# THE **INFOSEC** SURVIVAL GUIDE

## SECOND VOLUME

# Table of Contents

## Brought to you by:

**BLACK HILLS** | Information Security

# CREDITS

## Made by and for the community!

*and our team at BHIS*

## Writers

Dan Rearden ------ @Haircutfish
Martin Pearson ------ @chinno53
Ayub Yusuf ------ @whitecyberduck
Ashley Knowles
Erik Goldoff ------ @ErikG
Edna Jonsson ------ @ednas
Wade Wells ------ @WadingThruLogs
Ray Van Hoose ------ @_meta.
Max Boehner
Catherine J. Ullman ------ @investigatorchic
Blake Regan ------ @zer0cooL
Brian "BB" King ------ @BBhacKing
Melisa Wachs
Dieter Smith ------ @smithereens
Alex Minster ------ @Belouve
Amanda Berlin
Matt Thomas ------ @slegna
Serena DiPenti ------ @shenetworks

## Technical Editors

Serena DiPenti
*Unknown Security Analyst, Definitely Not Shenetworks*

Ashley Knowles
*Lead Security Analyst & Junior Cheese Connoisseur*

BB King
*Very Tall Security Analyst & Antisyphon Instructor*

Kaitlyn Wimberley
*Very Short Security Analyst*

Ben Burkhart
*Gas Station Snack Enthusiast*

Troy Wojewoda
*Purveyor of Digital Truths & Antisyphon Instructor*

## PROMPT# Crew

John Strand ------ Managing Intern & Publisher
Deb Wigley ------ Slightly Above Average Height Hat Rack & Copy Editor
Jason Blanchard ------ Liver Manufacturer & Excitement Co-Creator

*he was out the whole summer, showed up at the end and aced the test*

Kassie Kimball ------ Editor
Caitlin Cash ------ Curator & Creative Director
Shelby Perry ------ Production Coordinator
Megan Lucia ------ Cat Herder

## Look for all of us at cons and meetups!

## How and Why This Book Was Made

The First Edition of the Infosec Survival Guide looked a lot different. It explained who BHIS is and how the team can help with a wide variety of services. For this version, we wanted to create something that looked and felt more like a "survival guide" - something that would include EVERYTHING and help guide everyone - at any level - to more knowledge.

It all started with a spreadsheet, gathering a list of ideas of what that would look like. It looked like a lot. It looked like a whole damn textbook. A big idea for a very small team. Too big. So we scaled it down, making this the same size project as our PROMPT# zines, but with a twist: we asked you for help.

We reached out to our community leaders on Discord and asked for people to claim the topics included in this guide. We gave them a style guide, a bit of a prompt, and we were blown away with the responses. Then we had our BHIS team take a look and do "tech checks" to approve the technical information. We had a real victory moment when one of the comments from the team was "there's some resources in here I didn't even know about" - this is exactly why we want to make this guide.

The dream is for this to keep growing and cover all the topics, all the tools and tips and tricks and advice that the community has to offer. A one-stop-shop for all things infosec, beginner to advanced, but in a quick, condensed form. Just enough to help you understand what things are, and get you running in the right direction to more specialized sources.

Because we hope it will grow in scale, we made it look a bit different from our typical zines. By "different," we mean standardized throughout and less illustrative. There was concern that would be a bit less fun. We took inspiration from a book about magical creatures. It looked like a serious textbook, but it had little notes throughout that made us laugh. So instead of pictures and bright colors everywhere, we brought notes into this guide to keep the typical fun BHIS vibes in a more easily scale-able way.

This book is missing many topics that are important and vital to many in this community. We see you, we hear you, and we want your help to include your specialty in the next one. For now, we hope you find some nugget in this version that helps.

Thank you for all your help. Thank you for allowing us to build cool stuff like this. We couldn't do this without you.

**PROMPT#**

# CHOOSE WISELY

### Knowledge is power...

The world of information security is all about controlling access to information. The smallest things can have the biggest consequences... like your kid's name and that text you just sent saying you'll be late to pick them up from school. As you dive into the world of infosec, you'll learn all the tools, techniques, and tricks that both sides use to control and secure information. It will be solely up to you what you choose to do with those skills and the information you'll access.

### ...and with great power comes great responsibility.

We can't make you choose any specific route, but we can explain why we choose the white hats. Firstly, we don't like prison. It's not a fun place, and they don't let you leave. But more importantly, we love helping others, even if it doesn't make us rich. We proudly suck at capitalism, and just want to make the world a better place. We hope you do, too.
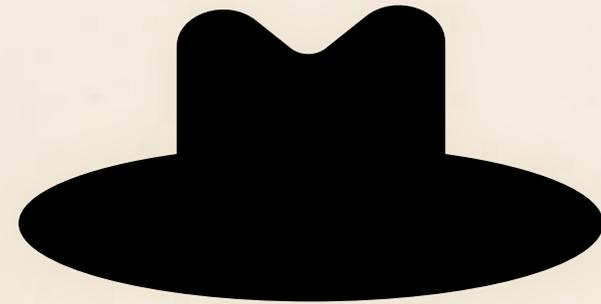
# CHOOSE WISELY

# ·▪ 5 PHASE PLAN ▪·

## For Breaking Into InfoSec

*Check out the full video of John Strand talking about his plan here:*
blackhillsinfosec.com/webcast-john-strands-5-year-plan-into-infosec-part-2/

## Phase 1

Learn your core operating systems. Build a lab. Get started with a language. Learn basic security fundamentals.

Start your education with the soft skills. Understand the technology: how are these machines used in business? What are people doing with them? You can be as technical as anyone, but if you don't understand the application of what you're trying to do and if you can't SPEAK THE BUSINESS SPEAK, you won't get far.

### Windows

Go to the Windows Evaluation Center. Install software from Microsoft. This is going to be painful. Some things are easy to install, like Active Directory. Some things are very, very difficult to install, like SCCM or Configuration Management. But these are important lessons for you to learn. Set up the things that you will be constantly defending (or constantly attacking) as a security professional.

Can I help you with that?
*nobody asked you*
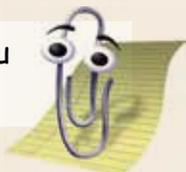
### Linux

Install everything... from scratch. Don't know how? Visit a search engine. Type your question. Click the button. Don't give up just because it's hard. Security isn't about taking the easy route – it's about constantly learning, even under exceptionally difficult circumstances. The only way to get good is by struggling. If you need to, remove your easy way out and uninstall Windows.

Also, learn Bash scripting (there are other shells, but Bash is the one you're gonna end up using more than not).

### Networking

Set up a network lab. First, get your stuff at home up-and-running and make sure you KNOW what it is doing. Then, get some simulators (*brianlinkletter.com/open-source-network-simulators/*). Get some gear. You can buy old equipment for cheap on eBay. Take it apart. Find out how it works. Buy two or three of things... you're gonna end up breaking a few.

### Coding

Learn to code. Python is the best place to start (though other languages are important to learn). Study online. Code Academy, Code Warrior, and Pluralsight are all great resources, among many others.

### Security Standards

Learn the 18 CIS Critical Security Controls. The AuditScripts Critical Security Controls Master Mapping spreadsheet (*auditscripts.com/free-resources/critical-security-controls/*) is an incredibly valuable resource. It can help you learn not only one framework, but directly apply that to a variety of other frameworks through its intensive cross-referencing. Knowing these is a big plus in your resume. It's strategic and high-level. Learn it.

## Phase 2

Time to start projects! (You may have already... that's fine!)
Move from being a consumer, to a creator
You should:
Start a security group (working on a team is an important experience)
 - At work
 - At school
Learn PowerShell (...this will take a while)
Keep up-to-date on security news
Eliminate distractions that hold you back

## Phase 3

This is the time of web apps – you'll have to know these
Start with PHP and ASP.NET (don't get distracted by anything else yet)
Feel free to branch out to networked iOS and Android Apps
Learn to code (badly)
Develop SOMETHING

**Dare** to suck at something. *Embrace the suck.* **It's okay.**
*failure is always an option*

## Phase 4

Time to start hacking stuff!
Learn IDA and Immunity Debugger
Pick a protocol and understand it
Hit online challenges
*(You've already been playing with Metasploit this whole time, right?)*
Download ZAP from OWASP
Use and learn ALL this:
Windows ATT&CK® for Enterprise Matrix
SANS Ultimate Pentest Poster

## Phase 5

PRESENT!
Give talks everywhere and anywhere
Present on things you JUST learned!
Take advantage of cons/events/webcasts as a speaker and...
PUT. YOURSELF. OUT THERE.

*be humble, but know your worth*

## In Closing...

**Feel free to:**
 Indulge in distractions
 Stick to this plan
 Ignore this plan
 Develop your own plan
 Get good at just one thing
 Get a degree
 Don't get a degree
 Get certifications
 Don't get certified

**Do NOT do the following:**
 Sink into video games
 Waste your time solving a Rubik's Cube
 Binge watch shows on Netflix
 Use Bing for anything
 Just barely learn Metasploit to impress people
 Spend more time on the hacker "look" than learning
 Get angry
 Blame others

*tony knows what he did.*

# ·■ QUALITY TRAINING ■·
## Where to Find and What to Avoid

*written by Dan Rearden || @Haircutfish || haircutfish.com*

*In our busy day-to-day lives, it can be hard to find the time to sit down and get some training done. What makes this even more difficult is the slew of so-called "trainings" out there whose only purpose is to take your money and waste your time.*

## What to Look For

*speak for yourself*

Everyone is different, and none of us are robots (at least not yet, haha). So when it comes to your learning, you want something that resonates with you. Meaning you want training that is:

- **Understandable -** well-written training should be easy to follow without holding your hand completely.
- **Accurate and reliable -** applicable to both the materials and the teacher. Not all trainings need a teacher though.
- **Affordable -** You shouldn't have to put a second mortgage on your house to learn.
- **Inspiring -** Great trainings should inspire your drive/passion to want to learn more.

> ■
> ## "Learning from a truly great teacher is discovery—not studying."
> — *- Unknown*

*preachy but accurate*

## Good Trainings

*The following are trainings that can help you to better gain the knowledge to not only break into the industry, but brush up on skills you may be rusty on. These trainings follow the bullet points mentioned above.*

### Antisyphon Training:
The courses' audience ranges from just starting out, to industry veterans looking for a knowledge boost on a swath of topics. Antisyphon offers not only live courses but on-demand training as well. They even offer a Pay-What-You-Can model for select courses, making them affordable and accessible to all.

### TCM Security:
TCM security has courses that range from beginner to advanced, with topics like Linux 101, Practical Ethical Hacking, and the GRC Analyst Master Class. TCM also offers different discounts throughout the year.

### TryHackMe & HTB Academy:
These both offer a gamified solution to help you learn cybersecurity. Using a practical approach, they emphasize on learning by doing. Each platform offers a plethora of rooms ranging from beginner to expert difficulty. Both offer free and paid options. If hands-on training is up your alley, this is a good way to go.

## Ways To Spot A Bad Training

*On the flip side of having great trainings available is the ones out there that are... not so great.*

*Here's a few things to check for:*

### Bootcamp in the name
These usually promise fast and amazing results, often popping up out of nowhere and providing little information on the people teaching it. While there are some good bootcamps out there, a lot of these trainings prey on people's desires to get what looks like quality training for a "cheap" price. Verify credentials to try to avoid scams.

### Reviews
Look for courses with verified reviews to see what they are like and what they truly offer. Look for indications that the course is up-to-date and provides meaningful and accurate information. If no review is found, ask the community to see if anyone has heard of it and what their opinion is.

### Word of mouth
Ask the community; there may be someone out there with knowledge and experience to help you. Find out from others what courses they have taken and what they recommend. Bad training has little-to-no good word of mouth.

### Big promises too good to be true?
This is when you really need to look at the two previous bullet points. Trusted reviews and word of mouth can go a long way in discovering if a training is offering more than it can deliver on, i.e. "Make six figures in 90 days! Earn 500k per year with no experience!" It may also help to look into why the training is cheap - is it a company goal to make quality education accessible? and why?

*look for why they started their company. the emphasis should be on accessible quality education, not a guaranteed result. YOU MAKE YOUR OWN RESULT.*

> ■
> ## Helpful Links
>
> **Antisyphon Training:**
> *antisyphontraining.com*
>
> **TCM Security:**
> *tcm-sec.com*
>
> **TryHackMe:**
> *tryhackme.com*
>
> **HTB Academy:**
> *academy.hackthebox.com*

# BUILD A HOME LAB

## Equipment, Tools, and Tips

*written by Martin Pearson || @chinno53*

*A home lab will not only enhance your learning opportunities, but can also ==give you a safe place to play by using virtual machines== to emulate a computer, giving you the ability to easily make mistakes with no fear of harm to your personal setup.*

*Practicing on entry-level products is a great way to get started. Think about what you want to learn and how your setup will help you meet your goals. You don't need the fastest equipment, the most storage, or the best memory to start your home lab. Even if you can afford the best, it won't suddenly make you a master hacker. It relies on your commitment, not your equipment.*

In general, the fundamental building blocks of a lab are a network, virtual machines, and the physical machine to run them on. It's common to have one Linux (Kali) machine and usually one Windows client/server. This will be enough to do some really fun stuff!

## VM Options

*There are lots of virtualisation software to choose from. Below are some links to get you started. (Don't worry if these mean nothing to you at this stage; it's just good to be aware.)*

- *proxmox.com/en/*
- *vmware.com/products/workstation-pro.html*
- *docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/*
- *qemu.org/download/*
- *virtualbox.org/*

## Equipment Considerations

- How many virtual machines do you want *(vs. how many you actually need)*?
  - » How many might you want in the future?
  - » The more virtual machines, the more memory/storage space you will need.
  - » ==Consider purchasing second-hand machines== first.
- It is better to have a separate network to avoid family/user arguments when you play –
  - » Consider a dedicated router or switch.
- ==**You WILL break things! Make a backup**== *(sometimes called a snapshot).*

## Other Considerations

- Both Windows client and server can be used in evaluation-mode legally *(no need to purchase).*
- Kali and Parrot are commonly used operating systems that will give you all the learning tools you need. Search Kali or Parrot ISO to find out more.
  - » To learn about the operating systems and their included tools:
    - https://www.kali.org/tools/
    - https://www.parrotsec.org/
- A journey of a thousand miles begins with a single step!
- Consider exactly what you're trying to achieve. ==**You don't need to know and do everything right away.**==

*That's good, cuz if you did, I'd be f~~ucked~~*

Depending on what you start off with and how your needs grow, you may decide to buy more machines. Remember, they are very easy to network, so no need to throw away your old equipment. Above all, have fun and learn!
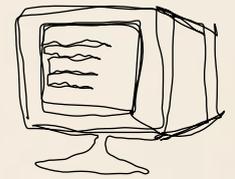
### How To Build a Home Lab for Infosec
with Ralph May
*youtu.be/9QoPmtpn-gs*

*an hour of awesome*

# ·▪ TO CERT OR NOT TO CERT ▪·

## That is the Question

*written by Ayub Yusuf || @whitecyberduck*

*To Cert or Not to Cert, that is the question:*
*Whether 'tis nobler in the mind to certify*
*The CPEs and renewal fees of outrageous fortune,*
*Or to take arms against the sea of recruiters!*

One of the fiercest debates within the information security community is whether one should pursue certifications or not. This article is not meant to persuade you one way or another, but to help you understand all the factors necessary to come to an informed decision!

## To Cert!

Earning a certification can be an excellent way to stand out to recruiters and hiring managers. Certifications can serve as a testament to one's expertise. The people hiring may even be seeking out applicants with a specific certification.

The job you're interested in may REQUIRE a certification. For many government and government contracting positions, certifications that meet the DoD 8570 benchmarks are required for those roles. No ifs, ands, or buts! On the civilian side, many consulting agencies justify their value by showcasing their accredited staff to clients.

Certifications can also facilitate growth in fields that otherwise would be neglected. It's natural to double down on the skills that you're already good at and avoid topics that one is less skilled at. Certifications can force you to become more well-rounded.

## Not to Cert!

There are other ways to show skills than just certifications! An active blog and vibrant GitHub profile can easily be more impressive than a few acronyms behind your name. Plus, plenty of excellent training doesn't even have associated certifications.

Everyone knows at this point that certifications can be expensive, but what is less obvious is the renewal fees, maintenance fees, and continuing education credits (CPEs) required to maintain many certifications. Many security professionals find themselves at a point in their career where they let their certifications expire because the maintenance requirements simply don't make sense anymore.

Pursuing a challenging certification can be like taking on a second shift. That's time away from your family, pursuing hobbies, and resting. The toll cert chasing can have on your mental health can lead to burnout.

## Conclusion

The primary, secondary, and tertiary purpose of any certification is to help you get a job!

- Check out job postings for roles you're interested in. What certifications are they asking for, if any?
- Study the LinkedIn profiles for those with the job title you want. Do they have any certifications? If so, which ones?
- Seek out reviews and ask mentors/friends to determine if the investment is worth it.

Ultimately, whether one should pursue a certification or not has to come down to opportunity cost. Opportunity cost is the value of what you lose when choosing between two or more options. In the case of certifications, it is the money and the time you spend pursuing it vs. the money and time you could've spent growing in other ways. No one but you can make this determination.

## Certification Roadmaps

*pauljerimy.com/security-certification-roadmap/*

*sans.org/cyber-security-skills-roadmap/*

*I love whoever made this... it must have taken WEEKS, but it's glorious*

## Jobs

-Threat Hunter-
GCFA
GREM
PJMR

-Red Teamer-
CRTO
CRTL
OSEP

-SOC Analyst-
Security+
GSOC
GSEC

-Pentester-
OSCP
GPEN
PNPT
HTB CPTS

-Incident Responder-
GCIH
GCFE

-Leader-
CISSP

-GRC-
CGRC
GSNA
PCI QSA

# HOW TO GET A JOB

## In Cybersecurity

*written by Gerald Auger of Simply Cyber*

You want to break into cybersecurity? That's AWESOME. I've been in the field for 20 years and I LOVE IT! *no, I'm just here for the sassy notes*

But embarking into a cybersecurity career can be overwhelming. There is just SO MUCH out there that parsing through it would be an endless task. This concise "cheat sheet" presents a solid 10-step approach to starting your career journey.

### 1. Gain baseline knowledge

If you don't understand how the tech is supposed to work, you won't understand when it's doing things anomalously. Learn fundamentals of operating systems, networking, and using a command line. You don't have to be a Linux admin or network engineer to move on to step 2, but get the fundamentals down and keep building your skills while you continue the process.

### 2. Build a strong LinkedIn profile

This is your digital resume. Many hiring managers will look you up when you are going for an interview. Plus, you can use it to start networking like a boss (step 9). Use Canva.com (for free!) for great, fast graphics for your bio pic, header image, and social posts.

### 3. Stay informed about industry trends

This is CRITICAL! You'll be asked in any cyber job interview how you stay current. There are many ways, and it takes vigilance, but it is needed in this industry.

> ### Daily Cyber Threat Briefing
> every weekday morning at 8AM EST
> *simplycyber.io/streams*

### 4. Identify your desired role

It's far too much to learn everything, so find the job/role you have passion for and lean into it.

### 5. Connect with role-specific communities

Network and learn from people doing your desired role already. There are lots of Discord communities for all aspects of cyber.

### 6. Acquire role-specific training

Practical skills reign supreme for employers hiring, so getting those sweet, sweet, hands-on skills will be valuable.

### 7. Tailor your resume to showcase skills

Use free ChatGPT to tune your resume for specific job postings and get all the benefits without the frustration and exhaustion of constantly tweaking your resume. *the award for "best use of ai" goes HERE*

### 8. Consider earning the Security+ certification

This is very specific, but most HR will put it on entry-level cyber job requirements, so it can pay dividends.

### 9. Network and hunt for job opportunities

Fun fact — Many jobs are never advertised because people know people that can do the job, so they get the job. Focus on delivering value, engaging within, and 'showing up' for your professional network. Networking is immeasurably valuable. *we have very different definitions of the word "fun"*

### 10. Ace the job interview

You've done all the work; this should be the easiest part. If you want a confidence boost, use free ChatGPT to mock interview you, tailored for the job you're going for and the person doing the interviewing!

> ### Secret Interview Hacks with ChatGPT
> *youtu.be/MIkZua2MKJY*

You've got the blueprint now! Grab it, execute it, grow your skills, contribute to the community, and enjoy the journey.

> ### FREE E-Book
> *for more info on job hunting*
>
> ### Cyber Unlocked
> The Ultimate Guide to Breaking into Cybersecurity
> *simplycyber.io/book*

*banjocrashland's ramblings: youtu.be/Air1c697tjw*

# ▪▪ BACKDOORS & BREACHES ▪▪

## Turn Practice Into Play

*a card game created by BHIS*

Tabletop exercises are a way to gather your team, discuss strategies, find improvements and create plans for incident response, but let's face it, they can be boring. Here at BHIS, we asked ourselves if we could find a way to make them more fun, without losing any of the function. So we gamified it, and you can too. Inspire discussions all about teaching and learning cybersecurity at all levels. From your interns to your most experienced vets, everyone can learn something from these games.
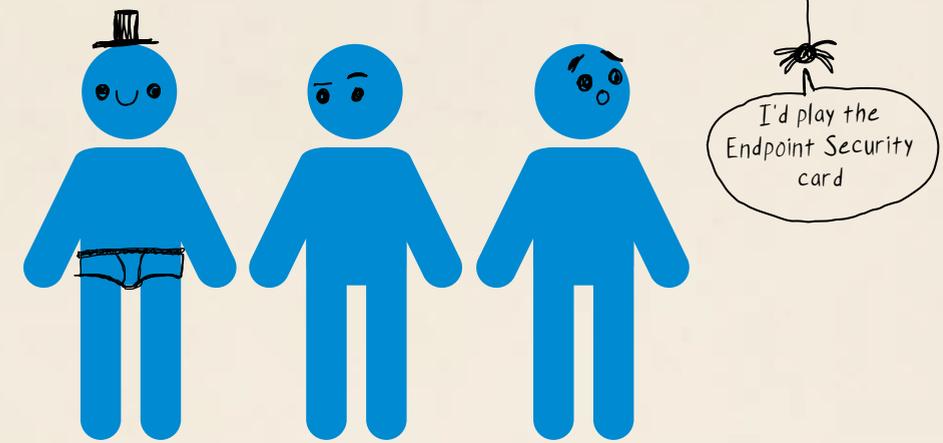
"Not without my hat!"

## INCIDENT CAPTAIN
1 CREATIVE LEADER

The Incident Captain draws one card each of
Initial Compromise, Pivot and Escalate, C2 & Exfil, and Persistence.

Without revealing these four attack cards to anyone else, the Captain weaves a tale of what this situation would look like to the Defenders. As the game goes on, the Captain continues to describe the imaginary incident, improvising and explaining the story as it unfolds.
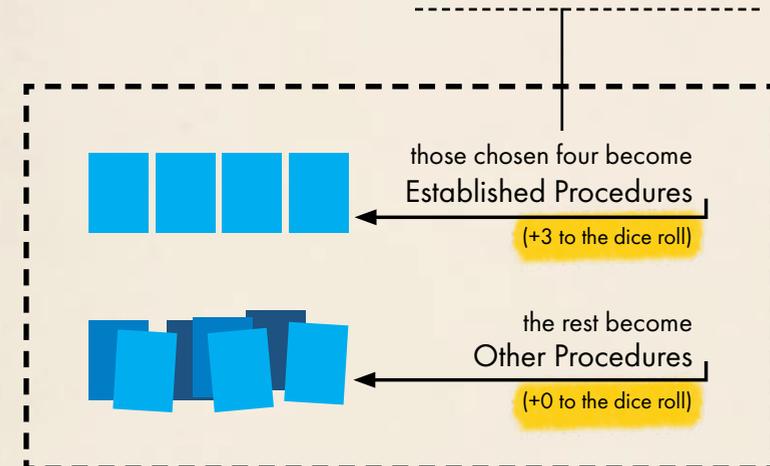
As procedures are played, it's up to the Incident Captain to ask The Defenders why those strategies do or don't work. If a procedure fails, is there a reason personally, politically, or financially that The Defenders can explain? Get your team thinking outside their computers.

The game works best if the Captain has a wide knowledge of cybersecurity, but what they lack in knowledge, they can make up for in confidence and question-asking.

I'd play the Endpoint Security card

## DEFENDERS
2+ ENTHUSIASTIC PLAYERS

The team of Defenders draw four cards of Procedures

those chosen four become
Established Procedures
(+3 to the dice roll)

the rest become
Other Procedures
(+0 to the dice roll)

With all the Procedures face up on the table, the team of Defenders discuss the situation described by the Incident Captain and devise a plan to detect and reveal all four attack cards. Agreeing on one Procedure to try, the team rolls a D20. 1-10 means the Procedure didn't work (3 bad rolls in a row triggers an Inject card), and no attack cards are revealed. 11-20 means the Procedure succeeded and applicable attack cards are revealed.

The game keeps going until all four attack cards are revealed, OR 10 turns pass, OR an Inject card ends the game, whichever comes first.

The game works best if the Defenders have a lot of enthusiasm and creativity! Ask questions, share knowledge, discuss in depth, and make it a goal to walk away with just one new thing to research more about.

do NOT overwhelm the team!!

For a more in-depth guide, hilarious video playthroughs, and helpful tips on how to be a fun and engaging Incident Captain, come check us out online at backdoorsandbreaches.com

# SOCIAL ENGINEERING
## How to Perform and Combat Social Engineering

*written by Ashley Knowles*

Social engineering is the use of deceptive tactics and techniques to manipulate users into providing confidential or sensitive information. This information can then be used for nefarious purposes.

## Performing Social Engineering

Typically, our red team assessments start with some way to obtain initial access. This initial access is normally obtained through the use of social engineering, whether that be through Microsoft Teams messages, phishing emails, smishing texts, or vishing calls. There are multiple ways to conduct social engineering and not every way is perfect for every organization. There is a lot of OSINT *(Open-Source INTelligence)* that goes into the development of the perfect social engineering ruse for an organization. Things like what the company does, what products they use, and even information provided by the client is used to develop an appropriate ruse.

Commonly, successful social engineering ruses are done from the perspective of an IT person calling to discuss a problem with an update that wasn't pushed correctly, or a computer that isn't calling home appropriately.

Recently, a tester posed as HR calling to ensure that employees have had their yearly review. Before continuing with the call, the HR representative attempted to verify the identity of the person they were calling with the last four of their social, date of birth, and employee number. After verification was completed, the tester proceeded with several generic questions about the review and the employee's experience.

This ruse proved to be incredibly successful. The tester then called the help desk to claim that they lost their phone which had their password manager on it and needed to join a new phone to their MFA account. With the social-engineered PII (personal identifiable information), the tester was able to join a new phone to their MFA account and reset their password. The compromised account could then be used to access sensitive company data.

*meanwhile, I write all my passwords on a little sticky note. Also bad, but in a different way.*

---

### Winning Friends and Influencing People
an Antisyphon Offensive Con talk
*youtu.be/r0lkcC_nH_o*

---

> **If in doubt, go through other means to verify legitimacy. No reputable person is going to request your password or login information.**

## Combatting Social Engineering   *aka CONSTANT VIGILANCE*

So, you may ask, how do we train our employees to recognize and report social engineering attempts? The answer is to always be on guard, have an easy to access and use escalation protocol, and conduct regular social engineering engagements against your team.

There are a few simple things, that when followed, can protect most users:
- Always check who is sending the email. This can be done by inspecting email headers on suspicious emails.
    - » If the sender's address does not match who is claiming to be sending the email, report it.
- For text messages or phone calls, the user can use a simple reverse number search on the phone number. Most VoIP phone numbers are suspicious. Threat actors like to use VoIP to hide their identity and VoIP numbers are easy to obtain.
- If in doubt on whether an email or call/text is malicious, go through other means to contact the actual person to verify legitimacy.

Some questions users can ask themselves that can indicate immediate red flags:
- What is being requested of the user?
- Is the user being asked to download software or navigate to a web application?
- Is it too good to be true?
- Are they being asked for their password, date of birth, last four of their social, or other sensitive information?

If you think that you are a target of a social engineering attempt, contact the sender via another method. For example, if the caller is claiming to be the company's internal IT, reach out to the IT department directly through a known good number to resolve the issue. No reputable person is going to request your password or login information. *except my roommate asking for the wifi password... again*

While social engineering attempts are becoming more advanced, the same general theme applies. With these rules and a proper escalation protocol established internally, you too can fight back against social engineering.
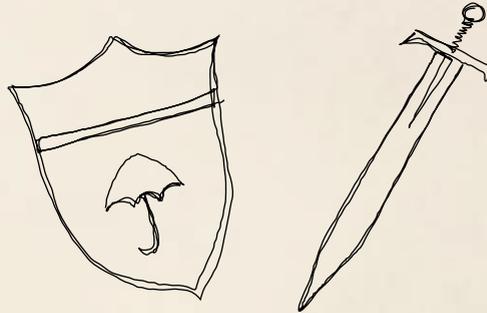
# BLUE TEAM
## Defend, Detect, Protect

*written by Erik Goldoff, CISSP || @ErikG || linkedin.com/in/egoldoff/*

*"Blue team" is a high-level term covering defensive security, whose goals are to reduce attack surface, as well as ==detect and respond to threats.==*

## Here are some, but not all, of the sub-topics under the umbrella of blue team operations:

- Defensive Security
- Infrastructure Protection
- End-User Education
- Incident Response (IR)
- Business Continuity/Damage Control
- Security Operations Center (SOC)
- Threat Hunting & Digital Forensics (DF)

Transitioning to blue team positions is easier for existing IT staffers (user support/help desk, operations, or network team). You need to be able to ==understand what is normal== for your environment ==in order to quickly recognize the abnormal== (potential security events). Your existing IT jobs are a great place to gain understanding of your environment from various fundamental perspectives.

As part of defensive security and/or infrastructure protection, it is vital that security stack components be configured and deployed properly — so as to not ignore threats, but not so stringent as to prevent productivity. You do not want your security solution to present the denial-of-service that you are trying to prevent. Endpoint security, endpoint detection and response (EDR), and security information and event management (SIEM) are tools used in defensive security.

goddammit cheryl

==End users are often the weakest link== in any organization with regards to security threats. You need to help them understand not only what to do, but also why, in order to help increase cooperation. Publishing periodic phishing test results by department can be more motivational than just individual training. *if i have to go to one more of those phishing seminars, i know who i'm blaming.*

Should your organization be breached by a cybersecurity attack, how do you proceed to mitigate the threat and damage while keeping your enterprise operating as it should? Your SOC and incident response teams can help identify the threat, the source, and the immediate remediation, while still maintaining "chain of custody" for any evidence found, as your organization may have legal requirements for cooperation with authorities and/or qualifying for insurance reimbursements.
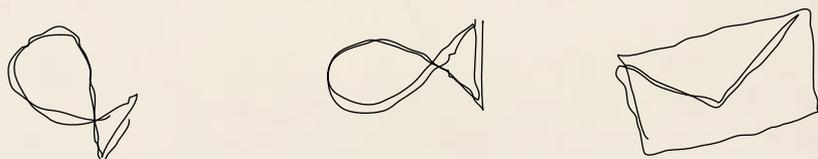
Being reactive is not enough. A proactive approach to threats is imperative for an organization. The threat hunting teams may find evidence of incursion before a major incident evolves. Did they find IOCs or EOCs (indicators/evidence of compromise) that alerted the DF/IR teams? Digital forensics (DF) gathers data on the attack methods, points of entry, incursion path, and potential exfiltration targets, while incident response (IR) helps to lock down the environment as necessary by disabling accounts, restricting network access, shutting down exfiltration paths, removing malware, etc. ==Different parts of cybersecurity work together== to detect, identify, and eradicate attacks.

If you are going to defend against cybersecurity attacks, you need to know about the tools and techniques available to defend with, as well as what tools and techniques your attackers are using. Knowledge is power! Where do you go to learn more?

## Resources

### Vulnerabilities

Vulnerabilities are tracked by their CVE (*common vulnerabilities and exposures)* number. Stay better informed on known vulnerabilities:

- *cve.mitre.org/*
- *nvd.nist.gov/vuln/full-listing*
- *cvedetails.com/index.php*
- *msrc.microsoft.com/update-guide/vulnerability*
- *support.apple.com/*

### ==News==

It is important for blue team members to stay current on evolving solutions to various cybersecurity problems:

- *youtube.com/@BlackHillsInformationSecurity/videos*
- *scmagazine.com/*

### URLs

To determine if a file or URL/link is malicious before you take defensive action, or as part of your forensics investigations:

- *virustotal.com/gui/home/upload*
- *urlscan.io/*
- *checkphish.ai/*

### Phishing

Good source for phishing tools, resources, and end-user training:

- *knowbe4.com/*

---
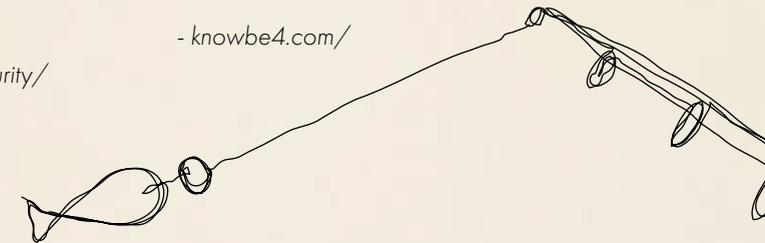
## Active Countermeasures
community, tools, trainings, and more
*activecountermeasures.com*

# ▪■ SOC ■▪
## Security Operations Center

*written by Edna Jonsson || @ednas*

## What is a SOC?    *a foot glove*

The SOC, or Security Operations Center, is a cybersecurity department that helps to identify threats and suspicious activity that take place within a company's network and devices. The entry position for the SOC is a SOC analyst. As a SOC analyst, you might work directly for the company or in a managed SOC (which provides companies with SOC services as a third-party). In order to become a SOC analyst, you need to have a good understanding of how computers work, as well as networking concepts and cybersecurity concepts. There are several ways that you can acquire the skills and knowledge needed for this position, such as a college degree, a training course, or self-study. Acquiring certifications will help prove you have a proficient knowledge of your area of study. You can use services like TryHackMe, Blue Team Labs Online, and Antisyphon Training to get started. In addition to the technical knowledge, it helps to be detail-oriented and have good communication skills.

## Tips

### Stay Up-To-Date

A good way to begin to understand the threat landscape and what the threat actors today are doing is to follow the news and cybersecurity professionals on social media, who will share what trends and threats they are seeing. There are also threat reports published, such as those by CrowdStrike, that are excellent resources for understanding threat actors, their tactics, and procedures.

### Safeguarding Communication

When communicating with stakeholders, fellow SOC analysts, and management or customers, you need to make sure that they won't accidentally visit malicious URLs that you are informing them about. The way to do that is to "defang" them; that is, to make them unclickable.

#### How to defang a URL:

Example malicious website URL — https://www.example.com/
https becomes hxxps
the . becomes [dot]
The end result is hxxps://www[dot]example[dot]com/

## Tools

Today, a SIEM (security information and event management) solution is the primary tool that is used in a SOC. This is a tool that collects and analyzes log events, and gives alerts on potential incidents. There are many different vendors for SIEM tools, such as Splunk, Microsoft, AlienVault, and more. In addition, the SOC might use an endpoint detection and response (EDR) tool, malware analysis tools, and vulnerability management tools.

## Resources

### Websites you will use as a SOC analyst:

These are helpful in verifying if the IP address or URL that you see is expected and if it is potentially malicious. CyberChef is a wonderful tool that can be used for decoding and deobfuscating code or text you encounter.

- *abuseipdb.com/*
- *virustotal.com/*
- *who.is/*
- *gchq.github.io/CyberChef/*

### Further reading:

*mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf*
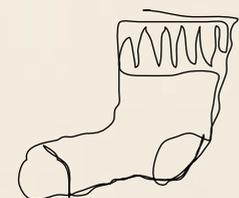
---

## SOC Core Skills

### learn the core security skills all SOC analysts need to have

Available Live and On-Demand
#### 16-hour Antisyphon course

*https://www.antisyphontraining.com/**live-courses-catalog**/soc-core-skills-w-john-strand/*
*https://www.antisyphontraining.com/**on-demand-courses**/soc-core-skills-w-john-strand/*

# ▪▪ THREAT HUNTING ▪▪

## An Active Search for Risks

*written by Wade Wells || @WadingThruLogs*

Threat hunting is a role as well as an activity. It can have different definitions depending on the organization. The base definition of threat hunting as an activity is *"the proactive search for malicious activities in a network."* Threat hunting is an iterative process that aims to identify potential security threats and risks that may not be detectable through automated security tools alone. It is a human-driven process that empowers organizations to stay one step ahead of cyber adversaries and improve their overall cybersecurity defenses.

A threat hunter should have the mindset that a network is already compromised. Threat hunters should also have an established baseline of the network's activities to determine abnormalities. A hunt can start with a hypothesis that guides the hunter's activities. An example would be, "Threat actors have used .iso files as the first stage to infect hosts on our network." The hunter will then establish if these activities have occurred within the network and if they are malicious.

As a role, threat hunters are usually in a senior position. People seeking this job typically pivot from security analysts, incident responders, or security engineers. All of these roles can perform threat hunting as an activity. A threat hunter should have a well-rounded knowledge of all things infosec and be comfortable wading through any logs. Understanding the blue team, red team, and threat intelligence tactics will improve your abilities in this role.

## Tips

- Use knowledge of your network and threat intelligence to help create a threat hunting hypothesis.
- Don't reinvent the wheel. Leverage community resources and security vendor reports to help improve threat hunting.
- If you're moving too fast to keep notes, slow down.
- Be constantly looking for misconfigurations and opportunities to harden the network while performing a hunt.

## Resources

Use the Sigma Project to view how others are detecting similar activities:
*github.com/SigmaHQ/sigma*

Use the ATT&CK® Powered Suit browser app to obtain information on MITRE ATT&CK® TTPs quickly:
*mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/attack-powered-suit/*

Great place to leverage what's going on in the news and think about it from a logging perspective:
*research.splunk.com/stories/*

Fantastic blog on threat hunting:
*kostas-ts.medium.com/threat-hunting-series-the-basics-cccadac830c6*

A full zine just on threat hunting:
*blackhillsinfosec.com/prompt-zine/prompt-issue-threat-hunting/*

Check out "MITRE ATT&CK® Defender™ ATT&CK® Threat Hunting" training on Cybrary:
*cybrary.it/course/mitre-attack-threat-hunting*

### Threat Hunting Class
an Antisyphon training course
*https://www.antisyphontraining.com/live-courses-catalog/advanced-network-threat-hunting-w-chris-brenton/*

## Hunting frameworks:

*splunk.com/en_us/blog/security/peak-threat-hunting-framework.html*

*youtu.be/TqMjMpvspJ4*

*github.com/TactiKoolSec/OTHF*

*https://www.gigamon.com/content/dam/resource-library/english/white-paper/wp-intelligence-driven-threat-hunting-methodology.pdf*
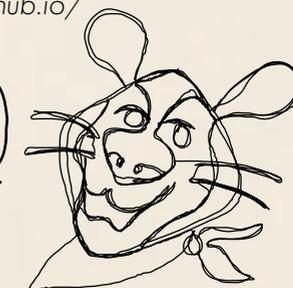
## Projects to try:

*acm.re/ac-hunter-community-edition/*

*lolbas-project.github.io/*

*loldrivers.io/*

*gtfobins.github.io/*

theeeyyyy'rreee MALICIOUS!

# RED TEAM
## Adversarial Simulation

*written by Ray Van Hoose || @_meta. || linkedin.com/in/-meta/*

*The question: How can we know how effective our security will be at detecting and mitigating the impact of a successful hack?*
*The answer: Red teaming.*

Red team operations utilize covert and strategic attack techniques in an attempt to infiltrate systems undetected. While the job titles may vary (operator, engineer, security specialist, etc.), the overall objectives remain consistent: to emulate adversarial actions, document response times and effectiveness, and proactively improve detection and response capabilities.

**What are the minimum tools one would need to survive as a red teamer?**

- a clipboard
- a USB stick
- a convincing story

*don't use the beekeeper story again - severely backfired*
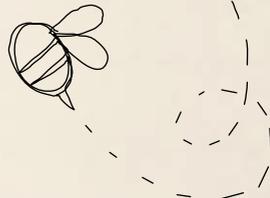
## Considerations and Job Requirements

- Strong communication and social skills
- Technical skills that cover a broad variety of domains
- Spy-gadgets and costumes would (likely) come from your personal budget
- Knowledge and understanding of blue team tactics, techniques, and procedures
- Ability to maintain composure while under pressure and in awkward situations
- Knowledge of the potential legal considerations and complications
- Solid understanding of the business side of the organizations

*bee suit was not cheap*

Finally, you should be aware that while executing some of these exercises, particularly in on-premise engagements, it is not uncommon to be arrested, including a chance of being jailed.

---

### Darknet Diaries
episode detailing potential legal complications
*darknetdiaries.com/episode/59*

---

## Skills and Techniques to Survive

### Communication
The most important skill. You'll be interacting with law enforcement, physical and cyber security teams, as well as debriefing leadership and working with developers and the blue teams to improve detection and mitigation capabilities.

### Documentation
Considering the range of legal complications and varied types of attacks, simply documenting the scope can be daunting. Commonly documented items also include attacks, exploits, the security team's responses to those attacks, artifacts created, steps to reproduce, and suggesting improvements to policies and processes of the blue teams.

### Exploitation
Many red team exercises require you to first exploit (social or technical) their systems. Even if you are given an "assumed breach" option to gain initial access, stealthily gaining more shells often requires additional exploitation.

Tools and techniques for gaining initial access:
- gophish - quickly and easily set up phishing engagements
  » *github.com/gophish/gophish*
- Use a SSO (Single Sign-On) vendor to provide a clean phishing link!
  » *jordanpotti.com/2019/08/26/phishing-with-saml-and-sso-providers/*

### Post-Exploitation
Exploiting a vulnerability to get you a foothold is only the first step. Ideally, this leads you to additional systems that you are able to stealthily exploit to gain persistence and all of the shells.

Brief list of tools commonly used within this craft:
- **Responder** - monitor and manipulate response in order to gain control of the network
  » *kali.org/tools/responder/*
- **Mimikatz** - extract passwords, hashes, PIN codes, and Kerberos tickets from memory
  » *github.com/gentilkiwi/mimikatz/*
- **Cobalt Strike** - commercial (costly) product providing tool(s) for adversarial emulation
  » *cobaltstrike.com/*

---

### What makes us different from pentesters?

- Diligent planning and execution
- We move like the 'g' in "lasagna"... silently
- We work with the blue teams to improve their ability to detect and stop malicious actors

---

# ·■ PENTESTING ■·

## Discover Vulnerabilities, Create Reports, Provide Guidance

*written by Ray Van Hoose || @_meta. || linkedin.com/in/-meta/*

*The question: How can we predict ways the bad guys will attack our systems, and how can we try to stop them?*
*The answer: Penetration testing.*

Penetration testing, especially in the past, included physical security assessments (i.e. breaking into buildings). Penetration testing has grown and evolved over the years, and currently tends to focus more on technical findings, leaving the physical security and social engineering (phishing emails, tricking folks on the phone, etc.) to the red teamers.

### What tools do I need to survive as a penetration tester?

- **Kali Linux:** open-source, Debian-based Linux distribution geared towards various information security tasks, such as penetration testing, security research, etc.
- **Nmap:** free and open-source utility for network discovery and security auditing
- **Burp:** Burp Suite is a comprehensive suite of tools for web application security testing

### What makes us different from red teamers?

- **Completeness:**
  - » We find and document as many of the vulnerabilities as we can, not just the vulnerabilities used to gain access.
- **Goals and approach:**
  - » Pentesters are "noisy" in their approach.
  - » Pentesters do not focus on things like response time and effectiveness of the defense teams.

## Skills and Techniques to Survive

### Communication
One of the most important, but least recognized, skills. Your primary deliverable is the report. Additionally, you will often debrief leadership, as well as work with developers, to fix the vulnerabilities discovered.

### Documentation
Few, if any, enjoy it, but the report needs to be presentable. Good screenshots and documentation are critical in this field.

### Command-line interface knowledge
Understanding Linux and Windows commands will provide —

- An interface for the vast majority of hacking and penetration testing tools (wget, cURL, Nikto, metasploit, sqlmap, etc.).
- 'screen' or 'tmux' allows you to launch, name, access, and manage a shell for each tool, or even split scans or tools across any number of shells.
- Improvement of screenshot readability (by only returning and displaying the most relevant data).

### Validation
Can you use different tools or techniques to validate the potential vulnerabilities that are discovered? Discovery and validation are key pillars of a good test.

### Exploitation
Often can be the trickiest part of the job. Sometimes, it might be as easy as configuring the tool to execute the appropriate payload... But quite often, you might spend a considerable amount of time tinkering to get a working exploit on that system.
Here are some popular websites that provide insights and (sometimes) working payloads:

- **Exploit-db** - *exploit-db.com*
- **Rapid7-db -** *rapid7.com/db/*
- **NIST** - *nvd.nist.gov/vuln/search*

Using these skills, knowledge, and tools, a successful penetration tester will be able to discover vulnerabilities, create reports that help inform leadership of security weaknesses, and provide meaningful guidance on how to remedy (or mitigate) these issues.

testing, testing 1 2 3 testing

### Introduction to Pentesting

#### 16-hour Antisyphon course w/ John Strand

*https://www.antisyphontraining.com/on-demand-courses/introduction-to-pentesting/*
*https://www.antisyphontraining.com/live-courses-catalog/introduction-to-pentesting-w-john-strand/*

**available live and on-demand**

yep looks like this pen works

# PURPLE TEAM

## With Our Powers Combined...

*written by Max Boehner*

## What It Is

Purple teaming is a collaborative activity performed by blue teamers and red teamers with the goal of improving defenses. In other words: red teamers share or demonstrate tools, tactics, and procedures (TTPs) to train the blue team. This can range from a one-off, "Do you get an alert if I run this attack tool?" to complex, repeatable, and defined processes.

## What It Isn't

Purple teaming is not red teaming, despite the involvement of red teamers. Red teaming tests the blue team's detection and response by performing simulated attacks without informing the blue team, while trying to remain undetected. During purple teaming, you want the blue teamers to be aware and on the lookout.

## Why Do It?

Blue teamers need to understand adversary TTPs to defend against them. Red teamers know these TTPs and can execute them. Purple teaming can be an effective way to bring this together.

**Here are some potential use-cases:**

- Validating that event logging and forwarding are working as expected
- Discovering detection gaps and developing new detections
- Establishing time-to-response metrics and discrepancies between attack activities and alert notifications

## Getting Into Purple Teaming

**The bad news first:** dedicated purple team positions are rare. Most organizations cannot afford dedicated full-time purple teams.

**The good news:** If you have experience in blue, red, or ideally both, and have a collaborative mindset, you can still do purple teaming. Folks starting in infosec might want to pick red or blue first, gather experience there, and then get involved in purple later on. A good way to train for purple activities is to set up a testing lab that includes machines to run attacks, with centralized logging configured to analyze the telemetry generated during an attack. Of course, you can also attend training courses that focus on purple teaming.

## Purple Teaming

**with Kent Ickler and Jordan Drysdale**

*youtu.be/_KqtVWrw_Gc*
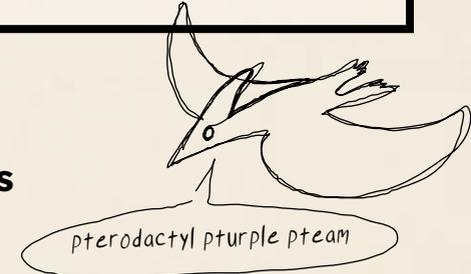
## Useful (and free!) Tools and Resources

**MITRE ATT&CK®** - *attack.mitre.org*

This knowledge-base of attacker behavior and techniques is a must-know. It is used as a common terminology for categorizing attacks.

**Purple Team Exercise Framework (PTEF) -** *github.com/scythe-io/purple-team-exercise-framework*

Further reading on purple teaming with different levels of maturity being described.

**Atomic Red Team -** *github.com/redcanaryco/atomic-red-team*

Library of executable attacks (atomics) that can be executed without deep red teaming knowledge in order to simulate adversary activity. It is utilized by many purple teaming frameworks and mapped to MITRE ATT&CK®.

**VECTR -** *github.com/SecurityRiskAdvisors/VECTR*

Free tool for planning, executing, and tracking purple teaming engagements. It can utilize Atomic Red Team atomics.

**MITRE CALDERA™ -** *github.com/mitre/caldera*

Platform that can be used for purple teaming engagements. It includes functionality for performing adversary activity through a command-and-control (C2) channel, among other things.

**DO-LAB -** *github.com/DefensiveOrigins/DO-LAB*

Lab environment that is easily deployable in the Azure Cloud. Includes Active Directory, attacker and victim machines, and log aggregation in Sentinel.

*pterodactyl pturple pteam*

# ·■ INCIDENT RESPONSE ■·
## Detect, Analyze, Respond

*written by Dr. Catherine J. Ullman || @investigatorchic*
*contributor to "97 Things Every Information Security Professional Should Know"*

Incident response (IR) is the process of detecting, analyzing, and responding to security incidents in an organization. It is reactive, meaning it happens only after something has already occurred. Incident responders coordinate the response and recovery teams, establish a timeline of events, and determine how best to respond to an incident with assistance from other security roles, management, lawyers, and IT. Incidents might include data breaches, malware outbreaks, phishing campaigns, or response to an APT.

Incident responders are typically responsible for guiding the process along during an incident, whereas digital forensic (DF) investigators are the ones typically doing the hands-on detective work. In some organizations, the same people perform both the IR and DF roles. Because digital forensics is often a part of an IR engagement, it is common for people to use the acronym DFIR (digital forensics and incident response) to refer to people in this field.

Good incident responders typically are guided by some form of framework. One of the most popular in use today is the SANS Incident Response Framework. This framework is laid out in their Incident Handler's Handbook, which can be found here: *sans.org/white-papers/33901/*

### The overall steps include:

- **Preparation:** Involves creating an incident response plan/process
- **Identification:** Involves recognizing signs of an incident
- **Containment:** Involves preventing further spread/damage
- **Eradication:** Involves removing all traces of the threat actor's activity
- **Recovery:** Involves carefully putting systems back in production
- **Lessons Learned:** Involves understanding what went right/wrong for future use

## Career Options

Typically, you will be looking for employment options from either medium to large organizations who have an in-house team for DFIR work or from security contractors who provide DFIR services. Contract work will expose you to many more incidents (and types of incidents) than an in-house job. A good place to start is by getting training and experience as a SOC analyst, and then supplement with some threat hunting training and additional security training and experience, such as digital forensics.

## General IR Recommendations:

- Avoid tunnel vision; do a "360" of the incident.
- Act, don't react; don't be misled by emotion.
- Don't panic; remain calm.
- Avoid making assumptions; look at the big picture.
- Avoid freelancing; follow a plan.
- Have patience; take a "beat" before proceeding.
- Pre-plan whenever possible — tabletops, documentation, IR plan.
- Document accountability — Access logs, etc.

*this is fine*

Incident response can be a very stressful job. People who excel at it are typically good under pressure, thrive in chaos, have significant amounts of patience, and have strong analytical, organizational, and communication skills, as well as self-confidence and leadership skills.

---

**The Active Defender**
Immersion in the Offensive Security Mindset
*A book by Dr. Catherine J. Ullman*

*got a signed copy at defcon - i'm a cool kid now*

# ▪▪ DIGITAL FORENSICS ▪▪

## Examine, Investigate, Report

*written by Blake Regan || @zer0cooL || blueteamtactics.net*

Digital forensics is the science (and art) of examining digital artifacts from operating systems and electronic devices to investigate events that may or may not have happened. This is accomplished by using various tools and techniques to establish a record of facts, and then reporting on that information to attempt to provide an answer. While TV may depict digital forensics as fast-paced and exciting, the reality is that system images can take time to capture, hashing of files can be a long process, and sometimes you simply can't find what you are expecting to find.

There are many scenarios where digital forensics can provide an advantage — corporate disciplinary matters such as employee investigations involving misconduct, illicit browsing, or legal matters concerning IP theft or data exfiltration by insiders. There is also digital forensics incident response (DFIR) which involves identifying the source of an intrusion and mapping an attacker's movements from system to system across the network. The two are often found together because of the versatility of application and use cases.

## Career Paths

The career path to digital forensics investigator is not always a straight line and can have a steep learning curve due to ever-evolving technology.

**Common pathways to digital forensics include:**

- System administration and IT generalization
- Blue team (SOC/IR)
- Military or law enforcement
- Being voluntold by your boss

*not the first time, won't be the last time*

No matter how one moves into digital forensics, it is important to have a passion for learning, be comfortable with detail-oriented work and documentation, and have a natural curiosity to explore different ways to answer a question.

## Collecting Evidence

### Volatility

When collecting digital evidence, it is important to consider the order of volatility to maintain fidelity of the data.

#### Examples:

**Volatile evidence:**

- System memory (RAM)
- Host routing tables (ARP)
- Cached data in CPU

**Non-volatile evidence:**

- Files stored on a hard disk
- USB storage
- SD Memory Cards

## Chain of Custody

Another thing to consider when collecting and preserving digital evidence is chain of custody. This is extremely important for legal matters. A good rule of thumb is to treat every incident like it will become a lawsuit. This will cover your bases if it does and give you great practice even if it doesn't.

**Chain of custody is the process of establishing**

- who had access to the evidence, and when
- how the evidence was collected, and when
- how the evidence was stored, and where
- anytime the evidence changed hands, and when
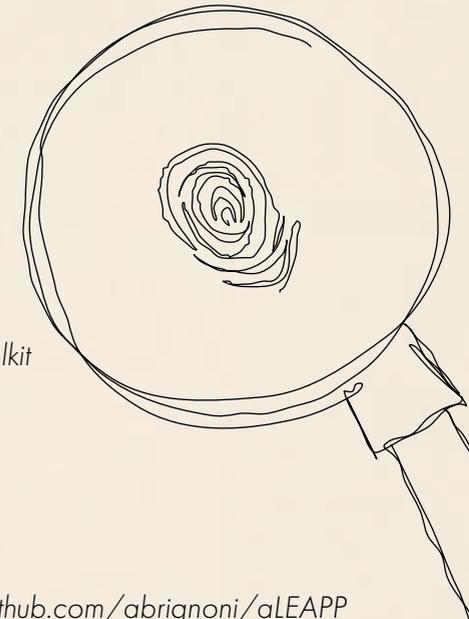
## Popular Open-Source Tools

**Forensic Tool Kit (FTK) Imager -** *exterro.com/forensic-toolkit*

**Autopsy Forensics Suite -** *autopsy.com*

**Volatility (memory analysis) -** *volatilityfoundation.org*

**Zimmerman Tools -** *ericzimmerman.github.io/#!index.md*

**Wireshark -** *wireshark.org*

**iLEAPP and aLEAPP -** *github.com/abrignoni/iLEAPP    github.com/abrignoni/aLEAPP*

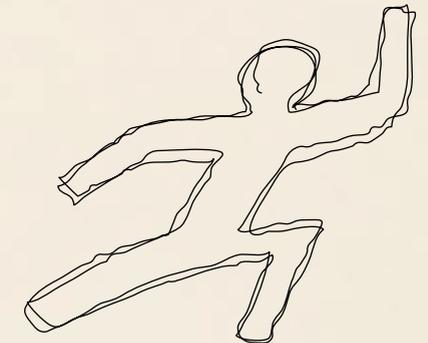**Klogg -** *klogg.filimonov.dev*

## Popular Commercial Tools

**Encase -** *opentext.com/products/encase-forensic*

**Cellebrite -** *cellebrite.com*

**Magnet Axiom -** *magnetforensics.com*

**X-Ways Forensics -** *x-ways.net*

**Grayshift -** *grayshift.com/graykey/*

In conclusion, there are many facets of digital forensics to consider for exploration. Big names in tech are constantly changing the way their products work, and new technology and products are created every day, bringing about new techniques and artifacts to research and explore. Digital forensics will always be evolving, which means investigators will need to evolve as well to stay relevant.

**Blue Team Tactics** ▪
a DFIR blog by Blake Regan
*blueteamtactics.net*

# ▪▪ HOW TO WRITE REPORTS ▪▪

## Effectively Communicating Observations

*written by BB King*

*So you like to hack stuff? To figure out how things work? That's awesome! But if you want to make a career of it, you have to take the next step: you must make it a habit to write clearly about what you observe, in a way that helps drive improvements. Without a report of some kind, there's nothing to show for all the hard work you do, and there's nothing to guide the people who hire you in their efforts to make their environment safer.*

As a pentester, your product — the thing you produce — is a report. The test itself is nothing more than your best effort to gather facts that you can put into the report. This should be too obvious to have to say, but maybe it isn't: any given test with an excellent report is worth more than that same test with a mediocre report.

**Nobody gets paid to do a pentest. They get paid for the report.**

The report should not be just a list of findings. That's what vulnerability scanners produce. You are smarter than that. A good report will include context for those findings.

> ## The report is... ■
>
> - A story of the environment as you, a security person, saw it.
> - A tool for guiding action.
> - A resource where interested readers can learn things.
> - Evidence of the state of the target at a point in time.

Don't stop at, "*this system has a known vulnerability,*" but show what can happen when an attacker exploits that vulnerability. We have all known of a team who has advocated for a long time to get resources to fix a known problem, but they just can't convince the decision-makers to approve the effort. It keeps getting buried under other objectives. If your report shows the harm that can come from that situation, it might just be the thing that finally gets that team the traction they need.

Your strong testing skills can't do that on their own. **It's your report that does the convincing.**

if it matters, measure it
if it matters, measure it
if it matters, measure it
if it matters, measure it
if it matters, measure it
if it measures, matter it

> ## Reporting for Pentesters ■
>
> spend time thinking about reporting and actively getting better at it
>
> ### 4-hour Antisyphon course
>
> *https://www.antisyphontraining.com/live-courses-catalog/reporting-for-pentesters/*
>
> **with BB King**
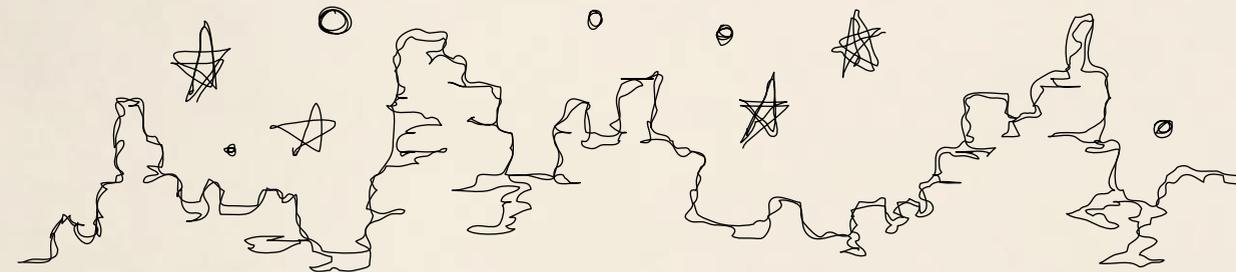
A good report also highlights things that are going well. If the common attacks that "always work" don't work this time, that's noteworthy! Point that out so the defenders get some much-deserved credit for their hard work, and so that their management doesn't accidentally force them to neglect those strong areas while they work on the weaker places you found.

Finally, show respect for your audience. Your report will be read by business people and technical people. You can be certain that people in both groups are good at what they do and want to do the right things. Let your writing show that you believe it.

We sometimes joke about each other's strange language. This group "shifts paradigms with key performance indicators." That one "recycles servers and rotates passwords." The pentesters "Kerberoast privileged service principals." **Write in a language your readers will understand, and don't make the mistake of thinking it's only necessary because they're somehow less smart than you are. They are not. They just focus on different things. On average, they're exactly as smart as you are. Treat them that way.**

hello fellow smart brain

# HOW TO SAY NO

## Telling a Client "No" - From a Business Perspective

### written by Melisa Wachs

*Pentesters and other professionals will each have their own reasons for refusing a client's request. In the realm of cybersecurity, the violation may range from contract scope to illegal asks. Sometimes clients simply need help understanding something, but on rare occasions it may be more malicious. No matter what the situation, always be kind in return.*

### 1. Be kind, yet honest.

You do nobody justice, including yourself, by trying to manipulate people and situations. Just be honest, say the truth of the situation, and —

### 2. Seek clarity.

Many issues can be solved by asking clarifying questions. Definitions are fluid at times, especially in this industry.

### 3. Offer solutions.

Tell them yes to what you can do and point to a positive with every negative: "We're fully booked for 2023, but we're offering strong incentives for January testing time. We can put you on our waiting list and we can invoice early, if needed."

### 4. Team up and take your time.

Don't say no right away, but rest easy in team decisions. For sensitive language, bring in a trusted teammate to work through drafts. Ensure your language is accurate and professional.

On a team, there may be those who shy away from any form of conflict and those who thrive on it. Balancing these two out as a whole is a good thing, and allows for a harmonious and mature dynamic.

### 5. Understand team roles.

We believe that our testers are our greatest assets, and we stand by it. At any point, we are there to support them, which means they never have to be the "bad guy" if something goes sideways on a test. Some testers rely on team support more than others, but below are a few examples of what we've dealt with in the past:

- If the customer asks for something out of scope, then we jump in to point back to scope so they don't need to argue with the customer. It should all be in the contract anyway, right?
- If a customer asks for something illegal, we jump in to say so on behalf of the tester. Testers have the right to bring in an authority to verify and show we've taken the request seriously. "I understand this may be disappointing. I'm bringing in Wile E. Coyote, our COO, if you'd like to discuss further."
- If a customer is rude, then be kind. Always return any adversarial language with kindness. Rule #1 with working remotely is to always assume best intentions, and this does include our customers

### 6. Understand when to say yes.

This should be done as part of a team discussion with advocates for both the customer and the testers. If it's a draw... the testers always win. We always take care of our own before we fear the loss of a customer.

> **If a customer is rude, then be kind. Always return any adversarial language with kindness. Rule #1 with working remotely is to always assume best intentions, and this does include our customers.**

*So, you have found that shiny new tool, amazing training opportunity, or need something and have to get approval from your boss? There are several things you can do before asking to make sure you get that "yes."*

## 1. Do your research

This is one of the biggest things you can do to have a positive interaction with your boss. How will your request help you, the organization, or your clients? Are there things that you're doing now, systems already in place, or will this be something new? How does that tie into initiatives across your company currently, and are there any regulations or mandates that can be met by your request?

## 2. Understand your boss's perspective

Your boss's primary concern is protecting the company, clients, and resources. You should be having regular conversations. The better your communication, the easier it will be to make requests, especially one that may have a price tag. If you look at your request from the approach of "what would I want to know to approve this request," you can be better prepared to make the request. Your tenure may also play into whether it's the right time to ask for something. If you are brand new to the organization, coming in demanding a lot of resources, time, and money may not be well received. Having those regular conversations will help you decide whether it's something your organization would support.

## 3. Know the objections

This step should be completed during step 1, but know and be ready to answer potential objections. Knowing the drawbacks, impacts, and concerns will give confidence to the decision-makers, and if you can answer how you'll address those objections, they'll have confidence in you to follow through. Are there free tools out there that aren't as good? Have you tried them out? Have you exhausted YouTube or other free resources to justify paying for that training?

## 4. Follow up

Depending on your organization's priorities, you may not get a yes immediately. Unless you get a flat "no," a little persistence may be rewarded. Ask your boss when it would be appropriate to follow up if your organization needs some time to digest your request.

**As long as you have the best interests of your organization at heart, and you have a good relationship with your boss, requests should not be something to be worried about. Do your research, make your case, and you may be surprised by the results.**

*and you'll see here, i made the little red line go up more*

# ▪■ TRIALS AND JOYS ■▪

## Cautionary Statements With a Positive Spin

*written by Alex Minster || @Belouve || TraceLabs.org*

*Infosec is no hacker movie with edgy anonymous handles. It is a challenging yet rewarding landscape with hurdles you might not be prepared for. In providing this list of potential pitfalls and triumphs, our aim isn't to deter you, but to equip you for a journey where we are better together. The trials and joys of this career shape us into the guardians of our ever-evolving digital world.*

## Why you don't want to do infosec

**You will be at the cutting edge.**

It is essential to stay abreast of new technology, vulnerabilities, exploits, "helpful" software updates or bugs, new security solutions... and now you're being asked about that comically named vulnerability that just dropped this morning and there's not much information available on it. The rapid pace of change and the need to stay informed creates a daunting challenge.

**You will likely be at the rusty edge too.**

Often, you'll have to advocate for the decommissioning of obsolete protocols or services, and deal with software or servers old enough to get a driver's license. You will need to research a lot to assure stakeholders that, yes, there are serious security implications in continuing its use and, no, turning it off or fixing it won't disrupt operations.

**You will frequently be the scapegoat.**

Security teams often find themselves blamed for operational issues (whether or not they're actually at fault). Overcoming this perception can be challenging, all because one time ten years ago, an asterisk was misplaced by security and everything got blocked.* The blame doesn't even have to make sense. When Carol's coffee maker makes bad coffee, your security modifications will somehow be blamed for that too. *that was ONE TIME

**You might lose out on good weekends.**

Security doesn't catch fire at convenient times. Hopefully, it will be a rarity for an incident to interrupt your weekend or holiday, but it is worth a word of warning. You'll end up saving certain contacts in your phone as "Cancel Your Plans" because they always call on the nights or weekends and it is never good news when they do.

**You'll sometimes be in bad situations.**

Most likely, you'll have some tense situations and bad days, and hopefully these are security incidents that can be resolved easily and give you experience. A risk of protecting and monitoring information systems is seeing or learning information you can't unsee or unlearn. Sometimes you'll have unique issues like being detained by armed guards, knocking something critical offline, getting banned, burning bridges, crawling through mud, or getting a scar. A lot of other jobs don't come with those risks.

## Now for some points on why you want to do this

**You get to learn some really cool new stuff.**

Being on the cutting edge means you'll constantly learn about new technologies and security measures, and offers an exciting opportunity for continuous learning of tools and tricks. There's a certain thrill in mastering the latest advancements and utilizing them to enhance security.

**You get to understand the really old stuff too.**

Yeah, you may have some dinosaur technology in your organization, but while working with securing legacy technologies can be frustrating, it can also be rewarding. Often, this involves revisiting fundamentals and learning how to articulate your concerns to build bridges of understanding across the organization.

**You're going to get real good at documentation.**

Good documentation skills, born from necessity, will soon become a cornerstone of your professional development. What starts as covering your backside turns into you quickly learning what matters and what needs to be written down. This can be a great benefit to your future self and teammates, and it's an opportunity to prove the value of security and foster a culture of shared responsibility. These skills not only help you to communicate effectively but also serve as a vital tool in offensive work, and can be critical in defensive work, intelligence, and incident response.

**You'll be protecting people's livelihoods.**

Whether directly, in sectors like the military, healthcare, finance, or investigations, or indirectly by safeguarding sensitive information, your work has far-reaching implications. Sometimes, you may be fortunate enough to assist in ensuring doctor access to critical life-saving information or providing intelligence that reunites missing persons. The impact you can have on people's lives makes every challenge worthwhile.

**You're gonna have some really cool stories.**

For every bad day, shocking encounter, lost weekend, received blame, miscommunication, and so forth... there's a lesson learned and a story to tell. These experiences shape you as a professional and make you a valuable contributor to an industry that needs you and is glad that you are here. And as AJR puts it: "A hundred bad days made a hundred good stories. A hundred good stories make me interesting at parties."

**So come join us at conferences, parties, or online hangouts, and share your stories – we can't wait to hear them!**

# MENTAL HEALTH
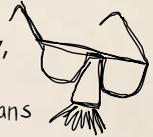
## An InfoSec Challenge

*written by Amanda Berlin of Mental Health Hackers*

*Cybersecurity is a rapidly growing field, and with it, comes a number of mental health challenges above and beyond our normal day-to-day living. We are all often under a great deal of stress, as we are responsible for protecting data, environments, and more from attackers, no matter what role we are in. This can lead to burnout, imposter syndrome, high levels of anxiety, and more.*
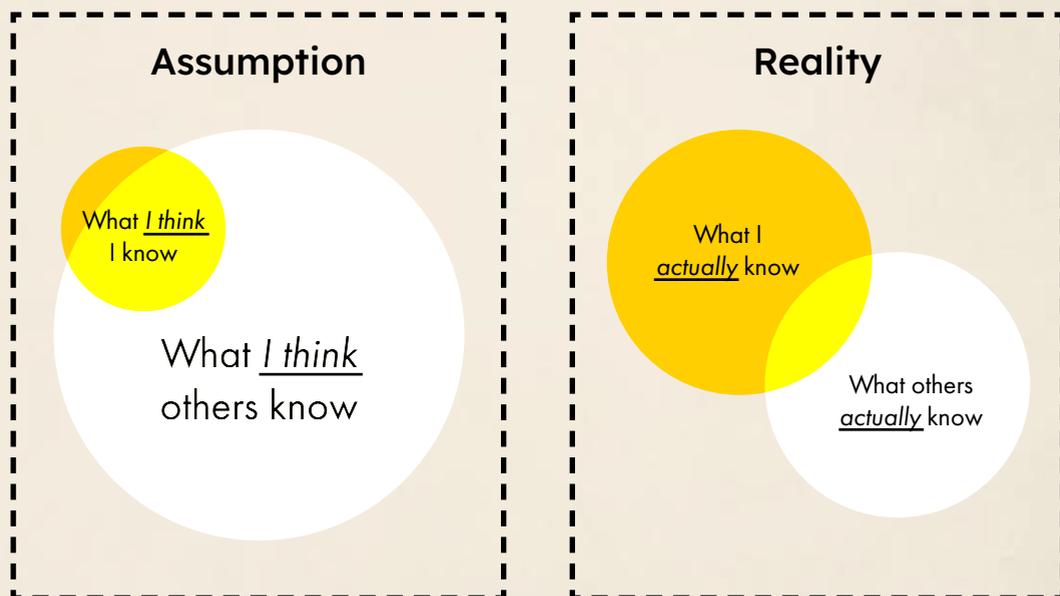
## Common Mental Health Issues in Cybersecurity

- **Burnout** is a state of physical, emotional, and mental exhaustion caused by prolonged stress. One of the reasons we are at risk of burnout is because of the constant bombardment of new threats, attacks, and vulnerabilities. We sometimes feel that we "always have to be on," even to the detriment of our own health.

- **High stress and anxiety** are common in the cybersecurity field. Our bodies aren't built to be in a constant "fight or flight" mode.

- **Imposter syndrome** is a feeling of inadequacy and insecurity, despite evidence to the contrary. We are often surrounded by highly skilled and knowledgeable people; it's one of the amazing aspects of our community, but can also be an indirect source of stress. *ok but i bought that mustache kit specifically for imposter shenanigans*

### Imposter Syndrome

| Assumption | Reality |
|---|---|
| What *I think* I know | What I *actually* know |
| What *I think* others know | What others *actually* know |

## Tips for Prevention

**Take breaks;** try not to stare at your screen constantly. Work/life balance is difficult. Overwhelmed or stressed? Go do something else to switch your brain off from work.

**Exercise** is a powerful way to reduce stress and anxiety. It's not just about getting fit, it's also about reconnecting your mind and your body. You don't have to hit the gym — even a simple, short walk can do wonders. If it's too difficult, start smaller... just start somewhere.

*Be kind to yourself, build trust with yourself that you'll take care of you.*

**Take care of yourself** by speaking to yourself as you would a friend, eating healthy, getting enough sleep, and exercising. This is easier said than done. Start small and work towards achieveable goals to establish healthy habits.

**Talk to someone** you trust. It could be a friend or a professional. It may take some patience and persistence to find the right fit, but therapists are professionals that can give you tools to succeed.

*Professional therapy isn't the only option. Help can take other forms. keep seeking out what helps you.*

## Places to Talk With Fellow Peers

- **Online forums:** Discord and Slack groups are available in all different areas of security. Many of these have dedicated mental health channels. If your community doesn't have a mental health channel, try asking for one.

- **Scheduled chats with friends:** Text, phone, or video, scheduling friend time is sometimes needed amongst our busy daily schedules.

Mental health is an important issue for *everyone.* Everyone struggles, you're not alone. By being aware of the signs and taking steps to prevent mental health struggles, we all improve our mental health and well-being.

**Lastly, and most importantly, it's never too late. You can find healing after burnout. You can recover from workplace trauma. Reach out and ask for help.** *the coffee machine, however, will not recover*

## More Help

The National Alliance on Mental Illness (NAMI) ---------------------------------------- *nami.org*
The American Foundation for Suicide Prevention (AFSP) --------------------------- *afsp.org*
Mental Health Hackers ----------------------- *mentalhealthhackers.org/resources-and-links/*
American Psychiatric Association's Resources for Employers ---- *workplacementalhealth.org*
Mental Health First Aid -------------------------------------------------- *mentalhealthfirstaid.org*
Sober in Cyber ------------------------------------------------------------ *soberincyber.org/about*

*If you find yourself or someone you love in a crisis, you can call 988 for the National Suicide & Crisis Prevention Line. The Lifeline provides 24/7 free and confidential support for people in distress, as well as prevention resources for you or your loved ones.*

# PROTECT YOUR PRIVACY

## How to Protect Your Own Privacy

*written by Matt Thomas || @slegna*

*Learning about infosec and peeking behind the curtain of digital safety can inspire fear and paranoia of privacy and all things cyber. If you want to keep using technology and still retain your peace of mind, there are ways to go about that.*

## Why you should care

Privacy is a human right. You don't need a reason to protect your privacy, but here are a few examples of why it's beneficial to:

- Reduce spam mail and calls
- Reduce risk of phishing, theft, and other attacks
- Escape harmful situations such as domestic abuse or political repression

Security and convenience are often in opposition, but basic security hygiene can reduce a lot of common issues we all experience.

> "You shouldn't confuse privacy with secrecy. We all know what happens in the bathroom, but you still close the door. That's because you want privacy, not secrecy. Everyone has something to protect. Privacy is something that makes us human."
>
> *privacyguides.org/en/*

*I know your secrets*

## How you're tracked and how your data is used

Every piece of identifying information about you can be used to track and correlate your activity. The aggregation of that data can be used to predict and influence your choices, made available for purchase by anyone willing to pay. On a personal scale, you may lose your reputation or your life savings. On a global scale, that aggregate data can affect the trend of ads, corporate policies, and even political outcomes.

## What you can do

The best way to learn how a few pieces of your data can be used is by learning OSINT techniques. A robust SecOps professional recommendation would normally delve into developing your own individual threat model to decide what you should worry about. Instead, our goal is to help every reader defend their everyday privacy.

### Delete data and unused accounts

For most of us, the proverbial cat is out of the bag; we already have a lot of data spread across many services. You can still take a proactive approach going forward. Most services allow you to delete your account or have your data removed from their services.

Michael Bazzell has a guide on removing your data from people search websites (*inteltechniques.com/workbook.html*).

### Change your habits

The most impactful thing you can do for your privacy is change the way you approach all of the companies that are constantly requesting your data. Ask yourself why you need to give that information to them. How will they use it? Can you give out false information? Always try to accomplish a given task without giving out unneeded data, permissions, or even installing an app. When choosing services to use, especially free ones, determine the service's business model. Do they make money selling subscriptions, selling hardware, from fees, or from selling your data?

## Tools

When choosing, look for tools with end-to-end encryption (E2EE). When implemented correctly, the service provider themselves can't even access your data.

### Password managers

We've all been told to use unique, secure passwords for every site, but that's a pain and impossible to remember. The best password managers generate and store strong, unique passwords for you, and some even help generate a unique email address alias.

- Bitwarden
- 1Password
- iCloud Keychain

*i used to name all of my passwords after bob ross phrases but this seems better than H@ppyL!ttl3CLØuds123*

### Payment Masking Services

These services provide digital debit/credit cards. Some services allow these cards to be one-time use, locked to a specific merchant, and set spending limits. The biggest convenience? When one card is compromised, you don't have to spend an entire day updating your payment information to dozens of subscriptions and auto-pays.

- Privacy.com
- MySudo.com
- Bank-provided virtual cards

### Secure Messengers

The most secure E2EE messaging service only works if the people you talk to use it. For that reason, keep it simple. Use Signal and get your friends and family on Signal.

### Email Aliases

Create new accounts without giving out your real email address and still get all your email delivered to the same inbox. Some password managers integrate with these services to create a unique email at the same time as your unique password.

- Proton Mail
- Fastmail
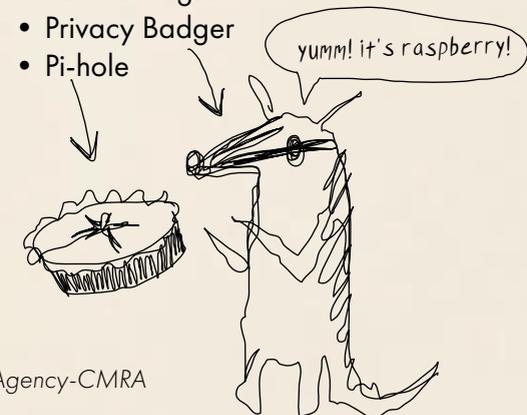- iCloud Hide My Email

### VPNs

The only thing VPNs mask is your IP address. If a site is censored or region-blocked, VPNs can help. Often though, legitimate services block VPN IPs, so they can be more hassle than they're worth for the average person.

- Proton VPN
- IVPN
- Mullvad

### Ad Blockers

Most of the trackers that follow you around the web can be blocked with a good ad blocker. Malware is also often delivered through ad channels.

- uBlock Origin
- Privacy Badger
- Pi-hole

*yumm! it's raspberry!*

## Resources

- *privacyguides.org/en/*
- *inteltechniques.com/*
- *ssd.eff.org/*
- *passkeys.com/*
- *haveibeenpwned.com/*
- *faq.usps.com/s/article/Commercial-Mail-Receiving-Agency-CMRA*

# ■ HOW TO PUT YOURSELF OUT THERE ■
## Networking On Social Media

*written by Serena DiPenti  ||  @shenetworks*

It is no surprise that growing your social network can help get your name out there and provide opportunities to advance your career. LinkedIn, one of the original career-focused networking sites, launched in 2003, making it older than Twitter, Facebook, and Myspace (by just 2 months). LinkedIn became so popular it was purchased in 2018 by Microsoft for a cool $26 Billion dollars. *Capital B.* LinkedIn might be the most popular career-focused networking website, but it's far from the only option.

However, career advancement is just one reason people might make content. I started my TikTok account because I was bored. It was a few months into quarantine; I was working from home and spending way too much time scrolling on TikTok. I liked the short form videos, the trends, sounds, and interacting with people who have similar interests. Maybe your motivation is different.

*i wanna be a STAAAR - haha. ha. just kidding, please never find me*

There are hundreds of blogs on how to get the best reach, what time of day you should post, how much you should post, etc. **In my experience, it doesn't really matter.**

**Don't overcomplicate it.** You don't need to be an overnight success; you just need to **share what you're excited about** and the rest will come.

SMASH THAT LIKE BUTTON

**If you're interested in putting yourself out there, here are some tips:**

**1. Identify your goal**

What is your motivation for creating content?

**2. Identify your preferred medium**

Do you prefer writing blogs? Recording videos? Streaming? Podcasting?

**3. Pick a platform that supports your preferred medium**

Look for platforms specializing in your preferred medium, not just the ability to upload the right file format.

**4. Make the content YOU want**

Don't worry about monetization or views. Create based on what you find interesting and would like to share with others.
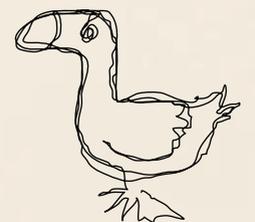
**5. Post your content**

Remember, done is better than perfect. You will improve over time and eventually find what works best for you.

**6. Interact with people**

Make friends and keep going.

*i want content of various animals touring IKEA but i don't think that's relevant to infosec... nor do i own a duck*

# UMM, ACTUALLY...

## This book is incomplete and already out of date

We know. And we still published this. We checked as best as we could, but this world is fast-paced. One of the biggest challenges in any job, tech or not, is keeping up with new apps, new tools, new knowledge, new everything. It's a daunting task, and when you choose to publish something in print, there's always a risk that between the print date and the time the reader receives their copy, a newer thing has already appeared.

If you're always worried about being the most up-to-date, the most complete, the most perfect, you'll be waiting forever. This book is full of useful knowledge, encouragement, and resources that can help people. One of the recurring notions is - just get started. Start small if you have to, just start somewhere. That's what we did with this book, too.

When we first drafted the idea for this format of the InfoSec Survival Guide, we came up with more than 100 different topics, and even more sub-topics within each category. Every time we talked to another person, more topics were added. Making a 300+ page book is a monumental task, so we started with an amount we know how to tackle - the same size as our PROMPT# zines. So a lot got left out... for now.

But we're not done yet.

We need your help.

We asked our community for help on this Survival Guide, and they were a delightfully helpful bunch. But if we want to keep going and make this guide more inclusive of every topic, every specialty, and every helpful nugget we can squeeze in, we need even more help.

If there's a topic you're looking for - ask us for it!
If there's a tool you want to share - share it with us!
If you're an expert and want to contribute - reach out!

*what if I just dress like an expert? I already have that beekeeper suit*

Thank you for taking the time to read what we've compiled and participating in this project. We really mean it when we say we couldn't do it without you.

**Better together.**

## Help us make this guide more complete

*infosecsurvivalguide.com*

*or send in pictures of your pets, they won't go in the guide, but it sure is nice to see floofs and fronds*
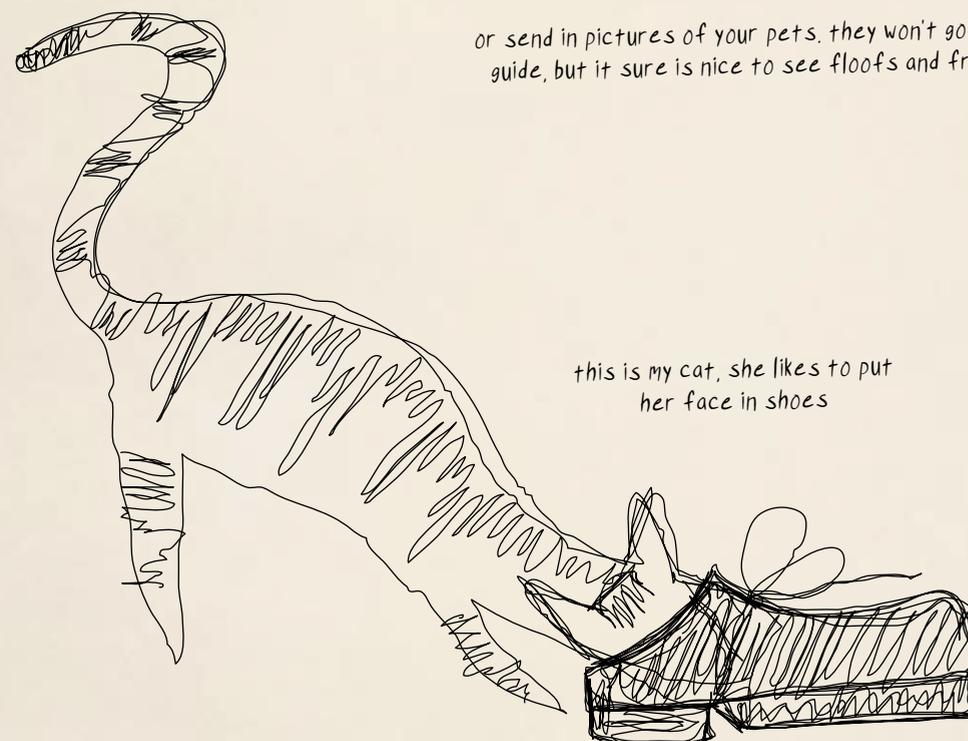
*this is my cat, she likes to put her face in shoes*

# ·■ WHO IS BHIS? ■·

Established in 2008, Black Hills Information Security has created a network of companies in the infosec industry dedicated to providing affordable, outstanding products and services that cover all of your information security needs from pentesting to training.

Each company helps to support the infosec community in their own way; offering free educational content, open-source tools, or even donating to various projects.

## We Offer

- Penetration Testing
- Red Teaming
- Active SOC
- Blue Team Services
- Purple Teaming
- Threat Hunting
- Incident Response
- Consulting
- Training
- IR Tabletop Demos

> **"Our main goal is not to prove that we can hack into a company but to help the customer develop a series of on-point solutions and technologies that will improve the overall security of the company. Testing should never be adversarial, but collaborative."**
>
> *– John Strand, Owner*

## We've worked with

- Credit Unions
- Banks
- Investment Firms
- Higher Education
- Health Care
- Medical Devices
- Insurance
- Law Firms
- Real Estate
- Retail
- Technology
- IT
- Software
- Utilities
- ICS/SCADA

From the smallest mom & pop shops to the biggest Fortune 5 companies, our top priority is helping you understand and achieve your security needs.

## OFFENSIVE

Our team of 40+ pentesters conduct more than 1000 security assessments every year.

Knowledge transfer from our team to yours empowers you to mature and grow, so we take special care in our reporting. Our reports provide you with not only what was successful in an engagement, but also highlight your current strengths by showing what efforts failed.

Our experienced testers help you understand and fortify your own system.

- Penetration Tests
- Red Teams
- Internal
- External
- Pivots
- C2
- Web Apps/APIs
- Mobile
- Physical
- Wireless
- Cloud
- Embedded Device

## DEFENSIVE

To stop an adversary, we must think like one. Let our extensive years of red team experience inform and support your blue team needs.

- Purple Teaming
- Hunt Team Operation Center (HTOC)
- Atomic Controls Assessment
- Compliance
- Audit
- Network Operations Active Directory Consulting
- BHIS Expert Support Team

**ACTIVE SOC:**
- Log Analysis & Active Directory Review
- Adversarial Simulation
- Cyber Deception
- Threat Hunting

## INCIDENT RESPONSE

With experience as both red and blue teams, our IR team knows the ways to hunt down threats and analyze the evidence because we've been on both sides.

Whether you've already been breached, or you're looking to prevent it, we've got you covered.

- Training
- Collection and Analysis
- IR Retainer
- Monitoring
- Consulting
- IR Checklists and Playbooks
- IR Tabletop

**BLACK HILLS | Information Security**

antisyphontraining.com    wildwesthackinfest.com    activecountermeasures.com    rekcahcomics.com    promptzine.com

*bhis.co*

# ▪▫ ANTISYPHON TRAINING ▫▪
## Affordable Education That Doesn't Suck

We're here to disrupt the traditional training industry by providing high-quality education to everyone, regardless of their financial position.

Tailored to beginners and seasoned professionals alike, our training features experienced instructors, full classes, and hands-on labs, at pay-what-you-can prices. From free to full price, or anywhere in between.

**Now everyone can afford high-quality education.**
*antisyphontraining.com*

## Pay-What-You-Can Courses

☐ Active Defense & Cyber Deception
*John Strand*

☐ Introduction to PCI
*Secure Ideas*

☐ Getting Started in Security with BHIS and MITRE ATT&CK®
*John Strand*

☐ Reporting for Pentesters
*BB King*

☐ Getting Started in Packet Decoding
*Chris Brenton*

☐ Professionally Evil CISSP Mentorship Program
*Secure Ideas*

☐ Regular Expressions, Your New Lifestyle
*Joff Thyer*

☐ SOC Core Skills
*John Strand*

☐ Professionally Evil Container Security (PECSEC)
*Secure Ideas*

☐ (PECSEC) – Kubernetes Under Siege: Mastering Penetration Testing Techniques
*Cory Sabol*

☐ (PECSEC) – Fortress Kubernetes: A Comprehensive Guide to Defending and Hardening Kubernetes Systems
*Cory Sabol*

☐ Professionally Evil Application Security (PEAS): Unveiling Server-Side Discovery and Exploitation
*Kevin Johnson*

☐ (PEAS): Mastering Application Reconnaissance and Mapping
*Secure Ideas*

☐ (PEAS): Mastering Client-Side Flaws and Exploitation
*Kevin Johnson*

☐ Professionally Evil API Testing: A Practical Course for Beginners
*Secure Ideas*

☐ Professionally Evil API Testing: AAA and Keys are Not Just for Cars
*Secure Ideas*

☐ Professionally Evil API Testing: GraphQL, SOAP, and REST Fundamentals and Techniques
*Jennifer Shannon*

## Full Course Catalog

☐ L ⊙D Advanced Endpoint Investigations
*Alissa Torres*

☐ L Advanced Network Threat Hunting
*Chris Brenton*

☐ L Alternative & Advanced Search Engine Intelligence (AASEI)
*Joe Gray*

☐ ⊙D Attack Emulation Tools: Atomic Red Team, CALDERA and More
*Carrie Roberts*

☐ ⊙D Bash Scripting for Server Administration
*Bill Stearns*

☐ L ⊙D Breaching the Cloud
*Beau Bullock*

☐ L ⊙D Defending the Enterprise
*Kent Ickler and Jordan Drysdale*

☐ L ⊙D Enterprise Attack: Initial Access
*Steve Borosh*

☐ L Enterprise Attacker Emulation and C2 Implant
*Joff Thyer*

☐ L Enterprise Forensics and Response
*Gerard Johansen*

☐ ⊙D Foundational Application Security Training (FAST)
*Secure Ideas*

☐ L Foundational Data Protection Training (FDPT)
*Secure Ideas*

☐ L ⊙D HackerOps
*Ralph May*

☐ L ⊙D How to be Irresistible to Hiring Managers
*Kip Boyle*

☐ L Incident Response Foundations
*Derek Banks*

☐ L Intro to Offensive Tooling
*Chris Traynor*

☐ L Introduction to Industrial Control Systems
*Ashley Van Hoesen*

☐ L ⊙D Introduction to Pentesting
*John Strand*

☐ L ⊙D Introduction to Python
*Joff Thyer*

☐ L Linux Command-Line For Analysts and Operators
*Hal Pomeranz*

☐ L ⊙D Linux Forensics
*Hal Pomeranz*

☐ L ⊙D Modern WebApp Pentesting
*BB King*

☐ L ⊙D Network Forensics and Incident Response
*Troy Wojewoda*

☐ ⊙D OWASP Top 10
*Jim Manico*

☐ ⊙D OWASP Top 10
*Kevin Johnson*

☐ L ⊙D PowerShell for InfoSec: What You Need to Know!
*Carrie Roberts*

☐ L Professionally Evil Network Testing (PENT)
*Eric Kuehn or Nathan Sweaney*

☐ L ⊙D Securing the Cloud Foundations
*Andrew Krug*

☐ ⊙D Security for MSPs
*John Strand*

☐ L ⊙D Security Leadership and Management
*Chris Brenton*

☐ L ⊙D SELinux
*Hal Pomeranz*

Live L
On-demand ⊙D

Subscribe to PROMPT# for free!

but Noah said to never
trust QR codes...

Brought to you by:

# BLACK HILLS | Information Security

antisyphontraining.com   wildwesthackinfest.com   activecountermeasures.com   rekcahcomics.com   promptzine.com

*bhis.co*

## MADE BY AND FOR THE COMMUNITY