Building a Security Program

Kendra Ash @securelykash

Background

A little about me

QA -> Software Engineer -> Security

Love learning new things!

I have many hobbies!

Job title

Secure All the Things?!

Hired onto a new team and the task is to build a security program.

Company X decides they need a security team and you are tasked with building it.

Overwhelmed

Initially it can feel like a large task. Especially if there is a lot of tech debt.

Stay calm!

When there is a lot to do, anything you do is likely helping improve security.

Agenda

Quote

Network and Guidance

Stakeholder Analysis

Risk Assessment

Security Champions

Quote

The Fearless Mind by Craig Manning

“Visualize the Mona Lisa.”

Focus on what is going well!

Small or Big

“Do not imagine the Mona Lisa with a mustache!”

Focus on what is right

Rather then saying what is wrong.

Start with discussing what we should do to improve the security of the organization.

Thank you goes a long way

Recognize anyone who helps improve physical, software, or enterprise security.

Masking PII. Locking down a security group in AWS.

Adding logging for when someone views a SSN.

Reporting a risk or vulnerability.

Rewards: Candy, Coffee, Slack Message, Shoutout

Network and Guidance

Listen to industry experts and people around you

Read when you have free time.

Ask others for recommendations.

OWASP meetup and training days.

Books and blogs

“Threat Modeling: Designing for security” By: Adam Shostack

“Red Team” By: Micah Zenko

“Turn the ship around” By: L David Marqet

“The Tangled Web” By: Michal Zalewski

Christian Hashek’s blog:
https://blog.haschek.at/2019/the-curious-case-of-the-RasPi-in-our-network.html

Podcasts / Videos

Darknet Diaries https://darknetdiaries.com/

Security as Nurturance https://blog.newrelic.com/technology/security-as-nurturance-modern-software-podcast/

YouTube: OWASP conferences, Bsides https://www.youtube.com/user/OWASPGLOBAL

Security Champion video: https://www.youtube.com/watch?v=-gzMmdHOF3U&t=1s

People

Most people at this meetup are willing to help you.

Questions:

- What has your company done to secure (infrastructure)?
- What tool are you using for intrusion detection?
- What tool are you using for logging security events?
- Do you have any book recommendations?

Stakeholder Analysis

Learn about the organization as a whole

Often departments have different views.

Who?

Engineering Directors

Engineers

Architects

Customer Experience Directors

HR / Training

Legal Department

Incidents

Ask the interviewee about any security incidents they were involved with or know about.

Record all incidents.

Incident Response Plan.

Categories

https://securityintelligence.com/137-security-questions-every-leader-should-ask/

Security Intelligence

Fraud

People

Data

Application

Infrastructure

Threat Intelligence

Questions

1. How many of your IT systems generate logs with relevant security-oriented data today?

2. How confident are you in your ability to demonstrate compliance?

Risk Assessment

Keep track of all the risks

Financial

Operational

Regulatory

Reputational

Record

Document all the risks you find or learn about from interviews.

Create a risk registry.

Calculate the risk.

What to capture?

Issue Summary

Priority (1-3)

Risk (Critical, medium, high, etc)

Status

Security Control Category

Description

Recommendation

Reporter

Jira / Pivotal

Let everyone know!

During team updates or presentations inform your users you’re tracking risks.

Let them know they can report risks to you.

Security Champions

Partner with engineering

Who?

Why?

Goals?

What?

Who to include?

Whoever is interested in security or maybe knows about it.

- Director of Engineering
- Architect
- Software Engineer
- Senior Software Engineer
- DevOps Engineer

Why?

Security Champions often can have immediate impact on the security of applications being built.

Allows security team to make progress while trying to staff up.

Goals

This is important to revisit when the group has made progress.

Recognize success.

What

Network topology

Threat modeling

Endpoint testing

Security audit

Audits

When

Every application before it goes to production.

Every 6 months for applications in production.

Who

Team who owns the application. Members from the centralized teams: DevOps, QA, Security

Process

Create a PR, review, meetings, demos

Data tiers

What data does your company store, process and share?

Create a policy for the different types of data and how it should be handled.

Tier 1: Unrestricted Data

- Id’s, counts

Tier 2: Confidential Data

- Personal Names, email

Tier 3: Highly Secured Data

- SSN, Payroll info

Tier 4: Restricted Data

- Contracts, PCI data

Audit questions

How are your application secrets encrypted at rest and accessed using least-privilege practices?

Please list any keys, credentials, or secrets used by the application and where they are stored, e.g. AWS account, database, etc.

Please describe all ports that are opened and why?

What security testing was performed?

Audit automation

DevOps team has created and maintains a tool.

Teams have access to run it, provides feedback.

Checks include:

- Deleting default VPC
- Enable VPC flow logs
- Test coverage
- Availability zones

Application security audits

Work with existing processes and identify if teams can add a security check.

Help teams become more aware of security.

Constantly work to improve this process.

What is next?

Slowly improve the security of the organization

Physical Security

Training

Policies

Security Tool Findings

Risk Registry

Physical security

Identify what controls are in place.

Badges?

Doors unlocked?

Elevators?

Training

Identify what documentation or training exists.

Work with appropriate teams to improve the security awareness training.

Secure coding training and practices.

Ask your network what tools they are using.

Policies

Identify what policies exist.

Partner with legal to develop new policies.

Also work with training or a communication team to distribute.

Ensure all policies have leadership buy-in and approval.

What policy to start with?

Depends on the organization.

Acceptable Use Policy

Cloud Computing Services Policy

How to get buy-in?

Identify who the key stakeholders are.

Get feedback early and often on new policies.

Create a first draft, start asking for reviewing and feedback.

Let leadership know your working on new policies to address this risk.

Security tool findings

What if you don’t have a budget for new security tools?

Evaluate and be creative with existing tools.

Tools are constantly evolving.

Reach out to other engineers let them know what you're looking for.

Logging, monitoring.

Risk registry

Now you have a risk registry with lots of things!

Start reviewing the risk registry on a regular cadence.

Identify critical risks.

Identify items you can partner with engineering to fix.

Slowly mitigate or remove the risk.

Closing remarks

Always staying calm when a new security vulnerability is discovered.

Build a Security Champion team!

Ask your network for guidance.

Thank You

Kendra Ash @securelykash