CYBERSECURITY WORKSHOP AGENDA

feat. defense against the dark cyber arts

by Vitaly Ford @ Arcadia University

July 2026

Big Picture

DAY 1

Intro, grant housekeeping, pre-workshop survey, core cyber concepts, cyber.org registration, OS security, intrusion detection

3

DAY 2

Sniffnet, pentesting (ethical hacking), OSINT, social engineering, simple malware analysis

24

DAY 3

Passwords (manager, hash, salt) & MFA, VPN, zero-trust model, backups, TryHackMe rooms

32

DAY 4

Speaker, cryptography, Linux, bash scripting, Capture The Flag (CTF), cyber competitions

36

DAY 5

Wi-Fi security, ethics and privacy, CTF Unplugged, unplugged exercises from teaching materials, famous hacks, VirtualBox/VMWare Workstation & Fusion and Kali Linux installation, feedback, closing

53

DAY 1

Intro, grant housekeeping, pre-workshop survey, core cyber concepts, cyber.org registration, OS security, intrusion detection

whoami

Introductions

Why are we here?

Structured and spontaneous scaffolded learning

Joint NSF Grant: Elmhurst University & Arcadia University

Grant Housekeeping

- Stipend ($400, prorated based on the attended ## hours) after the workshop ends
  - You will send W-9 directly to our Accounts Payable, and I will take care of the check requests
  - Stipend will be prorated based on the completed hours
- Up to 36 CE hours, reported to PDE at the beginning of August
- Availability of an extra $225 to register a student team at the Cyber Patriot competition
- Pre- and post-surveys (today and in the fall, respectively)
- Teaching materials
  - Each topic with a lesson plan, quiz [Kahoot-ready], homework, exercise, and slides
  - Also available as an online self-paced platform at https://cysia.vford.com (work-in-progress)
- Free existing resources outside of the grant, like cyber.org

CE Hours and PPID

- At the end of workshop week:
  - Signature list with your PPID if you need the hours to be registered
  - PPID can be found at

    https://www.perms.pa.gov/screens/wfpublicaccess.aspx
  - Hours will be sent to MCIU
  - MCIU will provide them to PDE

PRE-WORKSHOP SURVEY

bit.ly/4vu6yZs

AGENDA SLIDES:

vford.com/cyber.pdf

BIT.LY LINK GOES TO:

https://elmhurst.co1.qualtrics.com/jfe/form/SV_0cG1BBuzUGafXdc

Cybersecurity Careers

- Refer to https://www.cyberseek.org

Teaching Materials Google Drive Folder

- https://drive.google.com/drive/folders/1XCEZ2DmGTV_k-Bda59eHQV12IF6NAOy6

Cyber.org: Cyber Range Registration

- Refer to the Cyber.org teaching materials available in the previous slide's google folder
  - Direct link: https://drive.google.com/drive/folders/1M_L5NQ_WegqP2jjZYjGwlblBrFcYSfvx

“Hacker” Terms (ex. FB market)

- Threat
- Vulnerability
- Exploit
- Attack (passive/active, software/hardware/network/human)
  - Refer to:
    - https://attack.mitre.org
    - https://www.shodan.io/dashboard with search queries like `has_screenshot:true camera` and https://github.com/jakejarvis/awesome-shodan-queries

Core Cyber Concepts (ex. Website)

- CIA Triad (Confidentiality, Integrity, Availability)
- Authentication/authorization
- Non-repudiation
- Defense in Depth
- Secure by Design
- Least Privilege
- Risk Management (identify, impact, mitigate, monitor)
- User Education
- Zero Trust

Operating System (OS) Security

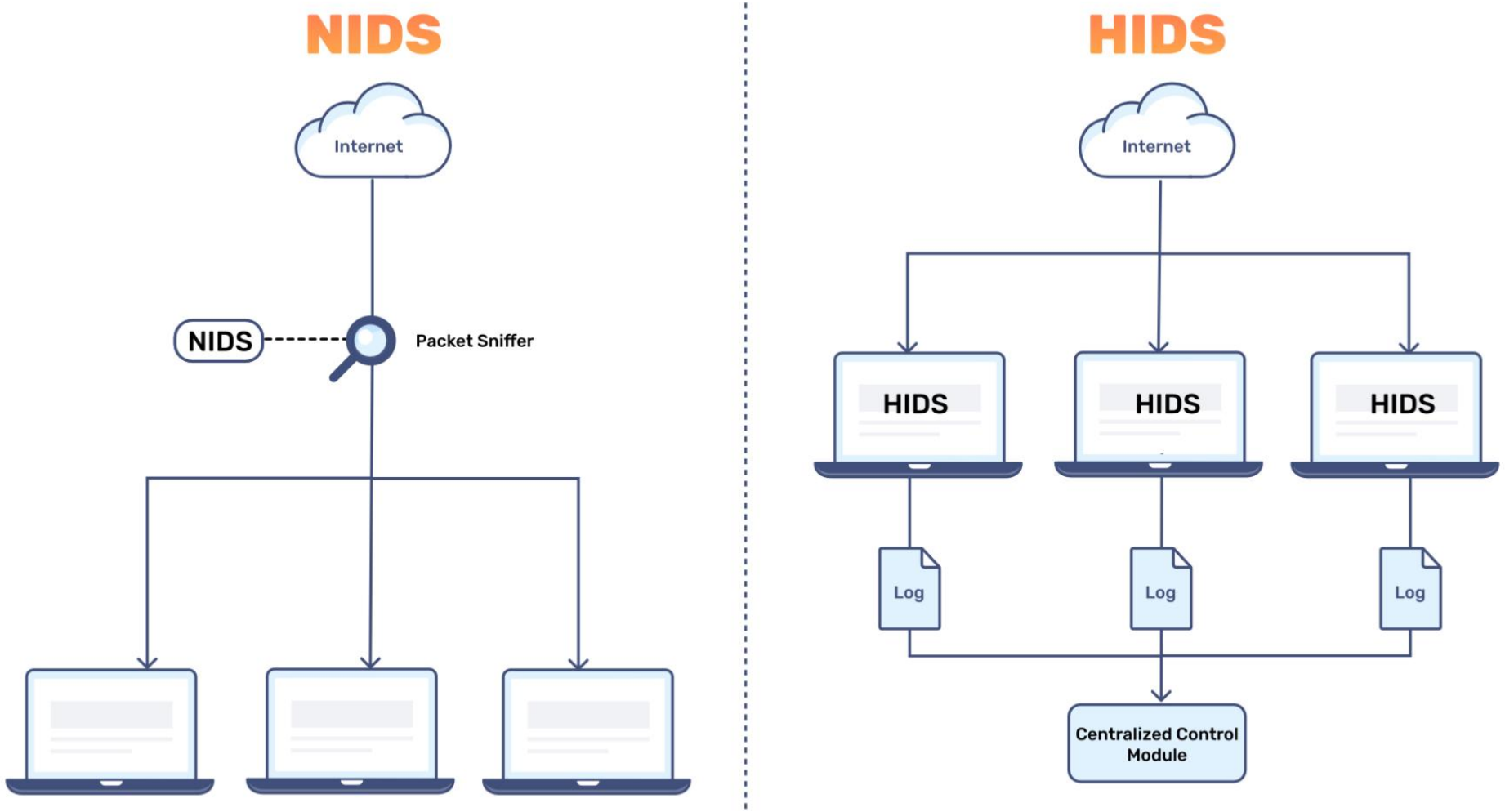
- How do people get hacked in the first place?
  - Refer to phishing, smishing, vishing, and malware teaching materials
- Default antivirus
- Free on-demand virus scanners (BitDefender*, Malwarebytes*)
- Firewall VS anti-virus
  - Intro to networking concepts: IP, port, host, network
  - Refer to the How the Internet Works teaching material and https://netflow.vford.com
- Adblocker (uBlock Origin; uBlock Origin Light for Chrome) or Brave Browser/DuckDuckGo (for mobile too)
  - But why?
- User/admin access/permissions/local security policies
- Domain-level restrictions
- Storage encryption, BIOS/UEFI password, TPM (Trusted Platform Module)
- Startup executables & sysinternals for Windows (or objective-see for MacOS)
- Windows Defender advanced settings

Defenses Against Intrusions

- IDS (Intrusion Detection System)
  - HIDS/NIDS (Host/Network-based Intrusion Detection System)
- IPS (Intrusion Prevention System)
- EDR (Endpoint [threat] Detection and Response)

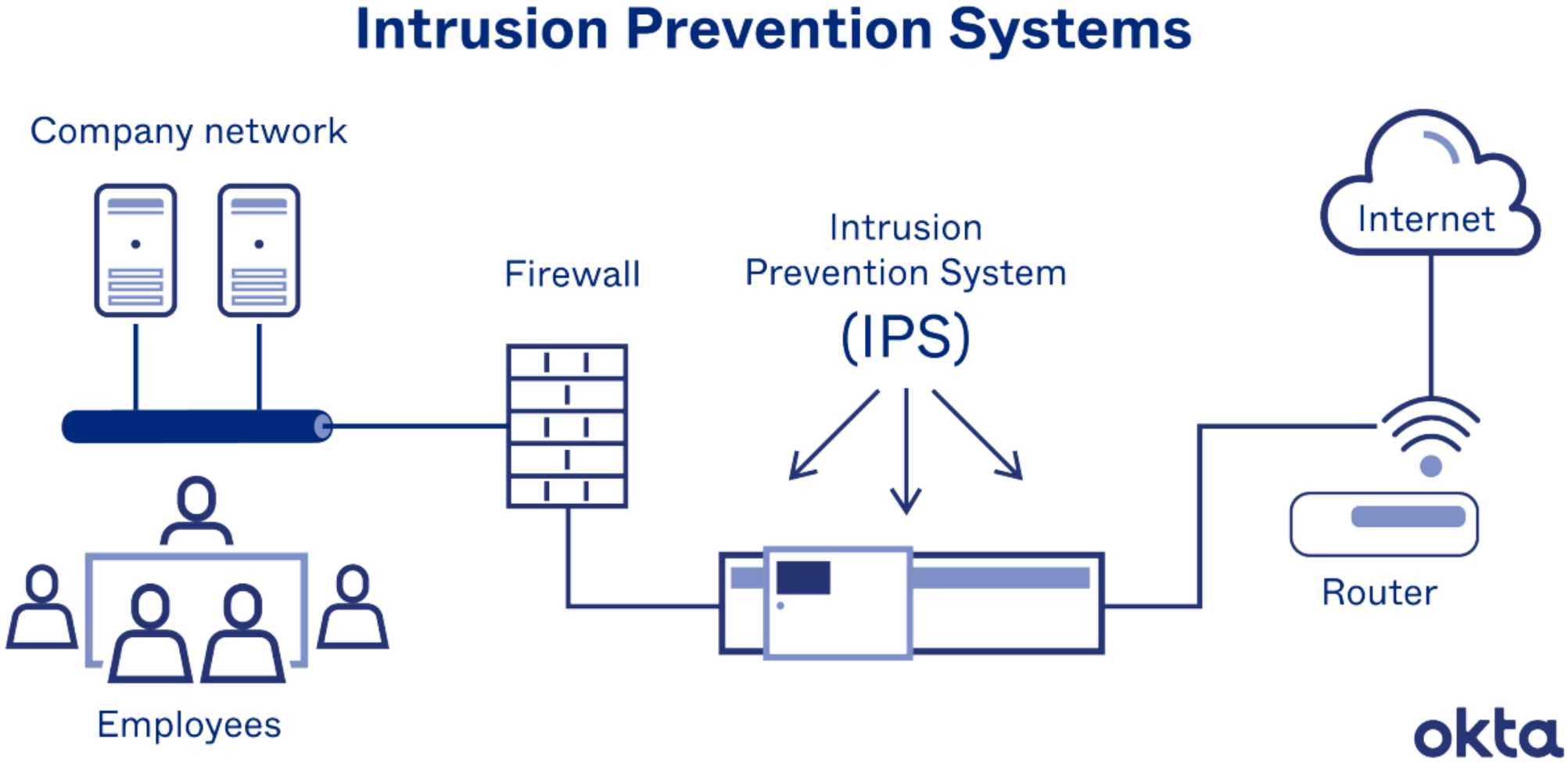
- XDR (Extended Detection and Response)
- SIEM (Security Information and Event Management)
- SOAR (Security Orchestration, Automation, and Response)
- SOC (Security Operations Center)

IDS (HIDS/NIDS)



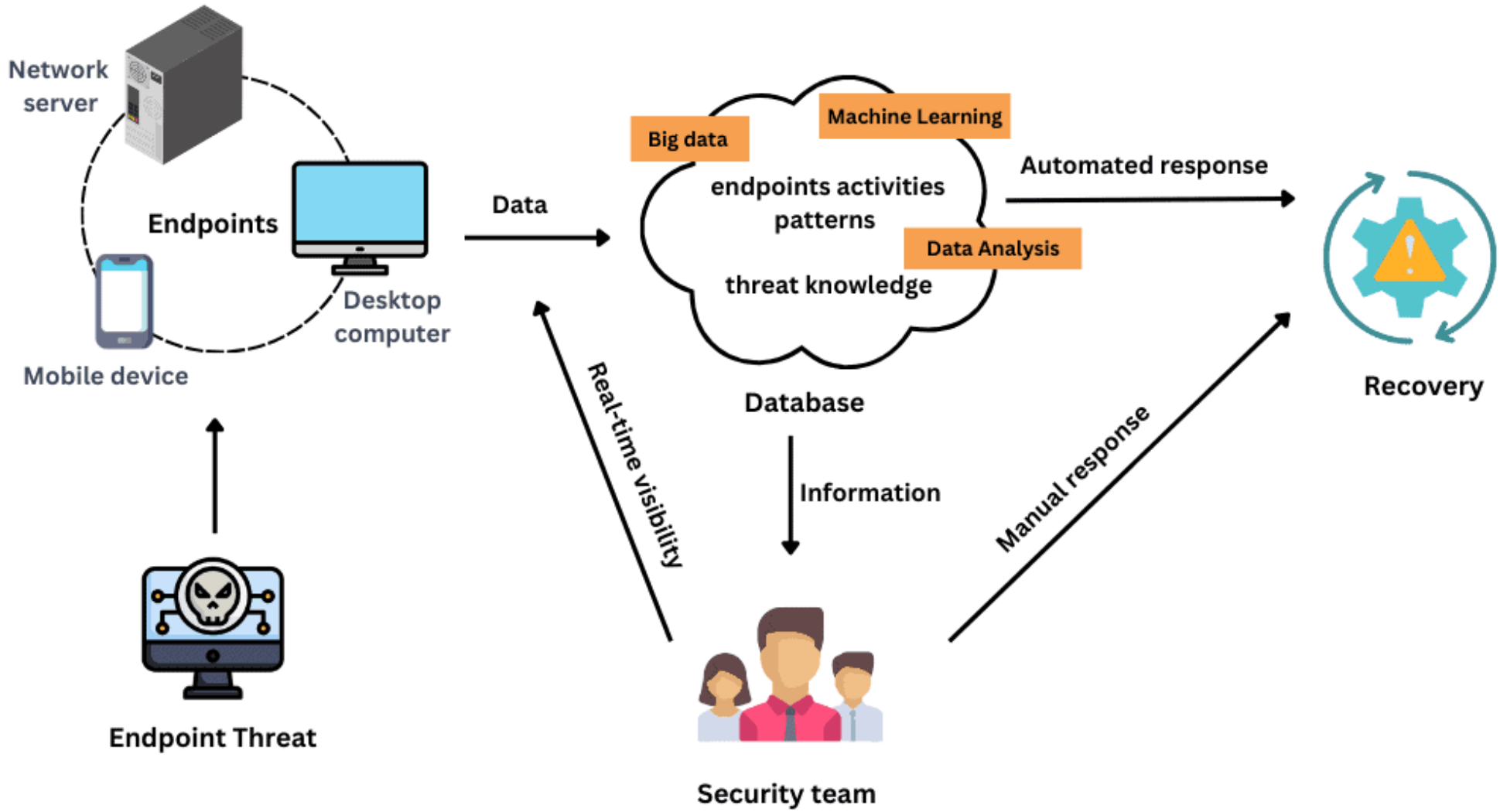
https://cyberhub.sa/posts/5259

IPS



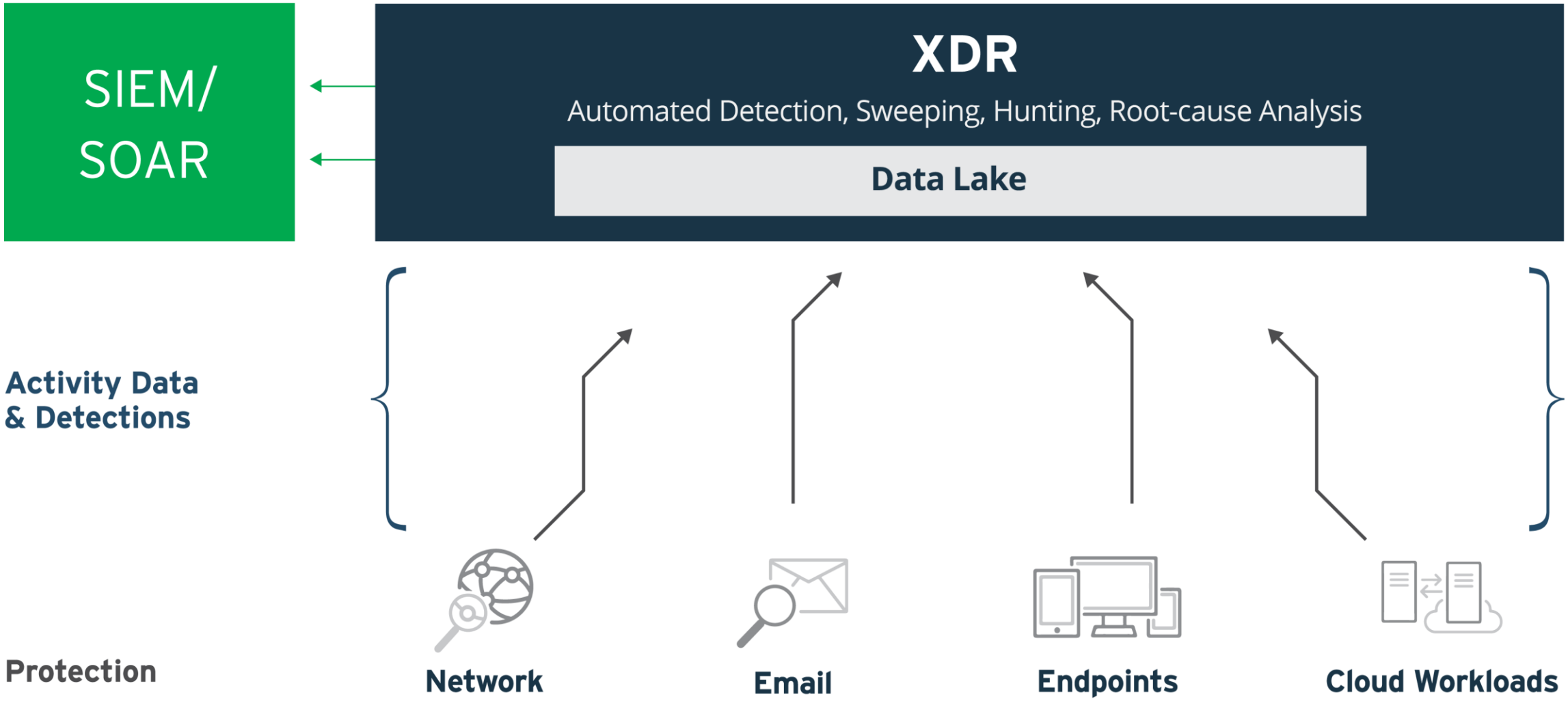
https://www.okta.com/identity-101/intrusion-prevention-system/

EDR



https://www.baeldung.com/cs/edr

XDR → SIEM/SOAR



https://www.trendmicro.com/en_my/what-is/xdr.html

Reports

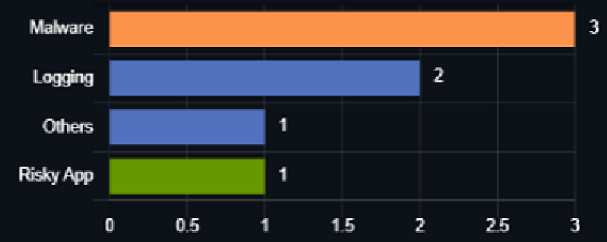
SOC

ALERTS BY SEVERITY See details

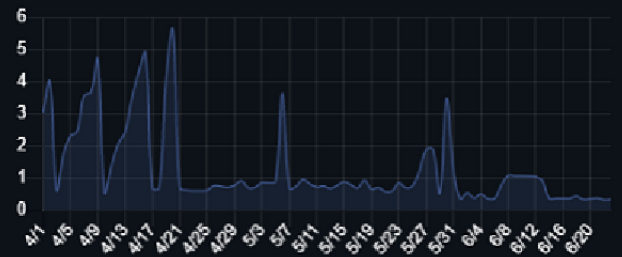
ALERTS BY STATUS See details

ALERTS BY SLA See details

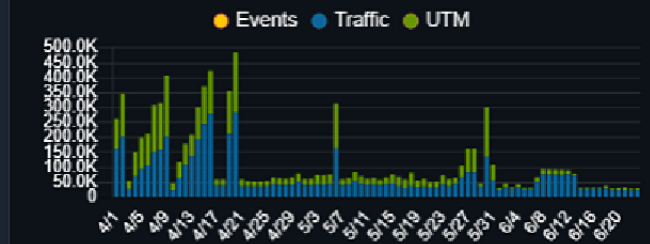
OPEN ALERTS BY CATEGORY See details



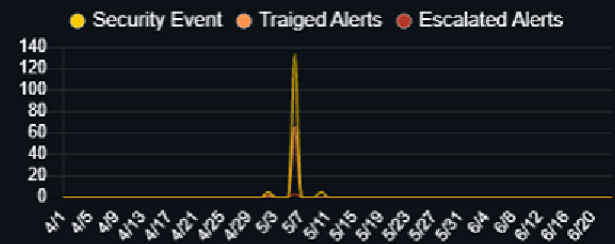
AVERAGE LOG RATE

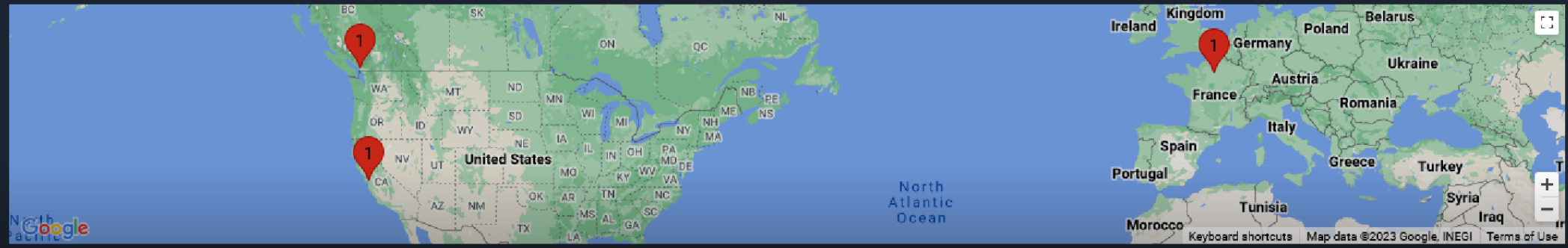


LOG COLLECTION BREAKDOWN



THREAT DETECTION TREND





List of Open Alerts 22

ID	Name	Severity	Type	Status	Affected Endpoint	Created On	Last Modified
37677	FortiClient Unable to quarantine Malware on V/		Malware	In Progress	172.16.198.152+ More	Wednesday at 3:34 P...	Today at 10:32 AM
77769	FortiClient quarantined Malware on VAN-9285		Malware	In Progress	172.19.23.200	Yesterday at 5:43 PM	Today at 10:31 AM
77295	FortiClient Unable to quarantine Malware on V/		Malware	In Progress	172.19.22.13	Wednesday at 3:34 P...	Today at 10:02 AM

Learning with Simulations

- Refer to https://app.letsdefend.io (part of HackTheBox)
  - Check out Practice for real SOC incidents
  - The Cybersecurity Student path is completely free
  - There are many other free learning practical exercises with the badge “Free”

Open-Source Security Platform

- Wazuh: https://wazuh.com/
  - Unified XDR and SIEM protection for endpoints and cloud

Cyber.org Cyber Range

- Get familiar with the machines
- If time permits, register on https://TryHackMe.com

DAY 2

Sniffnet, pentesting (ethical hacking), OSINT, social engineering, simple malware analysis

Monitor Your Traffic

- Sniffnet: https://sniffnet.app

Fun Cyber and Social Engineering

- Refer to the videos section at https://teachcyber.vford.com/nifty (skip password videos for later during Day 3)
- Will I ever be phished?
  - https://krebsonsecurity.com/2025/09/18-popular-code-packages-hacked-rigged-to-steal-crypto/
  - Refer to https://github.com/drk1wi/Modlishka
  - Refer to https://github.com/SygniaLabs/evilginx3
  - Refer to https://getgophish.com
  - Refer to https://github.com/Ahaz1701/EvilWorker

“I Bypassed The Firewall” (?!)

- A famous line in movies
- Let’s draw it out

Penetration Testing by Peter Kim

1. Intelligence Gathering
2. Initial Foothold
3. Local/Network Enumeration
4. Local Privilege Escalation
5. Persistence
6. Lateral Movement
7. Domain Privilege Escalation
8. Dumping Hashes
9. Data Exfiltration
10. Reporting

OSINT

- Open-source intelligence gathering
  - https://haveibeenpwned.com
  - https://truepeoplesearch.com
  - Google Dorking (GHDB), exploits databases (exploit-db, vulmon.com)
  - Automated toolsets
    - Metasploit: https://www.offsec.com/metasploit-unleashed
    - Sliver: https://github.com/bishopfox/sliver and https://sliver.sh
    - Cobalt Strike: https://www.cobaltstrike.com
    - Cybersecurity AI: https://github.com/aliasrobotics/cai and https://github.com/0x4m4/hexstrike-ai
    - Web attacks AI: https://github.com/KeygraphHQ/shannon

Simple Malware Analysis

- Refer to the malware teaching materials
- Refer to https://sandbox.pikker.ee
- Refer to https://virustotal.com
- Refer to https://any.run
- Refer to https://hybrid-analysis.com
- Refer to https://www.joesandbox.com

- Generate malware using `msfvenom` (Metasploit) and upload to the above

TryHackMe Rooms

- Register at TryHackMe and launch https://tryhackme.com/room/blue
  - If TryHackMe is giving us trouble with captchas, check out https://youtu.be/U4uZktyGfkM (my recording of a full compromise of Windows 7 using a generated malware with `msfvenom`)
- Show how to run your own Kali/Ubuntu box with VPN for TryHackMe access on Cyber.org
- If time permits, launch https://tryhackme.com/room/basicpentestingjt and use the OpenVPN (no limits) to connect to the room instead of the Attack Box (it's limited to 1 hour/day)

DAY 3

Passwords (manager, hash, salt) & MFA, VPN, zero-trust model, backups, TryHackMe rooms

Passwords

- Refer to the password videos at https://teachcyber.vford.com/nifty
- Refer to the passwords teaching materials
  - Hash cracking (+try on Kali on cyber.org)
  - MFA, 2FA, biometrics, passkeys
- Password manager (sign up and install Bitwarden)

Backups

- Ensure you backup your phone
- Use Google Drive, Dropbox, OneDrive, iCloud Drive
- Some cloud providers give you lifetime access for a lump sum
  - E.g., pCloud.com gives 2 TB for $400

TryHackMe Rooms

- Use Cyber.org Kali or Ubuntu machines
- Start with https://tryhackme.com/hacktivities
- Launch https://tryhackme.com/room/offensivesecurityintro and switch to https://tryhackme.com/soc-sim (SOC sim can take 10-15 mins)
  - While waiting to boot SOC simulator, go back to the offensive security intro room
- Go over https://tryhackme.com/room/introtonetworking

DAY 4

Speaker, cryptography, Linux, bash scripting, Capture The Flag (CTF), cyber competitions

SPEAKER

Sarah Putterman, retired teacher in Cheltenham

Cryptography (the next 4 slides)

- Refer to the cryptography teaching material
  - Simple ciphers
  - Asymmetric/symmetric encryption
  - Digital signatures and HTTPS certificates

confidentiality

asymmetric

symmetric

one key

encldecr

digital signatures

pub key

priv key

enc

enc

C I A

can we protect both?

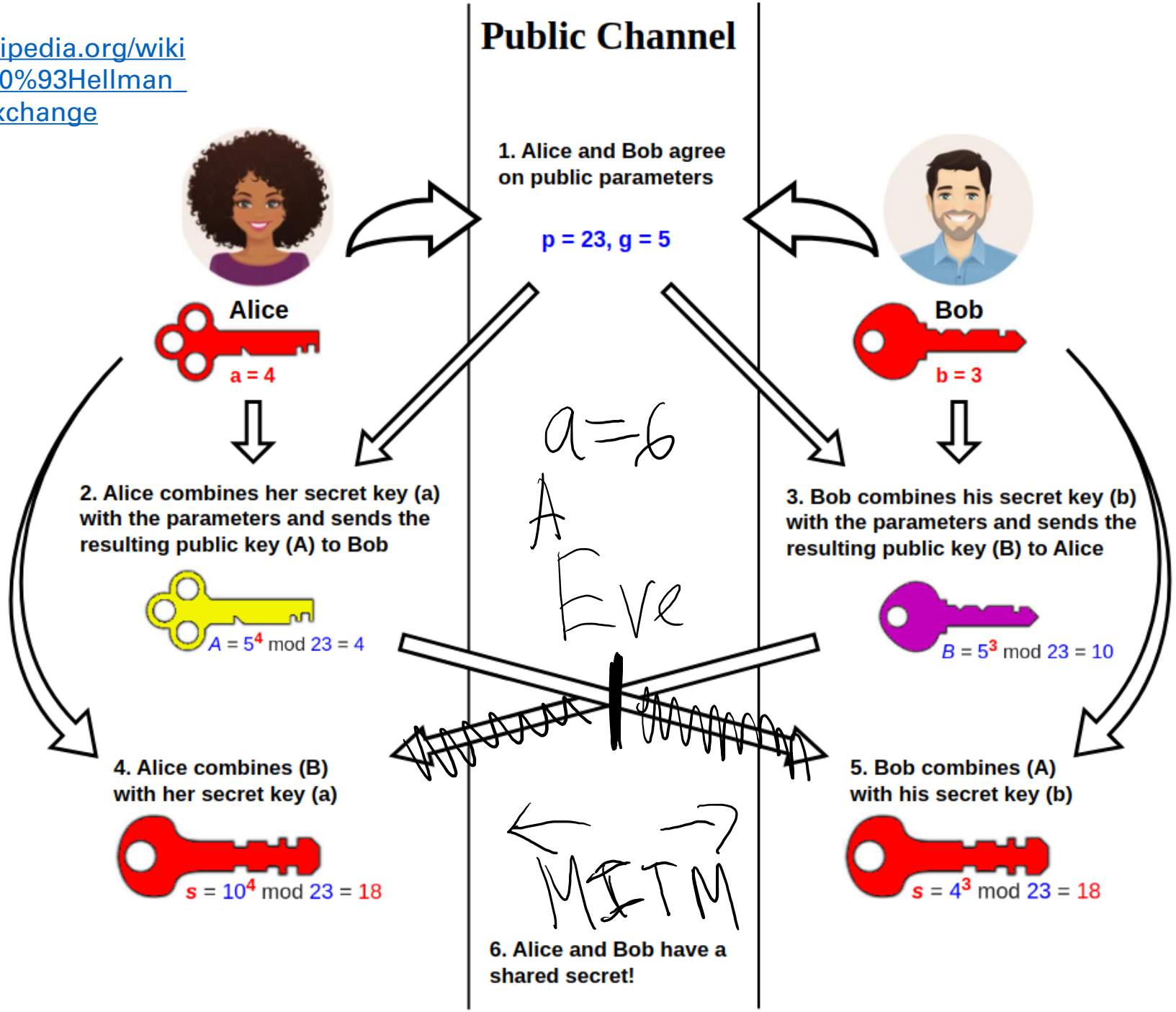
Alice ⟷ Bob

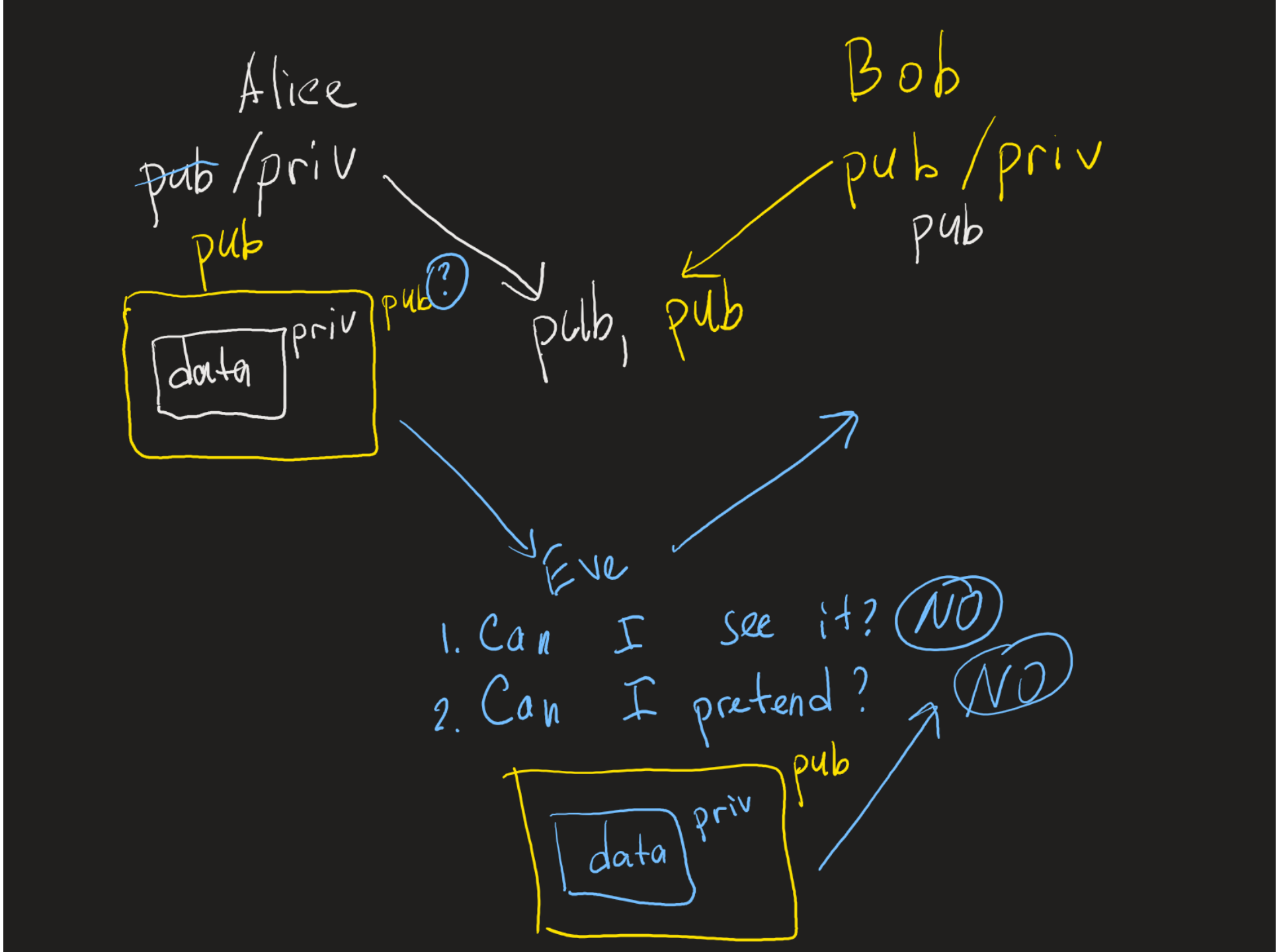
AES 256 bits key 128

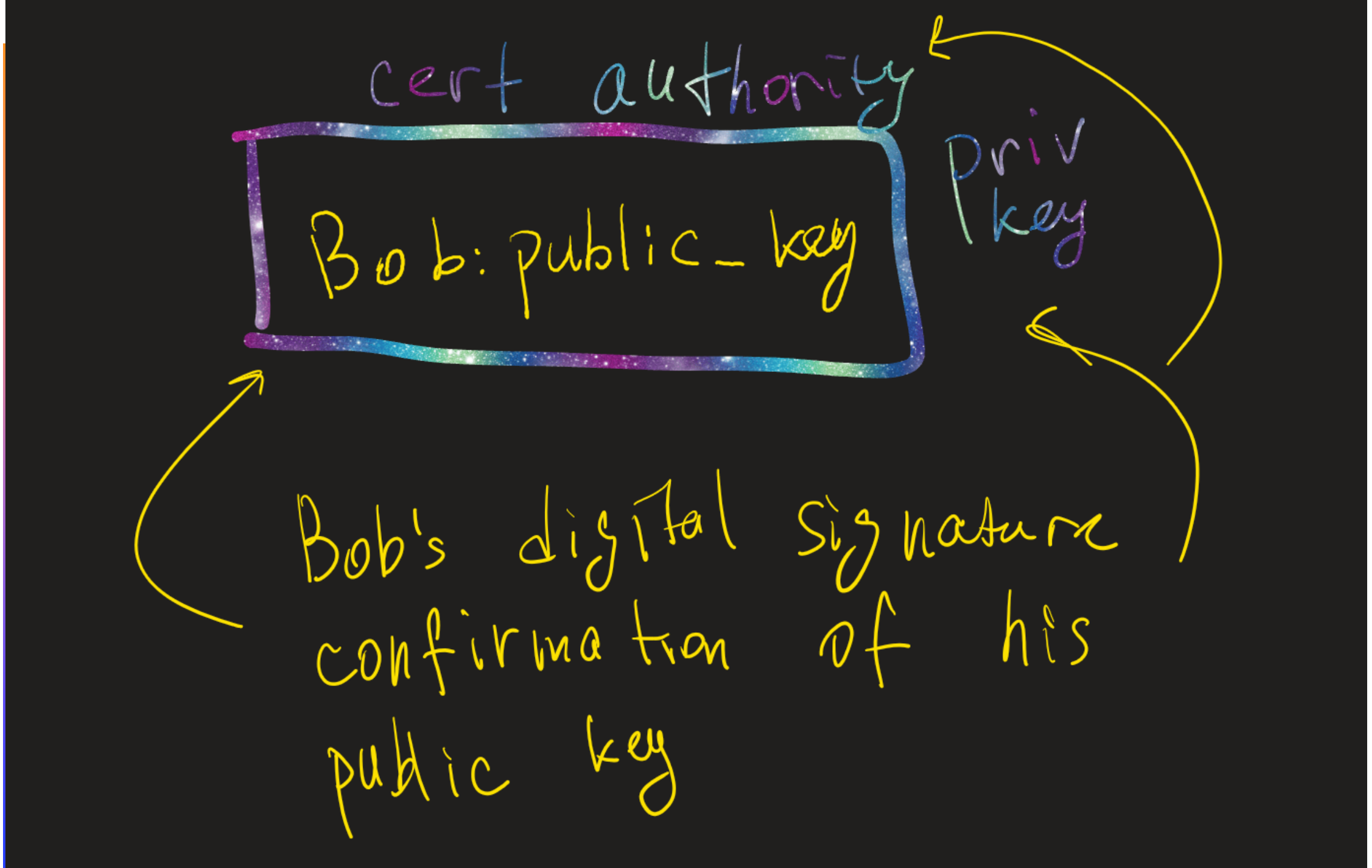
Eve

AES 256 bits key 128

https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange




Alice
pub /priv
pub
data
priv
pub
?
Bob
pub /priv
pub
pub, pub
Eve
1. Can I see it? NO
2. Can I pretend? NO
pub
data
priv


cert authority
Bob: public_key
Priv key
Bob's digital signature confirmation of his public key

Crypto Algorithms - Visualized

- Commonly used hashing: https://sha256algorithm.com/
- RSA: https://www.cryptool.org/en/cto/rsa-step-by-step/
- AES: https://legacy.cryptool.org/en/cto/aes-step-by-step

Linux

- Open and go into town in the Ubuntu and Kali machines on cyber.org cyber range
  - Refer to https://linuxjourney.com for Linux learning
  - Refer to https://overthewire.org/wargames/bandit/ to practice

Bash

- Refer to https://www.learnshell.org for Bash scripting and automation
  - You can even use ChatGPT for both Linux simulation and script generation

CTF

- Capture The Flag
  - https://practice.ctfcyber.org
  - https://picoctf.org
  - https://316ctf.com
  - https://ctf.vford.com (secure coding CTF)
  - https://gencybercoin.vford.com (secure coding CTF)
  - TryHackMe does Advent of Cyber every December
  - For more skilled folks, try hackthebox.com
  - List of global CTFs: https://ctftime.org
- CTF write-ups

CTF: Try it out

- Engage in cyber.org CTF and https://gencybercoin.vford.com for secure coding CTF (bug bounty hunting) and OSINT
  - Show https://gchq.github.io/CyberChef

Cyber Competitions

- **National Cyber Cup**: https://cyber.org/national-cyber-cup
- National Cyber League: https://nationalcyberleague.org
- Cyber Patriot: https://www.uscyberpatriot.org
- Local CTF competitions like https://sites.google.com/site/ccsceastern/participation/competition
- CSAW: https://www.csaw.io/ctf
- Learn (videos) and practice: https://mitrecyberacademy.org
- https://www.uscybergames.com

GenCyber Summer Camps

- Both camp types - teacher and students:

  https://public.cyber.mil/gencyber/camp-catalog

President’s Cup by CISA

- https://github.com/cisagov/prescup-challenges

TryCyber

- If we have time, let's try https://trycyber.us

Recordings

- A demonstration of generating and cracking a hash of a rockyou-leaked password using John The Ripper tool on Kali on cyber.org: https://youtu.be/wM49jWwPx9Q
- A demonstration of creating a cloudflare tunnel on a Windows machine to allow external users access it as long as they know the full (long) domain name that the Quick Cloudflare Tunnel generates: https://youtu.be/-3k5ESGHZW8
- A walkthrough of analyzing the PCAP file provided in forensicscontest.com/puzzles for Ann's AIM challenge, using Wireshark: https://youtu.be/nnZl0ZPC8rs

DAY 5

Wi-Fi security, ethics and privacy, CTF Unplugged, unplugged exercises from teaching materials, famous hacks, VirtualBox/VMWare Workstation & Fusion and Kali Linux installation, feedback, closing

Wi-Fi Attacks

- Evil twin like Hak5 Pineapple
- Rogue access point pretending to be real
- Man-in-the-middle (MITM) like bettercap
- Wi-Fi phishing captive portal
- MAC address (aka physical ID of the device issued by the manufacturer) spoofing
  - ARP spoofing as a follow up
- Refer to https://wigle.net

Wi-Fi Defense

- Do not use public Wi-Fi unless you have a VPN
  - Free unlimited VPNs usually have red flags, except Proton VPN and Cloudflare WARP (my personal top picks among free ones), Hide.me, and Windscribe (10GB)
  - Google Pixel and Pixel Tablets have built-in “VPN by Google”
- Ensure using the latest (at least WPA2, but better WPA3) security enabled at home, with a long passphrase
  - Hide your Wi-Fi SSID at the router level

Ethics and Laws (non-exhaustive list)

- **Permission** separates an ethical hack from an illegal activity

- **Take it Down Act** (2025)
  - Criminalizes publishing nonconsensual, sexually explicit images and videos (including AI-generated) and requires platforms to remove the content within 48 hours of notice
- **COPPA** (Children's Online Privacy Protection Act, 1998)
  - Requires websites to obtain parental consent before collecting, using, or disclosing personal information from children under 13
- **CFAA** (Computer Fraud and Abuse Act, 1986)
  - Prohibits unauthorized computer access

Tech and Privacy

- Apple vs. FBI (2016)
  - The FBI demanded Apple unlock an iPhone used by a terrorist; Apple refused to create a backdoor, citing privacy and security risks (q/a ideas)
- Facebook-Cambridge Analytica Scandal (2018)
  - Data from millions of users harvested without consent and used for political influence
- TikTok and National Security Concerns (Ongoing)
  - Concerns over Chinese ownership of TikTok and potential data sharing with the Chinese government.
- Google Project Maven (2018)
  - Google helped the Pentagon use AI to analyze drone footage, sparking internal protests from employees as their work would be weaponized

CTF Unplugged

- Available at https://vford.me/ctf-unplugged/CTF_Unplugged_May_2019.docx
  - Contact Vitaly Ford for answers

Go over unplugged exercises

- Refer to the teaching materials

Real Hacks and OSINT of Real Hackers

- Going after a famous Conti ransomware developer ($10m prize by FBI): https://justpaste.it/k72mv
- Famous hack of the Hacking Team by Phineas Fisher: https://gitlab.com/brn1337/phineas-fisher-collection/-/blob/master/2015_HackingTeam.txt?ref_type=heads

VMWare and Kali Linux

- Install VMWare Workstation (for Windows) or VMWare Fusion (for Mac) from Broadcom downloads (register a new account)
- Open downloaded Kali from kali.org -> downloads -> VMWare image (default credentials are: user and pass are both kali)

Resources

- Structured content (check out cyber.org teaching material for instructions): https://cyber.org
- Various random nano-modules for all levels: https://clark.center
- NCYTE Curriculum: https://www.ncyte.net/academia/faculty/cybersecurity-curriculum
- Comprehensive high school cyber PDF content in different languages: https://www.hackerhighschool.org/lessons.html
- Cybersecurity guide: https://cybersecurityguide.org
- Cyber seek interactive visualization for careers: https://www.cyberseek.org
- 15 hours of video, 10 week course, with notes and detailed demonstration of a full penetration test: https://github.com/hmaverickadams/Beginner-Network-Pentesting
- Networking videos: https://www.elithecomputerguy.com/2010/11/tcp-ip-and-subnet-masking/
- Find more at https://teachcyber.vford.com/diy/

News Feeds

- https://news.ycombinator.com/
- https://krebsonsecurity.com/
- https://www.reddit.com/r/netsec/
- https://bytebytego.com/guides/
- https://dev.to/

Open Discussion

- Sign and write down your PPID
  - Pass around the hours list for signatures
- Feedback: https://forms.gle/3op6kBYJPyPiozku6

- Time to reflect and chat

Stay Connected!

- Email: fordv@arcadia.edu
- Discord/LinkedIn: vitalyford