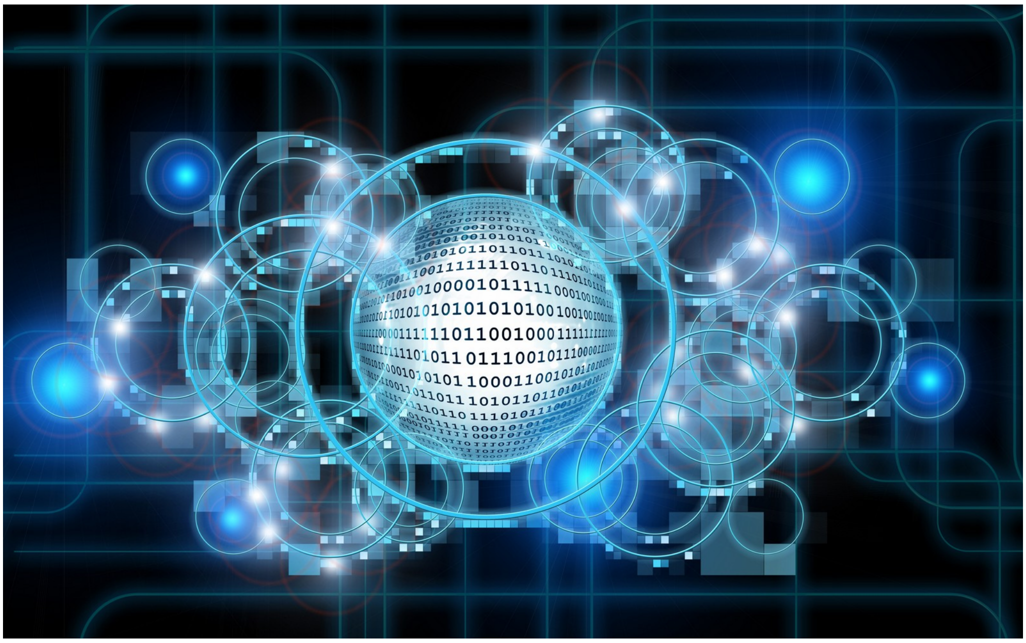
#InfoSec N00bs

How to Deal With Being New to the Scene

These Wide Open Spaces
What to do in #InfoSec
.page 3

What Now?
Should you get a degree?
Certifications? Just...start applying?
.page 7

Contents



Who am I, You, and Where Are We?

Who are we, how did we get here...and where the heck is here anyways?

Who am I?

Well, I'm a noob when it comes to InfoSec. I'm not exactly what one usually considers to be a newbie, though...while I am just getting my start in the field, I've been around for quite a while. When I first went to college, back in 1995, there wasn't an option for computer or information security as a degree-track, and it wasn't something taken seriously either, though it did fascinate me.

As a side-note, I tend to go with "Information Security" rather than "Cybersecurity" because at that time, using the term "Cyber" for anything other than "Cyberpunk" when talking about a specific tabletop RPG was, well, a great way to get laughed at. I don't actually feel that way myself: my concentration is specifically in Cybersecurity. But it still colors some of my word choice.

So I ended up not finishing college back in '95, got married, had a kid, moved around a few places, and ended up working in the hotel industry. I managed hotels and was the "unofficial IT guy" pretty much everywhere that I went, including setting up basic security precautions.

Long story short, I went back to school a couple of years ago to finish up, and ended up at the American Public University System (System because they are technically two schools, American Public University and American Military University) majoring in Information Systems Security, with a concentration in Cybersecurity. It has been a great ride, and my professors have had loads of real-world experience that they have drawn on to give some context to the regular lessons. I mean, my Cyber Warfare instructor was previously in charge of PsyOps (now called MISO) for the Army! That was an awesome class. I should be graduating here in a few months, and then I will be looking for a start in the field.

Who are You?

Well, I imagine that you are in a similar boat to me if you are reading this. You are likely new to, or trying to break into, Information Security as a career, or at least evaluating it. You may have taken the degree route like I did, and have finished or are currently still pursuing your degree. You may have taken the other common path, and gone after certifications, or are thinking about going after them. Others still might have no idea what to do, but know that they want to be here. In any case, welcome! From what I can tell, every path here is valid, there is no single "right way" to get here, and while location may make certain methods easier, you can pretty much just end up falling into InfoSec.

The other option here is that you are experienced and reading this to see where you can help out. Feel free! WE ARE WINGING THIS AND WOULD LOVE YOUR FEEDBACK!

Where Are We?!?

Well, welcome to the wide world of #InfoSec, Cybersecurity, Information Security, or "those paranoid IT guys who think the Russians and the Chinese want to steal our credit card numbers." Well, spoiler alert: They do, along with a lot of other stuff, but that's beside the point. "Here" covers an awful lot of ground. It's all connected, and you should have an idea of what's out there, but nobody expects you to know, or even like, everything about this field. It's too big to know it all, and too diverse for everyone to enjoy all of it all of the time. Take a look around, see what you like and look into that more. See what you don't like as much, and learn enough about it to recognize it and flag it for someone who gets their jollies that way. Chances are, you'll be able to find a position or job doing (mostly) the parts that you like most. It may take some time to get there, but it IS possible!

These Wide Open Spaces

There is something that most people who come into this field just don't expect, because it is very different from most career fields: This is NOT a single field, we're a bunch of related stuff lumped together because it's all "security related." Sure, Red/ Blue/Purple team stuff is related, if very different...but OSINT, DFIR, SOC, Analyst...all of these things are extremely different, and while some skillsets may overlap, they have very different priorities. Just because you don't want to be a "hacker" does not mean that you aren't wanted or needed in InfoSec...just maybe don't apply for Red Team stuff right off of the bat, unless you get interested in it later on.

So...what kind of areas might we look at? What's happening all around InfoSec? Below I'll list a few, but just remember: this is by no means an exhaustive list!

Security Analyst
This is not generally an entry-level position, though depending on how the job requirements are written, it might be. (We get a lot of that around here) An analyst is generally going to be someone who checks to see if there has been an incident, checks logs, looks at firewall rules/logs, and actually digs into policies, often writing at least outlines for what those policies should be. Security Analyst (or similar) is generally seen as a pretty broad, and therefore often senior, position.

Security Engineer
Like Security Analyst, the Security Engineer is not generally the new kid on the block. (Though that being said, there was a bank hiring for an "entry level" Security Engineer in the next town over. No degree requirement, but needed several certifications as well as several years of experience...for an "entry level" position.) These people really look at the nuts and bolts of securing a network and the applications that people use. For this job, you're going to need to know your hardware and software, and you'll be working in multiple different operating systems. Likely the network runs off of Linux, but there will still be (in most larger companies) plenty of Windows Server installs for that Active Directory goodness, só you have to know a little bit about everything.

SOC Analyst
So a SOC (Systems Operations Center) Analyst mght be someone completely new to InfoSec, or the most grizzled veteran

that works for the company. A good SOC team wants both. These people are tasked with knowing what is going on and responding when there is an issue. In order to do that effectively, a group really needs to have a diverse set of skills and knowledge. Knowing how to research is critical to the team, knowing how to effectively communicate, and not only with other people with technical knowledge, is highly prized, as are security engineers, coders, red teamers, blue teamers, managers, and pretty much anyone eles. From what I can tell, most people who want to set up an effective SOC are interested in results, and not in "business as usual." They want a group that can work well together, yes, but who can see outside of the box, and work with everyone else to make sure that the work gets done quickly, efficiently, and that lessons learned are applied to make future incidents less likely to occur.

DFIR (Digital Forensics Incident Response)
This is one of those "on the pointy end" positions. These are the people who respond to incidents that have occurred, investigate them, often interact with corporate investigators and law enforcement, make sure that things like chain of custody is enforced, testify in trials, and oh by the way make sure that the way that the incident occurs is something that doesn't happen again by working with other jobs on this list to better craft policies, procedures, and technological solutions.

OSINT (Open Source Intelligence)
Simply put, OSINT collects data from publicly available sources. Said that simply, it sounds...simple. For the people who do it all of the time, it likely becomes somewhat simple for mundane questions that they see every day, sure. To get the most basic idea of what this kind of thing can involve, go to https://osintframework.com and take a look at all of the tools that it displays. Now realize that each of those tools is a menu to more tools, which in some cases have sub-menus of their own. OSINT is not a trivial exercise, and it can take some time to get really good at it, but if you like "detective work" and solving mysteries, this might be a great path for you!

Penetration Testing
You wondered where "actual hacking" would be on the list, right? Everyone does, and here it is! There are ALL SORTS of ways in which you can make a career out of penetration testing. You might be on a red team for a company that is actually paid to attempt to compromise systems and write up vulnerability assessments. You might be a physical penetration tester that actually breaks into businesses and sees what information that they can find, or if they can physically in some way compromise their systems. Still others might work independently or for companies on bug bounty programs and the like.

Risk Analysis
If you have gone through college classes in information security, risk assessment has likely been a big part of what you have looked at. The people who work in this area have to know, or at least be familiar with, all sorts of areas of information security. The reason is, they work with (ideally) people at all levels of the company, and figure out what risks are present, how likely that risk is to become a threat, and how serious that threat would be if it became exploited. Risk management is not exactly a straightforward field, all of the time. Sometimes, sure, "You have an unsecured database online that contains customer personal and financial data!" is a fairly straightforward problem that every company is going to want to jump right on. The risk there is massive in terms of both money and reputation. On the other hand, "There is a database that, if accessed, gives part numbers as well as customer ID numbers (but not actual customer information) and how many of the parts that they have bought, and when their last purchase of that part was, but it is on the internal network and requires a password to log in. The database, however is slightly misconfigured, and will require an expensive rework to fix the issue." The executive you just made that report to just literally heard, "Meh" and "expensive" só while the risk is present, it would not likely be judged as important. This is why Risk Analysts tend to put things into frameworks and numbers, só that non-technical people still get an idea of how serious what they are saying is...or how not serious it is. Some risks, while extremely likely, simply don't have much in the way of business impact, and só they're left alone unless extremely cheap and easy to fix.

Compliance
This is the group that everyone loves to hate. Compliance people work to make sure that their business is following all of the laws, regulations, and standards to which their business is held to, and where possible those that they might end up being held to. Compliance, you will often hear, is not security, and in a way this is true. Compliance should really be the bare minimum of what a business does. However, if a company does not even meet the bare minimum, how secure are they really, anyway?

Frameworks
Frameworks groups are a lot like Compliance in some ways, and they do frequently work together. The people who work on implementing frameworks, such as the COBIT framework from ISACA, or any one of dozens of others, actually end up working with every part of the security department and beyond. They make sure that there are policies and procedures written down and accessible for everything from creating user names, passwords, and credentials to how long you have to keep archives of your text conversations on Slack with other co-workers. (Yes, that's a thing. A lot of times you won't realize it, because the framework guys just have that information captured and archived with no notification beyond the "terms and conditions" you agree to when you create your account initially.)

Security Architect
These are the people who build the systems and maintain them. The Architects are likely to have some pretty extreme levels of hardware knowledge, as well as knowledge of systems such as firewalls, IDS/IPS, VPNs, and many, many others. They have to choose (and usually implement) all of the hardware and software to make the system work together in a manner that is usable for the business, while still being secure enough that the business is not vulnerable. This can be a fine line to walk, especially with an ever-changing threat landscape. I always imagine that these are the people that, instead of a bottle of scotch hidden in their desk drawer, they have a case of Pepto Bismol hidden somewhere in their office.

Investigations/Forensics
Having already talked about DFIR and SOC roles, you might think that this has already been covered. In a lot of organizations that is true, though in others there are specialists that just handle the investigation and forensics parts. This is especially true in law enforcement, as the Detectives that handle computer crime aren't really part of a corporate SOC team, or handling incident response for them either. This is where you get into some of the more hardcore computer forensics and data trails out there. The mantra here is pretty much: chain of evidence, if the hash doesn't match we're screwed, and if it isn't written down and explainable to a jury then it might as well have not happened.

Threat Intelligence
Threat Intelligence is kind of like being the cybersecurity-CIA for your company. If you work for the government doing this, then you likely do work for the CIA or NSA...though at this point most branches have something in this regard. This is often not as exciting as that makes it sound like. Threat intelligence is often looking at trends, reading articles, and drawing conclusions about where threats are coming from, and what might likely be aimed at you in the future, and how to mitigate that possibility.

Auditor
Very few people have ever seen the term "auditor" and gotten excited. Having done this for hotels for years, I can tell you that...yeah, that's pretty accurate. Sometimes it can be a lot of fun, but usually only when we were solving a mystery such as "What the heck to Johnny on the front desk DO to make this be só screwed up?" Information security audits, however, are a LOT more in-depth than something like what I would do on a medium to small sized hotel's books on a nightly basis. Any business with the need for an information security staff is going to have a lot of information that needs to be audited. Every computer, for instance, is going to have an audit log, be it Windows or Linux. Those likely get copied to a remote log server. Every database is going to have an audit log. Every. Single. One. They typically log, oh, everything. The auditor's job is to set up all of these audits só that all of the information that they need is available to them, then to find out what they didn't set up and go set that up for the next round, then to look at all of the information and see if any policies or procedures need to be changed, access limits and the like, as well as seeing if there are any red flags indicating a data breach of some sort. And this (should be) done over and over again, in waves. I think it would be fun to be on an audit team for an audit cycle. I do not, personally, want to do it all of the time.

Security Manager
Well, we have looked at security staff, só obviously there would have to be someone to manage those staff, right? There are all sorts of different security managers. Some of them are the heads of individual teams. Some might be the person that multiple teams or managers report to. Some might manage several different sorts of teams, and handle an "area of responsibility." This might also effectively refer to the CTO or CISO in a smaller company. So the range on what a security manager does (and is thus paid) is pretty wide. If you like information security, but also like to manage teams and projects, this can be a great career path to shoot for.

Remember: This is was NOT an exhaustive list, but just a brief (ha!) look at SOME of the options available in InfoSec!

What Now?

Should you get a degree? Certifications? Just...start applying?

Just like virtually everything else, this will largely depend on what you have already done, what you want to do, and your personal preferences. Not very helpful, on the surface, is it? But, we can break it down at least a little bit more than that.

Already at work on your degree? Finish it. It certainly is never going to *hurt* you to have a degree, especially in a technical field. If nothing else, the gatekeepers at Human Resources like to see them.

Already have some certifications? Good! Again, a certification is never going to *hurt* your chances of getting a specific position. It may not particularly help, but also showing diversity in training and mindset can be a real bonus for some recruiters.

“Do I have to know how to program/code?” Alternately: “I know how to code, will that help me?” For most InfoSec positions, coding is not 100% necessary. On the other hand, knowing how is only going to help you. A lot of what gets done can be done more easily if it is automated, and knowing at least the basics of things like Python will go a long way in understanding that process.

“I just know I want to do X and don’t know where to go to get there.” This is something that I hear about all of the time on forums and groups. Someone wants to do a certain thing, but they don’t know how to get to that point. So, figure out what X is. If you already have a degree, you probably don’t need a new one. If you are in the middle of a degree path, see if you can pivot to something that is more representative of what you eventually want: sometimes that just isn’t feasible, but sometimes it surprisingly is. The big thing is to start learning the right skills. This can mean picking up “certs” (certifications) but not just any of them. If, for instance, you want to work in DFIR, picking up your CEH (Certified Ethical Hacker) or OSCP (Offensive Security Certified Professional) certs right off of the bat is, honestly, probably not going to help you too much in that direction, or at least not more than any “hey I have a certification” line on a resume. Certifications in Incident Response, Forensics, and even Project Management would look pretty good, though. On the other hand, if you want to do penetration testing, CEH and OSCP are definitely the way to go, along with working on Capture the Flag exercises and the like.

Basically, figure out what is relevant to what you want to do and go for those specific things. Specifics are always going to be of more help than generalities.

Still, there are some "general" types of things that you may want to look at that apply broadly. The CompTIA certification track provides a good learning framework and track, especially if you aren't yet up to speed on certain parts of the InfoSec world. The A+ certification teaches you about basic computer hardware, and is often looked at as the "first" cert to get, though if you already know this information you can probably skip it...unless you intend to work heavily with hardware. After that, I see Network+ recommended a lot. I can certainly see this,and plan to pick this one up myself. Just think of how much in InfoSec is about investigating and tracking things that happen over a network...if you don't know this material backwards and forwards, then this is probably a certification that you need to get. Even if you do, having this certification might not hurt, especially at the beginning of your career. Security+ is the first "real InfoSec" certification on here, and should pretty much be a basic for anyone going into the field at this point. There are a lot of "Is it worth it?" threads about this specific cert going around, and as someone who used to hire people let me just say: unless HR thinks that it is worthless, then it is worthwhile. Also, it does show a broad understanding of many different areas of InfoSec.

From that point, you can specialize or take more general-purpose certifications that might be useful to you. Work primarily on Linux machines and servers? Linux+ or LPIC might be good for you. Cloud-based certifications might be good. Plan on working as an architect eventually? Start reading up on things that nobody else does in InfoSec, like setting up and maintaining an Asterisk PBX system.

In the end, *nothing* that you learn about computers or networks is worthless. All of it relates to security in some way. Just figure out a way to pitch that knowledge to the people doing the hiring. This is where a resume writer or advisor might come in handy.

There is so much to do, and so much possibility, that it is really easy to get overwhelmed at this stage. Don't! Nothing here is really a waste of time, and as long as you have a vague idea of what you want to start looking at doing, and move generally in that direction, then you are making progress! Even if that focus changes as you become interested in new or other things, or find out that things in which you thought that you would be interested in really just aren't as fun as you thought. For me, this was computer forensics. I always thought that would be a lot of fun, and in some ways I still think so! The drudgery of it, however, just doesn't "do it" for me. Oddly, I *do* like forensics, but I like working with things like routers and firewalls, network forensics, rather than extracting hard drives from computers and imaging them. A lot of it is the same, but, well, I like what I like. So this has me looking at possibly doing something other than DFIR, though that was my first thought as to what I would like to do in InfoSec. It is perfectly OK (and normal!) to change your mind about what you want to do here, several times if you need to.

Social Media and Networking

Where to look for people to follow...

So…here we are. How do we meet new people? How do we find out about new opportunities, and news about what we're into? Well, just like so much of what we turn to in our private lives, Social Media is going to be key in InfoSec too. There are the obvious places such as Twitter (which, by the way, I barely used at all until recently...#InfoSec Twitter is a great community and you owe it to yourself to check them out!) and Facebook, as well as some places that many people have never heard of, such as Mastodon instances. I am not going to recommend specific people to follow, unless they are also a "brand" that provides training or resources. There are lots of people who are great to follow, and I don't have enough room to list all of them. An interesting side effect of the entire Covid-19 pandemic is that many InfoSec conferences have gone to an online format this year...which has led to several free “attendance” small virtual cons popping up all over the place. These are great resources to meet people as well!

Facebook (https://www.facebook.com)
I’m going to get this one out of the way. I don’t like Facebook. I don’t know if it’s the way in which it mangles my timeline so that things are completely out of order, the way it hides things that I want to see while promoting things that I am completely uninterested in, or if its the fact that I kind of think of Zuckerberg as an arrogant prick that basically stole the idea for Facebook from other people who were paying him to develop a site for them. All of that being said, though, Facebook is a great resource and it should not be neglected. For subject-specific content, Facebook Groups in particular can have a lot to offer. On the other hand, I have recently left a couple of groups who’s content was essentially new people coming on saying “My life dream is to be the Hacker Man, how do you teach me to do it?” This was simply not helpful, so I left those groups. What I am saying is: Facebook is noisy. Mute and remove the noise from your timeline, and eventually it will narrow to the point where you are seeing useful information.

LinkedIn (https://www.linkedin.com)
LinkedIn is a great professional resource. It is not, however, “exciting” like many other platforms. On the other hand, it does let you search jobs and apply directly, and allow you to maintain your resume available to recruiters. This can be a great community for finding out about trends and getting real-world advice for jobs and job hunting.

Peerlyst (https://www.peerlyst.com)
Peerlyst is technically a social media community, but really it’s a news hub. Its a great way to see what is going on in the industry, and to get (often unfiltered) takes on what is happening or needs to change straight from industry experts. I am still exploring here, but it is definitely one of my go-to resources for news.

Twitter (https://www.twitter.com)
Well, Twitter is something that I never used much before now. I created an entirely separate username to keep my information security searches and the like off of my “main” profile...and that information security profile has, with the exception of a few authors that I follow on my “old” profile, become my main one. People on #InfoSec Twitter do not just post about “InfoSec Stuff” 24/7. They talk about...everything, just like Twitter is supposed to be. (By the way, if you think that going onto someone’s feed an complaining that you followed for InfoSec content and you’re sick of seeing their cats is OK, then you are wrong, you are not OK, and you should mute yourself and stick to searching hashtags. This has been an issue lately, especially for the ladies and non-binary among us.) To get started, really just search for “InfoSec” and then pick someone who seems neat, read their timeline a little to make sure, and then start following people that they follow and people who respond in their threads, and do the same with those people. Your following will not “blow up” overnight, but within a few days you will likely be able to post something without it just being you speaking into the void, and at least someone will respond. A couple of people with good basic material for InfoSec on Twitter (generally in exchange for your email) is going to be @0xBanana and @shehackspurple. Both provide short or one-page info sheets with useful information and/or projects. Pay especial attention to the Raspberry Pi stuff from 0xBanana! It’s a great foundation, especially if you aren’t familiar with Linux yet, and it’s cheap to get started.

Mastodon (many URLs)
Mastodon is a lot like Twitter: it is a microblogging platform with character limits. The difference is that Mastodon is a linked (federated) group of servers run, generally by individuals, that can work across those servers boundaries to share stories and mutual interests. So while you can join up on the InfoSec Exchange instance (https://infosec.exchange) there is nothing stopping you from talking to and following someone on an entirely different server. Because these servers are run by individuals or small groups instead of large corporations, there are wide ranges of what is “acceptable behavior” on different servers, which is often enforce erratically, and gives the entire project something of a “Wild West” feel. This is where you are going to find the people who are hugely into open-source software, as well as the ones that are hugely paranoid about their data being stolen/collected/used by Facebook/Twitter/Google/etc. It is a great place to pick up some information, but it can be hard to get started. Just pick an instance, follow some people, and eventually you can curate this into a valid source of news and social interaction. It is going to take a little more time than the more “mainstream” options, however.

These are most of the resources that I use on a daily basis. There are tons more. Feel free to hit me up on Twitter at @Bpetty_InfoSec to give me any additional suggestions!

How to Deal With Being New to the Scene

You're new, I'm new, Everyone has been new.

I hate to say it, but every field has its assholes. InfoSec is no exception to this. That being said, overall it has been one of the most welcoming and diverse communities that I have encountered in my working life...which has now been more than half of my life.

One thing to realize: many of us in this scene are not what you might consider "typical." Many of us are neuro-divergent in some fashion. Many suffer from some form of mental illness. Many are disabled in some way. I have met many non-binary and transgender people. In short: if you are a bigot, we likely don't want you around, but otherwise you are going to be welcomed! The field has an energy where most of the established people are thrilled by the idea that they might learn something new from a new person, or might get a different perspective on something that they have known about for years from someone seeing it with fresh eyes.

Is it perfect out there, and full of sunshine and rainbows? No, not even hardly. But it is full of magical pokemon people and highly-caffeinated geese from which you can learn a lot. It is full of digital fruit and badasses that are not going to judge you for being somewhat different from society's "norms." Here, you can be, and are encouraged to be, yourself. Look around. Soak up the culture. Kick back, relax, and just start learning.

At the end of the day, that is how you deal with being new here: every day is new, and brings new things and new people. Never STOP being new, because then you stop learning, and if there is one thing that we know as an absolute in InfoSec: learning never stops because the competition will never stop innovating.

Really, what you should ask yourself isn't so much, "How do I deal with being new here?" but rather "How do I make sure that I keep this energy and drive to learn going forward?" You need it. We all need it. Don't lose it, and share it with us all.

Credits

This is something that I just threw together over a day or so while attempting to get my mind back on track while on heavy medication during the Corona virus seclusion times. Fortunately just some really bad pre-existing bronchitis for me, but given those symptoms plus the cold, it was a little scary for us all. So...forgive any rambling or typos!

All pictures and images are from Pixabay (https://pixabay.com) and are free for commercial use, with no attribution required.

Brian Petty

bwpetty@protonmail.com

@BPetty_InfoSec