SALES ENGINEERING AND GETTING INTO INFOSEC

- Adrian Kaylor

WHAT WOULD YOU SAY, YOU DO HERE?

- Sr Sales Engineer at Splunk
- The nerd they bring in to talk to the other nerds

- Discovery – Is this an opportunity worth pursuing?
- Demo – See how cool our stuff is?
- Proof of Concept (POC) – It even works for you!
- Renewal – Check in before the bill shows up

MY CAREER PATH

- Laptops and printers
- Helpdesk
- Network admin
- Trainer
- Product support
- Product Management
- Sales Engineer
- Formal education
- Certifications

OTHER PATHS TO SALES ENGINEERING

CUSTOMER TECHNICAL SUPPORT

CONSULTING

SALES DEVELOPMENT

SOC ANALYST

LAW ENFORCEMENT / MILITARY

BEING AN SE

- Get to talk to LOTS of customers
  - Facebook, Twitter, Google, SalesForce, Oracle, Pixar, VMware, Gap, Levi, Nvidia, Fitbit, PAN, Chevron, Dolby Labs, Electronic Arts, NetFlix, Pandora, PayPal, eBay, Square, Kaiser, McKesson, Dropbox, Pinterest, LinkedIn, Uber, Workday, Yahoo!, Adobe, Autodesk, New Relic
- Learn -> Explain -> Improve
- Work from home and extremely flexible
- The compensation is incredible.

SOFT SKILLS

ART OF THE DEMO

RESPONSIVENESS AND FOLLOW-UP

LISTEN MORE, ASK MORE QUESTIONS

FRAMING SOLUTION

TALK PRETTY

TECH SKILLS – HOME LAB

- PICTURE OF MY HOME LAB
- VMWARE'S ESXI HAS A FREE LICENSE
- XEN, DOCKER, KVM, AWS, AZURE, DIGITAL RIVER, ETC
- LINUX, LINUX, LINUX…AND SOME WINDOWS AND MAC

TECH SKILLS – SPEND TIME IN THE CLOUD

- Learn about AWS. Abuse that free year
- Azure - Don't underestimate Microsoft
- Other VPS providers like Digital Ocean
- Google Cloud - meh

TECH SKILLS - NO EXPERIENCE? NO PROBLEM.

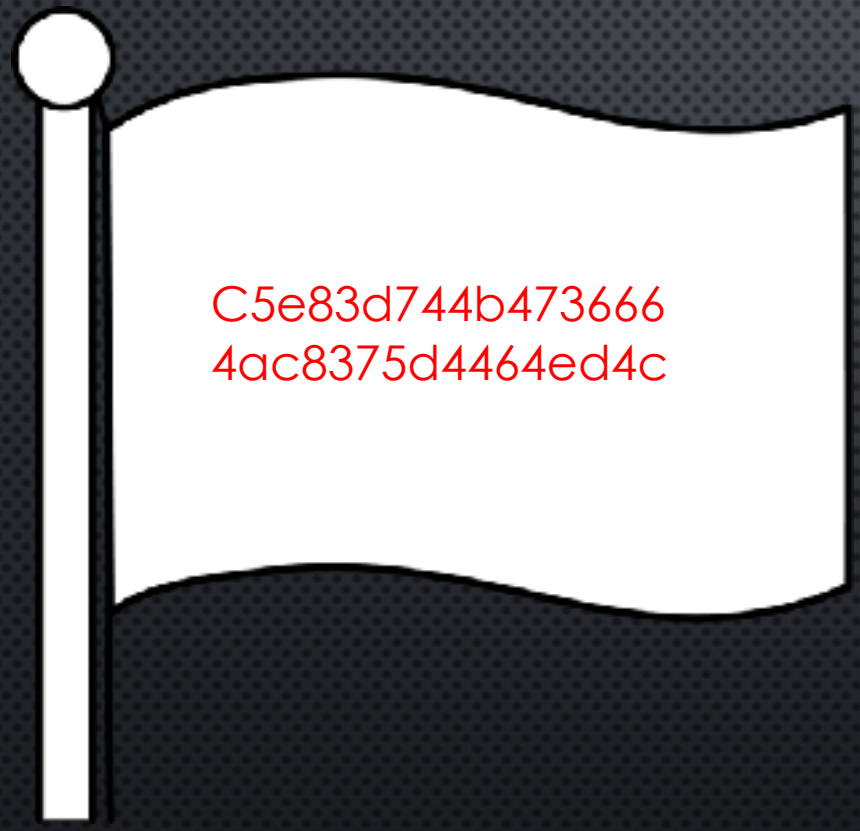
Deploy real stuff in your home lab

- SIEM like Splunk or….no, just use Splunk
- IDS/Network analysis- Bro, Suricata
- Config control - Puppet, Chef, Ansible
- Vuln Scan – Nessus, OpenVAS
- Firewall - pfSense
- EDR - osquery, GRR
- SOAR - Phantom, Demisto
- Web App Sec – OWASP, OWASP, OWASP
- Kali on a chromebook

Tech Skills – Talk Frameworks

- Lockheed-Martin Cyber Killchain
  - https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- CIS Critical Controls
  - https://www.cisecurity.org/controls/
- MITRE ATT&CK
  - https://attack.mitre.org/

CTF – Capture the Flag



- What/why is/to CTF?
- Attack and Defense
  - Most people think of these, Red vs Blue
  - Teams at a con
- Jeopardy
  - Also played at con's
  - Solo'able
  - Vendor and project based
- Security Games and Other stuff

What/Why is/to CTF?

- Incredible amount of fun
- If you win then other people lose!
- Humbling and motivating
- Very common recruiting tool

CFT – Attack and Defense

- No idea, never did one.
- Find a team and learn a specialty
  - Crypto
  - Exploit creation
  - Reversing binaries
  - Network analysis
  - Web apps
- Look for Academic teams
  - Like……WRCCDC
- r/securityctf/ or https://ctftime.org/

CTF – JEOPARDY

- Vendor run
  - Splunk Boss of the SOC, Boss of the NOC
- Community run
  - https://www.holidayhackchallenge.com/2018/
- Solo
  - Vulnhub.com
  - Pentesterlab.com
- Careful what you search for
  - Read write ups and blog posts later

CTF - GAMES

- All the "Learn to Hack" stuff
- Tend to be more instructional
- Check out OverTheWire.org, root-me.org, wechall.net/active_sites, etc
- flaws.cloud
- Except Pwn Adventure 3: Pwnie Island
- Wireless CTF
- SANS Holiday Hack Challenge or….KringleCon
  - https://kringlecon.com/

$&#@ THE NCAA, TURN PRO NOW.

- Bug Bounty programs can be zero barrier to entry
- Bug Crowd
- HackerOne
- SynAck

MAKE FRIENDS AND LEARN STUFF

- DEFCON
  - MOST MAJOR CONF OF THE YEAR
  - RELATIVELY CHEAP, $250-ISH
  - TRAVEL AND LODGING WILL KILL YOU
  - MAKE FRIENDS AND CARPOOL/SHARE ROOMS
- BSIDESSF
  - BEFORE RSA
  - CHEAP - $25-ISH
  - LOCAL
- VOLUNTEER AND GET IN
- GO TO LOCAL STUFF
  - MEETUP
  - OWASP, ISSA, ETC
  - HAK5 MAILING LISTS
- WATCH RECORDINGS ON IRONGEEK.COM
- YOUTUBE.COM/LIVEOVERFLOWCTF

I've been your presenter and I've been great.

- Adrian Kaylor
- akaylor@gmail.com

- If you only do one thing, read this…
- https://tisiphone.net/2015/10/12/starting-an-infosec-career-the-megamix-chapters-1-3/

FIELD INTERN PROGRAM

Sales Engineering

Training and Certification

Customer Facing Experiences

Technology and Analytics Project

- Every SE Intern will participate in Splunk Enablement Training
- Training will include product, technical and “soft” skills development
- SE Intern On-boarding will include:
  - Self-guided Splunk product training
  - EDU led product training
  - SE Bootcamp and Certification Training

Virtual Team Rotation

- Interns will become part of the SE Virtual Team
- Support the Virtual Sales Team
- SE Interns will rotate through domain groups:
  - Core, ITOA, Security, etc.
- Aim for Interns to deliver the Weekly Web Demos

P

- Interns will select, develop, document and present a project for the summer Internship
- Sample topics will be provided, or Interns can propose projects to Mentors
- Project work is meant to supplement training, enablement and customer facing work
- End of Program Summit:
  - Interns will meet and deliver TED talks on their projects