security mindfulness

dwayne. foley@eagledream.com

security mindfulness defined

- the quality or state of being aware that you need to build security into your daily practice

-the secure state achieved by focusing one's security awareness on what one controls, used to achieve a secure state and a good night's sleep

five steps to security mindfulness

1

You are in Control

Sphere of Influence

2

Understanding

Risk, Vectors, Value

3

Get in Touch

Detailed documentation

4

Practice

Build process into your daily activities

5

You are in the Zone

It becomes second nature

step 1:

you are in control of…

What is in your Sphere of Influence

as a security practitioner

your influence

- IT
- Business
- Management
- Users
- Customers

as an IT professional

their influence

- Network
- Windows
- Linux
- Application / Business owner
- Application dev and support
- Infrastructure (IAM, FW, DNS, Monitoring)
- DB
- Cloud
- Just a process

as a business professional

their influence

Business Process

Audits, Assessments, Compliance

Controls

Applications

PII, PHI and other NPI

Paper records & process

two security concepts

to think about when looking at what is in your sphere of influence

Least Privileged

Accountability

least privilege
(more than accounts)

Role Based Controls

Think Subsystems

- OS
- Web
- DB

System Hardening

- Remove unnecessary packages
- Configure / stop services

Limit ports and services

- Network
- Application
- Dev

Think Authentication

Think Authorization

accountability

Who did what when

Need to have logs and alerts

Across all systems and systems components

OS, Web, DB, Network (TACAC), Application, Dev

Aggregation and Correlation

Centralized logging

accountability

(a bit of a twist)

What system and processes are under your control

Define ownership and responsibility

Business owner

IT Owner / Custodian

Be clear on what you own and what you are responsible for securing

Be clear on the touch points (gray areas) -- the gap!

Be clear on what is not yours but make sure you know who owns it

hey it's the "security guy"

"I don't do security you do"

step 2: understanding

- Value of the data and systems to the business
- Risks
- Vectors of attack

understanding

what has value

What is the Classification

Intellectual property

Regulatory

Contractual

National Security

Sensitive

- PII
- PHI
- Financial
- Reputational
- PCI (PAN)

understanding risks

What type data do you have

Where is the data

What system components are you protecting

- OS
- Web
- DB
- Application
- Network
- Are you plugged in to get security updates from the vendors

understanding vectors

- Internal
- External
- What is the Security Maturity level of your environment?
- What controls do you have in place
- Have you limited access to need to know?
  - Least privileged
- How would you hold someone accountable?
  - Accountability – logs and alerts - review

you need to be plugged in

CTI

Know your environment

Get alerts and bulletins

Review how that matches your environment

Have an escalated patch plan

story about (not) understandin g risk

lack of encryption

not least privileged

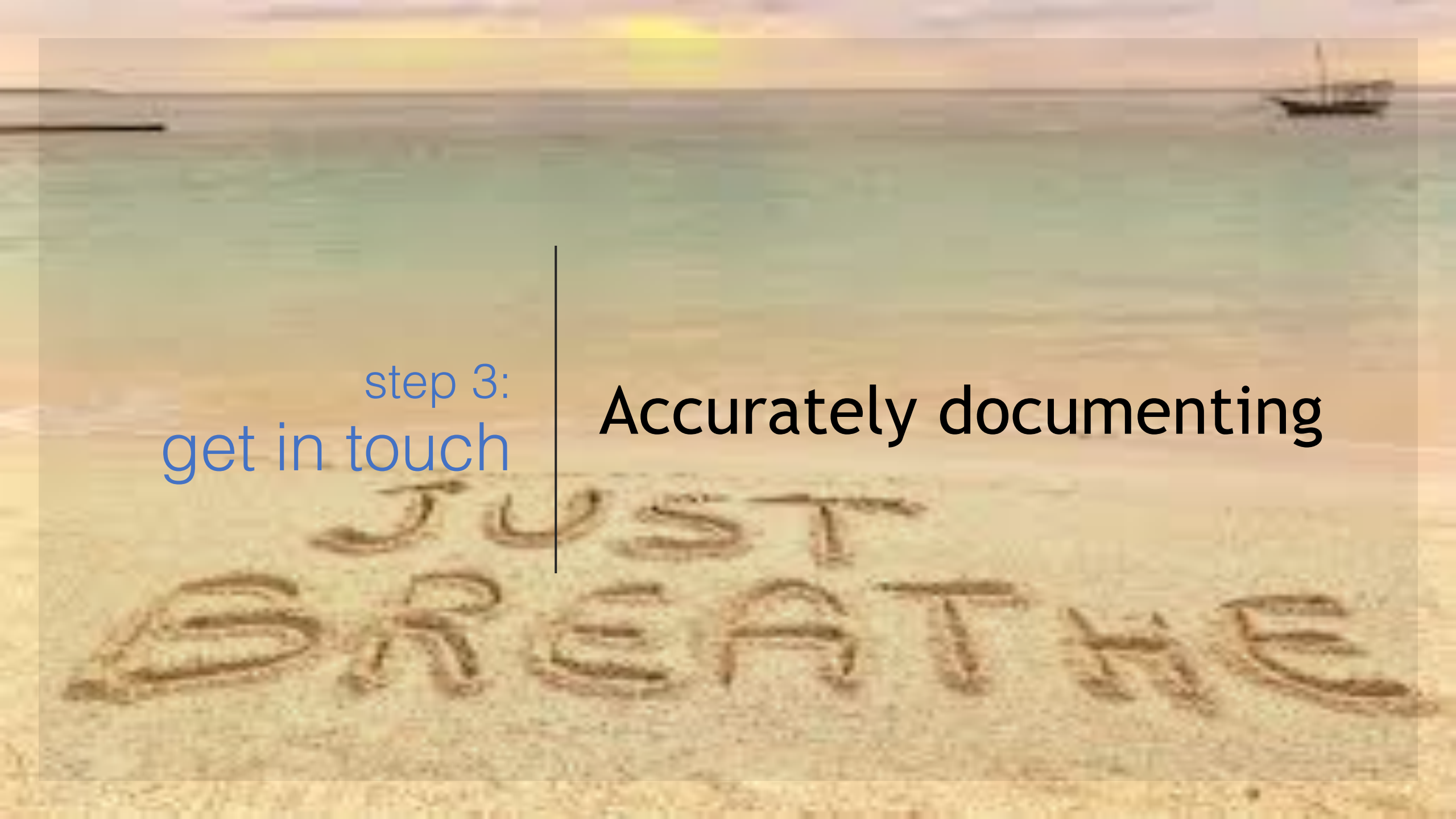
any any rules or viruses

not accountable not patched

step 3:

get in touch

Accurately documenting



diagrams and lists

Detailed Diagrams

Inventory

- Hardware
- Software
- Users

OS Levels

Patch Levels

Support sites to get patch alerts

Procedures
(patching example)

How to apply escalated patches

Approval

Who to notify

Who is impacted

Risk decision to escalate to

responsibility matrix

Who does what

Backup resource

Trained

Skill Set

least privilege role based controls

We often think about just the OS

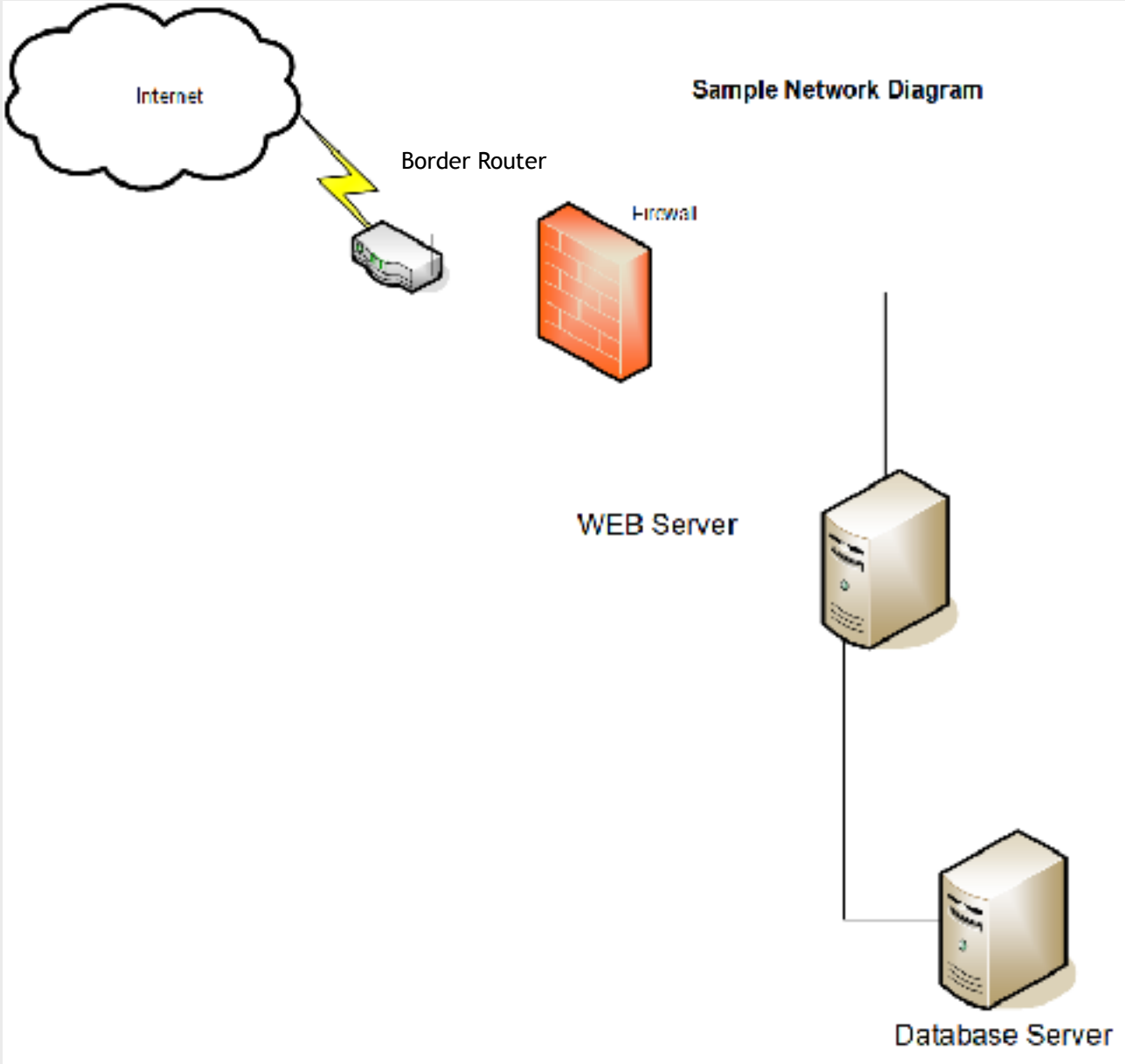
For each system component

- OS
- Web
- App
- DB
- Network

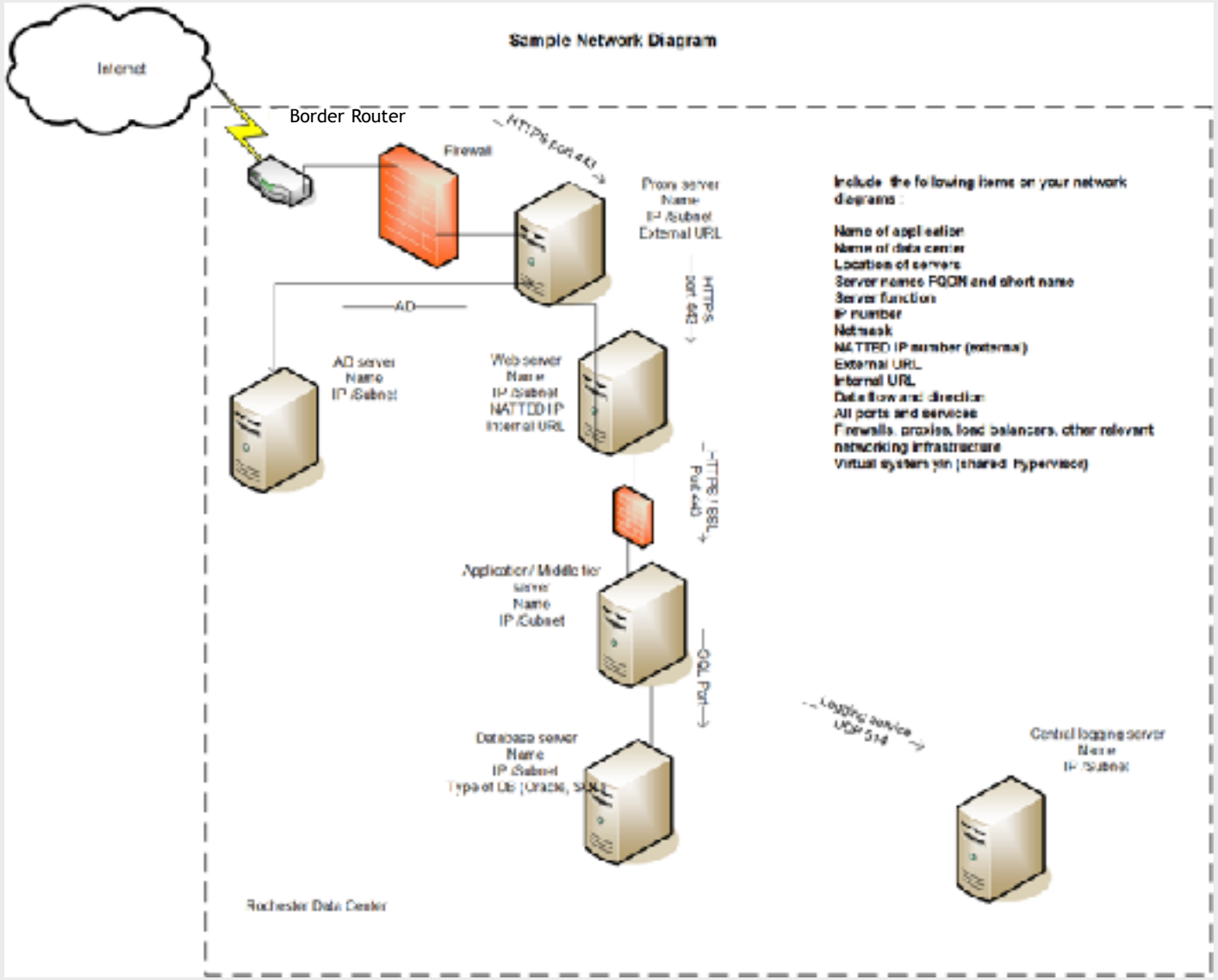
monitoring - logs and alerts

- Hard to do
- Need to document what is being logged
- Templates for each system component
- New tools
- Cloud
- Think Kill Chain and be smarter about what to log and alert on

example on docs



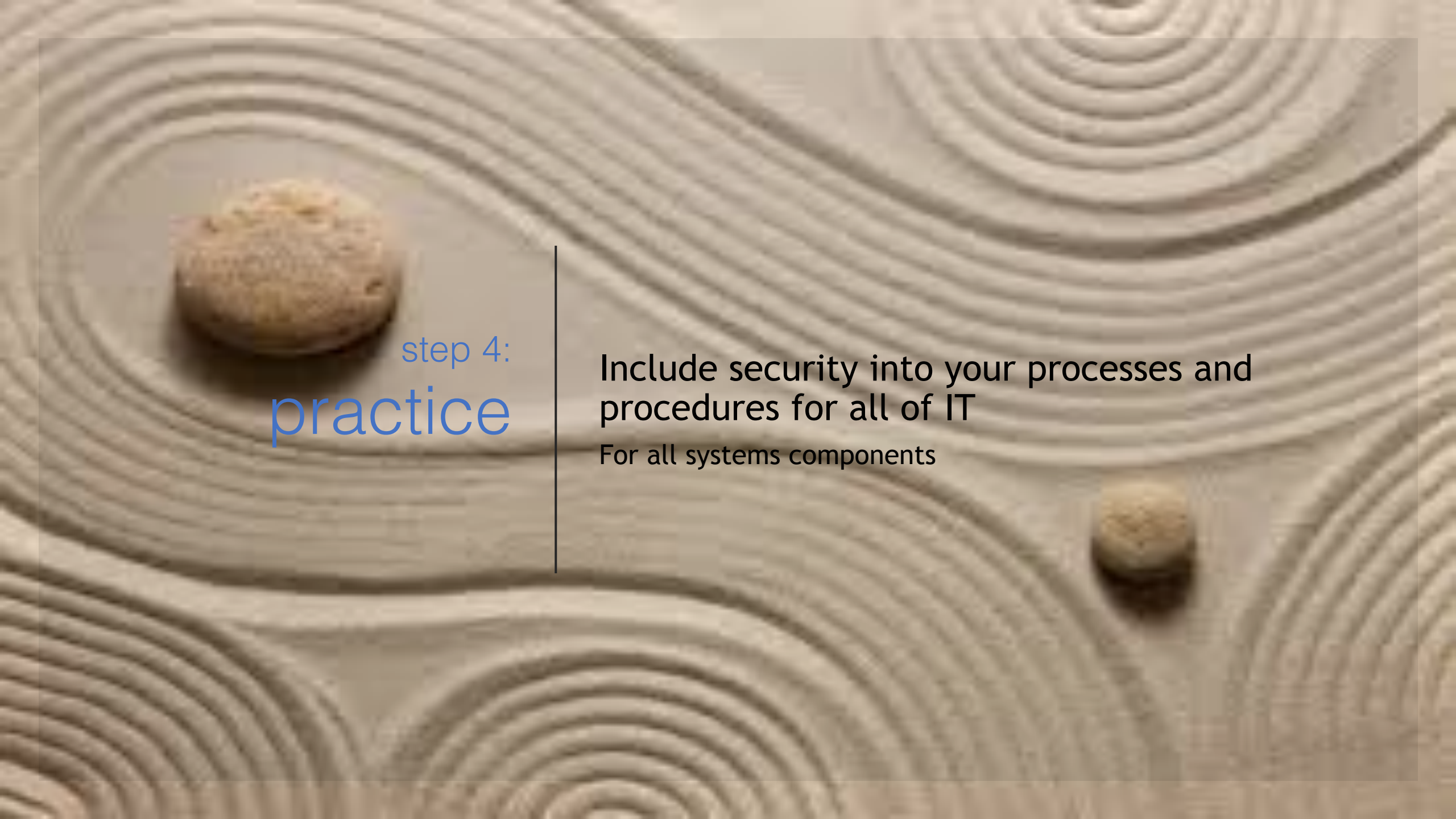
better diagram



Example documentation by application environment
(details needed)

xxx- Firewall Traversal Plan-<name>

Application			Partner Source				xxx Destination				Comments
							Actual		xxx Firewall		
Name	Business Contact	Technical Contact	Network/Address	Mask	Hostname	Destination Port(s)	IP Addr	Hostname	NAT Addr	NAT Hostname	



step 4:

practice

Include security into your processes and procedures for all of IT

For all systems components

hardware

Gold images

Check system hardening status after build

Checklist

Have it reviewed before deployment (like a code review)

software

Check update and patch levels

Know your dependencies

Know your inventory

Configurations, setting and modules

Checklists

daily and weekly tasks that include security

- Check audit trails
- Scan
- Review log reports
- Check for patches and updates
- Build metrics
- Improve

example on building into practice

Training required for anyone that wants to develop

All developers that build software have to have OWASP-type training

This one action had tremendous impact!

step 5:
it becomes second nature

Built into all pro[illegible]es and procedures

built into SDLC

OWASP training

Scan early , scan often

Code reviews

Dev opps - ZAP tool

In the cloud have a hardened image, in AWS CIS AWI

least privilege rule

- It is a mindset
- Across all systems components
- Don’t forget service accounts
- Review system and network , ports and services
- Review quarterly

accountability (both types)

Monitor,

- Alert
- Report on sensitive accounts

Review

- Quarterly
- Access controls
- Processes and touch points, makes sure cracks do not form

Update

- Review responsibility matrix
- Things change
- Processes change
- People change
- Needs to be evergreen

built into the job description

In the PEP

Part of the performance review

Metrics

Top down

built into the design

Security mindset needs to be part of the business requirements from day one of an idea, project, initiative

security becomes part of the base requirements

(not optional or phase II)
without this, it rarely gets done and never works efficiently

built into the culture

Prego “It’s in there”

wrap up

As the security practitioner you are the expert and the evangelist

You can’t fix it alone, you need everyone's help

Chunk it up

Empower

The mindset is an evergreen risk assessment and security plan

You don’t do security”, well, you do, but so does everyone commissioning, designing, building, maintaining, using the computing environment

questions

dwayne. foley@eagledream.com