DAY OF SHECURITY

May 11, 2022

Encompassing the Cybersecurity Spectrum from the eyes of an Infosec Professional

DAY OF SHECURITY

Who Am I?

I am Saman Fatima

- Cybersecurity Enthusiast
- Data Engineer - Macquarie Group
- Management Lead/Vice Chair of Board - BBWIC Foundation
- Committee member - OWASP WIA
- Volunteer Instructor - CyberPreserve
- Global Member - WiCyS
- Women In Cloud - Advisor and Ambassador
- Snyk Ambassador

DAY OF SHECURITY

Today's Agenda

1. Different Color Teams Introduction
2. Color Team Collaboration
3. Survey Results
4. Skills Required
5. Training Programs/Community Groups
6. Certifications & Conferences

Are you ready?

Let's begin!

Red Team

- Breakers | Offense
- **Overcome Cybersecurity Controls**
- **Strengthen** Organization’s Security Posture
- Social Engineering Attacks

Blue Team

- Defense | Defenders
- **Protect** the Organization’s Critical assets
- Risk Assessment
- Monitoring
- Education of Employees

Purple Team

- Collaboration between **Red** + **Blue** Team to maximize effectiveness
- **Not Permanent** but for a dynamic partnership

Yellow Team

- Builder
- Improve Application Security

  - Education

  - Convert to IaC

  - Automate Security Testing

Green Team

- Super Defenders
- **Blue** + **Yellow** Team
- Architecture & Coding Knowledge
  + Defensive & Operational Skills

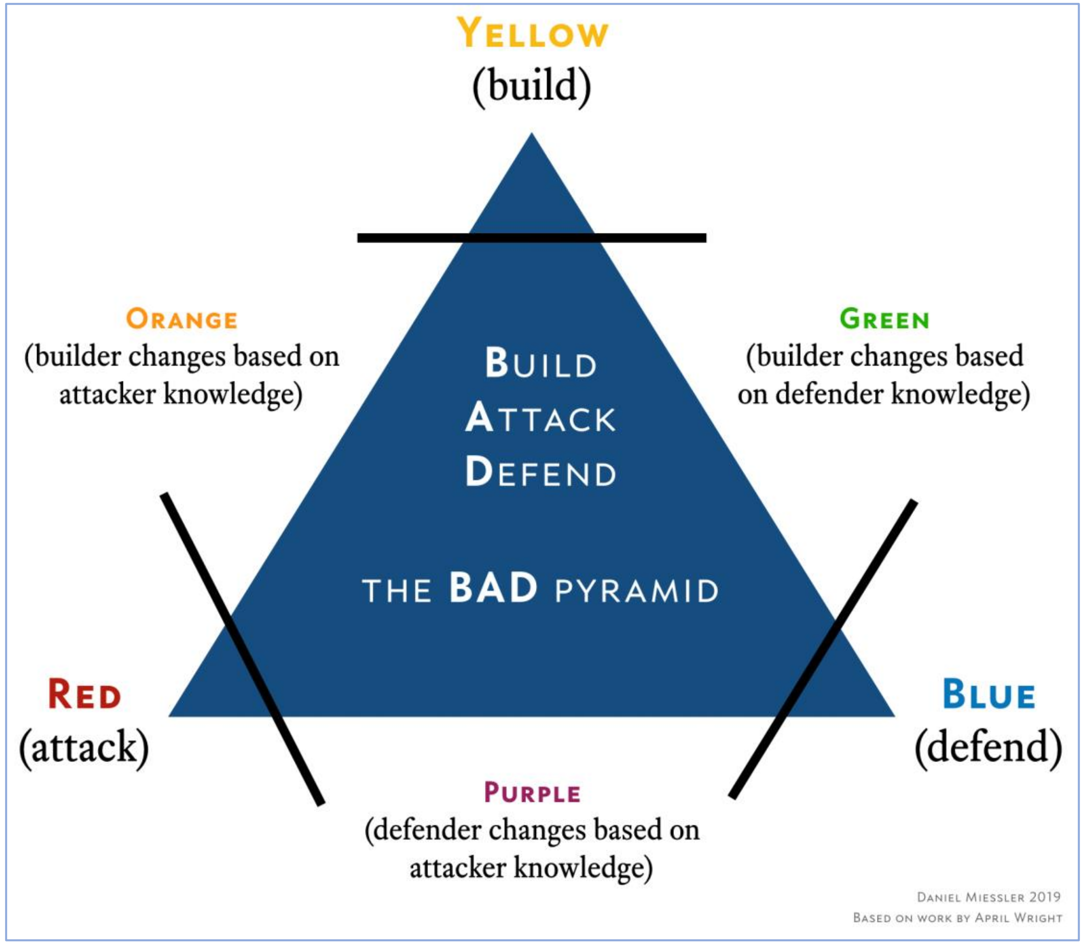
Orange Team

- Red + Yellow Team
- Secure Development Training
- Security Practices
- Build better systems and solutions

White Team

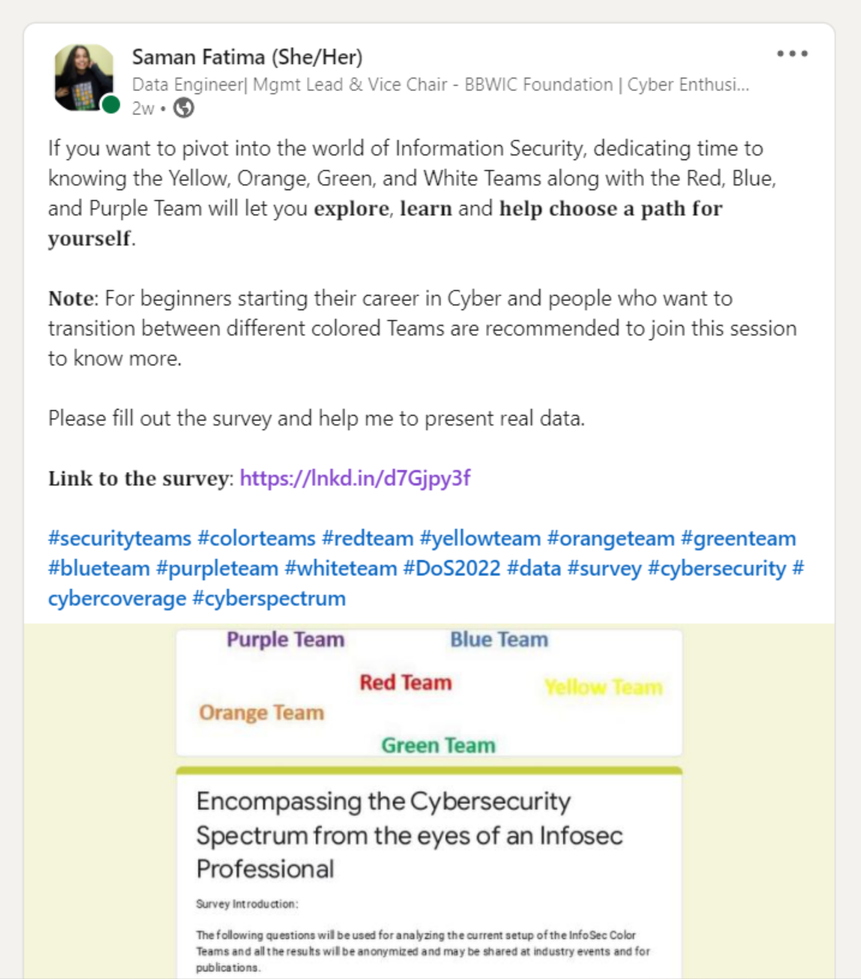
- Neutral
- Non-technical Responsibilities
- Mix of Senior Technical members, Management & Business sponsors

Team Collaboration


YELLOW
(build)
ORANGE
(builder changes based on attacker knowledge)
GREEN
(builder changes based on defender knowledge)
BUILD
ATTACK
DEFEND
THE BAD PYRAMID
RED
(attack)
BLUE
(defend)
PURPLE
(defender changes based on attacker knowledge)
DANIEL MIESSLER 2019
BASED ON WORK BY APRIL WRIGHT

DAY OF SHECURITY

Survey



Saman Fatima (She/Her)

Data Engineer| Mgmt Lead & Vice Chair - BBWIC Foundation | Cyber Enthusi...

2w •

If you want to pivot into the world of Information Security, dedicating time to knowing the Yellow, Orange, Green, and White Teams along with the Red, Blue, and Purple Team will let you **explore**, **learn** and **help choose a path for yourself**.

Note: For beginners starting their career in Cyber and people who want to transition between different colored Teams are recommended to join this session to know more.

Please fill out the survey and help me to present real data.

Link to the survey: https://lnkd.in/d7Gjpy3f

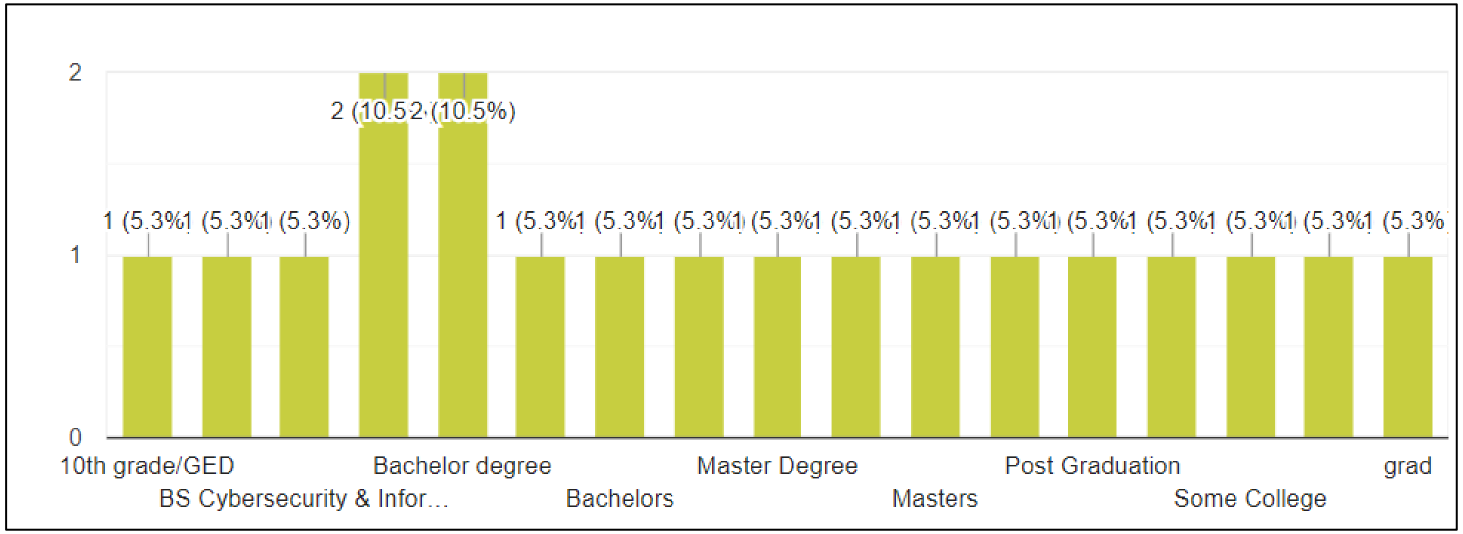
#securityteams #colorteams #redteam #yellowteam #orangeteam #greenteam #blueteam #purpleteam #whiteteam #DoS2022 #data #survey #cybersecurity #cybercoverage #cyberspectrum

Encompassing the Cybersecurity Spectrum from the eyes of an Infosec Professional

Survey Introduction:

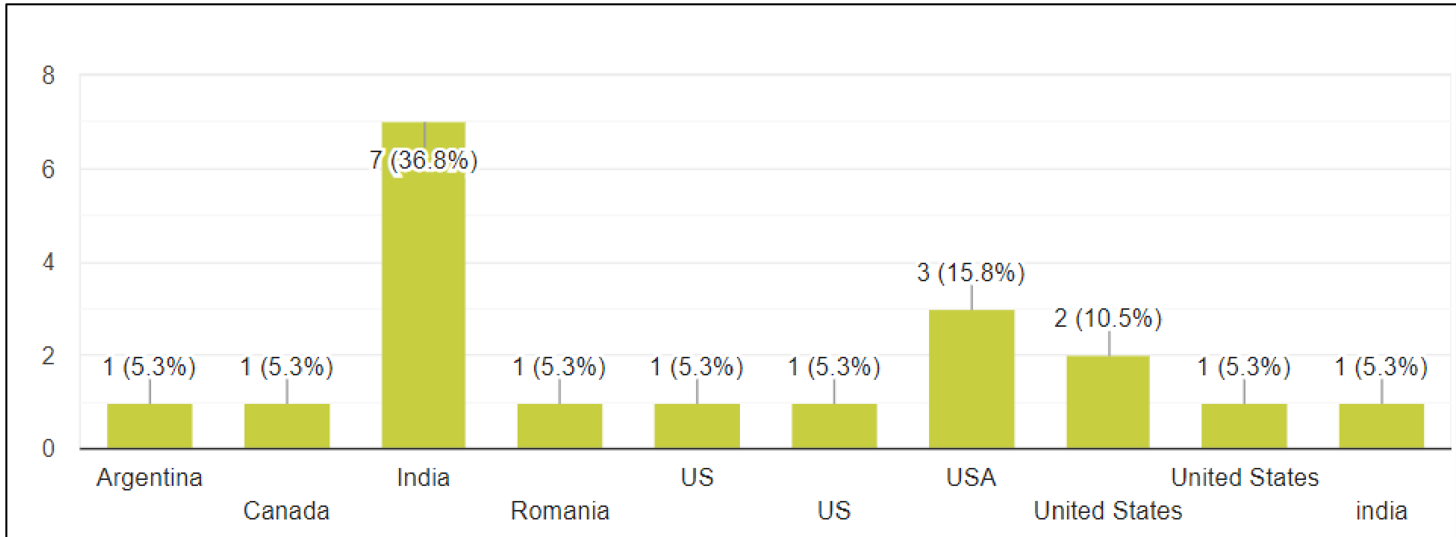
The following questions will be used for analyzing the current setup of the InfoSec Color Teams and all the results will be anonymized and may be shared at industry events and for publications.

Survey Results

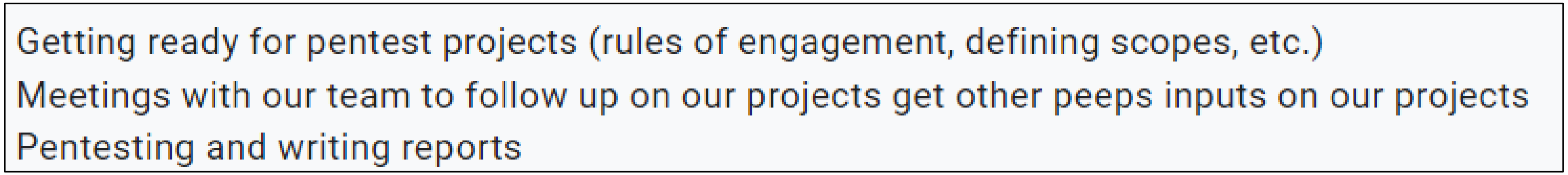


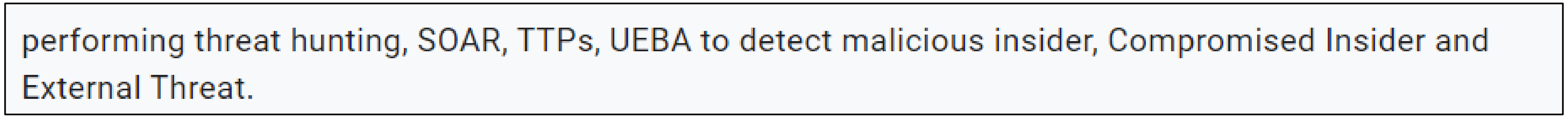
Highest Level of Education

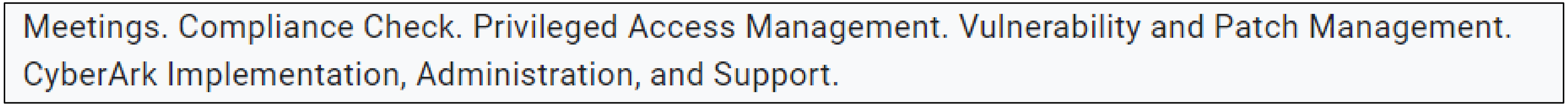
Country working in

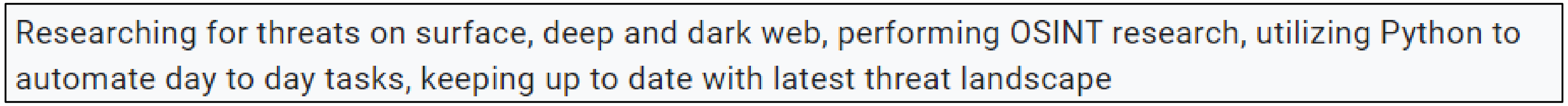


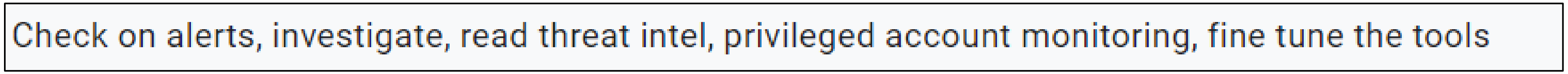
A day in your Work Role

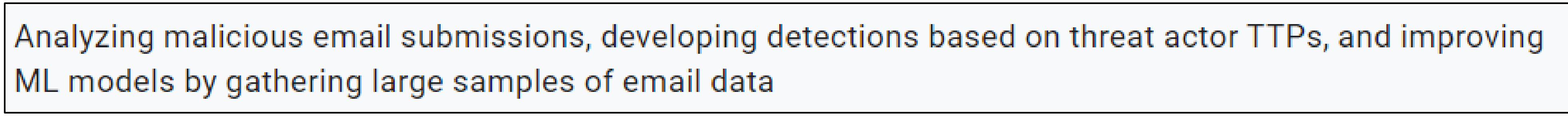

Getting ready for pentest projects (rules of engagement, defining scopes, etc.)
Meetings with our team to follow up on our projects get other peeps inputs on our projects
Pentesting and writing reports


performing threat hunting, SOAR, TTPs, UEBA to detect malicious insider, Compromised Insider and External Threat.

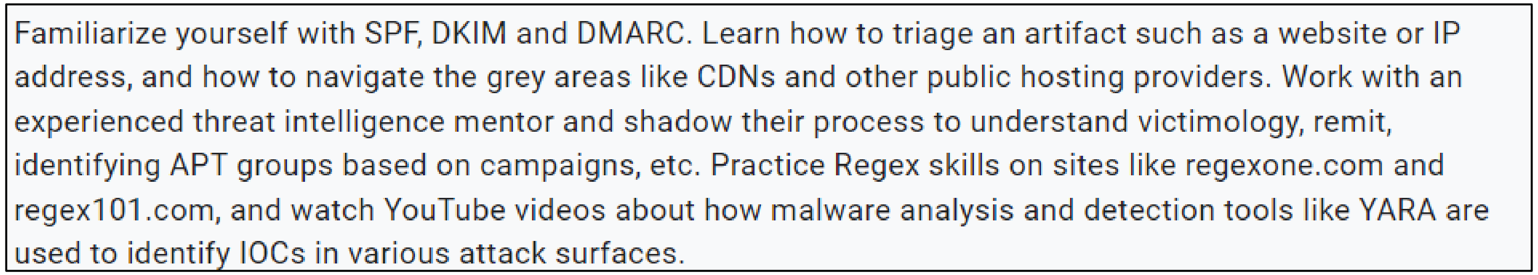

Meetings. Compliance Check. Privileged Access Management. Vulnerability and Patch Management. CyberArk Implementation, Administration, and Support.


Researching for threats on surface, deep and dark web, performing OSINT research, utilizing Python to automate day to day tasks, keeping up to date with latest threat landscape

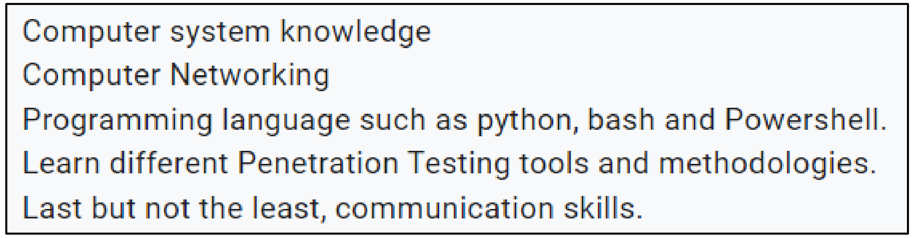

Check on alerts, investigate, read threat intel, privileged account monitoring, fine tune the tools


Analyzing malicious email submissions, developing detections based on threat actor TTPs, and improving ML models by gathering large samples of email data

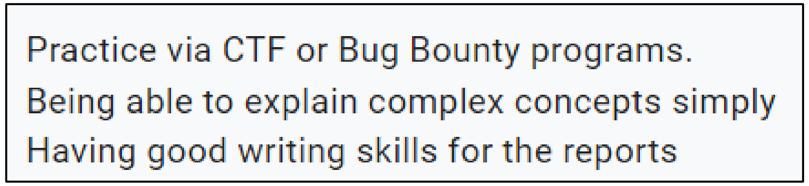
Skills Required



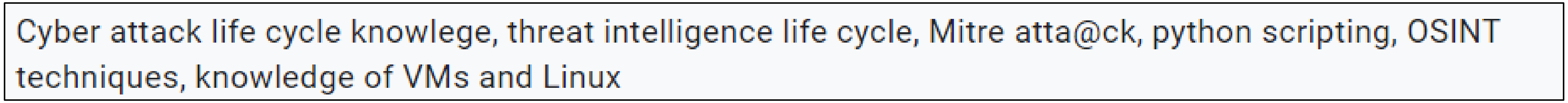
Familiarize yourself with SPF, DKIM and DMARC. Learn how to triage an artifact such as a website or IP address, and how to navigate the grey areas like CDNs and other public hosting providers. Work with an experienced threat intelligence mentor and shadow their process to understand victimology, remit, identifying APT groups based on campaigns, etc. Practice Regex skills on sites like regexone.com and regex101.com, and watch YouTube videos about how malware analysis and detection tools like YARA are used to identify IOCs in various attack surfaces.



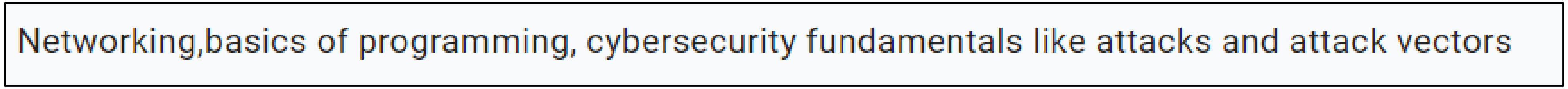
Computer system knowledge
Computer Networking
Programming language such as python, bash and Powershell.
Learn different Penetration Testing tools and methodologies.
Last but not the least, communication skills.



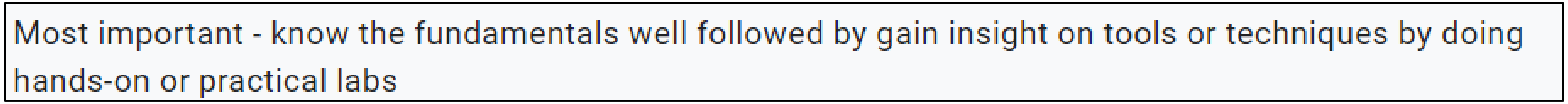
Practice via CTF or Bug Bounty programs.
Being able to explain complex concepts simply
Having good writing skills for the reports



Cyber attack life cycle knowlege, threat intelligence life cycle, Mitre atta@ck, python scripting, OSINT techniques, knowledge of VMs and Linux



Networking,basics of programming, cybersecurity fundamentals like attacks and attack vectors



Most important - know the fundamentals well followed by gain insight on tools or techniques by doing hands-on or practical labs

Training Programs/Community Groups

- Mitre Attack Framework, CIS Controls, NIST, SANS, OSINT(Joe Gray's training)
- **Platforms** - Cybrary, TryHackMe, Udemy, Coursera, Pluralsight, RangeForce, Immersive labs
- **Communities** - BBWIC Foundation, OWASP, Cyber Insecurity, Cyber supply drop, and Simply Cyber
- Rapid ascent (FB group)
- **CTFs** - Trace Labs Missing Persons

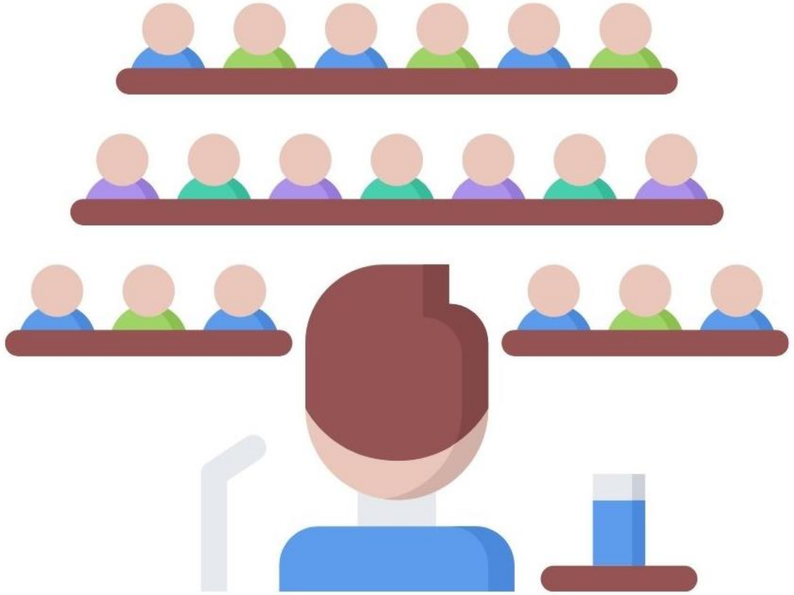
Certifications

- SC-200
- CEH
- ISO27001
- MAD
- CCSK
- CISSP
- GREM
- CySA+
- Pentest+
- OSCP
- Zero-Point Security certifications
- PNPT
- SANS red teamer certification
- eLearnSecurity certifications

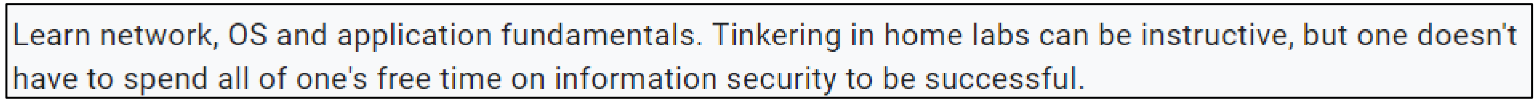
CERTIFIED
CERTIFIED
CERTIFIED

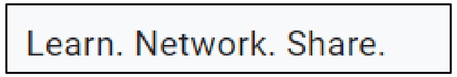
Conferences

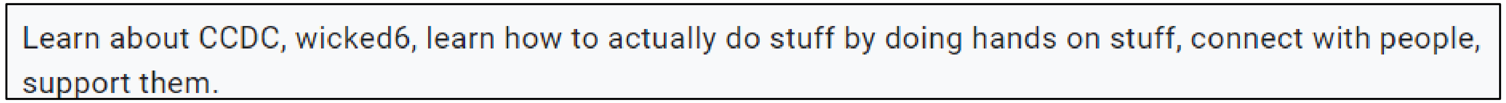
- DefCon
- Splunk
- SANS
- Blue Team Village
- NullCon
- AttackCon
- Purple Hat
- Hacker Halted
- TDI
- Black Hat
- RSA
- CCC
- Local BSides

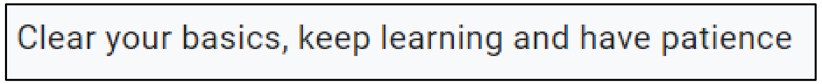


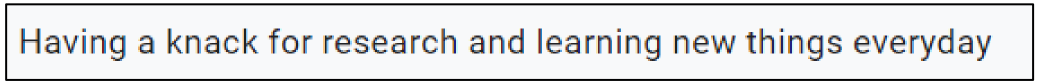
Advice from the Community

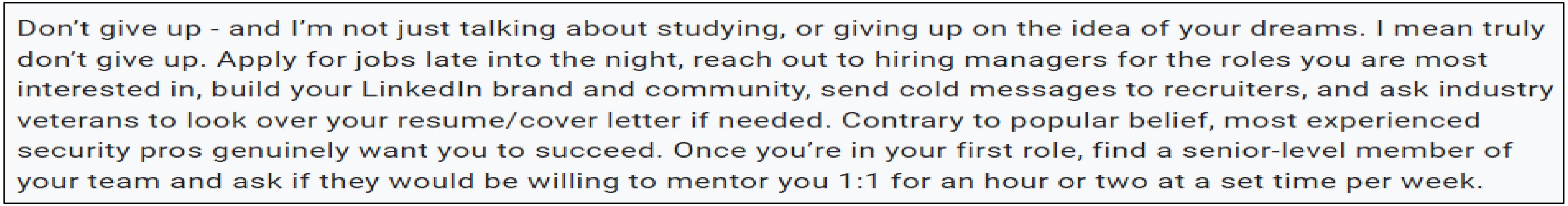

Learn network, OS and application fundamentals. Tinkering in home labs can be instructive, but one doesn't have to spend all of one's free time on information security to be successful.

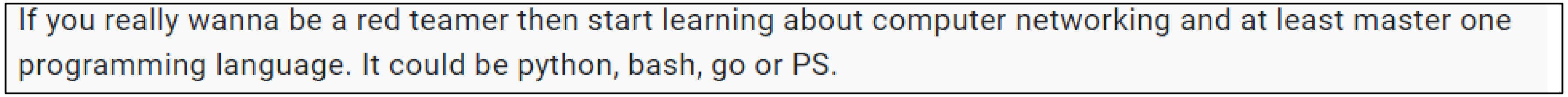

Learn. Network. Share.


Learn about CCDC, wicked6, learn how to actually do stuff by doing hands on stuff, connect with people, support them.


Clear your basics, keep learning and have patience


Having a knack for research and learning new things everyday


Don't give up - and I'm not just talking about studying, or giving up on the idea of your dreams. I mean truly don't give up. Apply for jobs late into the night, reach out to hiring managers for the roles you are most interested in, build your LinkedIn brand and community, send cold messages to recruiters, and ask industry veterans to look over your resume/cover letter if needed. Contrary to popular belief, most experienced security pros genuinely want you to succeed. Once you're in your first role, find a senior-level member of your team and ask if they would be willing to mentor you 1:1 for an hour or two at a set time per week.


If you really wanna be a red teamer then start learning about computer networking and at least master one programming language. It could be python, bash, go or PS.

“

Security used to be an inconvenience sometimes, but now it’s a necessity all the time.

~ Martina Navratilova

”

References

- https://www.blackhat.com/docs/us-17/wednesday/us-17-Wright-Orange-Is-The-New-Purple-wp.pdf
- https://www.youtube.com/watch?v=6s-G7u0w-wc
- https://sqa-consulting.com/cyber-security-index/

Any Questions??

- **Twitter:** @saman_3014
- **LinkedIn:** https://www.linkedin.com/in/saman-fatima-30/

DAY OF SHECURITY