INFORMATION SECURITY CAREER PATH

A Guide for the Newbies

Global Information Security Society for Professionals of Pakistan

If you are not willing to learn, no one can help you.

If you are determined to learn, no one can stop you.

PREFACE

Every now and then we get into debates on how one can begin his career into information security field and what he or she should be doing to become good information security professional. Most of the times such discussions will go on for a few hours and then get buried under other topics. We recently came across a situation, where a member of GISSP group was looking for a pen testing job with no practical experience in information security domain. Many of the senior members came up with suggestion and guiding comments, but all those will be of no use for any new comer in the group. We thought that it is time that we should play our part and guide our younger generation in a more symmetric way. INFORMATION SECURITY CAREER PATH – A Guide for Newbie is a collective effort by GISPP (Global Information Security Society for Professionals of Pakistan) members. The contributors mentioned below have compiled the data and added information in order to add value to the document. The document is classified as '**Public**' and should be shared among Pakistani IT professionals as well as computer science students; whereas the reproduction of this guide with any other name or any part of the content is strictly 'PROHIBITED'.

For any feedback and comments, kindly let us know on feedback@gispp.org

SHAHZAD SUBHANI

ABOUT GISPP

GISPP (Global Information Security Society for Professionals of Pakistan) is a small but conscientious group of Pakistani Professionals working worldwide and endeavor to be a leading cyber security platform to make Pakistan and rest of the world a safe cyber space and continue earning distinctive reputation for Pakistani Cyber Security Professionals worldwide.

GISPP is an initiative of Mr. Shahzad Subhani along with a group of Pakistani Information Security professionals living and working in Saudi Arabia. Despite being a humble start, GISPP is now actively present on different social connectivity platforms including WhatsApp, Facebook, LinkedIn and on Telegram.

GISPP's Vision

To be a leading cyber security platform to make Pakistan and rest of the world a safe cyber space and continue earning distinctive reputation for Pakistani Cyber Security Professionals worldwide.

GISPP's Objectives

- Develop a culture of knowledge sharing & seeking by engaging and educating INFOSEC aspirants.
- Provide diverse forum for exchange of views and experiences on Information Security.
- Initiate a wide range of educational programs related to Information Security.
- Promote expansion of Information Security Industry at all levels.
- Offer a professional networking, collaboration and knowledge sharing platform.
- Help GISPP members and member organizations in finding suitable jobs or skilled employees.
- Promote Open Source Technologies usage for Information Security, wherever possible.
- Promote the ethnic development in Information Security.
- Advise and influence policy makers for the best interest of community at large.
- Bridge the gap between local and international Initiatives & communities.

Connect with GISPP

If you are a Pakistani and working in Information security field anywhere in the world, you are welcome to join GISPP by following the links mentioned below.

LinkedIn: www.linkedin.com/groups/10314172
Facebook: www.facebook.com/groups/976571862396454/
Facebook Page : https://www.facebook.com/gispp.org
Website: https://www.gispp.org/

ACKNOWLEDGEMENTS

We would like to express our gratitude to the contributors and reviewers for this guide for giving their precious time and worked on this guide with interest.

Contributors

- Mr. Sajjad Haider [www.linkedin.com/in/sajjadjanjua]
- Mr. Shahzad Subhani [www.linkedin.com/in/shahzadsubhani]
- Mr. M.Farrukh Mahmood [www.linkedin.com/in/muhammad-farrukh-mahmood-a21ba015b]

Reviewers

- Mr. Umair Aziz [www.linkedin.com/in/umairaziz27]
- Mr. Saquib Farooq Malik [www.linkedin.com/in/saquibfarooq]
- Mr. Kashif Iqbal [www.linkedin.com/in/kashifccspccnp]
- Ms. Suman Siddiqui [www.linkedin.com/in/suman-siddiqui-infosec-grc]

Contents

Introduction

Every day in our professional life, we come across people who work in the field of Information Technology and want to pursue their career into the field of Information Security due to their personal and professional reasons. At the same time, there are students and fresh graduates who have heard of Information Security and want to begin their career in it. We have tried to address all those categories by writing this guide for both fresh graduates and professionals. Crux of the matter is, that you can start anywhere you want to start. However, you should focus on what you want to do and then focus on finding the best place to do that and stay there.

In this guide, we came up with some suggestions and we are optimistic that you will find them very useful.

Keep yourself **mentally** focused and **spiritually** connected with your career goals.

Suggestions

If you are already working in IT field, then you can start from point 3 onwards. However, if you are a student or a fresh graduate then you should be starting from point 1.

1. Get yourself registered on any of the following sites:
    a) edx (https://www.edx.org/)
    b) URDU IT Academy (https://www.urduitacademy.com/)
    c) Cybrary https://www.cybrary.it/
    d) UDEMY (https://www.udemy.com/)
    e) SANS (https://www.sans.org/)
2. Enroll yourself in free basic security courses i.e. introduction to security, cybersecurity basic, building cybersecurity toolkit, etc.
3. Please refer to Cyber Security Career Advise by URDU IT Academy . It is a very informative video by our Partner organization , URDU IT Academy .
4. Identify the security domain of your interest and want to pursue. For each domain, there are some vendors, who are leaders in that domain and most of them have very good learning resources available on their website or YouTube channels.
5. Use the "For Dummies" series publications for learning, some good recommendations are:

Computer Security for Dummies	Cyber Security for Dummies	Hacking Wireless for Dummies
Network Security for Dummies	Computer Forensics for Dummies	Firewall for Dummies
Hacking for Dummies	Computer Virus for Dummies	Rootkits for Dummies

A detailed list of "for dummies "series on the topic of security can be found at: https://www.dummies.com/store/Computers-Internet/Security.html

6. Some most common information security domains are mentioned here:

Information Security Domains	
Governance	Security Operations/Controls (Email Gateways, Anti APT Solutions etc.)
Compliance (ISMS, PCI and other standards)	Network Security (IDS/IPS/Firewalls/NG Firewalls)
Vulnerability Assessment/Management	IR (Incident Response)
Penetration Testing	Forensics (System/Network)
IOT(Internet of Things)	Scripting(Python/Perl for Hardware Security)
Enterprise Security Architecture (ISSAP,TOGAF,SABSA)	Risk Management
Security Monitoring via SOC (Security Operations Center)	Application Security (Web+ Mobile)
Pre-Sales (Technical/Marketing)	Systems Security
ICS (Industrial Control Systems)	Cloud Security

7. Use Twitter to follow various security vendors, magazines and some experts in order to enhance your knowledge and understand new trends and technology. Some famous handles are:

@Symantec	@JuniperNetworks	@Unit42_Intel
@CiscoSecurity	@PaloAltoNtwks	@dvk01uk
@threatintel	@TalosSecurity	@Mandiant
@NakedSecurity	@avast_antivirus	@qualys
@IBMSecurity	@CISecurity	@SearchSecurity
@FireEye	@securitytwits	@WindowsATP
@QradarUG	@SANSDefense	@SwiftOnSecurity
@CISAgov	@GbhackerOn	@bitdefender
@SANSPenTest	@IBMSecurity	@moixsec
@metaspolit	@cnn	@Peerlyst

See Appendix C for list of twitters handles with description for each ID.

Your Only limit is **You** and Your **Attitude** determine Your **Altitude**.

8. Learn about TCP/IP and other protocols (HTTP, SMTP, SNMP, HTTPS etc.).
9. Learn about application security guidelines, especially from OWASP.
10. Learn to read and understand logs in order to develop log analysis skills.
11. Watch videos about different products (if available).
12. Setup a lab or join any online paid labs and work on tools like Kali Linux or Ubuntu, Python and PowerShell languages.
13. Get in touch with security professionals and expand your circle by attending security conferences, seminars and webinars.
14. Clarify your concepts by engaging in discussions with your peers, friends from the same domain. Healthy professional discussions are always beneficial to clarify any doubts.
15. If you are a GISPP member, pay attention to group posts and if any jargons or concepts are difficult to understand, google about it for better understanding.
16. Try to learn something new every day, if you cannot do that, review what have you have learned yesterday.
17. Share your knowledge, this will help you to learn more.
18. If needed, invest money on yourself for learning by sitting for a certification exam, purchasing recommended learning material or even attending paid training programs. If you have a shortage of cash, get a soft bank loan or use traditional 'Chit' system to gather funds (recommended).
19. Look for a mentor, but never fully depend on one. More the better.
20. Get out of your comfort zone and reach out to other information security professionals.

Skill and Toolbox

There are multiple skills that you may require to improve during the job, job search or during your studies. Toolboxes and apps can help you improve on this. We have tried to highlight the important ones below. Keep in mind that all these skills should ad can be continuously improved.

Soft Skills

Soft skills are also referred as transferable skills or **professional skills**. As this term implies, these are skills that are less specialized, less rooted in specific vocations and more aligned with the general disposition and personality. Some important ones are:

Presentation Skills	Listening Skills	Creativity Skills
Communication Skills	Reading Skills	Time Management Skills
Writing Skills	Situation Handling Skills	Teamwork Skills
Verbal Skills	Problem Solving Skills	Public Speaking Skills

Learning how to learn is a very important life **skill.**

Technical Skills

Your technical skills are your weapons and you need to hone them and adapt new ones with the drift of technology, so you need to improve on or start learning at least two of the skills mentioned below.

Network Security	Scripting (VB /Batch /Power Shell)	Web security
System Security	C or C++	Unix/Linux
Database Security	Python	Regex creation
kubernetes security	SQL	Cloud Security
DevSecOPs	Data analytics	AI for security

Later, in the learning process, aim for an industry certification, which will testify your level of expertise.

Certifications are mentioned in figure 1 (Certification Map).

Remind yourself between **exception and norm** on periodic basis.

Security Toolbox

Toolbox helps you to learn new technologies, some important are mentioned below.

Basic Emulator & Terminal Tools	Basic Services knowledge	Protocols
Cygwin	Web services (Apache or IIS)	TCP/IP
MobaXTerm	Proxy services (Squid or ISA)	IMAP
Putty	Mail service (Sendmail and Exchange)	POP
Secure CRT	Snoop	SMTP
FTP, TFTP	Iptables or route tables	Kerberos
SFTP, WinSCP	NFS services	SSH
Wireshark	SMB services	SSL
Trace route	DHCP services	TLS
NMAP	DNS Services	Protocols/Ports

Try to **get hands on experience** for at least first 7 years.

Tips and Tricks

Here are some tips based on our members' experience.

Job Searching Tips

1. Information security is vast domain, so analyzing the job market in a particular region will be wise and will help a newbie to select some area of Information Security to start with and focus on it.
2. LinkedIn is a good tool to check regional and global job trends and market demands in the InfoSec sector.
3. If you are targeting a specific company, check company profile and its employees' reviews on glassdoor.com. You can get an idea of the culture of the company.
4. For any job posted on LinkedIn, never write any comment like "interested" Instead, get in touch with the recruiter or the person who posted it and open a well-crafted conversation- this is all about your social network skills.
5. For making a perfect LinkedIn profile, follow Sohaib Hasan on LinkedIn (www.linkedin.com/in/sohaibhasan) and his channel on telegram for daily tips and articles. He is highly recommended for professional advice for making your profile and job hunt through LinkedIn.
6. Review Stock Market web pages, this will help you to understand which sector is growing most and which is not.
7. Target jobs in specifics sectors i.e. Financial, Government, Telecom, Energy, Fast moving consumer goods (FMCG), Health and the Automotive sector and review job posting for those sectors, this will also help you understand the requirements for different industries.
8. If you are multi-skilled and want to apply for jobs of different domains, make sure to have 2-3 different CVs for each domain you are interested in.
9. On average recruiters spends 20 seconds on each CV, make those 20 seconds count by listing only the required information which the recruiter might be looking for.
10. Go through the 'Job Description' in detail and reflect those on your CV from your experiences.
11. Review your CV before applying to any job, CV is your marketing tool.

12. Most importantly be honest with yourself, if you feel that you have the required skills as mentioned in JD only apply then. There is no point in applying for every job that doesn't seem suitable as per your experience.

Work Hard and **dedicate** yourself to being better **every single day.**

Interview Tips

1. Be good at what are you taught at university and clear your concepts.
2. Challenge yourself learn to practice and then answer the questions from this link & this link. Do not memorize the answers. Prepare as much as possible for network security concepts, ISO 27001 and read the 11th hour CISSP study guide by Eric Conrad as it can give you a good idea about different security domain .
3. Be ready to defend what is written on the CV. (don't mention anything which you cannot defend).
4. Develop all the skills and practice. Sometimes the interviewer goes through your resume line by line.
5. It is ok to say no if you do not know an answer. Try to show the interviewer that you are a good learner and hard worker.
6. A day before the interview, start speaking to yourself by putting yourself in some situation or asking questions to yourself. This will help you to answer well in the interview.
7. Remember you have one chance to sell yourself, so be a bestseller.
8. Show positive body language.
9. Use hand gesture while explaining.
10. Use analogies while answering any question for example in situation xyz we can do abc and there is opq as well. But to my understanding, abc is much better.
11. In some interviews people ask you to tell your weakness, get yourself prepared to answer this question and just don't tell your real weakness, just tell something that give positive impact e.g. I like reading security blogs and I feel, I am spending too much time on reading blogs, but it helps me a lot

in learning new stuff as well or in-service delivery job it is really hard to say “no”, but I am learning that art.

12. Dress professionally, behave and speak professionally.

Focus on learning and not on earning in the initial years of your **career**.

On Job Tips

1. Be clear on what is expected from you.
2. Develop a good working relationship with other teams.
3. Always asks questions to understand the business objectives.
4. LinkedIn is a good tool to check regional and global job trends and market demands in InfoSec sector.
5. Start learning the culture, policies, company values and basics, business directions and demand.
6. Always try to seek advice from industry senior professionals.
7. Read books that help you to understand enterprise cultures, leadership and gives you motivation. I.e. Tony Robbins, Jack Welch, Jeffrey J.Fox, etc.
8. Follow leaders or successful people from your industry.
9. Keep improving yourself because this is not your last destination.
10. Spend at least 2 hours on yourself learning every day.
11. Keep your motivation high and do not let any negativity surround you .
12. Learn from your mistakes and other people’s experiences.
13. Be confident but do not try to act over smart .
14. Don’t run away from criticism, face it. It will make you stronger and let you learn your weakness.

Remember, you can outsource the **responsibility** but not the a**ccountability**

Certification Roadmap

Given below is a suggested certification and skills roadmap. Most People go for CISSP in the beginning of their career which is not recommended, and it won't be helpful at all as some of the concepts and domains will be new to you and might fly right over your head. You should aim for it after spending a few years in any of the Information Security domain.

Experience	Suggested Certification/Skills	Skills	Method
Fresh Graduate/Less than a year	CCNA , CCNA Cyber Ops MCP, RHCE,MCSA	Networking , Infrastructure ,Operating Systems, Standards	Self-Study Or join an institute
Between Year 1-Year 3	MCSE ,Vendor Certifications ,CEH ,Security+ , ISO 27001 LI/LA	Advanced knowledge of OS ,Applications ,Firewalls , Log Analysis VA/PT , Security Applications/tools	Self-Study
Between Year 3 - Year 5	OSCP, CCSK/CCSP	Penetration testing, Cloud Security	Self-Study
Year 5 onwards	OSCE, CISA/CISSP/CISM ,GIAC,CHFI	Security management, advance penetration testing/incident handling/forensics.	Self-Study

Self-drive yourself and stay abreast with **latest trends**.

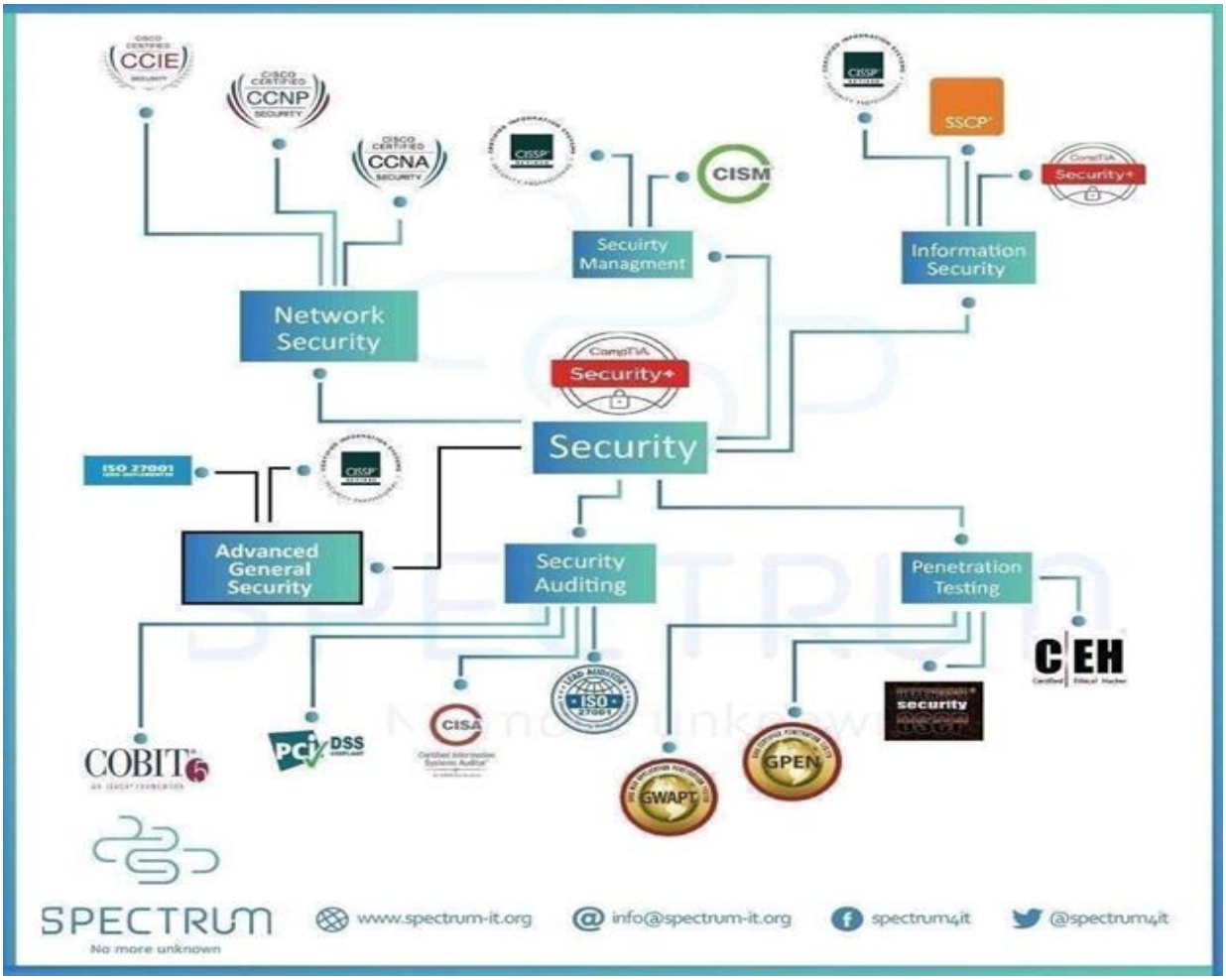


Figure 1 Certification Map

Great Achievement always requires **Great sacrifices**

Appendix A – Courses List (edx)

List of few recommended courses.

Course Name	Course Code	At
Cybersecurity: The CISO's View	UWashingtonX: CYB002x	edx
Building Your Cybersecurity Tool Kit	UWashingtonX - CYB003x	edx
Cybersecurity Fundamentals	RITx - CYBER501x	edx
Cybersecurity and Privacy in the IoT	CurtinX - IOT5x	edx
Cybersecurity Capstone	RITx - CYBER525x	edx
Cyber Security Basic : A Hands on approach	UC3Mx - INF.2x	edx
Computer Forensic	RITx - CYBER502x	edx
Cybersecurity Risk Management	RITx - CYBER503x	edx
Cybersecurity and Privacy in the IoT	CurtinX - IOT5x	edx
Web Security Fundamentals	KULeuvenX - WEBSECx	edx
CS50's AP® Computer Science Principles	HarvardX - CS50	edx
Cloud Computing Security	USMx - CC617x	edx
Enterprise Security Fundamentals	Microsoft - INF246x	Edx

Appendix B- Coursers List (Cybrary & Udemy)

Available Courses at Cybrary and Udemy are mentioned below.

Cybrary	Udemy
Intro to Infosec	Network Security Essentials
CompTIA Security	Hacking Academy: How to Monitor & Intercept Transmitted Data
CompTIA Cyber Security	Anti-Hacker Security | Step By Step Guide
CompTIA Network+	Cyber Security Course for Beginners - Level 01
Network Security	System Security Plan (SSP) for NIST 800-171 Compliance
Malware Fundamentals	
Organizational Data Security	
Enterprise Security Architecture	
Fundamental Vulnerability Management	
Security Operations	
Security engineering	
Fundamental System Security	

Appendix C – Twitter Handles List

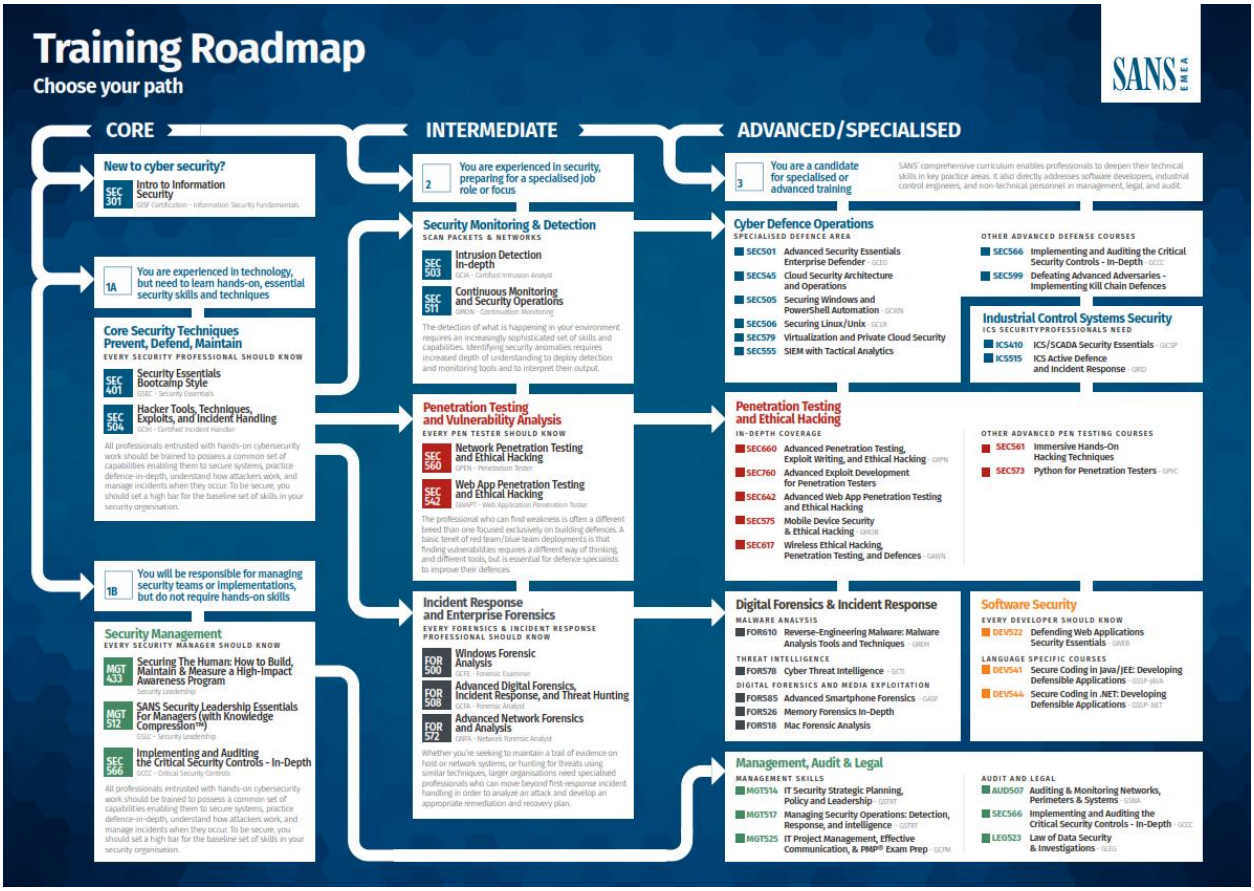
List of twitter handles.

Twitter ID	Type	Description
@Unit42_Intel	Vendor	the Palo Alto Networks (@paloaltontwks) Threat Intelligence Team
@dvk01uk	Security Alerts	My Online Security @dvk01uk Windows Insider MVP | Security Alerts | virus Alerts | Malspam alerts
@Mandiant	Vendor	Responding to the most critical cybersecurity incidents & empowering orgs to protect their assets. A @FireEye company
@qualys	Vendor	The pioneer and leading provider of #cloud #security and #compliance solutions
@SearchSecurity	Security portal	The latest cybersecurity news, tips and features from the reporters and editors of http://SearchSecurity.com. Security threats, data breaches, research and more.
@WindowsATP	Microsoft	Windows Defender Advanced Threat Protection (ATP) - Unified platform for preventive protection, post-breach detection, investigation and response
@SwiftOnSecurity	Security author	Talk systems security, industrial safety, author https://DecentSecurity.com + http://GotPhish.com, write Sci-Fi stories, sysadmin, & use Oxford comma. they/them
@bitdefender	Vendor	Award-winning cybersecurity software
@moixsec	Vendor	Moix Security is a software security company. We can hack you before bad guys do.
@Peerlyst	Security vendor	Peerlyst is the largest community of security professionals. Join us in building the largest repository of free security knowledge http://www.peerlyst.com
@InfoSecInstitute	education	provide world class security awareness and phishing simulation software in addition to IT certification training.
@PolySwarm	Threat feeds	The first decentralized threat intelligence community.
@HaveIBeenPwned	Password breach detection	Check if you have an account that has been compromised in a data breach. Created and maintained by @troyhunt
@BrianKrebs	Security influencer	Independent investigative journalist. Writes about cybercrime. Author of 'Spam Nation', a NYT bestseller
@cyberdefensemag	Cyber defense magazine	Cyber Defense Magazine - The Premier Source for IT Security and Compliance Information
@INTERPOL_Cyber	Cyber police	INTERPOL equips police with tools and expertise necessary to tackle cybercrime. Tweets do not indicate INTERPOL involvement in cases.
@WDSecurity	Vendor	Security information, news, intelligence, and next-gen security technologies from Microsoft
@securityblvd	Security Blogger	Home of the Security Bloggers Network. Latest Cybersecurity news, articles, interviews & analysis.
@2600	Magazine	The Hacker Quarterly

@ppentestlabs	Security labs	**Practical Pentest Labs**, For every #infosec enthusiast interested in learning the art of vulnerabilities discovery, exploitation & #hacking. | We teach valuable skills not just ideas.
@threatintel	Vendor	Symantec Security Response brings you the latest threat intelligence from the IT security world
@FireEye	Vendor	FireEye offers a single platform that blends innovative security technologies, nation-state grade #threatintel, and world-renowned @Mandiant consulting
@CheckPointSW	Vendor	**Check Point Software** Our on-going vision is making Internet communications and critical data secure, reliable and available everywhere. #Cybersecurity
@FSecure	Vendor	One Step Ahead of the Criminal Mind -- Need help? http://bit.ly/FSHelp
@InfosecurityMag	Magazine	The only magazine dedicated to the strategy and technology of information security, delivering critical business and technical information for IT professionals.
@eweeknews	News Portal	Enterprise tech news, reviews, and analysis since 1984.
@SecurityWeek	News Portal	Internet and Enterprise Security News, Threats, Insights and Expert Analysis #SCADA #infosec Coverage
@threatpost	Security News	Threatpost is the first stop for fast-breaking security news, conversations and analysis from around the world.
@thehackersnews	Security News	Most trusted, widely acknowledged news source for cybersecurity researchers, hackers, technologists, enthusiasts and nerds.
@kaspersky	Vendor	Kaspersky Lab is the world's largest privately held vendor of Internet security solutions for businesses and consumers. For help and support, tweet @kl_support
@SCMagazine	Magazine	The official Twitter feed for all things IT security. Like us on http://facebook.com/SCMag scmagazine.com
@hackread	Security News	Bringing the best hacking, infoSec, surveillance and tech news from the web.
@ITwire	Security and Tech News	iTWire is a powerful source of top-line IT and tech news, information and community for IT and telecommunications industry professionals
@CSOonline	Security Portal	CSO provides news, analysis and research on security and risk management.
@securityweekly	Security Influencer	Founder & CEO of Security Weekly & @stogiegeeks, @OffensiveCM CEO, hacker, and podcaster.

Appendix D - Training Roadmap

Here is a suggested training roadmap.



Extra Reading

Below links can be used for further reading and understanding.

1. https://expel.io/blog/a-beginners-guide-to-getting-started-in-cybersecurity/
2. https://doublepulsar.com/8-things-to-know-before-getting-into-cyber-security-ab9010a4ff1c
3. https://www.cybary.it/
4. https://www.udemy.com/
5. https://www.schneier.com
6. https://www.urduitacademy.com/courses/detail/(ISC)2
7. http://krebsonsecurity.com
8. http://www.darkreading.com
9. https://threatpost.com
10. https://www.offensive-security.com/blog
11. https://nakedsecurity.sophos.com
12. http://www.securityweek.com
13. http://www.securityfocus.com
14. http://taosecurity.blogspot.com
15. http://securityweekly.com
16. http://blog.uncommonsensesecurity.com
17. http://www.securitybloggersnetwork.com
18. https://www.lynda.com/
19. https://www.freecodecamp.org/
20. https://linuxacademy.com/
21. https://cloudacademy.com/
22. https://www.pluralsight.com/learn