REBUILDING SECURITY CULTURE WITH SECURITY CHAMPIONS

Ann Marie Fred
Senior Principal Software Engineer, Red Hat

Siddharth Pareek
Senior *Vice President - Consulting, NatWest Group*

DEVOPS ENTERPRISE SUMMIT
AN IT REVOLUTION EVENT

A LITTLE BIT ABOUT

ANN MARIE

- 20+ years of Software Dev
- 10+ years of DevOps
- 3 years as a DevOps Days conference co-organizer
- Active in Linux Foundation and CD Foundation open source projects
- 3 years as an HR manager
- 4 years as a Security Focal
- Previously at IBM
- Currently at Red Hat

A LITTLE BIT ABOUT

SIDDHARTH

- Leading DevOps Centre of Excellence Practice for NatWest Group (NWG).

- Driving Chaos Engineering, Security Champions, Cultural Transformation tracks for the NWG.

- Governing Board Chairperson for Ortelius (an OS project under Linux Foundation)

- Co-authored book on Site Reliability Engineering and Digital Skills Whitepaper resp.

- On Board of Expert Panel for Cloud Credential Council

- Global Ambassador for DevOps Institute

- On Influencer Panel for DevOps & Agile Skill association (DASA)

- Community Manager for Atlassian NWG and regional chapter resp.

Disclaimer: These are our personal experiences, not the official position of IBM, Red Hat, or Natwest Group.

“THERE ARE ONLY TWO TYPES OF COMPANIES: THOSE THAT HAVE BEEN HACKED, AND THOSE THAT WILL BE.”

- former FBI director Robert Mueller

24%

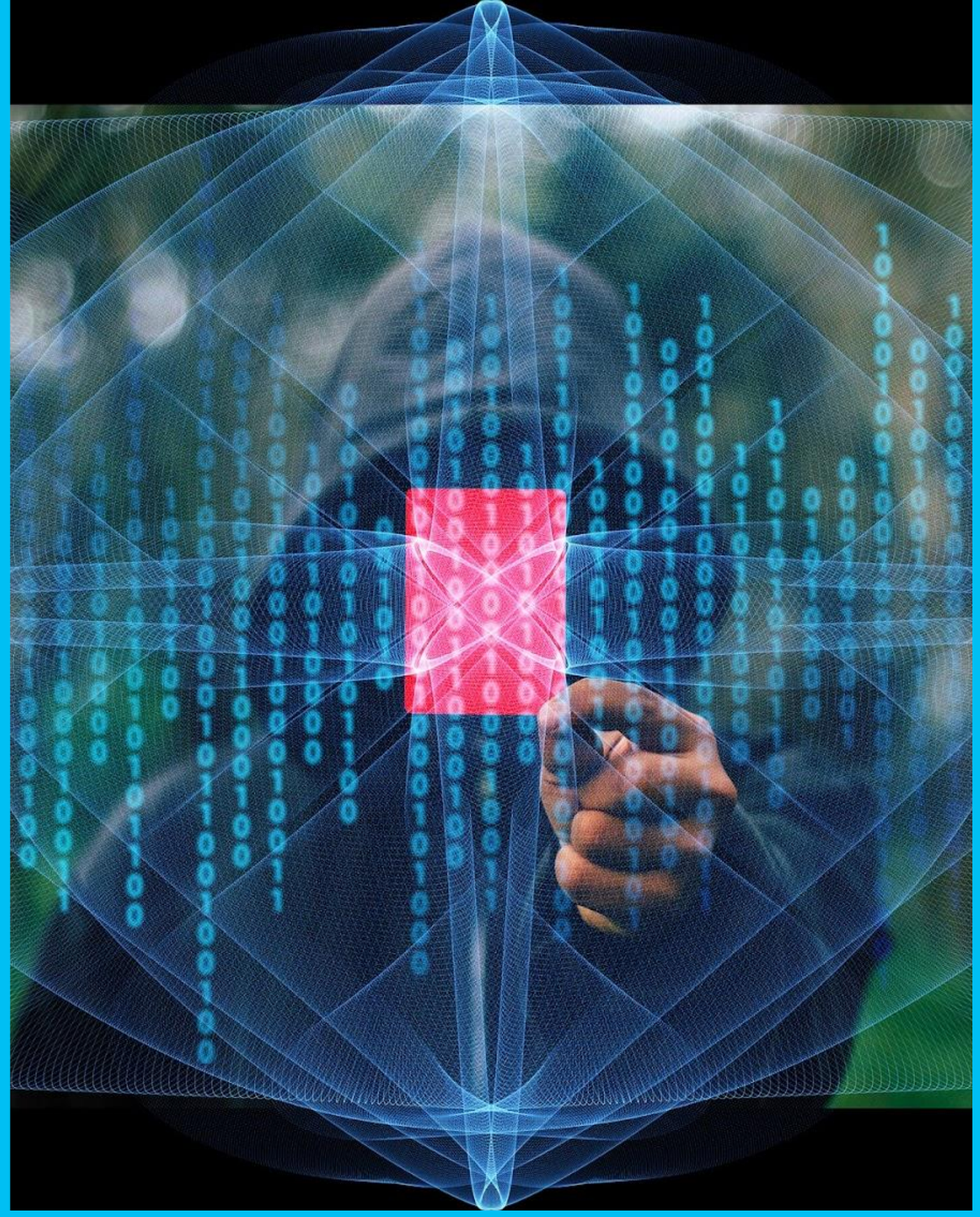
OF ORGANIZATIONS SUSPECT OR HAVE VERIFIED A SECURITY BREACH IN THE PAST 12 MONTHS.

2020 SONATYPE DEVSECOPS COMMUNITY SURVEY HTTPS://WWW.SONATYPE.COM/2020SURVEY

MOST BREACHES TARGET DATA!

COST OF A DATA BREACH

- GDPR and other privacy regulations hold companies liable for security breaches.
- Ignorance is not a defense.
- Can cause major damage to a company's reputation. (Facebook, Equifax, LinkedIn, Anthem, etc.)



$4.24 MILLION

AVERAGE COST OF A DATA BREACH IN 2021

IBM 2021 COST OF A DATA BREACH REPORT HTTPS://WWW.IBM.COM/SECURITY/DATA-BREACH

“THE TIME BETWEEN A VULNERABILITY BEING ANNOUNCED AND THE EXPLOITS APPEARING IN THE WILD USED TO BE 45 DAYS. THAT HAS COMPRESSED BY 93% OVER THE LAST DECADE TO 3 DAYS.”

- DEREK WEEKS, VICE PRESIDENT AND DEVOPS ADVOCATE (AT THE TIME), SONATYPE
THE DATA BEHIND DEVSECOPS: WHY 3 DAYS MIGHT BE YOUR NEW NORMAL

IT’S A RACE. WE NEED CONTINUOUS SECURITY!

“FOR EVERY 100 DEVELOPERS, THERE IS ONE SECURITY PROFESSIONAL.”

- TOBY IRVINE, CEO AT SECURE DELIVERY

BECAUSE OF SCARE RESOURCES

SECURITY IS OFTEN NEGLECTED IN TRANSFORMATIONS

- Cybersecurity professionals are a scarce resource
- Security as a last-minute gate
  - Threat model (right before pen test)
  - Penetration test (manual)
  - Fix vulnerabilities (but usually not all of them)
  - Ship it!

OVER 18,000 CVE DISCLOSURES

SECURITY EXPERTS REPORT ABOUT 18,582 VULNERABILITIES (CVES) CAUGHT SO FAR [IN 2021], COMPARED TO 17,041 DETECTED IN 2020. MOREOVER, 2021 WAS MARKED WITH A SIGNIFICANT INCREASE IN REPORTED ZERO-DAYS. AT LEAST 66 ZERO-DAY ISSUES HAVE BEEN PUBLICLY REVEALED THIS YEAR, DOUBLING THE TOTAL NUMBER OF THOSE IDENTIFIED IN 2020. - HTTPS://WWW.CYBERSECURITYINTELLIGENCE.COM/BLOG/TOP-10-MOST-SEVERE-VULNERABILITIES-IN-2021-6046.HTML

AT LEAST 66 ZERO-DAY VULNERABILITIES

SECURITY EXPERTS REPORT ABOUT 18,582 VULNERABILITIES (CVES) CAUGHT SO FAR [IN 2021], COMPARED TO 17,041 DETECTED IN 2020. MOREOVER, 2021 WAS MARKED WITH A SIGNIFICANT INCREASE IN REPORTED ZERO-DAYS. AT LEAST 66 ZERO-DAY ISSUES HAVE BEEN PUBLICLY REVEALED THIS YEAR, DOUBLING THE TOTAL NUMBER OF THOSE IDENTIFIED IN 2020. - HTTPS://WWW.CYBERSECURITYINTELLIGENCE.COM/BLOG/TOP-10-MOST-SEVERE-VULNERABILITIES-IN-2021-6046.HTML

A SMALL CYBERSECURITY TEAM CAN’T FIND AND FIX VULNERABILITIES WITHIN 3 DAYS WITHOUT HELP.

TO MOVE FASTER WHILE BEING MORE SECURE

WE NEED TO UP OUR GAME

- Tech teams need to be more self sufficient w/r/t cybersecurity
- More application security subject matter experts: scale up from 1% to 10% of the technical population
- More people digging into the details of security tool findings

SPECIFICALLY,

WHAT MOTIVATED US?

- IBM Digital: Internal DevOps surveys identified security work as one of the top 3 pain points for our developers.
- Red Hat: Re-structured its product security programs in response to the May 2021 Executive Order on Improving the Nation's Cybersecurity. Supply chain!
- Natwest Group: Responding to the Log4J/Log4Shell vulnerability in late 2021.

LOG4J

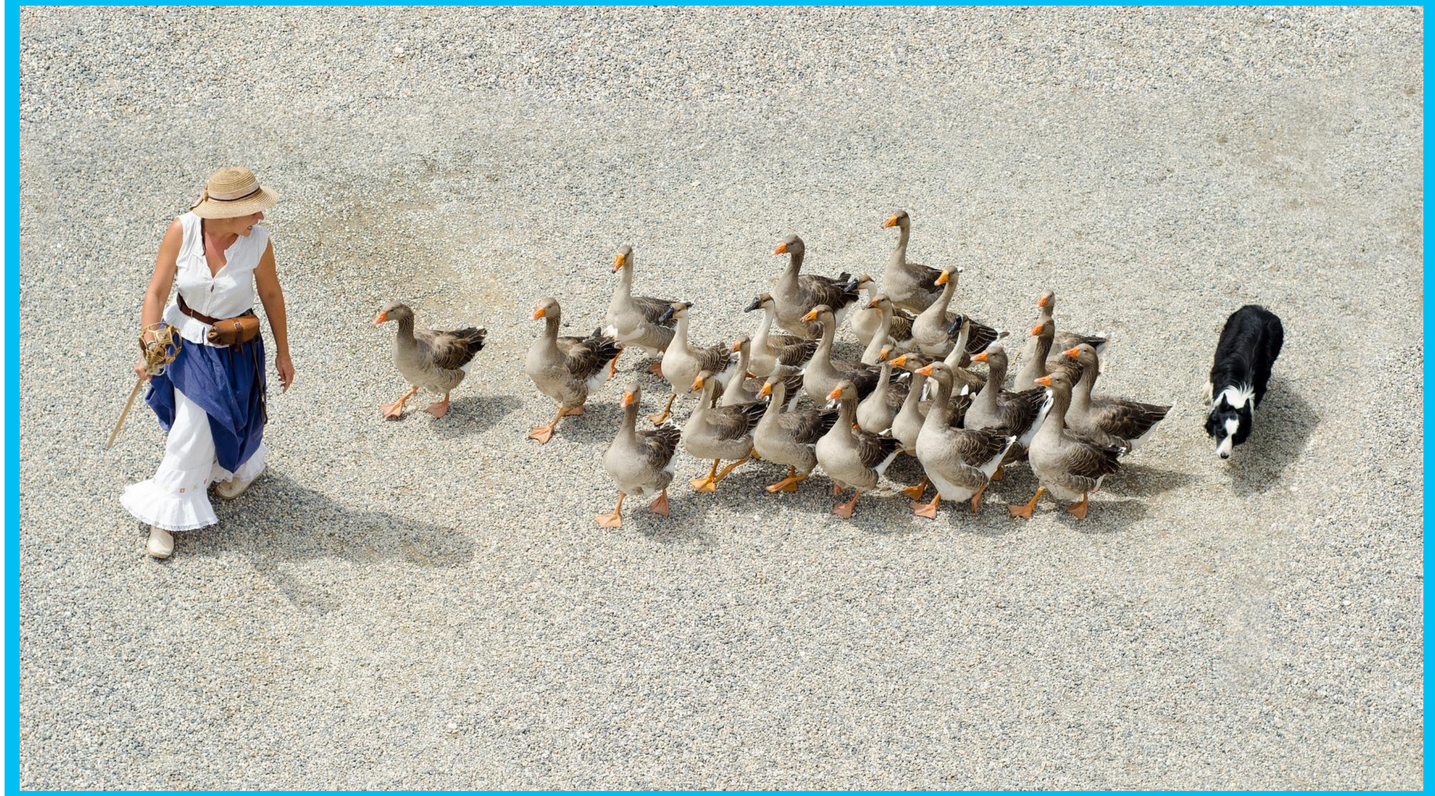
LOG4SHELL VULNERABILITY

- Log4J is a very common and widely trusted open source library - used by hundreds of millions of devices
- In 60% of these software projects, it’s used INdirectly
- Allows arbitrary code execution, the holy grail of exploits
- Can be exploited over the Internet without authentication

IT'S ALL ABOUT

BUILDING A CULTURE OF DEVSECOPS

- A security culture means that everyone – from C-suite members to Grads – must care about security and take steps to sustain it.
- Inject security into Agile Development by having localized knowledge.



SO...

WHY DO WE NEED SECURITY CHAMPIONS?

- 1 Cybersecurity professional to ~100 developers - spread too thin.
- The people closest to the code are the best equipped to keep it secure, IF they have some basic security training.

TELL ME...

WHAT ARE SECURITY CHAMPIONS?

- One management-designated person per small team or squad.
- At least 1/10 of the development population. (Developers, architects, testers, SREs, etc.)
- ~10-15 hours of application security training. Enough to be a local SME for their team.

SECURITY FOCAL VS. SECURITY CHAMPION

-Security Focal

- -~50-100% time commitment
- -Advise ~5-15 teams or squads
- -Work closely with other Security Focals, across a division or business unit
- -Primary point of contact with corporate Cybersecurity experts
- -Ensure that Security Champions are reacting quickly and reporting back status on urgent and important security work

-Security Champion

- -~25% time commitment
- -Advise 1 small team or squad
- -Work closely with other Security Champions and with their Security Focal
- -Monitor communications from their Security Focal, get work done within their own teams and report back

PLAYBOOK

HOW TO

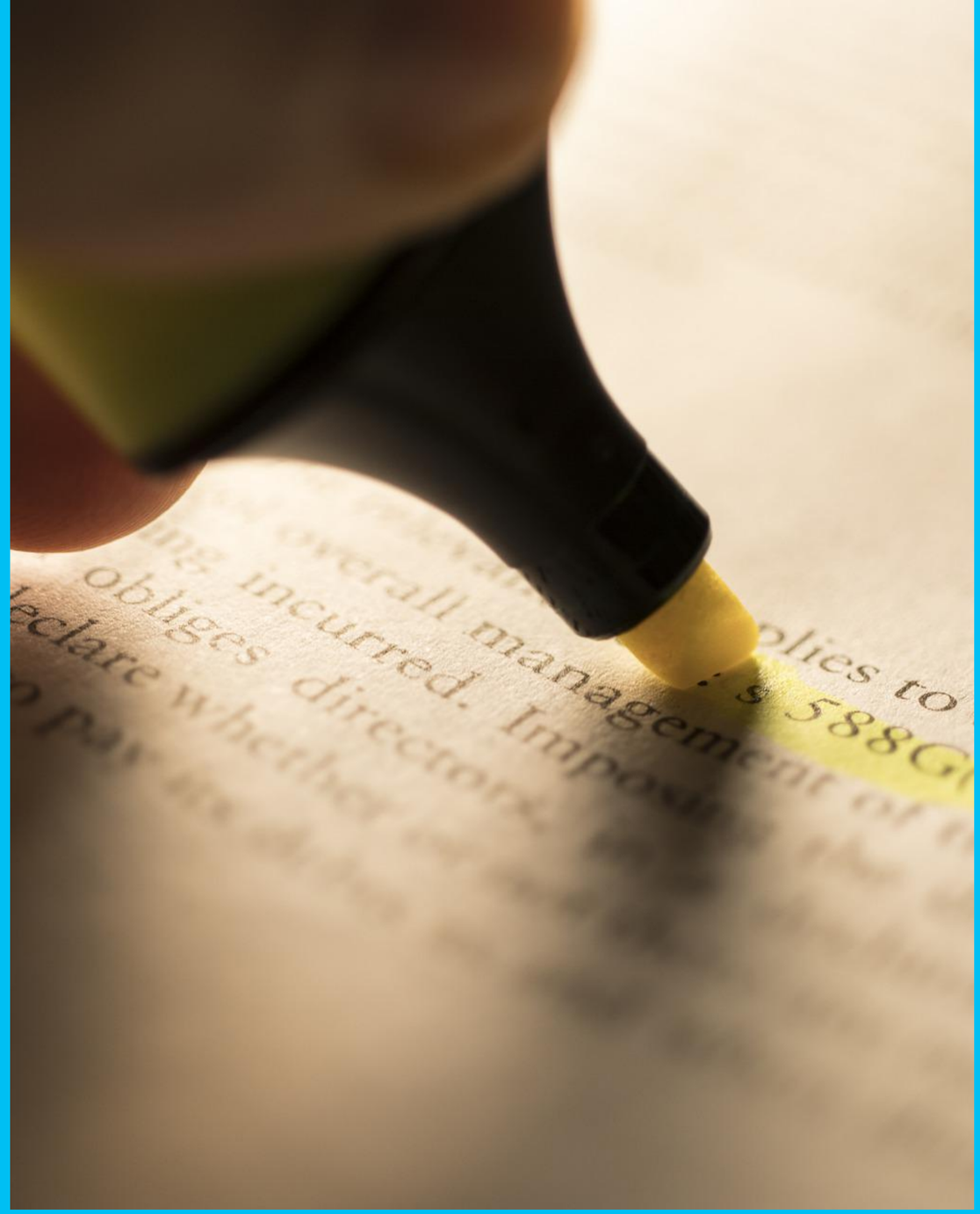
START A SECURITY CHAMPIONS PROGRAM

- Small working group for the program
- Create/publish a program description
- Get management & exec buy-in
- Choose a training plan, pay for it, set the training due date
- Managers appoint a designated Security Champion from each small team/squad
- Set up communications channels
- Kick off the program

SECURITY CHAMPION

PROGRAM DESCRIPTION HIGHLIGHTS

- Introductory info: what, why
- Expectations: time, training, communications, responsibilities
- HIGHLY VALUED subject matter experts
- Not necessarily the technical lead or most senior person - but they should be motivated
- NOT the only team members responsible for the more tedious security work



CHOOSING A

TRAINING PLAN

- Some examples in Slack
- Cybersecurity Basics - everyone in the company; 1-2 hours
- Security and Privacy for Developers 101 - all techies; 3-4 hours
- Additional training for the Security Champions:
  - Security and Privacy by Design; 3-5 hours
  - OWASP Top 10, Sans Top 25; 4-5 hours
  - Threat Modeling basics; 1-2 hours

DEVELOPERS WHO RECEIVE TRAINING ON HOW TO CODE SECURELY ARE 5X MORE LIKELY TO ENJOY THEIR WORK.

- SONATYPE 2020 DEVSECOPS COMMUNITY SURVEY HTTPS://WWW.SONATYPE.COM/2020SURVEY

INTERLOCK:

SECURE ENGINEERING GUILD

- Attendance expected for Security Focal(s) and Security Champions; open to others
- Recording or good agenda & minutes
- Topics
  - Status of time-sensitive work
  - Corporate initiatives or security alerts
  - Security tools and tool adoption details
  - Pen testing and remediation
  - Security in the News
  - 5-10 minutes of education

OTHER

COMMUNICATION CHANNELS

- Instant messaging is great for real-time conversations - a private channel for the Security Champions and Security Focal(s)
- Email lists: Security Champions, Security Focals, managers, etc.
- Bug tracking - security bugs may require embargoes and auditability
- Work tracking system for squads to certify that other time-sensitive work is done (Jira, Github Issues, etc.)

SOME CHALLENGES

CHALLENGES

Day to day life roles reflects on security

Challenges -

- The amount of time people have & make security important for them,
- the skill & capability that the developers has and how to make them aware about the impact of security on their jobs.
- support colleagues get (inc. from senior management) and the environment they work where they can call out security issues (by SMEs / Security experts).

Recommendation:

- E - Education
- A - Awareness
- I - Involvement
- R - Responsibility

CHALLENGES

NATWEST: LACK OF AWARENESS

Challenges -

- Lack of awareness of security principles within the delivery teams.
- Lack of awareness of what is truly susceptible or how exploits occur.

Recommendations:

- Ensure security awareness becomes ingrained in a company's culture, training becomes more effective then.
- inside development teams, establish and grow autonomous security champions.

CHALLENGES

NATWEST: BUY-IN

- Being a Bank is heavily guided by compliances, risks, governance and extra layers of regulators making security of paramount importance.
- Buy-In from Cyber Security, Compliance Security Technology BUs, Change Security,
- Recommendation: Create a sense of urgency by stirring conversation including leadership rep. especially from Security, conduct open forums brainstorming & share findings with C-suites, take shared (initiative) accountability for actions.

Challenge

TRUST AND COLLABORATION BETWEEN STAKEHOLDERS

Challenges

- Negative language and blame game of attributing employees as “weakest link”.
- Security relationship being dysfunctional

Recommendation

- Recruit security champions to act as a conduit

European Symposium on Research in Computer Security

↳ ESORICS 2021: **Computer Security. ESORICS 2021 International Workshops** pp 335–356 | Cite as

Why IT Security Needs Therapy

Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M. Angela Sasse & Imogen Verret

Conference paper | Open Access | First Online: 08 February 2022

469 Accesses

Part of the Lecture Notes in Computer Science book series (LNSC,volume 13106)

Source: https://link.springer.com/chapter/10.1007/978-3-030-95484-0_20#Abs1

CHALLENGES

ALL 3 COMPANIES: GLOBAL TEAMS

- IBM, Red Hat and Natwest Group all have globally distributed development teams working across time zones. Finding a time for the Security Guild to meet is difficult, and everyone tries to schedule recurring meetings in the same time slots.
- Recommendation: Choose a meeting time that works for your most engaged people. Or, have two meeting times: one for the Eastern hemisphere and one for the Western hemisphere.
- Recommendation: Encourage and support asynchronous communication with instant messaging, shared documents, meeting recordings, email and so on.

CHALLENGES

RED HAT: TRAINING FUNDING

- At Red Hat, one challenge we ran into is that the training program we chose cost about $250 per user, and by the time we got the budget approval, we only had 3 months left on the contract for the training plan. So, we had to wait for our Security team to negotiate a new contract.
- Recommendation: Choose an online training plan and request funding early! This could take a while.
- Recommendation: If you already have a good training plan available to you, start with that.

CHALLENGES

IBM: COMPLIANCE FATIGUE

- At IBM, our developers were already spending ~25% of all of their time on things like DSRs, privacy and security reviews, internal audits, patching software with security fixes, etc. This felt like yet more compliance work.
- Recommendation: One of the goals we chose for our Secure Engineering Guild was to automate as much of this manual toil as possible. We shared new automation in the Guild meetings and also pair-programmed with each other to implement changes.
- Recommendation: We also partnered with our CISO organization to pilot new tools.

WINS

12 MONTHS LATER...

IBM DIGITAL

- 10% of our developers became SMEs
- Critical alerts (“CISO overrides”) often handled within 1-3 days
- No teams falling through the cracks; more than 100 applications covered
- Far fewer security reports (pen testing, security tools, hackers) marked as “false alerts” or “could not reproduce”
- Uncovered new vulnerabilities
- Broader adoption of threat modeling
- Teams thinking about security every week

LET'S DO IT!

KEY TAKE-AWAYS

- A Security Champions program is straightforward and repeatable
- Requires:
  - Management support
  - A few people, 1-3 months to get the program started
  - Funding for online training
  - 1 Security Champion per team
  - 1-2 Secure Engineering Guild leads per org (usually a Security Architect or Security Focal)

FINALLY...

WHAT HELP DO WE NEED?

- We would love to hear if you have tried something similar yourself. What worked and what didn’t work?
-
- On what I should not waste time and what I can cheat from you ?.
-

THANK YOU!

Ann Marie Fred

@DukeAMO on Twitter

https://www.linkedin.com/in/amfred/

Siddharth Pareek

@pareeksiddharth on Twitter

https://www.linkedin.com/in/siddharthpareek/

Images sourced from Pixabay unless noted otherwise on the slide

BACKUP

SECURITY CHAMPION PROGRAM DESCRIPTION

- Introductory info similar to these slides: what, why, how Security Champions fill a need
- 1-2 designated Security Champions per team or squad; appointed by manager
- Security Champions are HIGHLY VALUED subject matter experts
- Not necessarily the technical lead or most senior person - but they should be motivated
- NOT the only team members responsible for the more tedious security work; everyone will keep up with patches, fixes, etc.
- Expectations: attend sync-up meetings; monitor communications channels; respond to requests
- Link to the chosen training plan(s) and expected completion dates
- Link to a document listing the Security Focals and Security Champions by team
- Link to the relevant communications channels:
    - Weekly or biweekly sync-up meetings
    - Private Slack channel

CHOOSING YOUR TRAINING PLAN

- Roughly ~10-15 hours beyond Cybersecurity Basics
- Cybersecurity Basics - everyone in the company; 1-2 hours
    - Phishing, secure passwords, how and when to report an incident...
- Security and Privacy for Developers 101 - all techies; 3-4 hours
    - validate input, escape output, handling personal/private/confidential data
    - company cybersecurity standards, processes, and people
    - how to report a software risk or vulnerability
- Security and Privacy by Design; 3-5 hours
    - secure application configuration, security in CI/CD, code reviews w/security mindset
- OWASP Top 10, Sans Top 25, finding and mitigating these vulnerabilities; 4-5 hours
- Threat Modeling basics; 1-2 hours
- Examples in Slack

LOG4SHELL

ACTIVE EXPLOITS

- 800k attacks within 4 days, 4m within a week
  - Botnets
  - Crypto miners
  - Nation state actors
- 40% of all corporate networks attacked within 4 days
- US gov't: "Assume compromise"

- Sources: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance, https://www.cybersecuritydive.com/news/log4j-what-is-known/611718/, https://blog.checkpoint.com/2021/12/13/the-numbers-behind-a-cyber-pandemic-detailed-dive/, https://snyk.io/blog/log4j-vulnerability-software-supply-chain-security-log4shell/

Image Source: The Log4j vulnerability explained - Its attack vector and how to prevent it (securecodewarrior.com), Datto's Response to Log4Shell

ENGAGE YOUR TECH TEAMS

To go beyond checking the boxes and doing the minimum, you need to energize and engage your architects, developers, and operations staff.

- **Show them the threats**
- **Make it interesting and concrete**
- **Teach them what to look for**
- **Give them control and responsibility**
- **Reduce the toil through automation**
- **Share what we're learning**