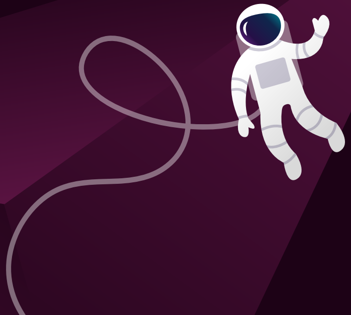
THE LIFELONG ADVENTURE OF LEARNING CYBER SECURITY & DFIR

By @j3st3rjam3s



HELLO!

My Name Is JAMES KAINTH

I am here to talk about how I got to here ;)

You can find me at @j3st3rjam3s

jameskainth.com

1878

DISCLAIMER

- There Is More Than One Way To Do It.
- I can give you advice, tips, and tricks, but you and only you can fuel the fire inside to keep going for what I can only hope, will be an adventure for you as it is for me.
- Mental Health Is Important, Take Care of Yourself. Burnout is real. Imposter Syndrome is real.

WHERE ARE YOU?

Phase 1

Beginner

Phase 2

Intermediate

Phase 3

“Advanced”

PAUSE - LET'S TALK FOR A SECOND

- What are your goals?

- Where do you see yourself in 1, 2, 3, years?
- Do you have a position you're aiming to be in?
- Being Human, S.M.A.R.T , kind with yourself

PHASE 1.
STARTING OUT/BEGINNER

MASTER THE FUNDAMENTALS!
& EMBRACE THE FIREHOSE*

[illegible] t overwhelmed [illegible] e having
[illegible] learning

LET'S GET STARTED!

- Computer Networking (Subnetting, Routing, Firewalls, NAT, Packet Tracer, TCP/IP, Wireshark/TCPDump), Python(or any starter programming language), Active Directory & DNS

- Network/System Administration (Powershell, Bash, Large Scale Automation, Ansible, Docker, Kubernetes, Chef, etc.), Set Up Your Own SIEM (Splunk, Elastic Stack)

- Set Up Your Own Lab Environment! [Cloud, Virtual (Vmware/VirtualBox/Parallels), Physical]

STAYING UP TO DATE

- Feedly (Get All Your News In One Place and read it 5 times as fast) #NotASponsor
- Podcasts (The Cyberwire, Recorded Future, Hacked: Into The Minds of cyber security Leaders, Darknet Diaries)
- Embrace New Technologies Because TBH You Have No Choice 😂

EVERYTHING ADDS UP - SO START WITH A STRONG FOUNDATION

"Compound interest is the eigth wonder of the world.

He who understands it, earns it...
He who doesn't...
pays it."

- Albert Einstein

Read 500 pages every day. That's how knowledge works. It builds up like compound interest.

— Warren Buffett —

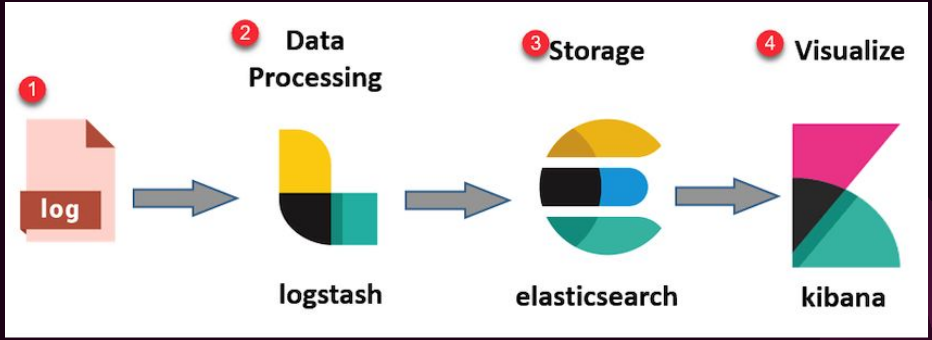
An investment in knowledge pays the best interest.

(Benjamin Franklin)

"The most important thing to do is start investing now so you can unlock the power of compounding."

DON'T DELAY
START THREAT HUNTING TODAY!

- Set Up An Elastic Stack In a Virtual Lab
- Learn about LOLBAS(Living of the Land Binaries and Scripts) because you'll start to see them now on your own computer.

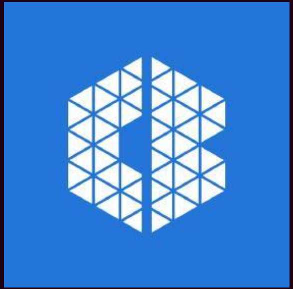


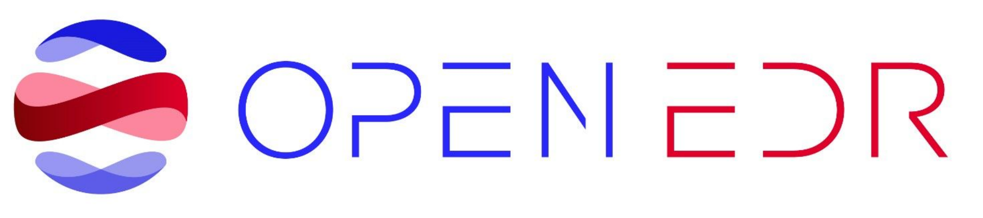
PHASE 2.
INTERMEDIATE

GOING FROM PADAWAN TO JEDI KNIGHT

- *PenTesting(HackTheBox, OWASP10)*
- Security Operations (SIEMS, EDR/MDR, More Log Analysis)
- Purple Teaming & DF Analysis (Deadbox 4n6, Memory, Event Logs)
- Threat Intelligence [APTs(Advanced Persistent Threats), Indicators of Compromise (IoCs), Tools Tactics and Procedures (TTPs)

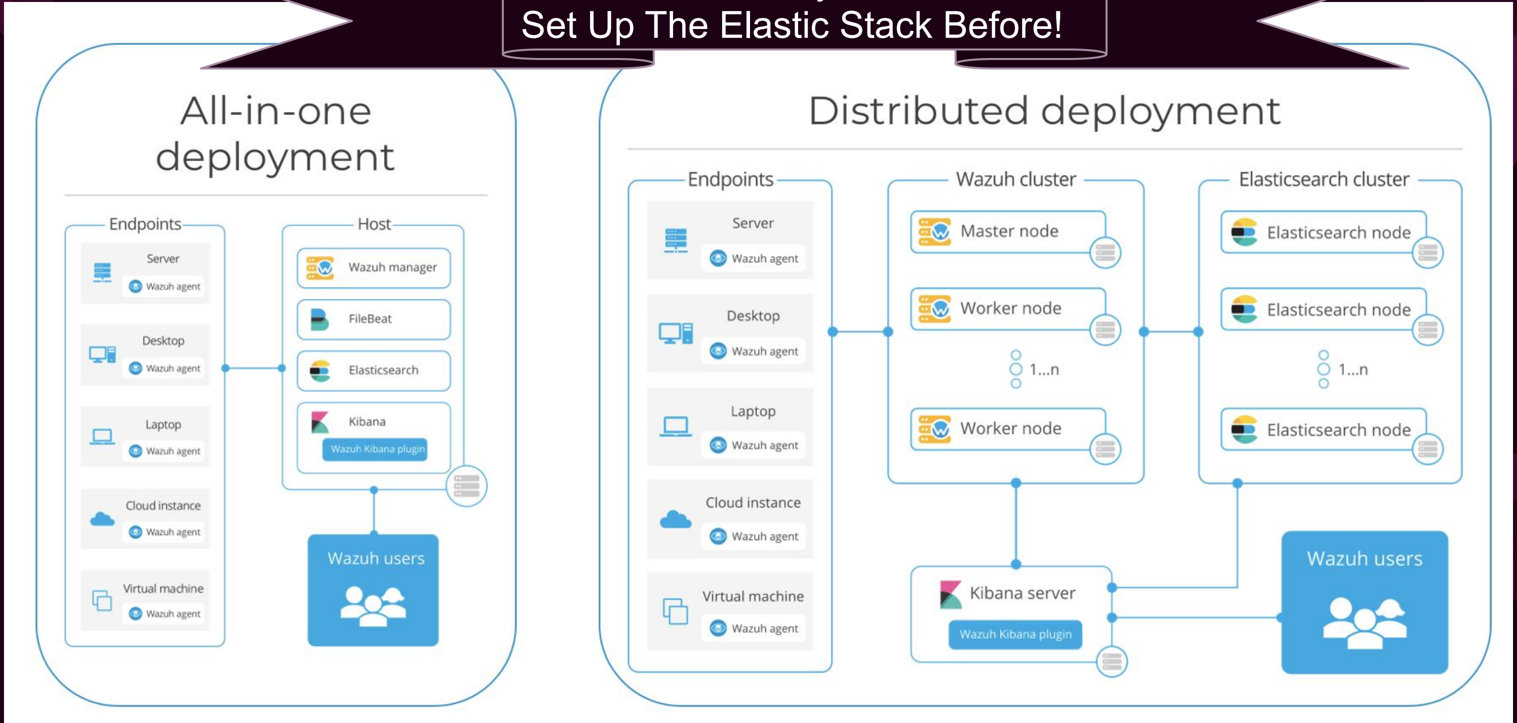
SECURITY OPERATIONS - MONITORING THREATS PROACTIVELY & IN REALTIME





YOUR SECURITY OPERATIONS: EVOLVING FROM SIEM TO EDR

Half of It Is Already Built B/c You Set Up The Elastic Stack Before!



PURPLE TEAMING & DF ANALYSIS

- Purple Teaming (Red Team A VM You Set Up)
- Deadbox Forensics
  - Registry
  - Event Logs
  - Amcache
  - ++ SO MANY MORE ARTIFACTS
- Memory Forensics
- IoCs (Indicators of Compromise) & Yara Rules
- You never know what data you'll have

ACCESSDATA
ForensicToolkit (FTK)

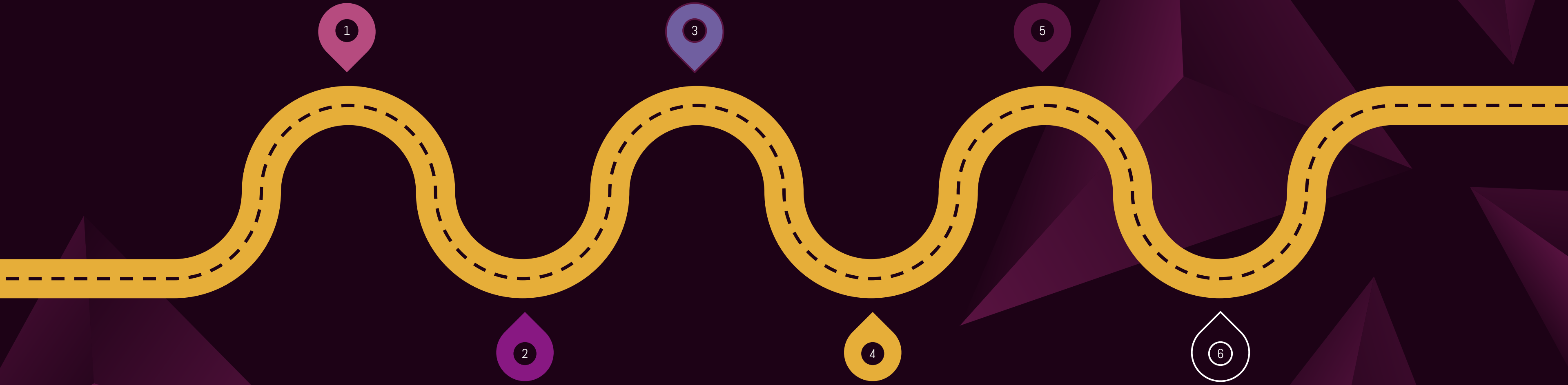
Autopsy

ARSENAL RECON

Loki
SIMPLE IOC AND INCIDENT RESPONSE SCANNER

VOLATILITY

PLOTTING A COURSE FOR SUCCESS



1 Computer Networking

2 Network/System Administration

3 Break & Reinforcement

4 Security Operations

5 Purple Teaming & Digital Forensic Analysis

6 There's No Turning Back Now (͡° ͜ʖ ͡°)

LEVELING UP!

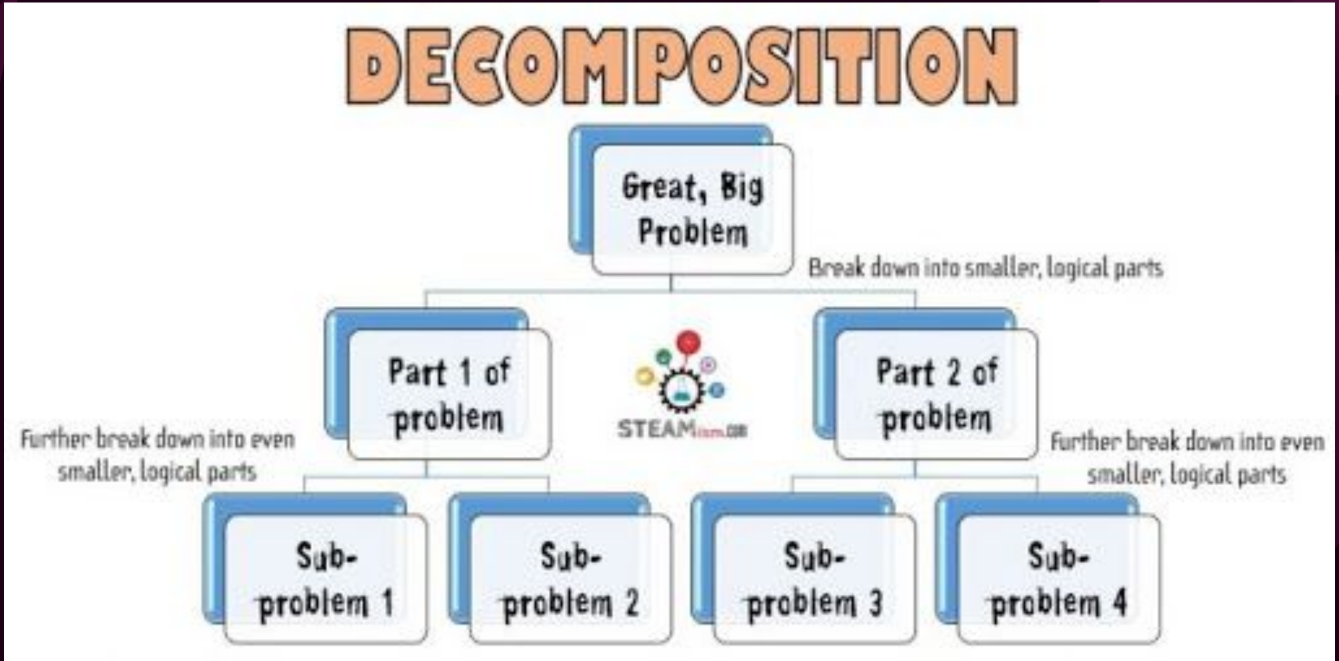
- Learning New Tools & Building Your Tool Box
- Incident Response & Triage
- Processes & Procedure (Mindset/CYA)
- Crisis Management (Mindset)
- Finding a Job & Team that fits
- You can see see your *potential* & what's next, while also being able to appreciate how far you've come

FINDING A JOB

- Networking (LinkedIn, Twitter, Community Discords)
- Home Lab, Testing and Practice Environment
- Take Advantage of Free SANS Resources
- There’s a lot of free resources out there
- Communication (“People don’t buy what you do, they buy why you do it” - S.S.)
- Talk To Me (I will personally help you, I was a peer career coach in college)

IMPOSTER SYNDROME

- Befriend it(“Hey Fear, I know you're just looking out for me, but you're not needed right now. I can take it from here.”-E.G.)
- Understand where it comes from
- Visualize Success and validate yourself when you progress towards it. Reward yourself
- Leverage Psychology [CBT - ACT(Acceptance and Commitment Therapy)]



DECOMPOSITION

Great, Big Problem

Break down into smaller, logical parts

Part 1 of problem

Part 2 of problem

Further break down into even smaller, logical parts

Further break down into even smaller, logical parts

Sub-problem 1

Sub-problem 2

Sub-problem 3

Sub-problem 4

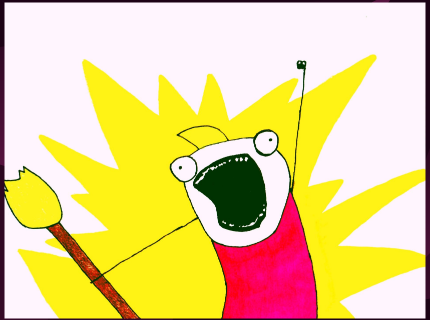
GETTING BETTER AT WHAT YOU DO MEANS YOUR PROBLEMS WILL GET TOUGHER. THAT’S THE NATURE OF GROWTH

PHASE 3.
“ADVANCED”

Let’s go I got this, let me learn ALL THE THINGs!

BECOMING A JEDI MASTER REQUIRES "ADVANCED" RESEARCH

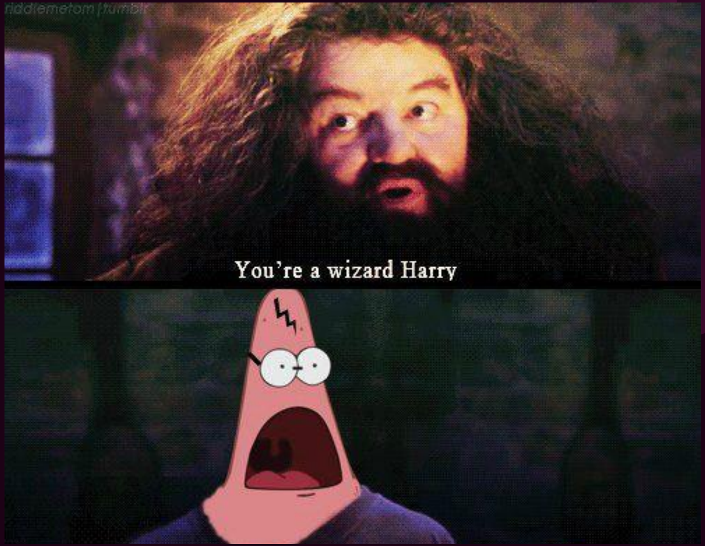
- Time (Be patient)
- 4n6 All The Things!
- Reverse Engineering
- Red Teaming & Exploit Development
- Niche DFIR
- Case By Case Weirdness (Testing Things In a Lab)
- Curiosity & Exploring

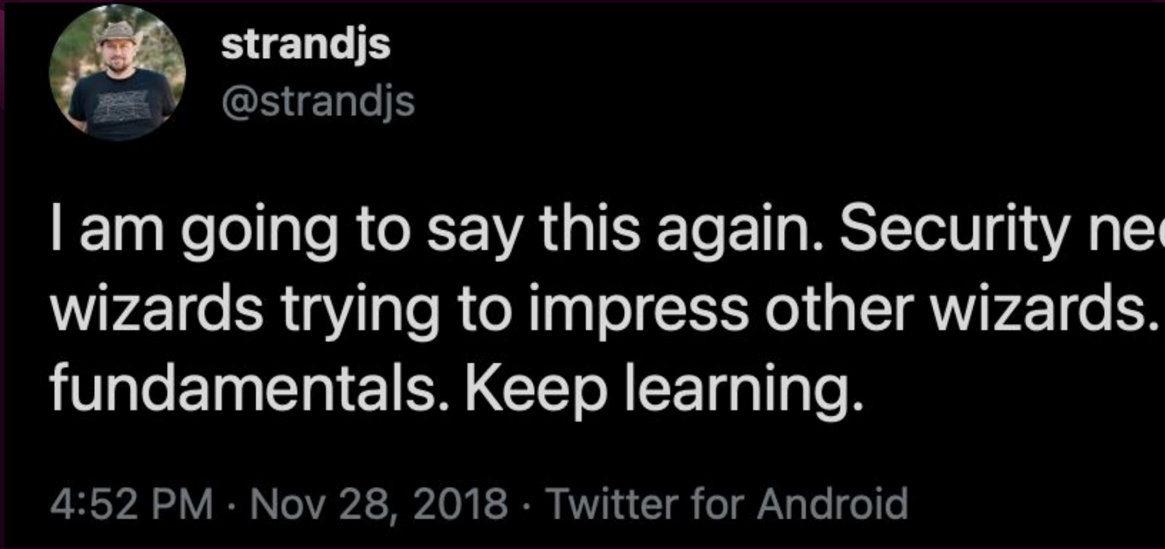


NICHE DFIR

- ICS (Industrial Control Systems)
- Drone
- Mobile Device
- IoT
- Cloud
- Blockchain
- SO MANY NICHES With Not Enough Support!
- MORE ARE ON THE WAY! (Technology progresses - Quantum Computing, AI/ML, etc.)

“ADVANCED” (WHY QUOTES?)



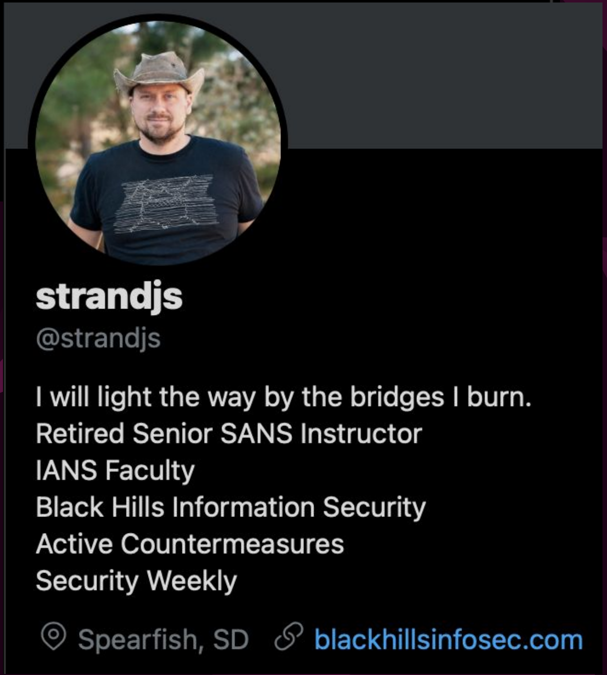


strandjs
@strandjs

I am going to say this again. Security needs to stop being wizards trying to impress other wizards. Focus on the fundamentals. Keep learning.

4:52 PM · Nov 28, 2018 · Twitter for Android

FUNDAMENTALS NEVER CHANGE! (usually ;) Think TCP/IP & RFCs for Protocols

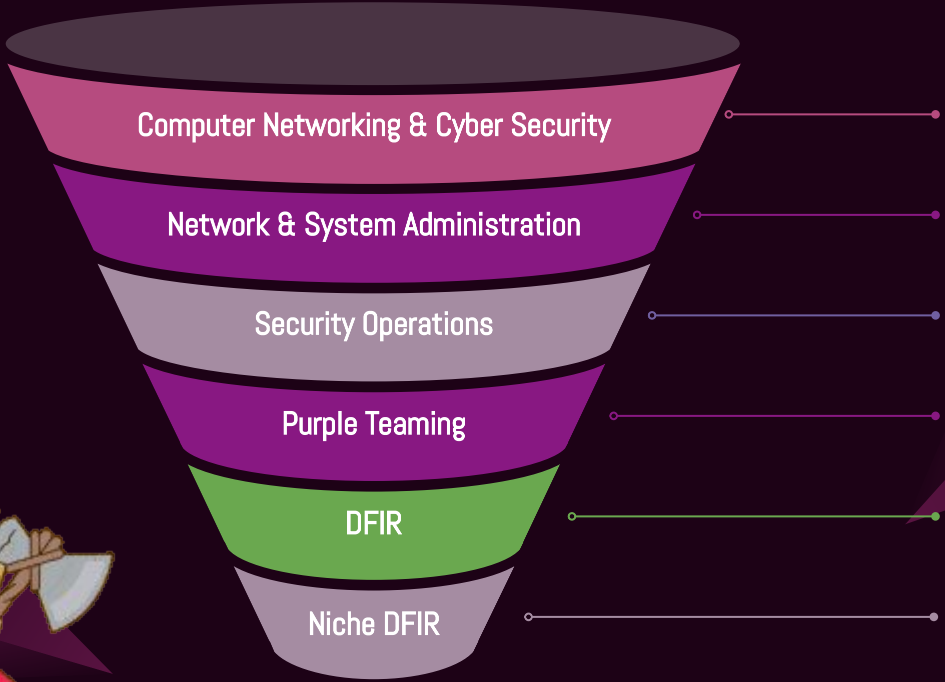


strandjs
@strandjs

I will light the way by the bridges I burn.
Retired Senior SANS Instructor
IANS Faculty
Black Hills Information Security
Active Countermeasures
Security Weekly

Spearfish, SD blackhillsinfosec.com

LET’S RECAP



Computer Networking & Cyber Security

(Subnetting, Routing, Firewalls, NAT, Packet Tracer, TCP/IP, Wireshark/TCPDump), Python(or any starter programming language), Active Directory & DNS, PenTesting

Network & System Administration

(Powershell, Bash, Large Scale Automation, Ansible, Docker, Kubernetes, Chef, etc.), SIEMs (Splunk, Elastic Stack) Log Analysis

Security Operations

SIEMS, EDR/MDR, More Log Analysis

Purple Teaming

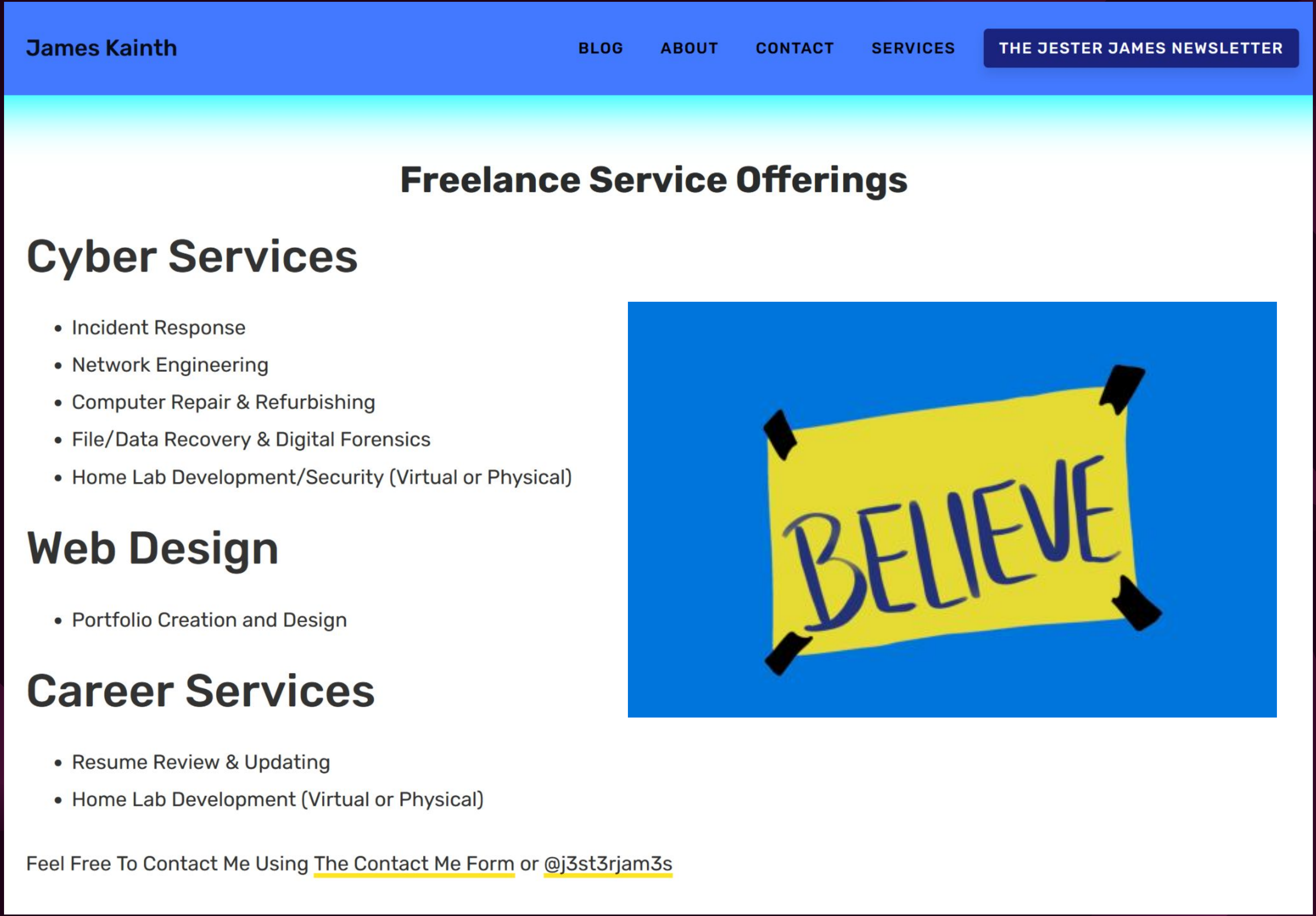
Red Team (PenTesting) and Blue Teaming (Forensicating) Your Own Systems for practice, research, and discovery of artifacts

DFIR

Deadbox Forensics, Registry Analysis, Event Logs , Amcache, ++MANY MORE ARTIFACTS, Memory Forensics IoCs (Indicators of Compromise), Yara Rules

Niche DFIR

Industry Specific, Research Oriented, Very Specific Built on Foundations



James Kainth

BLOG ABOUT CONTACT SERVICES THE JESTER JAMES NEWSLETTER

Freelance Service Offerings

Cyber Services

- Incident Response
- Network Engineering
- Computer Repair & Refurbishing
- File/Data Recovery & Digital Forensics
- Home Lab Development/Security (Virtual or Physical)

Web Design

- Portfolio Creation and Design

Career Services

- Resume Review & Updating
- Home Lab Development (Virtual or Physical)

Feel Free To Contact Me Using The Contact Me Form or @j3st3rjam3s

QUESTIONS & THANK YOU!

Remember “The Fact That We Acknowledge Our Potential Makes It That Much Closer To Reality”

Keep In Touch @j3st3rjam3s

JamesKainth.com

The Jesters Castle on Youtube!

https://bit.ly/TheJestersCastle

https://y.at/🐧😜💻

IMAGE SOURCES

https://assets.pokemon.com/assets/cms2/img/pokedex/full/007.png

https://cdn2.bulbagarden.net/upload/0/0c/008Wartortle.png

https://cdn2.bulbagarden.net/upload/thumb/0/02/009Blastoise.png/1200px-009Blastoise.png

https://assets.pokemon.com/assets/cms2/img/pokedex/full/004.png

https://cdn2.bulbagarden.net/upload/4/4a/005Charmeleon.png

https://assets.pokemon.com/assets/cms2/img/pokedex/full/006.png

https://cdn2.bulbagarden.net/upload/2/21/001Bulbasaur.png

https://cdn2.bulbagarden.net/upload/7/73/002Ivysaur.png

https://cdn2.bulbagarden.net/upload/thumb/a/ae/003Venusaur.png/1200px-003Venusaur.png

https://cdn.business2community.com/wp-content/uploads/2016/07/fundamentals-dont-change-1.png

https://emjayandthem.files.wordpress.com/2015/09/information_hose.jpg

https://www.chrisbell.com/images/compound-interest-quotes.png

http://pm1.narvii.com/6117/1218db362feb3be6abf131e68837d73ae63da1ba_00.jpg

IMAGE SOURCES

https://lh3.googleusercontent.com/proxy/HFw_Wd3zekwVaHX869_g6iNYkRjVpQfp9BQgm3UAiWqshp_c7mCqw3I5iAGovjM5OhPacJVPqFbAGMA0vbcAlhy_URXhWhb-gfOVpU191sNj9ckyWc7LyK35wEqdNmnNGizJllc_o7E

https://funvizeo.com/media/memes/d237fdc1f2ad0f17/7-youre-a-wizard-harry-did-stutter-meme-d7d3237afde558fd-da866c3e88faf308.jpg

https://i.pinimg.com/originals/0f/25/66/0f256661c9eb97e2d41b65a716a89418.jpg

https://i.pinimg.com/originals/3e/4c/e2/3e4ce263a285c6a81df3551a74841721.jpg

https://pbs.twimg.com/profile_images/497252082106122240/DsFZEZlE_400x400.png

https://pbs.twimg.com/profile_images/1071486739632525314/_OgA3_qy.jpg

https://www.recordedfuture.com/assets/google-results-logo.png

https://www.kroll.com/-/media/kroll/images/headshots/directors/eric-zimmerman.jpg

https://volatility3.readthedocs.io/en/develop/_static/vol.png

https://i.kym-cdn.com/photos/images/original/000/095/610/demotivational-posters-oh-god.jpg

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSkp0l8sdoaX3i45bERq4x1u62H-IFrlZdUJKVldVoZWapB_w2N2Md1P5dZx5Y_hqSGHvM&usqp=CAU

https://3.bp.blogspot.com/-dmIFjUe-m_o/Vym1T87pOOI/AAAAAAAAD04/HGT0fkWnKwY11efIBWB8WDvC-DnSxUROACLcB/s1600/IMG.jpeg

https://pbs.twimg.com/media/EbSwmMKVAAAqJDh.jpg

IMAGE SOURCES

https://media-exp1.licdn.com/dms/image/C4E0BAQFXP6rIfo489A/company-logo_200_200/0/1524076923596?e=2159024400&v=beta&t=M5Y0EMcjtWFOGA2Vi2EuK4m4HOaGU4Q3e-UkMpMW2LY

https://documentation.wazuh.com/current/installation-guide/index.htm

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSR-63l-dmal47_5krM07ulfE9umSQAGzR-N4d0flA-sNshqQ4-zu05vOesKS73iTKa99s&usqp=CAU

https://cloudprotectionworks.com/images/icons/falcon-shield-red-darkred.png

https://avatars.githubusercontent.com/u/2071378?s=280&v=4