Building a Security Program

Kendra Ash @securelykash

Background

A little about me

QA -> Software Engineer -> Security

Love learning new things!

I have many hobbies!

Where am I working?

My job!

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

Network and Guidance

Stakeholder Analysis

Risk Assessment

Security Champions

Security

Is everyones job!

Developer
System Administration
Product
Analyst

@securelykash

Focus on what is going well!

Small or Big

Rather than 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.

@securelykash

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, RSA 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

Categories

Questions

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

Security Intelligence

Fraud

People

Data

Application

Infrastructure

Threat Intelligence

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?

@securelykash

Incidents

– – –

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

Record all incidents.

Incident Response Plan.

Record incidents

Capture incidents for historical purposes

- Date found
- Date resolved
- Reporter name
- Screenshots
- Notes / Info

Leverage historical incidents

Incident Response Plans

- Build a IR plan for the most frequent incident
- Gain approval of the IR plan
- Next time execute the IR plan (since it is already approved)

IR plans

Who has incident response plans?

Examples

- Phishing
- Compromised Password
- Upset Employee Leaves Company
- Guard Duty Alerts

Risk assessment

Keep track of all the risks

Financial

Operational

Regulatory

Reputational

Risk types

Financial: the organization could lose money

Operational: the organization risks being able to operate normal business functions.

Regulatory: the organization now has to comply with new laws and regulations.

Reputational: the potential for negative brand or public recognition.

Record

Create a risk registry.

Document all the risks you find big or small.

Calculate the risk.

@securelykash

Calculating risk

- OWASP risk rating
- DREAD
- Risk probability and severity

Example of a risk

– – –

Scenario: An un-authenticated endpoint in a in house application (back office, admin)

- Leaking internal ID’s

- URL company.com/backoffice/something.php

	Severity			
Probability	Catrastrophic 4	Critical 3	Marginal 2	Negligible 1
Frequent	High 20	High 15	High 10	Medium 5
Probable 4	High 16	High 12	Serious 8	Medium 4
Occasional 3	High 12	Seious 9	Medium 6	Low 3
Remote 2	Serious 8	Medium 6	Medium 4	Low 2
Improbable	Medium 4	Low 3	Low 2	Low 1

Example of another risk

– – –

Scenario: An un-authenticated endpoint in a in house application (back office, admin)

- Leaks personal identifiable information

- URL company.com/backoffice/something.php

	Severity			
Probability	Catrastrophic 4	Critical 3	Marginal 2	Negligible 1
Frequent	High 20	High 15	High 10	Medium 5
Probable 4	High 16	High 12	Serious 8	Medium 4
Occasional 3	High 12	Seious 9	Medium 6	Low 3
Remote 2	Serious 8	Medium 6	Medium 4	Low 2
Improbable	Medium 4	Low 3	Low 2	Low 1

What to capture in risk registry

– – –

Issue Summary

Priority (1-3)

Risk (Critical, medium, high, etc)

Status

Security Control Category

Description

Recommendation

Reporter

Jira / Pivotal

Owner

Risk registry

Let everyone know!

- Team updates
- Lunch and learns
- Slack channels
- Communicate how they can report

Security champions

Partner with engineering

Who?

Why?

Goals?

What?

@securelykash

Application security

According to vmware:

“Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.”

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

Secure code review

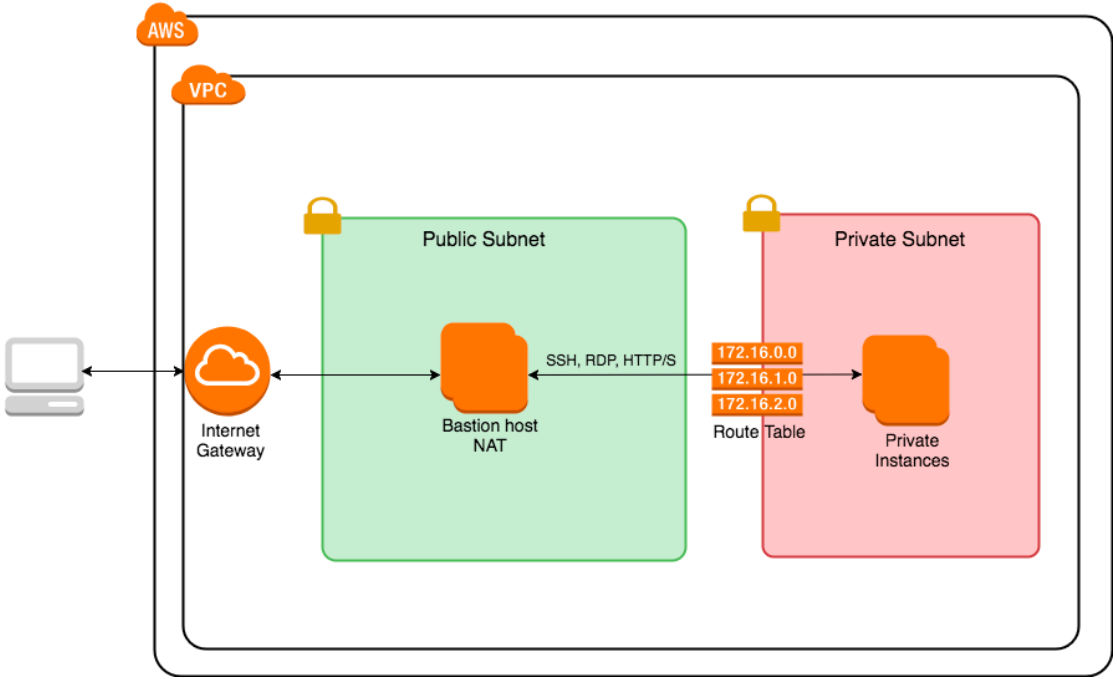
Network topology in AWS

– – –

- VPC
- Security groups
- Egress and ingress
- IAM roles

Virtual Private Cloud (VPC)

“Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined”



Security groups

“Security Groups - Act as a firewall for associated AWS resources, controlling both inbound and outbound traffic at the instance level.”

- Define what ports are open and what IP’s can hit those ports
    - 80 (http)
    - 443 (https)

Egress and ingress

Outbound: Egress traffic beginning inside the network and flowing out to the internet (outside the network)

Inbound: Ingress traffic coming from outside the network (anywhere on the internet) to inside the network.

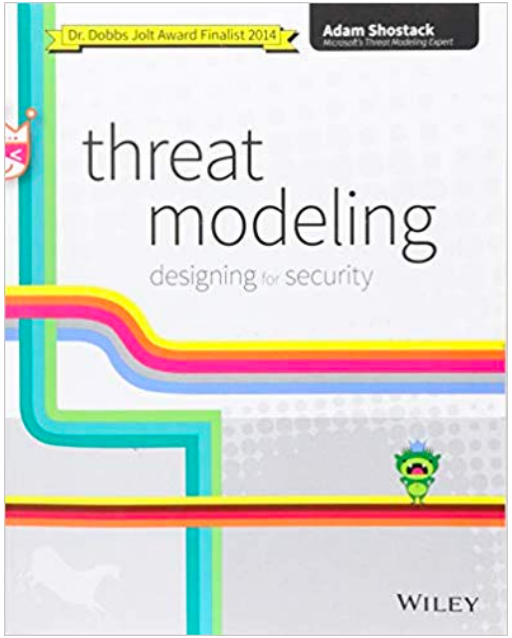
Identity Access Management (IAM)

“An IAM *role* is an IAM identity that you can create in your account that has specific permissions.”

- Humans and machines
- AWS designed it to be default deny. Start out with 0 permissions
- Avoid using * or *AllAccess*

Threat modeling

“Threat modelling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.”



@securelykash

Threat modeling

What are we working on?

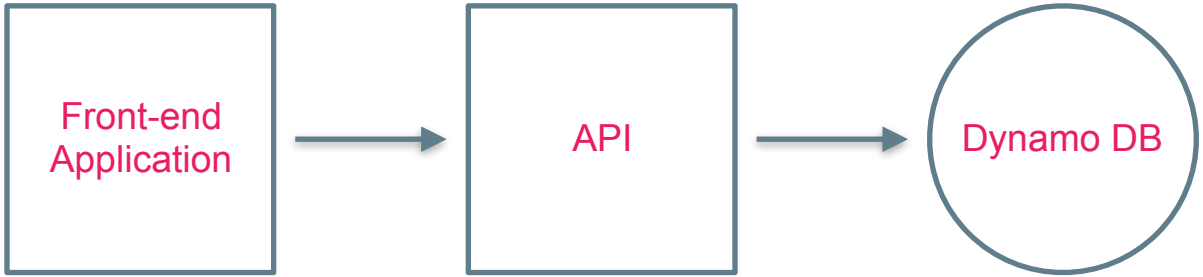
What can go wrong?

What are we gaining to do about it?

Did we do a good job?

Threat model example

Front-end application, with a backend API, and database living in AWS. What threats might we have?



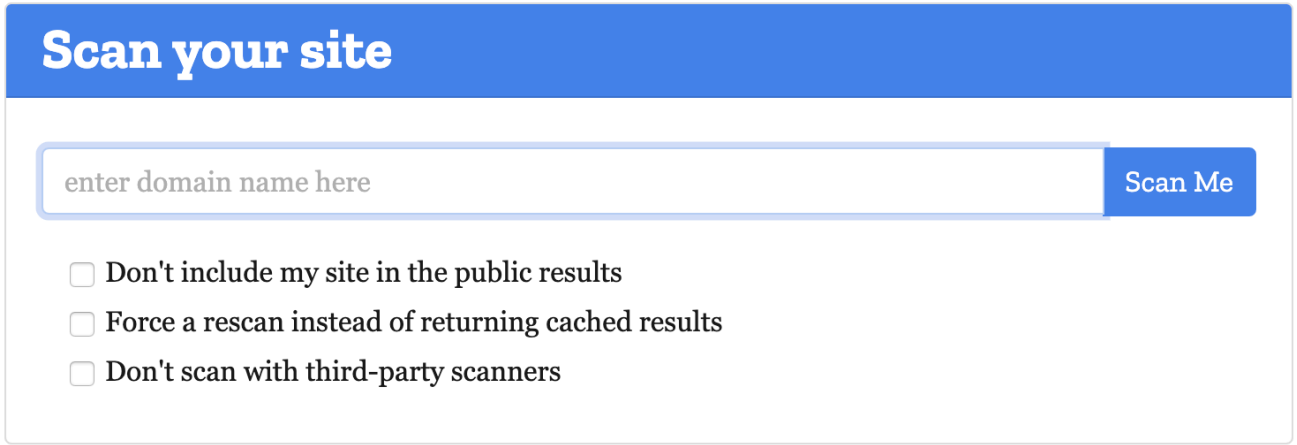
Threat model continued

– – –

- OWASP top 10 https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet
- OWASP serverless top 10 https://github.com/OWASP/DVSA/blob/master/AWS/LESSONS/README.md

Endpoint testing

The Mozilla Observatory has helped over 170,000 websites by teaching developers, system administrators, and security professionals how to configure their sites safely and securely.



@securelykash

Background on audits at my company

– – –

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
- RDS encryption

Application security ~~audits~~ PRR's

– – –

Add unit test to verify security things.

- Authentication errors are consistent for users and non users
- Test a user without permissions
- Test a user hitting your api who has an expired token

Application security ~~audits~~ PRR's

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

Help teams become more aware of security.

Leverage automation.

Mozilla Observatory free endpoint security tool

Secure code review

– – –

#SheHacksPurple blog about secure coding top items

- Input validation
- Parameterized queries
- Output encoding
- Sanitize logs

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?

Host meetups and require sign in?

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

Data Classification Policy

Data Retention 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.

References

https://code.likeagirl.io/pushing-left-like-a-boss-part-5-1-input-validation-output-encoding-and-parameterized-queries-ad1d4e7136c9

https://observatory.mozilla.org/

https://darknetdiaries.com/

https://www.vmware.com/topics/glossary/content/application-security

https://docs.aws.amazon.com/index.html?nc2=h_ql_doc

Thank You

Kendra Ash @securelykash