

Guide to Product Security

...

Creating an appsec program
at a high-growth company

For Central Ohio ISSA InfoSec Summit 2020

Assumptions

- You're not a security nihilist
- You have access to some resources (if only a few)
- You care about product quality
- You believe perfect is the enemy of good
- You don't use the excuse, "That's not my job."

QUESTION:

At the most basic level, the following two statements are true...



1. Every application is a product?
2. AppSec is a product risk concern?



I can't, no, no I'm not doing that, I'm sorry

Applications are products!

- Do they have requirements?
- Do they have users/customers?
- Do they have stakeholders?

A man with dark hair, wearing a dark blue suit, white shirt, and patterned tie, is shown from the chest up. He has a slight, knowing smile. The background is a light blue wall with vertical panels. Overlaid on the image is the text 'Step 0: Embrace Chaos' in a bold, yellow, sans-serif font, and below it, the word 'Chaos.' in a larger, bold, yellow, sans-serif font with a black outline.

Step 0: Embrace Chaos

Chaos.

Adopt a new mindset

- Who is your customer?
- What are their needs?
- How might you deliver value?
- How might you communicate that value?

MEDDDIC: what is the 10,000 ft. overview?



METRICS – What is the economic impact of the solution? Metric proof points.



ECONOMIC BUYER is the person who has discretionary use of funds. They create budgets.



DECISION CRITERIA is the formal criteria used to compare vendor's offerings – capabilities, vendor info, and financial hurdle rates.



DECISION PROCESS The process used to select, & purchase a vendor's offering. The events and timeline - validation and approval process



IDENTIFY PAIN What is the pain?; the link to business consequences (KPI's) and a compelling event? Define the cost of doing nothing.



CHAMPION is the key player who has the power and influence in driving the opportunity; Sells on your behalf.



A still from a video featuring two people. On the left, a woman with long dark hair and glasses is looking down with a somber expression. On the right, a man with long blonde hair is looking up with his mouth open in a surprised or perhaps indignant expression. The background is a dimly lit room with a fan and some shelves visible.

Step 1: Do Nothing

Are you even listening

Learn by listening

- Identify “economic buyers”
 - Leadership, IS personnel, product leaders, engineering personnel
- Look for their quantifiable, measurable results
 - Both “above the line” and “below the line”
- Where are they trying to go?



#GAMEOFGAMES





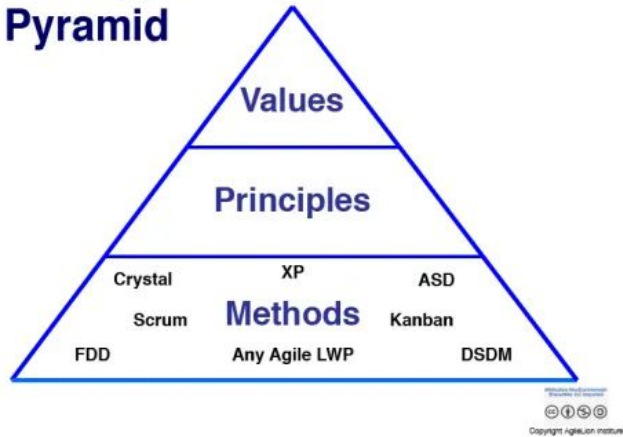
Listening Questions

- What's needed to carry out the company vision?
- What are your goals? Do they differ from the company vision?
- What's your growth plan? What would impede it?
- How do you measure success?

Value Questions

- What keeps you up at night?
- What would be the impact if X were affected?
 - Ie. X being quality, speed to market, change in priorities
- What are your biggest risks?
- What is the cost of doing nothing?
- What are your constraints?

The Agile Pyramid



Understand the system

- Which roles have decision making power?
- Which roles influence decision makers?
- How does work get done?
- **Who is accountable?**
- What are the requirements?
 - ie. the definition of done, quality, etc
- Which systems do you employ?
 - Scrum, Kanban, LESS, etc

What we have

- A definition of done
- An organizational chart
- A method for communicating value

What we know now

- The real stakeholders
- What's important to them
- What keeps them up at night
- How work is done

A medium shot of Tom Hanks sitting on a blue couch, gesturing with both hands open as if explaining something. He is wearing a dark suit jacket over a black shirt. The background features ornate silver-colored metalwork and dark wood paneling.

Step 2: Exhibit Patience

Just wait

Avoid perfect world scenarios

- Government regulations
- Contract / legal requirements
- Leadership risk appetite
- Best practices for not doing dumb sh%t
 - NIST CSF, OWASP ASVS, BSIMM



Stage a small resistance

- Start with a vision
- **Ground your actions in what you heard and know**
 - “So I heard you say this is important...”
 - “Can I get your commitment to...”
- Tie back to core values, company goals and principles
- Document your vision to one page
- Include the names of participants

Collecting people (part 1)

- Find “champions” in responsible parties
- Find “economic buyers” in **responsible parties**
 - Access to resources
- Give your champions something to be a part of
- Give your EB something to be responsible for...



Collecting people (part 2)

Create a security snowball

- Establish a guild
- Identify and assess something small
- Build a healthy body of work and fun

Security Community of Practice (Security CoP)

Created by Jay Bobo, last modified on Oct 02, 2019

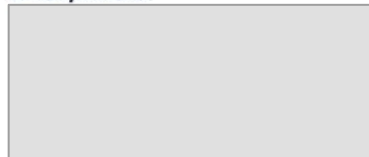
Sponsored by:

ITGRC & SecOps

Contents:

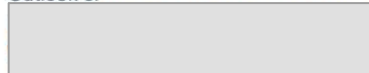
> [Table of Contents](#)

When/Where:



How to Receive Invites:

Add yourself to our distribution list on Outlook or



Contact Us:

cop-security (Slack)

Security Working Group:

See description & responsibilities under About Us:

About Us

Our vision is to develop strong security standards for our products and platform, focused training efforts to [redacted] and to aid CoverMyMeds in advancing cross-vertical security issues.

Our mission is risk mitigation and improved security through communication, shared knowledge and experience, and best-fit practices and standards.

We are composed of **two bodies**:

- The Security Community of Practice
- Security Working Group

What's the difference between the SCoP and SWG?

> [Learn more here...](#)

What We're Working On:

- Pharmacy - **Security Tasks and Priorities**
- Customer Operations - **Security**
- Pharma - **Application Upgrades**
- Provider - **Refined Work**
- Payer - **Security**
- Patient - **tbd**
- Specialty - **Security**

Our FY2020 Priorities:

Each security working group member representing their vertical selected the following company-wide priorities. We will report back quarterly to our Engineering Directors on the progress made: **FY20 Security Priorities**

Collecting people (part 3)

- Be visible and establish a cadence
 - Attend events; shadow teams
 - Attend refinements & department meetings
- Provide accountability
 - Standards (“Utilize security champions to pool their expertise”)
 - Transparency (“Security reports sponsored by the group”)

FY2020 Q1 State of Security Report

Created by Jay Bobo, last modified on Jun 28, 2019




- FY2020 Q1 Customer Operations State of Security Report
- FY2020 Q1 Patient State of Security Report
- FY2020 Q1 Payer State of Security Report 2019-06
- FY2020 Q1 Pharmacy State of Security Report
- FY2020 Q1 Pharma State of Security Report - June 2019
- FY2020 Q1 Provider SoS - June 2019
- FY2020 Q1 - Specialty State of Security Report

API Security Recommendations - WIP

Created by Rachit Sood, last modified on Apr 16, 2019

DO's

Level	Strategy	Definition	Where	When to use
No Auth	Tokens without secrets / API Keys	A static token (GUID) is sent with every request	Header	1) No PHI/No Risk if creds are compromised. 2) Not recommended.
Baseline	Basic Auth	Base64 encoded header with username+password is sent with every request	Authorization header	1) Low Risk if creds are compromised 2) API accepts data 3) B2B 4) API is internal only
Level 1	Username + Password	Authentication credentials sent in the payload with every request.	Body/ Payload sent with every request.	1) B2B 2) Externally facing API
Level 1.5	IP Whitelisting*	The IP of the calling application is checked on every request and compared against a preloaded set of IPs. Traffic from unknown APIs is rejected. Must be used in addition to secret based authentication	Application / Firewall/ Load Balancer / WAF	1) B2B 2) Client IPs are manageably low and do not change often/ static. 3) External API only 4) Use in addition to Basic / Username + Password
Level 2	Sessions	User has already established a session from a previous "recent" authentication. Expires.	Application	1) B2C 2) Browser Based Traffic 3) Single Page Apps / Client Heavy JS frameworks 4) External or Internal 5) Mobile Apps
Level 3	OAuth2 / OpenID Connect	Not a supported capability yet	Bearer Tokens (Dependent on the OAuth Flow in use)	1) B2C/ B2B4C 2) B2B 3) Mobile Apps
Level 4	Mutual Auth	Client is challenged to present a cert when negotiating TLS	WAF	1) B2B 2) B2C is the standard



Step 3: Execute!

Assess

- Identify owners
- Categorize systems by risk
 - Employee surveys
 - Threat models & tool reports
 - Checklists
- Educate
- Assess & Triage
- Remediate



Close the loop

The team that builds/manages the product must...

- Participate in conducting a risk analysis of their work
- Must have security tools implemented in CI/CD
- Have access to penetration tests, risk assessments, scan reports, maturity model data

Educate and train

Document, document, document!

- Document your process
 - What needs to be done?
 - When does it need to be done?
 - Strive for consistency
- Document your flexibility
- Don't overburden; focus on what's important
- Provide receipts (ie. supporting material)

Train them to fish

- Hold first class events
 - Have staff share personal security stories
 - Encourage transparency!
- Marinate and add spices
 - Tie it back to company core values
 - Tie it back to company goals
 - Tie it back to revenue
 - Tie it back to code; use real world examples
- Keep it spicy and mix up training

Reward and publicly acknowledge
your supporters and security champions.

A man with a shaved head, wearing a black martial arts gi with a white V-neck collar, is shown in a ready stance. He is looking slightly to his right with a focused expression. His hands are positioned in front of him, palms facing forward, fingers slightly curled. The background consists of a building with a grid-like pattern, possibly a dojo or a traditional Japanese structure.

Step 4: Welcome Challenges

No fluff

Determine your priorities by associated risk. It's not a moral issue; it's a clarity issue.

- Leverage “Yes and...”
- Boil things down to a Yes/No risk decision.



Summary

WHOOOP

MEDDDIC: what is the 10,000 ft. overview?



METRICS – What is the economic impact of the solution? Metric proof points.



ECONOMIC BUYER is the person who has discretionary use of funds. They create budgets.



DECISION CRITERIA is the formal criteria used to compare vendor's offerings – capabilities, vendor info, and financial hurdle rates.



DECISION PROCESS The process used to select, & purchase a vendor's offering. The events and timeline - validation and approval process



IDENTIFY PAIN What is the pain?; the link to business consequences (KPI's) and a compelling event? Define the cost of doing nothing.



CHAMPION is the key player who has the power and influence in driving the opportunity; Sells on your behalf.

The End is the Beginning is the End

1. Listen actively to build trust
2. Use product language to align with business
3. Identify a common goal
4. Start small with a band of allies
5. Use transparency to effect change
6. Assess, train, remediate, repeat!

Q&A

CONTACT:
jbobo@paircolumbus.org