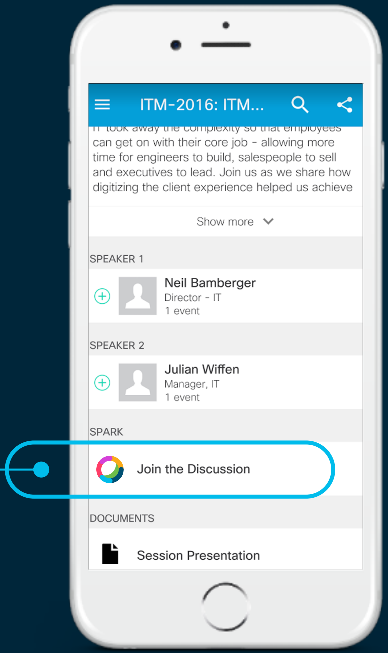
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat
with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



ITM-2016: ITM...

IT took away the complexity so that employees can get on with their core job – allowing more time for engineers to build, salespeople to sell and executives to lead. Join us as we share how digitizing the client experience helped us achieve

Show more

SPEAKER 1

Neil Bamberger
Director - IT
1 event

SPEAKER 2

Julian Wiffen
Manager, IT
1 event

SPARK

Join the Discussion

DOCUMENTS

Session Presentation

DEVLIT-4020

cisco Live!

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Learn more about the new DevNet Certifications and how you can prepare now!

	Associate Level	Specialist Level	Professional Level	Expert Level
Engineering	CISCO CERTIFIED CCNA	CISCO CERTIFIED SPECIALIST	CISCO CERTIFIED CCNP	CISCO CERTIFIED CCIE
Software	CISCO CERTIFIED DEVNET Associate	CISCO CERTIFIED DEVNET SPECIALIST	CISCO CERTIFIED DEVNET Professional	CISCO CERTIFIED DEVNET Expert Future Offering

Start Here | Upcoming Cisco DevNet Certifications

- Start at Meet DevNet

  DEVNET-2864: Getting ready for Cisco DevNet Certifications
  Offered daily at 9am, 1pm & 4pm at Meet DevNet

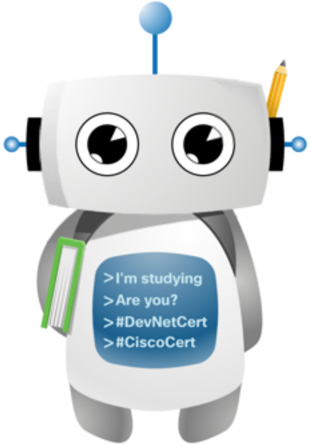
- Attend a brownbag session

  DEVNET-4099: DevNet Certifications: Bringing software practices & software skills to networking
  Offered daily 12:15-12:45 in the DevNet Zone Theater

- Visit the Learning@Cisco booth

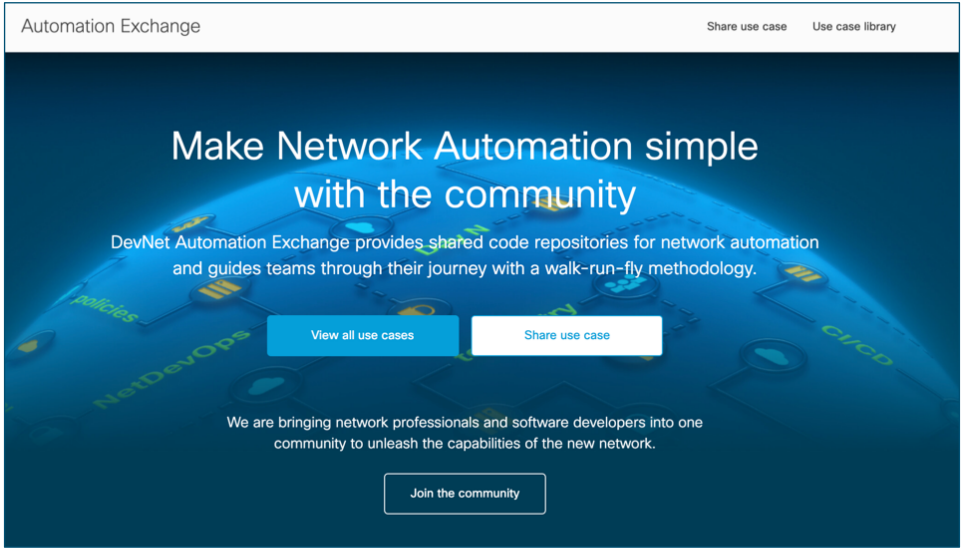
- Scan this code to sign up for the latest updates or go to http://cs.co/20eur02

DEVNET



Find shared code repositories of use cases for network automation & more!

Don't miss our 5 **Automate Infrastructure demos** in the DevNet Zone!



Automation Exchange

Make Network Automation simple with the community

DevNet Automation Exchange provides shared code repositories for network automation and guides teams through their journey with a walk-run-fly methodology.

We are bringing network professionals and software developers into one community to unleash the capabilities of the new network.

Scan this code or go to the URL to **learn more**

DEVNET

http://cs.co/20eur01

Start at **Meet DevNet**

DEVNET-3010 [a-j] Learn how to make Network Automation Simple with the Community

Offered Monday 2pm & 5pm, Tuesday & Wednesday 10am, 2pm & 5pm, and Thursday 10am & 5pm at Meet DevNet

cisco Live!

Thank you

You make **possible**