One Person Army: How to be the first Security Engineer at a company

Kashish Mittal © 2019
Disclaimer - Opinions expressed are solely my own and do not express the views or opinions of my current or former employers.
Who am I?

- Head of Security at **Mobile Data Labs, Microsoft (formerly MileIQ)**

- Previously worked at Elevate Security, Duo Security, CyLab, Bank of America, Deutsche Bank, etc.

- This is how I speak, I have an Indian accent.
  - I’m not doing a bit or pretending to be ‘Apu’ from The Simpsons

Kashish Mittal © 2019
How did I get into Security?

- BS, MS from Carnegie Mellon with a focus on security
- Security Research at Cyber Security Lab (CyLab).
- Member of Plaid Parliament of Pwning (PPP)
- Learned a lot of security through CTFs
Let’s do some exercise -
Any of you have started a Security team or were the first Security person in a company or its division?
Any of you who don't identify as Security Engineers have managed Security temporarily?
What makes me qualified?

- Experience of building Security teams from the ground up
- Mostly worked in **hyper-growth** and **high-risk** startups
- Started and helped build the **AppSec** team at **Duo Security**
- **Founding Engineer** at **Elevate Security**
- Started and building **Information Security** at **MileIQ, Microsoft**

Kashish Mittal © 2019
DUO SECURITY

- 2FA and Auth company, highly sensitive, recently acquired by Cisco
- First dedicated Application Security Engineer
- Team of 4 by the time I left
- Helped build the S-SDLC life cycle
- Threat Modeling, Design Reviews, Code analysis, Security assessments, Bug Bounty
ELEVATE SECURITY

- Founding Engineer
- Helping enterprise teams build their Corporate Security initiatives
- Security Training and Awareness, Phishing campaigns etc.

Kashish Mittal © 2019
MILE IQ

- Mileage tracking and expenses; acquired by Microsoft
- First Security Engineer; little to no Security before that
- Head of Security now
- AppSec, CorpSec, InfraSec and part of Privacy and Compliance
Objective

Share key learnings from building Security teams and programs from the ground up
Ideology

‘One Man Army’ - “a heavily armed and well-trained combatant able to face numerous enemies alone” - Wikipedia

One Woman Army / One Man Army -> One Person Army

Kashish Mittal © 2019
First things First

- Familiarizing yourself with the organization
- Similar to the 'Re-con' phase in Pen-Testing
- Decision making, stakeholders, pace etc.
- Stack and tools
- Identifying key associates who 'get Security'
- Aligning Security to Business needs!
Make an impact early

- Show the value of having a Security Engineer
- Catch the low hanging Fruit
- Top 3 - 5 things in the first 30 – 90 days
- War stories
  - No 2FA + Personal emails + Horrible Password Hygiene
  - GitHub - remove all code
  - Extract all customer data including PII
Secure, Document, Repeat!

- Find insecure stuff
- Secure it
- Document it
- Repeat!

Example - Azure VMs and subscriptions; Data storage guidelines

Takeaways – Efficiency, Availability and Repeatability
Data Storage guidelines

1. Encryption at Rest - Data needs to be encrypted (not in plaintext) while not being used i.e. at rest. Enabled by default in Azure SQL Database - https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql

2. Encryption in Transit - Data needs to be encrypted during transmission. Use TLS v1.2 or later as earlier protocols have security bugs in them. "In your application's connection string, ensure that you specify an encrypted connection and not to trust the server certificate." Provided by default for Azure SQL Database. Please make sure you are using the latest SQL Servers - https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server


4. Role Based Access Control (RBAC) - Set up Owner, Admin, Contributor and Reader roles and grant access accordingly. For detailed steps, see https://docs.microsoft.com/en-us/azure/sql-database/role-based-access-control/overview


7. Storing credentials exclusively in Azure Key Vault → [Configuration]
   - Secrets management in KBS + ACS/ACSE/AKS + VSTS](https://wiki.atlassian.net/wiki/spaces/Eng/pages/53762546)

8. Rotating credentials every 90 days → How to store and rotate keys and secrets

Education, Evangelism and Communication

- Biggest part is educating yourself and others about Security
- Evangelizing your work and its impact
- Communication is key:-
  * Shock and awe / Fear
  * Helping Hand
  * Private vs public
Workshops and Knowledge transfer

- Needed for both technical and non-technical employees
- Developer Security workshop
- Security 101 training
- Examples -
  "SECURITY is incomplete without U!"
  "How to keep yourself safe at work and at home"
Developer empathy

- “Security? We didn’t have to do that earlier”
- New for them
- High intensity and strict deadlines
- Product focused
Motivation

It’s not just about whether they are able do it ... maybe they **don’t care about it**
SECURITY CHAMPIONS program
WHAT?

Non-Security dedicated employees helping out with Security stuff

Also known as Security Ambassadors / Security Satellites program

Police asking Citizens to be their eyes and ears!

For both technical and non technical employees
HOW?

Composition -

A Security champ per team
At-least 1 per geographical location
Roughly 1 per 20 FT employees

Executive Sponsor – Someone in ET who has organizational power
Responsibilities of the Security Champs

• First POC for teams for Security related stuff
• Drive security improvements within their teams and products
• Engage Security team as and when needed especially with 'Security critical' stuff
• Get trained in the relevant areas of Security
• Expect to spend about 10-20% of your time on contributing to Security stuff instead of regular activity
Perks of being a Security Champ

• Enhance their Security knowledge and awareness
• Helps in career development. Security is a booming field.
• Recognition and appreciation from LT and their co-workers.
• Swag - Tshirt, stickers, goodies
• Free food during meetings (Find out what motivates them the most!)
Advantages

• Establish a Security mindset amongst ‘non-Security dedicated’ employees
• Enhance the org's Security culture
• Help scale security
Automation and Alerts

- 1 person or small team = not enough time
- Can’t operate a SOC or monitor tools 24 * 7
- Set up meaningful and actionable alerts
- Have alerts inform and guide your response
Build vs Buy

- Need to find the right balance
- No use re-inventing the wheel
- Buy products that work off the shelf
- Build custom tools or interactions for unique characteristics
Azure Security

- Key Vault
- Security Center
- DBs
- And many others
iPad signing Technique

- Mentor story
- Risk consumption
- Buy-in
- Safeguard yourselves!
CorpSec initiatives

- Phishing – 2FA vs Yubikeys
- Passwords
- Malware execution
- Data access control
Security Training and Awareness

- Current methods of security training and awareness are **not great**
- Training needs to be **customized** to have maximum ROI
- Important to **motivate** your employees to care about security
- **Active and experiential learning** can improve retention
- **Measure the effectiveness** of your training
- Try **CTFs**!
Before you say Yes

- Alignment with upper management
- Motivation
- Goals
- Timeline
- Budget
- Headcount - outsource, consultants
It's not all rosy!

- Tough days
- Frustrating

- Remember your goal – You have to secure the organization to the best of your abilities and resources!
Questions?
Citations

- Vir Das, Abroad Understanding
- https://www.wpclipart.com/signs_symbol/alphabets_numbers/color_numbers/number_1_green.png.html
- https://www.logolynx.com/topic/red+0
- http://clipartmag.com/infinity-clipart