Welcome!

WWCode San Francisco - Backend Study Group

March 1, 2023

- We'll start in a moment :)
- We are **RECORDING** tonight's event
- We may plan to take screenshots for social media
- If you are comfortable, turn the video ON. If you want to be anonymous, then turn the video off
- We'll introduce the hosts & make some time for Q&A at the end of the presentation
- Feel free to take notes
- Online event best practices:
  - Don't multitask. Distractions reduce your ability to remember concepts
  - Mute yourself when you aren't talking
  - We want the session to be interactive
  - Use the 'Raise Hand' feature to ask questions
- **By attending our events, you agree to comply with our Code of Conduct**

WOMEN WHO CODE® /san-francisco

Introduction & Agenda

- Welcome from WWCode!
- Our mission: Empower diverse women to excel in technology careers
- Our vision: A tech industry where diverse women and historically excluded people thrive at any level
- About Backend Study Group

Prachi Shah

Host

Senior Software Engineer, Unity

Director, WWCode SF

Anubha Nagawat

Instructor

Security Architect, Pure Storage

ex-Stripe, ex-Meta, ex-Cisco

- Title: An introduction to a career in security:
  - Security is a complex field
  - Different careers in cybersecurity
  - Security Mindset
  - Q & A

- Future sessions:
  - Threat Modeling
  - Web vulnerabilities and OWASP
  - Low level languages
  - More topics to be decided

- Feedback form

Disclaimer:

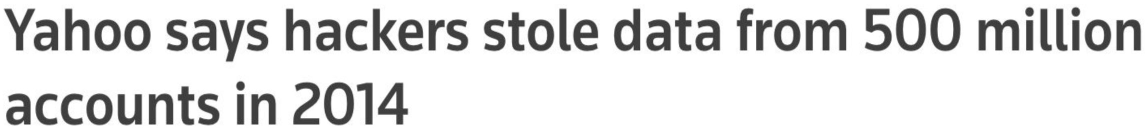
- Sessions can be heavy!
- Instructor doesn't have copyright on any of the images, all sourced from the Internet.
- Lots of acronyms
- Instructors don't know everything

WOMEN WHO CODE /san-francisco

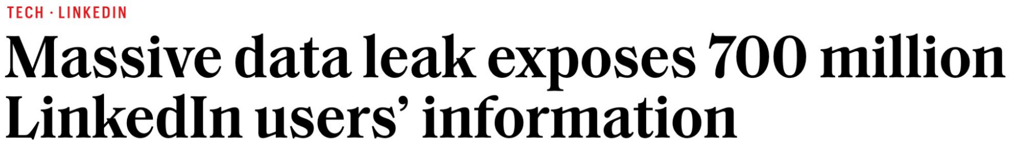
Security - A complex field

- 2022: 1802 data breaches known

- 2018 estimates: 3500 Security Vendors in USA alone



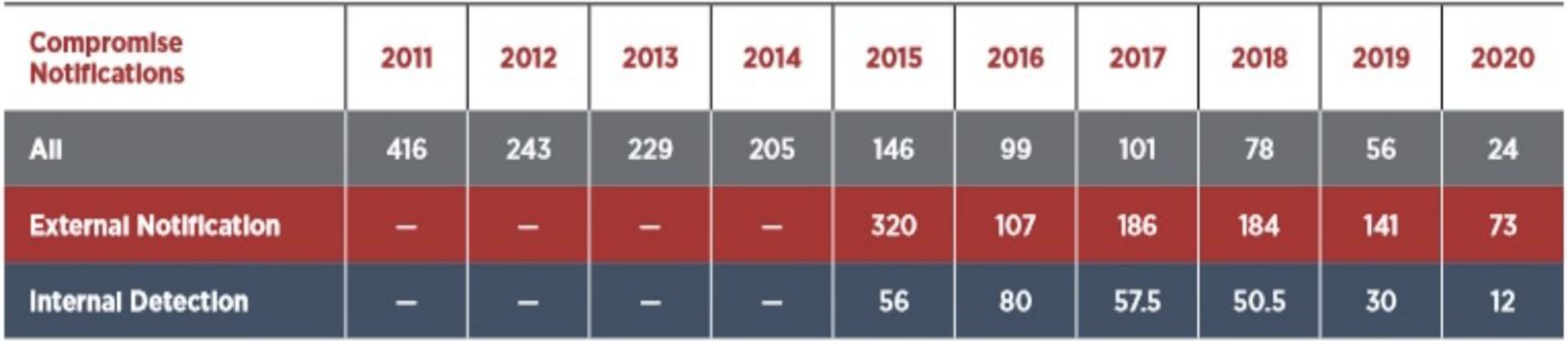
Yahoo says hackers stole data from 500 million accounts in 2014



TECH · LINKEDIN

Massive data leak exposes 700 million LinkedIn users' information

Security - A complex field



Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
All	416	243	229	205	146	99	101	78	56	24
External Notification	—	—	—	—	320	107	186	184	141	73
Internal Detection	—	—	—	—	56	80	57.5	50.5	30	12

Source: *https://vision.fireeye.com/editions/11/11-m-trends.html*

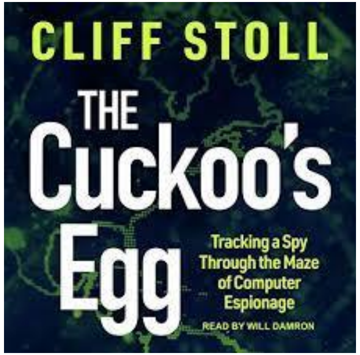
The Complexity - Interdependence

- Everything is connected

The Complexity - Macro AND Micro

- Macro - policy, product features, user behavior, trends, economics, use cases…

- Micro - specific lines of code, CVEs, a tiny unexpected behavior

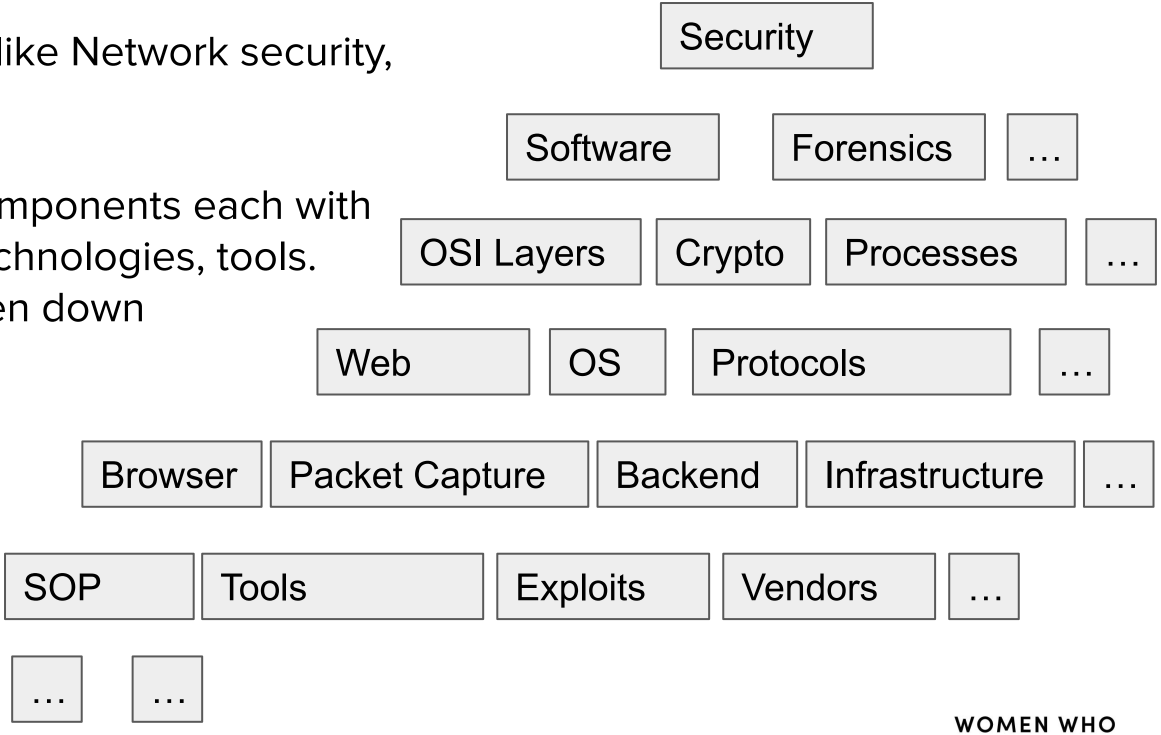


WOMEN WHO CODE®
/san-francisco

The Complexity - Breadth and Depth

- Consists of many different fields like Network security, Forensics, Policy

- Every field has many different components each with their own concepts, paradigms, technologies, tools. Each of these can be further broken down



Security

Software | Forensics | …

OSI Layers | Crypto | Processes | …

Web | OS | Protocols | …

Browser | Packet Capture | Backend | Infrastructure | …

SOP | Tools | Exploits | Vendors | …

… | …

WOMEN WHO CODE /san-francisco

The Complexity - Skill Stacks

Reverse Engineering
IDA Pro
Assembly Language
GDB
Understand the stack
Shellcode …

Web vulnerabilities
XSS
CSRF
SSRF
DDOS
IDOR …

Low level languages
Memory safety
Dangerous functions
Overflows
Command injection
Garbage collection …

Forensics
Disk
Memory
Autopsy
Legal procedures
Tools …

Hacking
Kali Linux
Packet capture
Bash
Scripting
Domain information ..

Compliance
ISO 27001
SOC
NIST-800
Common Criterion
…

Infrastructure
AWS/Azure/.. controls
Log analysis
Sandboxing
Containers
Terraform …

Operations
Threat Intel
APTs
MITRE ATT&CK
Dark Web
…

WOMEN WHO
CODE®
/san-francisco

The Complexity - Speed

Change is the only constant

- Things in security change at a massive speed because anything changing in any of the underlying fields has a direct impact on security
- New JS framework introduced
- New policy came up
- New CVE
- Exploit found in a well established protocol/ standard/ framework etc
- New political dynamic which changed the attacker landscape eg Russia-Ukraine War

The good news

- It never gets boring
- Forefront of technology
- Applicable across all domains
- Not going anywhere

The good news

- In 2022 there was an annual talent shortfall of 53,000 workers for cybersecurity professionals

- There are 561,743 additional openings requesting cybersecurity-related skills, and employers are struggling to find workers who possess them

- On average, cybersecurity roles take 21% longer to fill than other IT jobs

Source: cyberseek.org

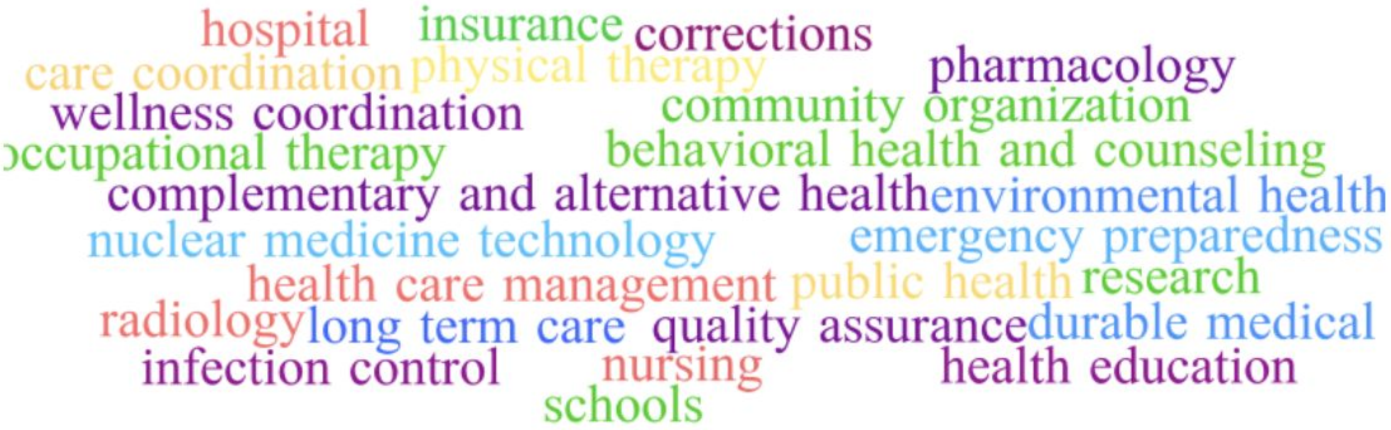
How to learn

- Everyone will give different recommendation

- Top Down
- Bottom Up
- Project Based
- Apprenticeship

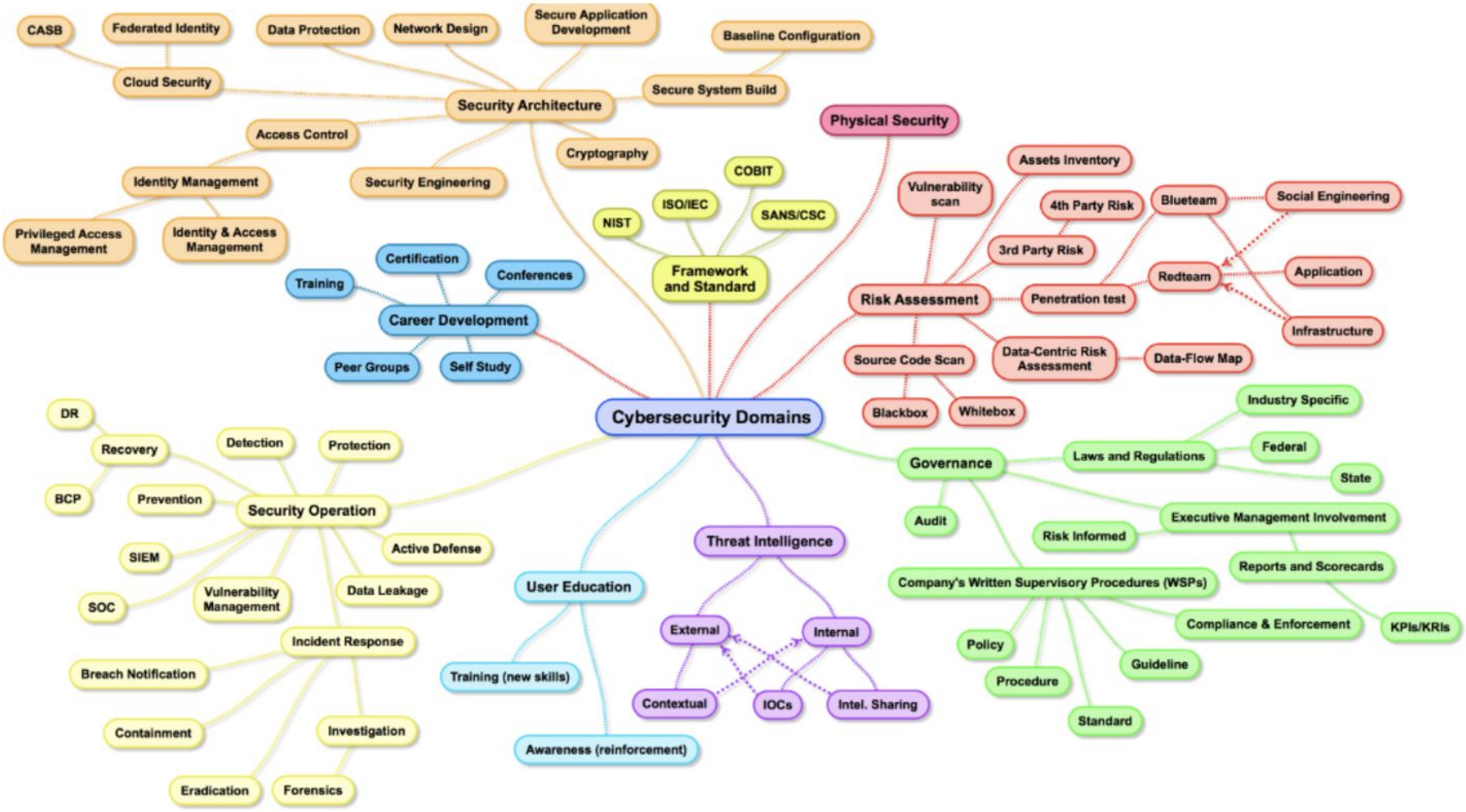
- Courses
- Capture the Flags
- Certifications
- Projects
- Internships

Careers



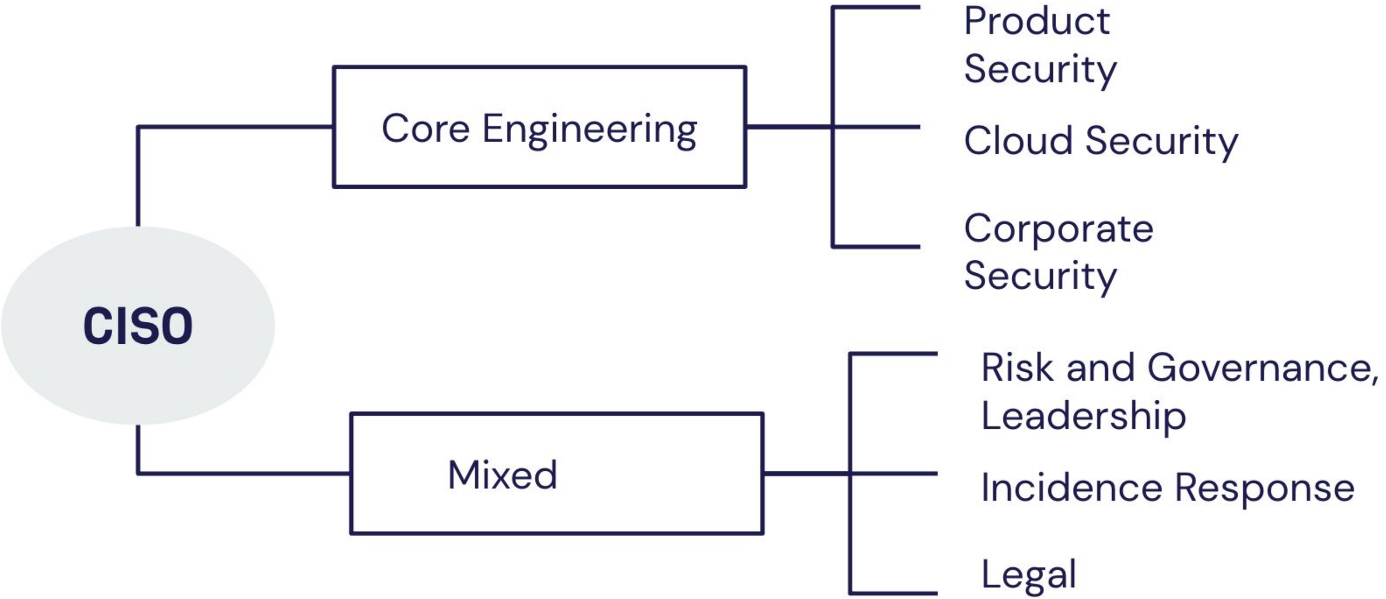
WOMEN WHO CODE®
/san-francisco

Careers



WOMEN WHO CODE®
/san-francisco

Different teams in enterprise



Different teams in enterprise

- Security Software Engineer
- Application Security Engineer (Product Security)
    - Pentest | Code Review | Security Design Reviews | Security Consultant
- Red Team
- Incidence Response
- Forensics
- Threat Detection
- Enterprise Security (Corporate Security)
- Platform Security (Cloud Security)
- Risk and Governance
- Security Legal
- Leadership, etc.

Security Software Engineer

- Coding - Intermediate (making tools) to Expert (frameworks - Full stack development likely)

- AppSec - Basic broad understanding preferred but not required. Expertise in a particular area likely will develop if developing framework in that area

- Ability to work cross teams - Low - Intermediate skills. Need to work with AppSec and Legal teams for initial requirements, design and feedback

- Cloud Sec - No

- Threat Detection - If working in Attacker Engineers then OS fundamentals. Low level programming. Else not needed

- Policy - No. Basic understanding can develop on the job

Appsec/Prodsec Engineer

- Coding - None to Intermediate in writing code. Expert in reading code
- AppSec - Expertise
- Ability to work cross teams - High. Appsec engineers work across teams on a daily basis.
- Cloud Sec - Intermediate
- Threat Detection - Low - Intermediate
- Policy - Intermediate

Red Team

- Offensive Security practices
- Security Mindset - Expert
- Pentesting - Expert
- Coding - Expert at Scripting. Broad Software Dev not needed
- Knowledge of zero day vulns. CTF practice
- Cloud Security - Intermediate to Expert

Incidence Response

- Respond to active incidents
- Coding - No
- Work under pressure and odd working hours

Forensics

- Post incidence exploration
- Compile evidence for legal cases
- Security expert counsel to attorneys and law enforcement
- Skills:
  - Forensics and Security and a wide variety of other tools - Expert
  - Laws concerning security, evidence admissibility and investigations - Expert
  - Ability to dismantle devices, retrieve lost data, rebuild systems

Threat Detection

- Detecting threats in the wild
- Log analysis
- Malware analysis
- Dark Web
- Scripting

Enterprise Security

- IT Team
- Endpoint security for all laptops, AV systems, camera etc within the company
- Knowledge of tooling

Cloud Security

- Infrastructure Security
- AWS/GCP/Azure
- Configure and set minimal baseline policies
- Threat modeling
- Scripting: Chef, Terraform

Security Legal

- In house Lawyers
- Compliance
- Audits
- PR

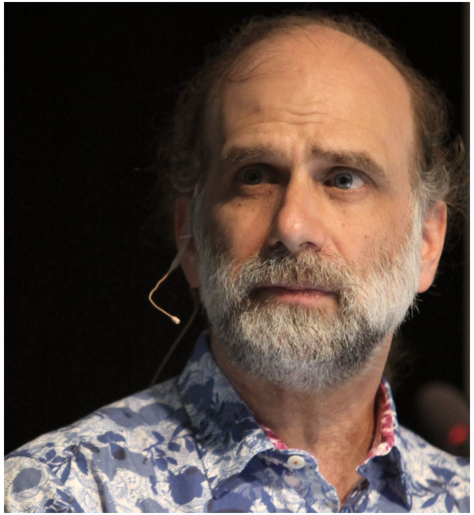
Leadership

- Similar skills to other leaders in industry
- Exclusively people with some security or legal background

Security Mindset

“I think Computer Security is most exciting part of Computing right now. Because it has something that nothing else has. It has an adversarial relationship. If you do graphics or operating systems, there is no one there trying to thwart you at every turn. That’s what you have in security. That’s what makes it exciting, and interesting. That’s what makes it something that’s forever changing and involves psychology and economics and computing and law and policy and so many things. “

- Bruce Schneier



Security Mindset

- Non Functional | Functional Requirements
- Abuse Cases | Use cases
- What if
- Everything except the happy path

WOMEN WHO CODE®
/san-francisco

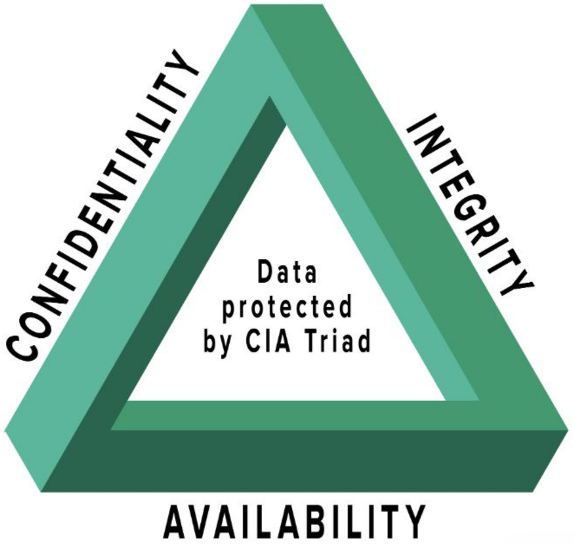
Security Mindset

- Amazon Go similar item same weight swap location
- Service car pickup - checking name and id
- uint64 index1 + uint64 index2 → 2^64 + 1
- Javascript in input box

Terminology / Fundamentals

- CIA Triad
- Defense in depth

CIA Triad



WOMEN WHO CODE /san-francisco

CIA Triad

- Confidentiality
  - No one should be able to get the call contents
- Integrity
  - User should hear what the other person has said on the call. An adversary or bug shouldn't alter the call details or metadata
- Availability
  - User should be able to place calls in most cases. Corner case emergency scenarios

Defense in Depth

Perimeter
Network
Endpoint
Application
Data

People | Process | Technologies

Development | Policy | Operations | Detection | Response

Backend Study Group

References:

- Conferences: Defcon, BlackHat, Usenix Security, RSA, BSides, Meetups
- Twitter
- Magazines and Newsletters: CyberWire
- Courses: Coursera and Udacity
- Youtube Videos and MIT 6.858 Computer Systems Security, Fall 2014 - YouTube
- Image Courtesy: google.com

Backend Study Group:

- Presentations on GitHub and session recordings available on WWCode YouTube channel
- System Design Series:
  - March 8th, 2023: Part 2 - Data and Scale
  - March 16th, 2023: Part 3 - Interview Questions
- April 6th, 2023: SQL Queries 101

Women Who Code:

- Technical Tracks and Digital Events for more events
- Join the Digital mailing list for updates about WWCode
- Contacts us at: contact@womenwhocode.com
- Join our Slack workspace and join *#backend-study-group*!

You can unmute and talk or use the chat

WOMEN WHO CODE®
/san-francisco